machine learning & knowledge extraction

MDPI

Article

A Survey on GAN Techniques for Data Augmentation to Address the Imbalanced Data Issues in Credit Card Fraud Detection

Emilija Strelcenia * and Simant Prakoonwit *

Department of Creative Technology, Bournemouth University, Fern Barrow, Poole BH12 5BB, UK
* Correspondence: strelceniae@bournemouth.ac.uk (E.S.); sprakoonwit@bournemouth.ac.uk (S.P.)

Abstract: Data augmentation is an important procedure in deep learning. GAN-based data augmentation can be utilized in many domains. For instance, in the credit card fraud domain, the imbalanced dataset problem is a major one as the number of credit card fraud cases is in the minority compared to legal payments. On the other hand, generative techniques are considered effective ways to rebalance the imbalanced class issue, as these techniques balance both minority and majority classes before the training. In a more recent period, Generative Adversarial Networks (GANs) are considered one of the most popular data generative techniques as they are used in big data settings. This research aims to present a survey on data augmentation using various GAN variants in the credit card fraud detection domain. In this survey, we offer a comprehensive summary of several peer-reviewed research papers on GAN synthetic generation techniques for fraud detection in the financial sector. In addition, this survey includes various solutions proposed by different researchers to balance imbalanced classes. In the end, this work concludes by pointing out the limitations of the most recent research articles and future research issues, and proposes solutions to address these problems.

Keywords: Generative Adversarial Networks; fraud detection; imbalanced data; synthetic data; deep learning

Citation: Strelcenia, E.; Prakoonwit, S. A Survey on GAN Techniques for Data Augmentation to Address the Imbalanced Data Issues in Credit Card Fraud Detection. *Mach. Learn. Knowl. Extr.* **2023**, *5*, 304–329. https://doi.org/10.3390/make5010019

Academic Editors: Edgar Weippl and Francesco Buccafurri

Received: 14 February 2023
Revised: 5 March 2023
Accepted: 8 March 2023
Published: 11 March 2023

1. Introduction

Recently, credit card usage has been regarded as a more convenient mode of payment [1,2]. However, at the same time, new credit card fraud techniques have made it difficult to detect fraud on time, thus leading to monetary losses for commercial banks and individuals [3,4]. Credit card transactions display the highest degree of the class imbalance problem [5]. Imbalanced datasets contain observations that consist of bad applications (minority class) and good applications (majority class). The bad applications (fraudulent transactions) occur rarely when compared to good applications (legal transactions) [6–8]. To deal with this issue, researchers and banks have to make sure that the learning frameworks are able to generalize learning from multifaceted patterns across the datasets and reduce the incorrect positives affectively within the fraud detection systems [9]. Fraud can be defined as any event that involves a criminal motive, which, most of the times, is hard to identify. Nowadays, online fraud is a growing concern all over the world. Fraud involves criminal intentions, which are generally difficult to detect.

Credit card fraud is a growing concern among researchers and financial institutions. On the other hand, fraud detection is a rather hard task using standard methods. The recent technological advancements have created further difficulties in detecting credit card fraud. So, at present, the introduction of sound credit card detection methods has great importance among businesses and academia. In more recent years, machine learning methods, specifically deep learning, have been extensively used to detect credit card fraud. These methods are able to analyze large streams of data, identify hidden patterns, and detect abnormalities that may point out illegal activities. In addition, deep learning methods can

learn and adapt from new data, improving the efficiency of identifying emerging fraud instances. Additionally, the credit card fraud domain is a vital area of study, as it has implications for other areas beyond financial fraud. For instance, the same methods can be used to detect anomalies in insurance, healthcare and other areas. Researchers argue that credit card fraud detection is a key area, as it can help prevent monetary loss.

Nevertheless, due to the issue of imbalanced classes in the real-world credit card dataset, researchers use various types of data augmentation techniques prior to training classifiers to enhance the efficiency of learning models [10]. It is imperative to mention that many deep learning machine algorithms are introduced to handle imbalanced classification problems [11–14]. Data augmentation is the process of generating new training data from original data. It is an important technique to enhance the reliability and performance of deep learning models, making them highly efficient in real-world applications. Using the data augmentation method, we can enhance the size and diversity of the training data instead of collecting more data. Data augmentation helps to reduce overfitting and enhance the robustness of the model by making it highly adaptable to new data. Furthermore, the data augmentation technique reduces the need for time-consuming and costly processes of data collection and labeling protocols, specifically in the domain where data are limited or hard to acquire. Data augmentation is used in machine learning to synthetically increase the dataset size by creating modified versions of the original dataset. The modifications can be done by applying transformations to the dataset—for instance, scaling, translation, or flipping. By generating new instances, the algorithm is able to access more examples of the same class, thus improving the performance and accuracy of the model [11]. In recent years, data augmentation has become more common in the computer vision task. For instance, image rotation by a few degrees or image flipping can generate new variations of the same class, helping the model to improve its performance. Data augmentation is used to generate additional training data by applying transformations to the real-world dataset. Similarly, in the credit card fraud detection domain, data augmentation is used to generate synthetic fraudulent transactions through transformations, such as changing the location and time of the transactions, or adding noise or altering the amount of transactions. The generation of additional examples of fraudulent transactions allows the deep learning model to identify indicative fraud features and patterns, even in cases where the number of labeled examples is limited. Data augmentation is highly useful in credit card fraud detection, as it helps in improving the overall accuracy of the model and reducing false positives. The issue of false positives arises when the model incorrectly classifies a legal transaction as fraudulent, which can lead to monetary losses for the financial institution and customer dissatisfaction. The model can learn to discriminate legal transactions from fraudulent transactions more accurately by generating synthetic fraudulent data.

While working with machine learning, it is vital to have an appropriate and well-represented dataset to train the algorithm [15,16]. This denotes that the dataset should be large enough and cover as many cases as possible. At the same time, it should demonstrate reality. A good dataset allows the programs to have an excellent model of the essential traits of the data, and makes it possible to generalize these characteristics [17,18]. In this case, the generation of artificial data can be helpful for multiple reasons, such as creating new data to maintain the original dataset's confidentiality and oversampling the minority class [19,20].

One of the main reasons for generating artificial data is oversampling the minority class [21]. Oversampling is performed to learn the unbalanced datasets. In many real-world datasets, the problem of imbalance persists. In the credit card fraud domain, the number of fraudulent activities is minimal when compared with legal activities, thus creating an imbalanced class problem [22]. In this scenario, it becomes difficult for the classification algorithms to identify the minority class (fraudulent transactions) [23]. Augmentation of the minority class data is a way to deal with the imbalanced class problem. This is possible by producing new instances with similar traits to the original data. Augmentation helps to avoid the underrepresentation problem of the minority class, while simultaneously

avoiding overfitting as well [24,25]. Another reason for generating artificial datasets is to use synthetic data to avoid government regulations and the confidentiality of customers [26]. For example, financial data, such as credit card transaction data, contain sensitive details about the customers, and training using them could risk customers' privacy. One way to deal with privacy concerns is to generate artificial datasets to train the model [27]. Among the generative methods, one of the most popular is Generative Adversarial Networks (GANs), developed by [28]. In this survey work, we are seeking to check the flexibility and scalability of GANs to generate artificial samples for credit card fraud detection. Thus, this study aims to make additions to the existing literature on GANs for data augmentation for imbalanced class learning. Researchers [29–32] have argued that using GANs is the more fitting and effective technique for handling imbalanced class problem compared to other machine learning approaches. In addition, it is highly robust towards overlapping and overfitting due to its ability to understand hidden structures of data and their flexibility. For the said purpose, we reviewed past studies conducted by researchers in the fraud detection domain using GANs to augment credit card data.

The main contributions of this study can be summarized as follows:

1. Comparison of GAN variants for data augmentation in credit card fraud detection domain;
2. Detailed discussion of the most recent and relevant GAN variants for fraud detection;
3. The most common evaluation metrics are discussed and elucidated;
4. This report reviews the recent advancements in using GANs in data augmentation;
5. We also provide an analysis and comparison in terms of strengths and limitations across the GAN variants discussed in this paper.

Organization of this Survey

This survey is structured as follows:

- Section 2 provides the background of the imbalanced class challenge, the definition and structure of GAN, and the importance of data augmentation using GANs;
- Section 3 briefly describes different GAN approaches used in the credit card fraud domain to handle imbalanced class challenges. In addition, this section also presents the tabular evaluation of several GAN methodologies based on precision, recall and F1-score;
- Section 4 concludes this research survey and provides future research recommendations.

2. Background

2.1. Class Imbalance Challenge

The imbalanced class challenge is the most commonly occurring issue in credit card datasets, where the data distribution is highly skewed [33,34]. Several studies in the literature based on data mining and machine learning algorithms have been dedicated to addressing this problem. Machine learning techniques have made significant advancements in recent times. However, these techniques rely heavily on large datasets representing the whole population. Similarly, fraudulent payments rarely occur in credit card transactions compared to legal payments [35]. The illegal transactions datasets need to contain more samples to train machine learning methods effectively to generalize them to the population set [13]. In other words, the number of cases of credit card fraud is in the minority when we compare them with legal payments, creating a class imbalance problem. This creates an under-representation of one class when compared with the other. Furthermore, the class imbalance results in poor classification performance of the machine learning approach for the least minority classes [36–39].

Scientists argue that synthetic data generative methods are one of the most effective solutions to the imbalanced class challenge [37,40–42]. These methods not only rebalance classes, but also reduce model overfitting. One of the most popular data generation methods is Generative Adversarial Networks (GANs), which can be employed in big data settings.

2.2. Generative Adversarial Networks (GANs)

Generative Adversarial Networks, or simply GANs, are generative ML approaches first proposed by [28]. GANs gained popularity due to their easiness and efficiency [43,44]. In a short period, a significant development was made in the first GAN application in generating synthetic images [45–47]. Other than that, multiple GAN variants have also been proposed to enhance GANs' applicability, from computer vision to credit card fraud detection in commercial banks, hence the model introduced in 2014 represent a large development, and GANs' applicability is continuously expanding [48]. Moreover, the applicability of GANs in finance, when compared with other domains, is still considered novel, which makes it a fertile area of research. Since the research is in the development stage, it is logical to consider that more applications of GANs are yet to be introduced and elaborated upon. Currently, a lot of research is in the transitional phase. The intention of this study is to show the recent work in the credit card fraud domain.

GAN is regarded as the most familiar machine learning model in unsupervised and semi-supervised learning. In theory, GAN lets supervised learning advance to unsupervised learning by creating synthetic/fake data [49]. Furthermore, Wang et al. [50] discussed the significance of the detection and classification of malicious code, which is highly important in the cybersecurity domain. The authors emphasized that conventional signature-based techniques are no longer able to deal with the continuous evolution of malware, and new methods are crucial to enhance the efficiency and accuracy of malware detection. To deal with the associated challenges, the authors introduced a technique combining GANs and Convolutional Neural Networks (CNNs) to classify malicious code families. This novel framework converts code into images, which can then be fed into a CNN for feature extraction and classification. The function of GAN is to generate images of malicious code families to augment training dataset and enhance the capabilities of CNN. Moreover, Wang et al. [50] used multiple datasets of malicious code families, and compared their method with other models, such as Random Forest and a conventional CNN classifier. The findings of their study show that their model outperforms the baseline methods and achieves excellent performance on the datasets. The study by Jiang et al. [51] proposed a dynamic ensemble algorithm to detect anomalies in imbalanced datasets from IoT devices. Their framework is designed to deal with imbalanced data streams, such as class imbalance and concept drift issues, by changing data distributions. Their proposed algorithm combines various base classifiers and adjusts their weights based on each classifier's performance. The empirical findings of their study on original datasets suggest that their algorithm performs well when compared with state-of-the-art anomaly detection techniques. In addition, the study conducted by Jiang et al. [51] is inventive in its dynamic ensemble approach, which allows it to adapt to the changes in the distribution of the data and attain high accuracy in anomaly detection. However, the only limitation of their experiment is that they conducted experiments on limited datasets. Future experiments should be on multiple ranges of datasets with different traits and complexities to attain more insights into the robustness and generalizations of their algorithms. In addition, their study does not offer a detailed discussion of the scalability and computational complexities of the proposed algorithm, which is essential for applicability in large-scale IoT systems. In recent years, since the development of blockchain technology, smart contracts have come to high usage in IoT, healthcare, finance and other domains. Due to the high usage of smart contracts, their security has also received immense attention as monetary losses cause by vulnerabilities. The traditional analysis tools can detect these vulnerabilities. However, these tools rely mainly on hard rules defined by experts while detecting vulnerabilities. A study by Zhang et al. [52] proposed a deep learning model, CBGRU, to detect smart contract vulnerabilities. CBGRU combines deep learning models and various word embeddings in order to extract features from the input source code of smart contracts. They then used the extracted features for classifying the smart contract as either vulnerable or non-vulnerable. For their study, the authors used a real-world smart contracts dataset. The empirical findings of their study confirm that their method performed better when

compared with other methods in terms of detection rate and accuracy, which indicate its ability to enhance the security of blockchain systems.

In more recent years, researchers have shown great interest in GANs due to their ability to leverage large unlabeled data. The study conducted by Creswell et al. [53] offers a comprehensive overview of GANs for the signal processing community. Their study highlights multiple applications of GANs in domains such as data generation, video and image generation, data augmentation and style transfer. The paper also discusses various techniques used to improve the performance and stability of GANs, for instance, employing regularization techniques, network frameworks and loss functions. According to Creswell et al [53], GANs offer ways to learn deep representations without annotated training data. GANs achieve this by deriving back-propagation signals using a method with a pair of networks. They also pointed to the limitations of GANs, such as mode collapse and training instability, and discussed possible solutions to deal with them. The study conducted by Park et al. [54] presents a detailed review of GANs, with a focus on their application in computer vision. The paper also discusses the basic framework of GANs, such as architecture, loss functions and training phases. In addition, the paper reviews different GAN variants such as conditional GANs, Wasserstein Generative Adversarial Networks (WGANs), Wasserstein GAN-Gradient Penalty (WGAN-GP), and Self-Attention Generative Adversarial Networks (SA-GAN), and discusses the advantages and disadvantages of these GAN variants and their applications in various computer vision domains, such as image translation, image editing and image generation. Furthermore, the study also covers the limitations associated with GANs, such as training time, instability and mode collapse. They also mention different methods that have been proposed to deal with these limitations, for instance, optimization algorithms, network architecture and regularization methods. In addition, the study also highlighted ethical concerns linked with GANs, for instance, the use of deep fakes and other deceptive generations.

Shorten et al. [42] present a survey on several image data augmentation methods used in deep learning for improving model performance. The study explicates the need for data augmentation, its advantages and its restrictions. Additionally, the study presents a brief review of conventional and novel data augmentation techniques. Other than that, their study also discusses the impact of data augmentation on the generalization of the model and its ability to reduce overfitting.

2.2.1. Definition and Structure

Generative Adversarial Networks (GANs) have made progress in machine learning modeling [53,55]. This machine learning approach discriminates networks to discriminate between synthetic and real data. Contrary to classical machine learning algorithms, GANs act in such a way that they can learn the joint distribution of the whole dataset. GANs utilize two neural networks: Generator (G) and the Discriminator (D) networks [56]. The function of the G is to input a random noise vector into synthetic data that nearly reflect the real data. At the same time, the objective of the D is to take real samples, and act as a teacher who can evaluate the performance of the output and check if the data are fake or real. Both G and D are trained in such a way—through the Min–Max game—that the losses of G are minimized, and the losses of D get maximized. The function of GAN is given below.

$$\min_G \max_D V(G,D) = E[\log D(x)]_{x-p_{data}(x)} + E[\log(1 - D(G(z)))]_{z-p(z)} \quad (1)$$

Furthermore, Figure 1 shows the basic framework of the original GAN. In Figure 1, the noise "z" is randomly generated, while "G(z)" indicates how "G" attempts to learn a distribution PG from the distribution of noise "Pz", and makes "PG" closer to the distribution of real-world data, which is denoted by "P" data. In addition, the Discriminator attempts to confirm whether the sample is fake or real. On the other hand, the input is needed to adjust both the Discriminator and the Generator until the Discriminator fails to

discriminate between real-world data and the generated data while training. Consequently, we can reach the optimal point whereat P data are equal to PG.

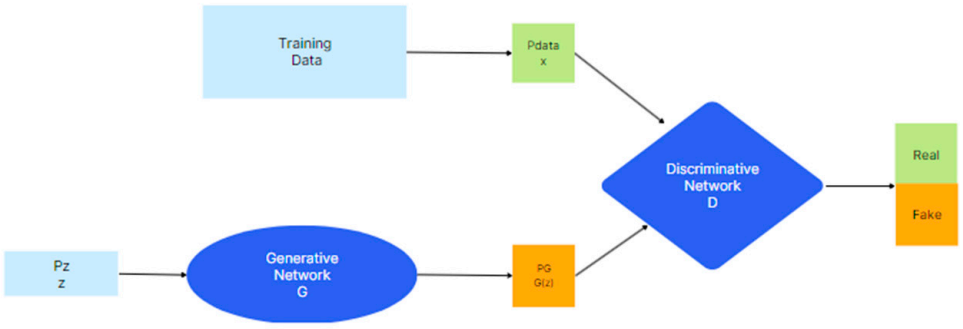


Figure 1. This figure presents the basic GAN structure. The two models learned during the GAN training process are the Generator (G) and the Discriminator (D). Here, "z" is random noise, and G(z) indicates how G attempts to learn the distribution PG from distribution Pz. Pdata denotes the real-world dataset.

2.2.2. The Discriminator

The Discriminator is a network that serves as a classifier. It takes in both real data and synthetic data generated by the Generator, and tries to differentiate between them [57]. The architecture of the Discriminator can vary depending on the type of data it is handling. It is connected to two loss functions that are used at different stages of training. When it classifies real or synthetic data, it is penalized for incorrect classifications, and its weights are updated through back-propagation from the loss [58].

2.2.3. The Generator

The Generator (G) network makes use of the feedback it receives from the Discriminator (D) in order to learn to generate artificial data that resemble the real-world data [59]. The goal of G is to create data that can be classified as original by the D. The network receives random input, a sort of noise, from which it generates output. The generated output is evaluated by the G and results in a G loss, which penalizes the G for not deceiving the Discriminator [60]. A GAN is able to produce a variety of outputs through sampling from multiple places.

2.2.4. Loss Functions

The training phase of GAN utilizes loss functions, which appraise the distance between the real data and distributions of the generated data to evaluate their resemblance [61]. Before now, various methods have been introduced to deal with this challenge. In the conventional GAN, a mini–max loss was proposed. The mini–max loss architecture mimics the cross-entropy and Jensen–Shannon divergence between generated distributions and real ones when the Discriminator is in its optimal state. Moreover, for the Generator, minimizing the loss is equal to minimizing log [1D (G (Z))], as it cannot affect term log D(x) directly in the function. Furthermore, in a traditional GAN design, the G and the D losses are derived from a single measure of distance. Both the terms are updated in an alternating fashion [62].

2.3. GANs in Credit Card Fraud Detection Domain

Recently, GANs have gained immense popularity in domains such as credit card fraud detection for generating artificial samples. Researchers argue that GANs are the more fitting and effective technique for handling imbalanced class problems compared to other machine learning approaches [63–65]. In addition, they are highly robust towards overlapping and overfitting due to their ability to understand hidden structures of data and their flexibility [66]. As a result, a sufficient amount of research has been done on GANs.

Recent studies on GANs compared their performances on imbalanced datasets against other well-known methods.

In their empirical study, Ngwenduna and Mbuvha [67] explored multiple aspects of GANs. They argued that GANs are more the appropriate and effective frameworks for handling imbalanced class problems than other sampling models. They emphasized the effectiveness of GANs, employing several facets such as architectural design, difficulties associated with GAN, the multiple variants to address specific traits, application areas and so on. In addition, they also conducted empirical studies to evaluate GANs with the help of metrics. In addition, they also conducted a relative study on the performances of GANs with other resampling methods, such as the Synthetic Minority Over-sampling Technique (SMOTE) established by [58]. Their study reveals that GAN is more effective than other resampling methods. Furthermore, the finding of this study reveals that GAN variants such as Wasserstein Generative Adversarial Networks (WGAN) [59] and Wasserstein Generative Adversarial Networks Gradient Penalty (WGAN GP) [60] are highly effective in mitigating the imbalanced class problem. Additionally, Kim et al. [61] employed various GAN models for synthetic data generation in credit card transactions. The results from the research suggest using CTAB-GAN, a conditional GAN-based tabular data generator. By modelling mixed variables, CTAB-GAN surpassed the preceding state-of-the-art approaches and offered superior generating capabilities for imbalanced categorical variables and continuous variables with complex distributions.

Furthermore, Saqlain et al. [62] used a Generative Adversarial Fusion Network to detect fraud in imbalanced credit card transactions. The study used IGAFN, a model that could be used repeatedly to predict a user's creditworthiness based on the user's profile and past actions. In order to function, the model relied on the data imbalance issue in credit scoring being addressed and the multi-source heterogeneous credit data being integrated. The experimental outcomes proved the credit scoring approach's viability by merging features and class balance. IGAFN has been shown experimentally to be superior to other methods for overcoming these restrictions, and it would play a crucial role in the forecasting of credit risks for banks and other financial organizations. In addition, Ba [63] attempted to solve the imbalanced class challenge. To do so, they chose the work of [5] as their base paper for training GAN to generate synthetic samples of fraudulent credit card transactions to handle imbalanced classes in the training set. The data used for this study were highly imbalanced, so the augmentation of data on the minority class was performed to pick up the classification results. Their findings demonstrate that GAN-based augmentation does better than other approaches, as it improves generalization more notably than other training methods. The study by Sethia et al. [64] aimed to review several aspects of GAN architectures. First, the authors considered GAN architectures such as Conditional GAN (cGAN) [65] and explored the pros and cons connected with these GAN variants. The study by Charitou et al. [66] is unique compared to the above studies, as their study examined GAN in a theoretical and mathematical way. This study has provided a deep insight into the training complications associated with GAN variants. In addition, this study has presented three different points of view to tackle the problems while training GAN. These are skills, GAN structure and the objective of the framework. The authors of this study assert that inception score, multi-scale structural similarity, model score, and freshet inception distance are the most influential metrics in evaluating the capabilities of GAN. Additionally, Ngwenduna and Mbuvha [67] focused on the limitations and suitability of GAN in dealing with banking challenges. Their study used the WGAN GP variant to augment the data. The findings of their study identify a major increase of 5% in the recall value of the XG Boost classifier after training on augmented data rather than real-world data. It is also noteworthy that they detected a decrease in F1 score and precision values.

2.4. Data Augmentation using GANs

Generative Adversarial Networks (GANs) are used to augment data effectively. GAN is a class of generative models that can create new data based on actual training data. The

applicability of GANs is diverse, and they can be used in multiple fields, including the credit card fraud domain.

Data scarcity is a significant problem, since a large quantity of data is required in fraud detection to train deep learning models. Data augmentation is one of the most efficient ways to deal with this problem [13,68]. In recent years, researchers have conducted various studies in this particular area. Below are a few reasons to employ GANs for data augmentation.

2.4.1. Limited Training Data

One of the main issues that arise while training datasets is the limited training data available in many application domains [68–70]. In some areas, data collection is not possible. For instance, it is not possible to train the original dataset to detect fraudulent transactions in the credit card fraud domain due to privacy concerns. Furthermore, data collection is a time-consuming and sometimes costly task. In contrast, algorithms need extensive data for training. An effective way to deal with the limited training data is data augmentation. This is a method used to generate data from real-world data synthetically. Data augmentation reduces both the time and costs associated with acquiring the required data. Furthermore, it decreases the issue of sample inadequacy in deep learning models [13].

2.4.2. Lack of Relevant Data

In addition to the limited training data, the need for more relevant data is a big challenge in training models. Large quantities of relevant data are required to improve the accuracy of deep learning models. Data augmentation can provide solutions through different methods to enhance the size and quality of training datasets to get a better outcome [71].

2.4.3. Model Overfitting

Furthermore, model overfitting is also regarded as a big challenge. Deep learning models require significant data to avoid the issue of overfitting. Overfitting is a modeling error that arises when a model too closely fits the available dataset. In addition, when a model is trained on an inadequate dataset, it will be difficult for the model to generalize it perfectly for a new dataset. In addition, when these models are tested for any new data, they will not provide accurate predictions, making the model useless. Therefore, the model needs more datasets to deal with the challenge of overfitting [13]. However, data augmentation lessens the issue of overfitting by training the model with a large set of appropriate data [72]. Furthermore, data augmentation regularizes the model and enhances its ability to generalize [73].

2.4.4. Imbalanced Data

Besides the above challenges, imbalanced data is a significant problem in real-world applications. This problem is prevalent in financial institutions, specifically in terms of credit card fraud detection, as there are too few fraud transactions compared to legal transactions. In addition, deep learning models require a large quantity of data to classify correctly. However, the available data could be more balanced, which creates a difficulty in training deep models and affects the overall accuracy. Data can be rebalanced to solve this challenge; however, data augmentation can help this issue, dealing with highly imbalanced datasets by creating data for training machine learning models [57,74].

2.5. Challenges and Limitations of GAN Based Data Augmentation

It is important to mention that data augmentation encounters a few limitations when training models with limited and low volume datasets [75]. The improvement achieved with data augmentation is limited, as data augmentation, to some extent, transforms an existing sample to a modified sample [76,77]. Thus, it can be said that data augmentation does not generate entirely new data, which contain information not present in the data

to be changed. For instance, in credit card fraud detection, data augmentation cannot generate entirely new minority instances if the original dataset does not have minority samples [13]. One of the challenges of using GANs for data augmentation in credit card fraud detection is that they can be difficult to train and stabilize [78]. GANs are composed of two neural networks (the Generator and the Discriminator) that are trained simultaneously in a game-theoretic framework, and this process can be prone to instability and mode collapse. Therefore, it is important to use appropriate architectures, training methods and regularization techniques to stabilize the training process [79].

Another challenge when using GANs for data augmentation in credit card fraud detection is that the generated synthetic samples may not be representative of real-world fraudulent transactions [80]. Therefore, it is important to evaluate the quality of the generated samples and compare them to real-world fraud data to ensure that they are realistic and useful for training machine learning models [80,81]. Moreover, mode collapse occurs when the generator produces synthetic data that are only a small subset of the real data distribution [82]. This can be mitigated by using techniques such as mini-batch discrimination, but it is still a limitation that needs to be considered [83,84].

In general, GANs have shown promising results in data augmentation in credit card fraud detection tasks, by allowing the generation of synthetic samples of fraudulent transactions that can be used to train machine learning models more effectively. However, it is important to note that GANs are complex models and their training process can be challenging, and there is ongoing research on improving their performance and stability.

2.6. Recent Advancements to Deal with the Challenges and Limitations

To deal with the key training issues, such as mode collapse and vanishing gradient, studies have introduced two main frameworks: the application of different loss functions and the introduction of new network designs. In this context, a study by Wang et al. [85] demonstrated that the GAN's performance is linked to the network and batch sizes, showing that effectively implemented frameworks have a vital impact on the output quality. In addition, the remodeling of loss functions also achieves better training stability. It is imperative to mention that advancements are targeted at precise applications, thus there is currently no single solution for all domain.

3. Literature on Architecture-Variant GANs

Since the introduction of GAN, various GAN variants have been proposed in the literature. Researchers, in the literature, have proposed several GAN variants for the fraud domain. Furthermore, the extensive implementation of GANs by scholars and academicians encouraged the developments in network-optimization methods, such as Wasserstein GANs [86], cGAN [87] and so on. To present a broader picture of recent GAN-based research, we will review recent developments in this field. This section presents various GAN models on the basis of their functions, strengths and limitations. By doing so, this survey gives a brief description of the architectures of different GAN variants. Furthermore, this section offers a review of the literature on GAN variants in terms of their applications in the fraud domain.

3.1. Duo-GAN Approach

In their recent study, Ferreira et al. [88] introduced a novel generative framework called Duo-GAN as demonstrated in Figure 2. This model employs two GANs: one to generate fraudulent synthetic transactions and the second to generate synthetic legal samples. This approach helps us to overcome the issue of highly imbalanced datasets. The synthetic data generated via Duo-GAN can be used and shared with banks and other financial institutes to deal with customers' privacy concerns. This framework maintains privacy and ensures a high success rate in detecting illegal credit card transactions. This approach aims to generate artificial data that display the same traits, distributions, and patterns of real data without affecting customers' confidential information.

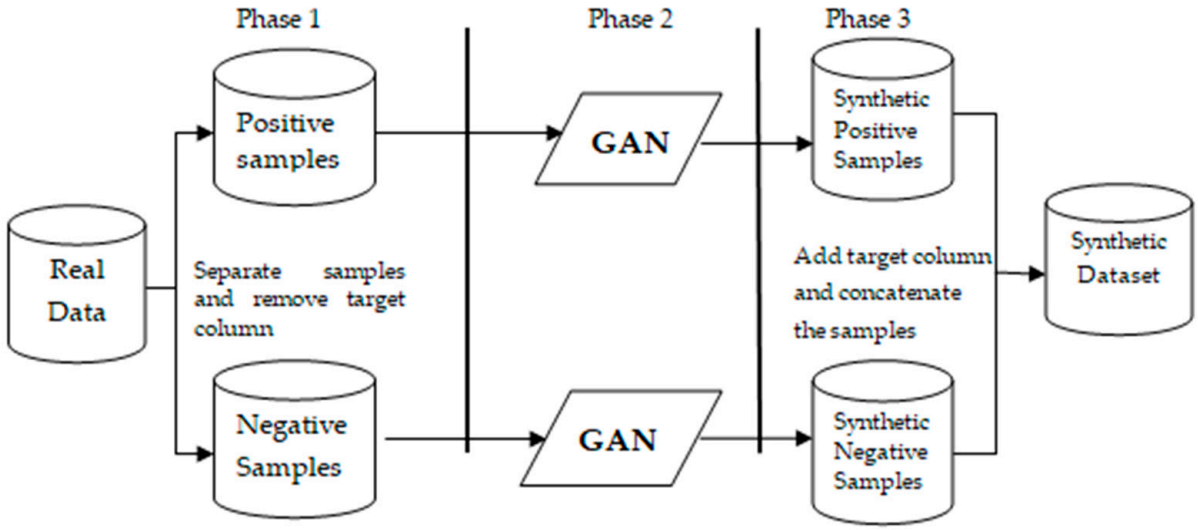


Figure 2. The architecture of the Duo-GAN. Duo-GAN employs two GANs: one to generate fraudulent synthetic transactions and the second to generate synthetic legal samples.

The findings of this approach to fraud detection demonstrate that it can capture the underlying distributions of the data. Furthermore, results show that the framework's reclassification model that is trained on artificial data surpasses classifiers trained on data generated by a one-GAN model. In addition, this approach produces artificial data that can be used to train classifiers and achieve outcomes comparable to models trained on real data.

3.1.1. Process

1. This approach employs two GANs instead of one to create synthetic data.
2. This approach enables each Generator to learn the class-conditional distributions and the correlation of each class so as to learn the distribution and relationship of the actual data.

3.1.2. Strengths

1. This novel framework can generate artificial data for highly imbalanced datasets.
2. It can generate artificial data without overfitting the real data.
3. It outperforms classifiers trained on data generated by one-GAN models.

3.1.3. Limitations

1. This framework does not incorporate the computational resources and time required to train the models.
2. The divergence metric encounters some problems when dealing with the continuous characteristics.

3.2. Majority-Minority GAN Transfer

In addition, Langevin et al. [13] used GANs to solve the class imbalance issue. They proposed a majority–minority GAN transfer framework as demonstrated in Figure 3. This framework models the conditional distribution of the majority class first. After doing so, the framework then uses some segment of the learned majority-GAN structure to train another GAN on the minority class. The primary hypothesis is that the majority class can be modeled more accurately.

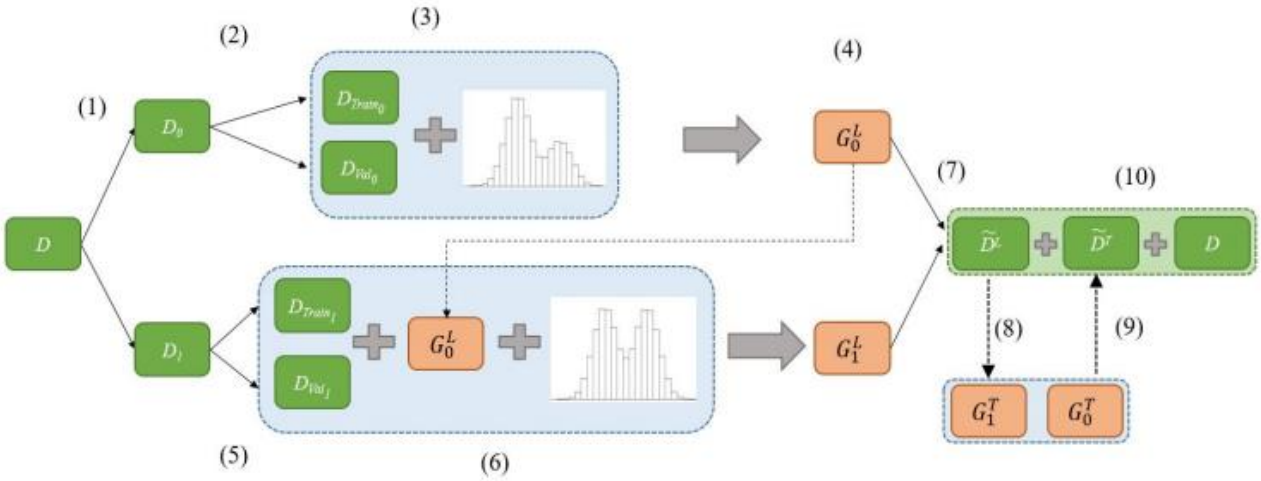


Figure 3. The majority–minority GAN framework.

3.2.1. Process

1. This process investigates the use of synthetic data from not only the minority class, but also the majority class. By doing so, the Generator captures more information about p data.
2. The model retrains the fraud case model directly on actual transaction data.

3.2.2. Strengths

1. This framework used to generate synthetic samples can generate data streams with one or multiple minority classes.
2. It trains the Generator first so as to model conditional distribution.

3.2.3. Limitations

1. This GAN variant performed well compared to other GAN generators, but struggled in modeling log-transformed variables on some occasions, mainly where univariant histograms are incredibly skewed.
2. This technique lacks feature transfer to control distributional differences.
3. Further investigations are needed as this framework is in the initial phase.

3.3. The Conditional Table GAN (CTAB-GAN)

Furthermore, Zhao et al. [89] proposed a novel conditional table generative adversarial network (CTAB-GAN) as demonstrated in Figure 4. The objective of their study was to utilize the potential of data sharing without affecting customer data privacy and complying with governmental regulations. Furthermore, they aimed to design a model that can address the weaknesses of previous GAN algorithms: (a) encoding mixed data, (b) excellent modeling of long-tail continuous variables and (c) robust categorical variables with skewed continuous variables.

The proposed algorithm was tested on five extensively used machine datasets: Credit, Loan, Adult, Cover-type, and Intrusion. In addition, the proposed GAN variant was also tested against four popular GAN-based algorithms: CWGAN [90], Med-GAN [91], CTGAN [92] and Table-GAN [93]. The findings of this experimental study show that CTAB GAN not only performs better than all these algorithms in terms of Accuracy, F1-score, and AUC, but it also gives greater distance-based privacy guarantees than Table-GAN.

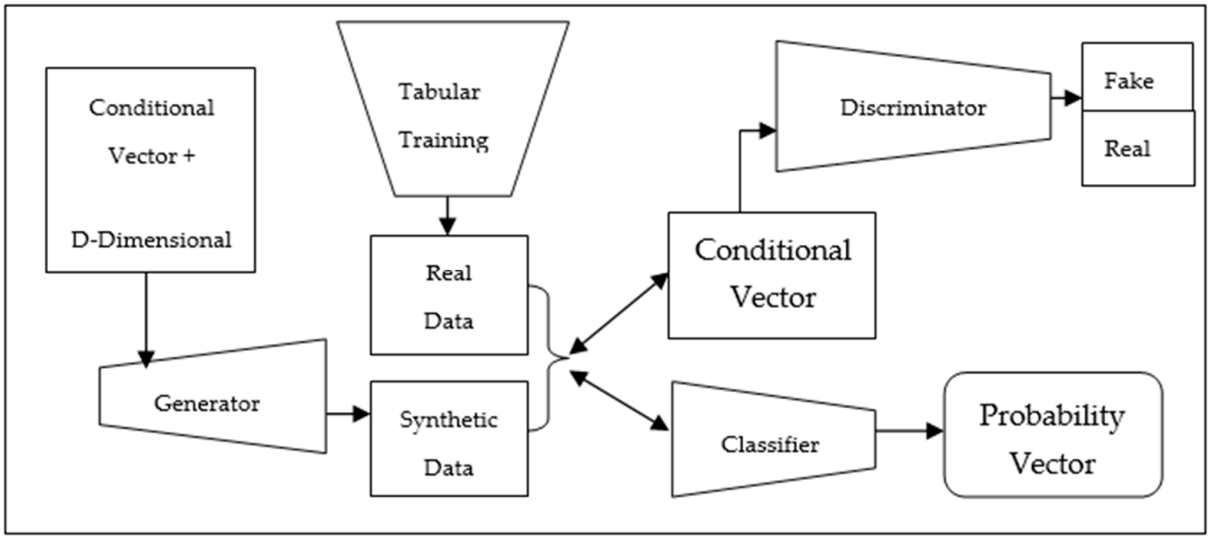


Figure 4. The CTAB-GAN design. Conditional GANs are an expansion of conventional GANs, where both the G and D have to consider additional information. Here we have represented the additional information as c. Here, c can be information of any type.

3.3.1. Process

1. Encodes mixed data.
2. Efficient modeling of long-tailed continuous variables.
3. Deals with highly skewed distributions for continuous variables.

3.3.2. Strengths

1. Outperforms other state-of-the-art generative algorithms.
2. Provides better distance-based privacy guarantees than Table GAN.
3. Preserves data privacy.

3.3.3. Limitations

1. CTAB GAN functions well with complex datasets, but cannot converge to a better optimum for small and straightforward datasets.
2. There is still room to enhance the performance of CTAB GAN. For example, it generates more zero values than in the original distribution, as it amplifies the dominance of zero values in mixed data-type variables.

3.4. Synthetic Data Generation GAN (SDG-GAN)

In addition, Charitou et al. [66] introduced a novel GAN to generate synthetic data to train a supervised classifier. This approach, Synthetic Data Generation GAN, can outperform density-based over-sampling methods and enhance the classification ability of benchmark and real fraud datasets. Furthermore, this algorithm can be widely used to handle highly unbalanced datasets in fields such as credit card fraud, as well as the Pima Diabetes and Breast Cancer Wisconsin (Diagnostic) datasets.

After that, they applied the model to generate machine-made data to handle the imbalanced class issue in the real-world fraud detection gambling dataset. The finding shows that this technique's accuracy is much better in credit card fraud datasets. In addition, this technique outperformed the other oversampling techniques when compared.

3.4.1. Process

1. The "G" and "D" in SDG-GAN are feed-forward networks with an MLP architecture.
2. Feature matching loss was adopted in this technique instead of the regular loss.
3. The "G" attempts to learn the actual distribution of the data.

4. This technique is based on conditional GAN.

3.4.2. Strengths

1. This technique can be used in multiple fields.
2. The feature matching technique was used in this novel GAN. This technique changes the cost function for the "G" to lessen the statistical disparity between real and artificial data traits.

3.4.3. Limitations

1. This proposed GAN outperformed the other four techniques in three out of four observed imbalanced datasets. This indicates that there is room to enhance the ability of SDG-GAN.

3.5. One-Class Adversarial Nets for Fraud Detection (OCAN)

Zheng et al. [94] argue that most online fraud detection techniques require training datasets with both legitimate and fraudulent transactions. On the contrary, usually, there are few or no records of fraudulent users in real datasets. To overcome this issue, [94] developed a One-class Adversarial Net (OCAN) for online fraud detection. OCAN only uses legitimate users to train the datasets.

Firstly, OCAN uses the LSTM autoencoder to learn the representation of legitimate users from the patterns of their online actions. Secondly, OCAN detects fraudulent users by training a discriminator of a GAN model, which is different from the Discriminator of the traditional GAN model. The findings of this experimental study reveal that OCAN dominates all other one-class classification models and can attain a comparable performance similar to the novel multisource LSTM model, which needs the data of both fraudulent and legitimate users.

3.5.1. Process

1. In the first training phase, the LSTM autoencoder is adopted to learn representations of legitimate users from the sequences of their activities.
2. The encoder figures unseen representations of the inputs, and the decoder calculates the reconstructed inputs.
3. In the second phase, containing training, a complementary GAN comprises a Discriminator that distinguishes the legitimate and fraudulent users.

3.5.2. Strengths

1. OCAN outperforms other one-class classification GAN models.
2. Details about fraudulent users are not required in this technique. Thus, this framework is more adaptive to fraudulent user identification tasks.
3. Unlike single-class classification GAN models, OCAN generates complimentary samples of fraudulent users.
4. It can capture the sequential details of the user's actions.

3.5.3. Limitations

1. OCAN can detect fraudulent activities; however, more evaluation is needed to evaluate the accuracy of this model.
2. The stability of OCAN is lower than the normal threshold.

As demonstrated in Figure 5 there are two training stages in the OCAN framework. In the first stage, the LSTM-autoencoder is adopted to learn benign user representations from benign user activity sequences. The LSTM-autoencoder is a model consisting of two LSTM models—the decoder and encoder. The encoder computes the hidden representation of the input, and the decoder computes reconstructed inputs. In the second stage, the training of a complementary GAN with D takes place. The Discriminator discriminates benign users from malicious users. On the other hand, the Generator of this model generates benign

samples and the Discriminator works to distinguish between complementary and real benign users.

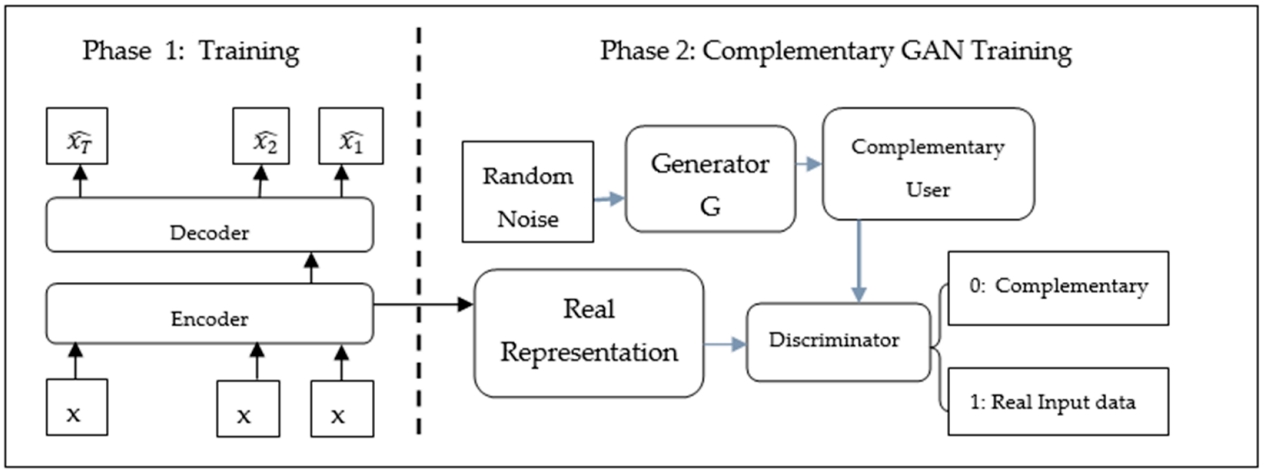


Figure 5. The training architecture of OCAN.

3.6. Conditional Wasserstein GAN (cWGAN)-Based Oversampling Method

Similarly, [90] introduced an oversampling model based on a Conditional Wasserstein-GAN with the ability to model tabular data streams effectively with categorical and numerical variables. Furthermore, the proposed model approaches the downstream classification tasks via an auxiliary classifier loss. In addition, they also benchmarked their method against conventional oversampling methods and the imbalanced baseline on actual datasets.

3.6.1. Process

1. This method has several elements not present in conventional methods, such as the AC loss, the W-GAN GP, etc.
2. The authors employed the cGAN framework to estimate the distribution to sample the minority class.

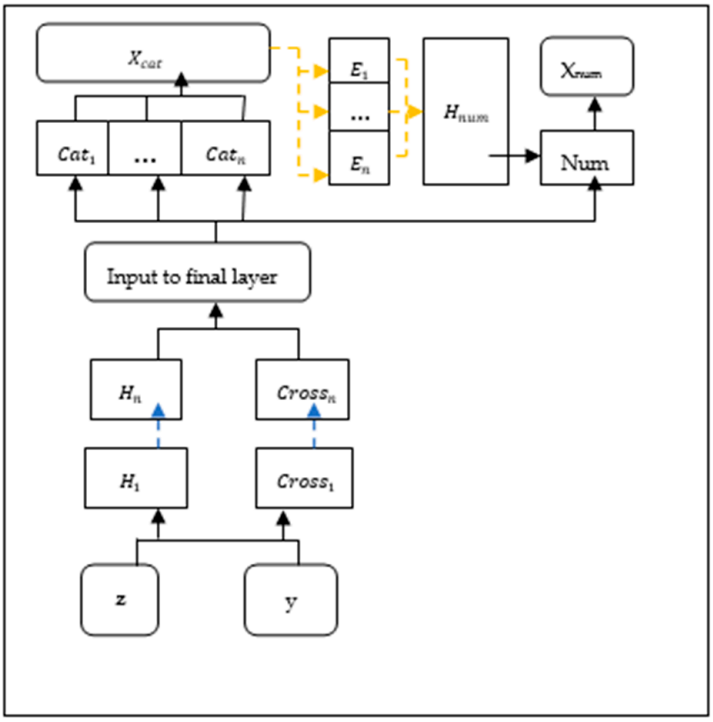
3.6.2. Strengths

1. This method efficiently models tabular datasets with categorical and numerical variables.
2. This novel method pays extraordinary attention to the downstream classification task via an auxiliary classifier loss.
3. This method also works well for nonlinear datasets.

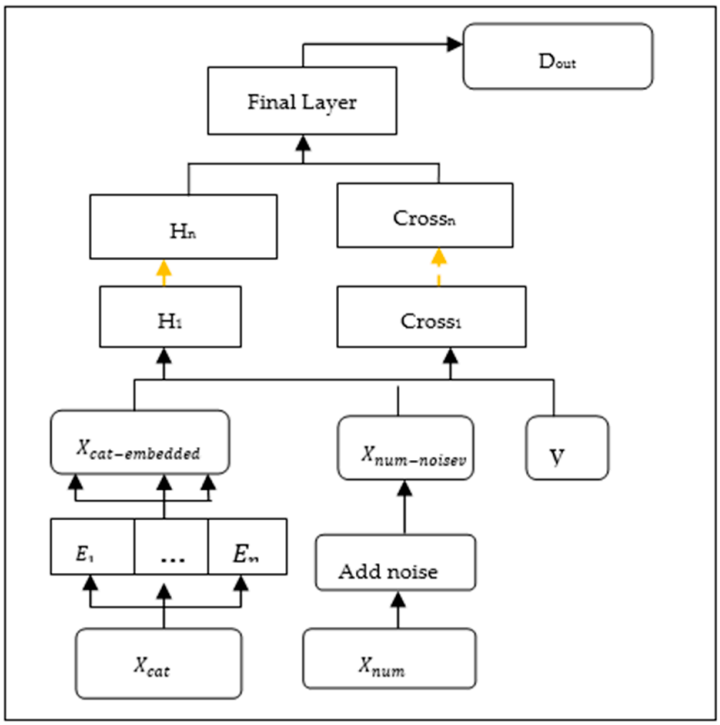
3.6.3. Limitations

1. Yet to test on heavily unbalanced datasets.
2. Model enhancement is imperative to identifying better default hyper-parameter settings.
3. Improvement is needed in fine-tuning this model.

In the WGANGP framework as demonstrated in Figure 6a,b, the loss function is augmented by adding AC loss to boost the generator. This figure indicates the AC output predicting minority class membership for samples of the real-world dataset that belong to the majority class and minority class. The dashed line shows the cut-off AC loss values.



(**a**)



(**b**)

Figure 6. (**a**) Structure of the Generator network of WGANGP. (**b**) Structure of the Discriminator network of WGANGP.

3.7. ScoreGAN

In their study, Shehnepoor et al. [95] proposed ScoreGAN to detect online shopping fraud. This novel framework generates reviews with precise semantics to address fraud detections' lack of high-quality data. ScoreGAN uses both review ratings and review text scores to detect and generate progression. The findings of this study show that

customization of the machine-obtained reviews based on the score leads to considerable progress in detecting fraud reviews by 5% on Tripadvisor and by 7% on the Yelp dataset against the data obtained from the state-of-the-art systems.

3.7.1. Process

1. The Discriminator D differentiates between human fraud reviews from fraud bot reviews, and calculates the probability of a score based on fraud reviews and corresponding scores.
2. After that, the Discriminator can differentiate genuine reviews from fraud reviews.
3. On the other hand, the Generator takes the score and random noise, generating fake bot reviews.

3.7.2. Strengths

1. This framework can convert the discrete form into a continuous one. This research work used the Tripadvisor and Yelp datasets, which are more reliable than datasets labeled by humans.
2. This proposed method outperforms other systems when applied to the used dataset, according to the metrics.

3.7.3. Limitations

1. The Discriminator can only estimate the reward for generating complete sentences, not partial ones.

3.8. Conditional Generative Adversarial Network (CGAN)

The Conditional Generative Adversarial Networks, or simply CGANs as demonstrated in Figure 7, consider the classes to which the instances belong. Initially proposed by [87], this GAN variant shows excellent results for datasets with a target class. Since their introduction, Conditional GANs have been applied in multiple areas, including image datasets [90]. Recently, Choi et al. [91] applied the Conditional GAN framework to the credit card dataset to generate synthetic data. Conditional GANs generate a synthetic credit card dataset, which can be used indistinguishably for training without revealing the actual dataset. The findings of their study show that deep learning techniques can be used with excellent outcomes to generate synthetic credit card data.

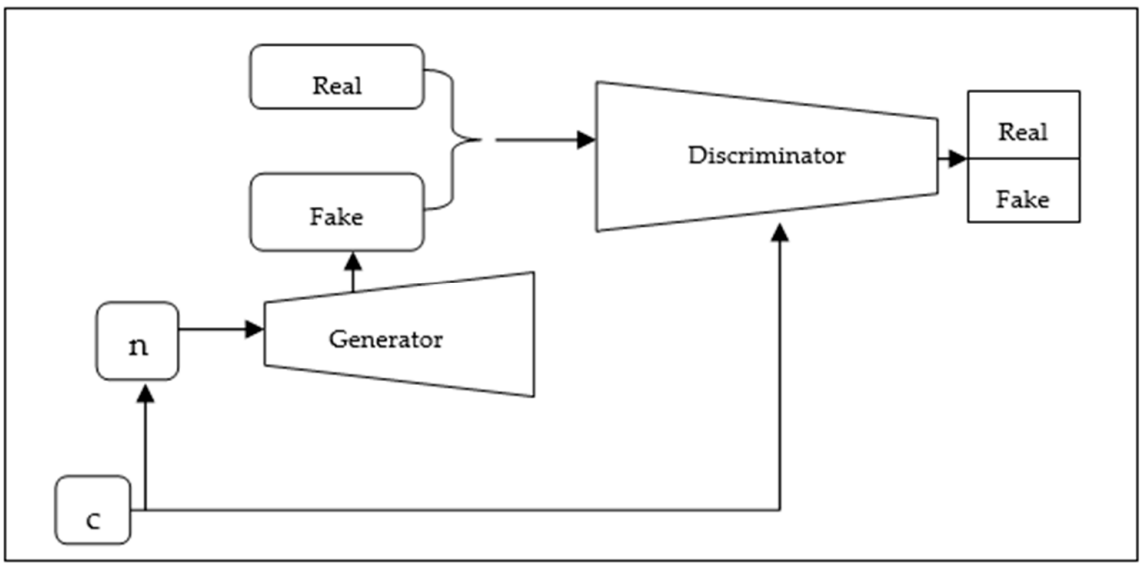


Figure 7. The Conditional GAN design is quite similar to the design of the conventional GAN, except the addition of class C, to which the instances belong.

3.9. GAN-RF

In another study, Lee and Park [40] argued that deep learning methods perform better than machine learning techniques when dealing with large quantities of datasets, such as credit card transaction datasets. They insist that more of the previous studies that deal with the imbalance class challenge have limitations that are outcomes of overfitting and data loss. For the said purpose, they used GAN and a proposed model to deal with the imbalanced class issue. Their proposed method, as demonstrated in Figure 8, was then classified as Random Forest to determine the detection ability after dealing with GAN-based data augmentation. The findings of their study reveal that their proposed model performed better than the model classified without dealing with the imbalanced class issue. Furthermore, it was identified that their proposed model is superior to the models proposed in previous studies.

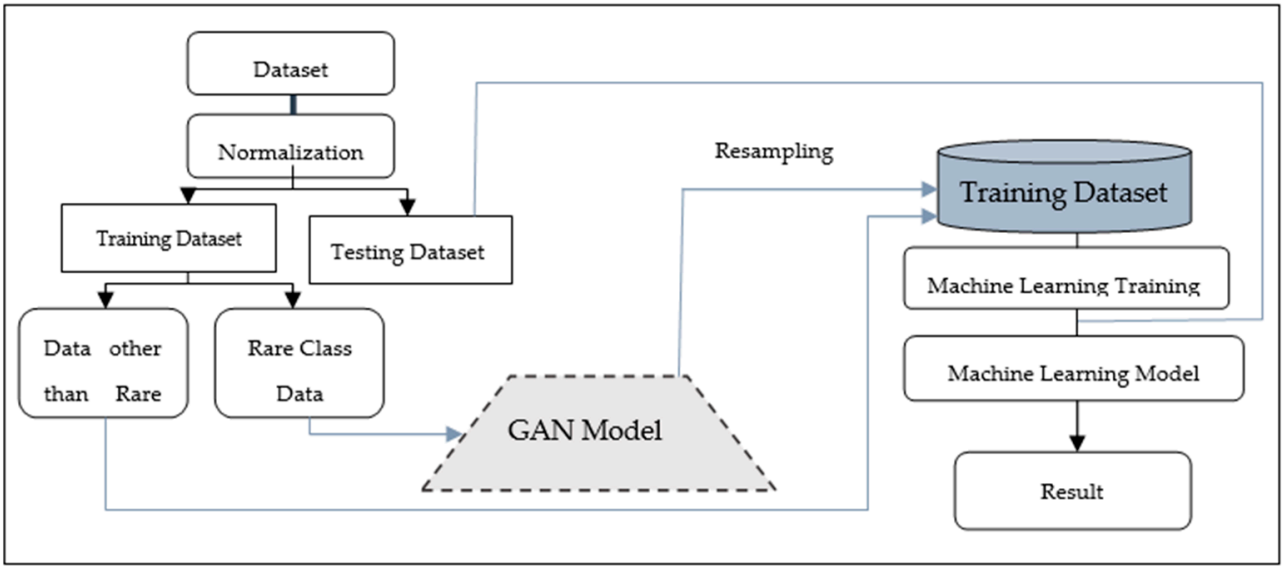


Figure 8. The GAN-RF framework.

3.10. Tuned-GAN

Similarly, Fiore et al. [5] presented in their work a new way to deal with the imbalanced class challenge in supervised classification to detect credit card fraud. They produced an augmented tuned set, consisting of more samples of fraudulent transactions with respect to the original dataset. They created artificial examples with a tuned GAN as demonstrated in Figure 9, which means that the Discriminator network was unable to discriminate artificial samples from the real samples. It is also noteworthy that the proposed framework is inherently dependent on the accessibility of labeled instances of minority examples. To check the validation of their method, the researchers performed an empirical study on a real-world credit card dataset with imbalanced classes. Their method achieved superior sensitivity at the cost of a marginal increase in false positives.

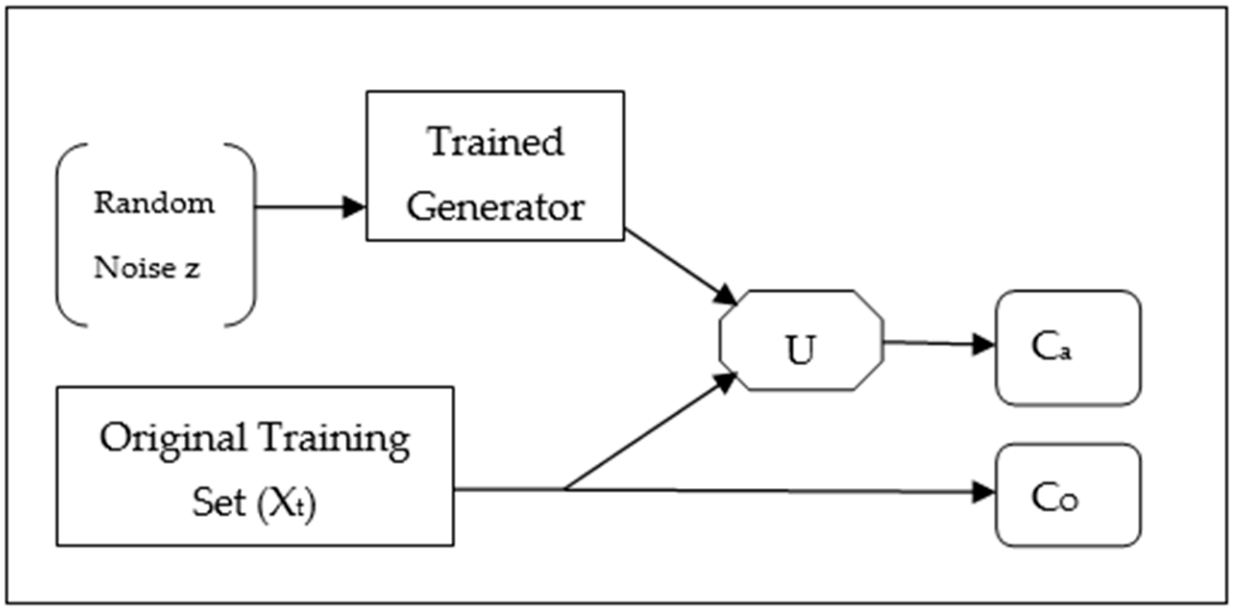


Figure 9. The G* is fed with z (random noise) and the output is merged with x_t. Other than that, the classifier C is trained on original and augmented training sets (C_O and C_a).

4. Tabular Comparison of Different GAN Variants

This part of our survey presents an overview of the various GAN-based methods used to deal with the imbalanced class problem.

Detailed Discussion on the Above-Reviewed GAN Variants

In this study, we introduced the most considerable challenges faced by the conventional GAN architecture, vanishing gradient and mode collapse, that arise while updating the Generator. To deal with this challenge, we surveyed important variants of GAN that have the potential to solve these issues. The GAN variants discussed in this study offer more architectural alternatives for GANs. Furthermore, this study explained the main causes of these issues in the conventional GAN. This study also shed light on the modified loss functions presented by GAN variants to solve these issues. In addition, Table 1 offers a performance summary of different GAN variants discussed in this paper. In [91], the authors discussed synthetic data generation using the cGAN model. The study aimed to employ a Conditional Generative Adversarial Network to generate new synthetic data from the "Default of Credit Card Clients" datasets. To circumvent disclosing sensitive information, the study presented a CGAN that created new synthetic data from training data that may be applied interchangeably to the same tasks. Since the training data included a class label that was taken into account during the production of new data, this network type was employed instead of a standard Generative Adversarial Network (GAN). The outcomes were measured in two ways: firstly, the correlation between the new and old data was low, allowing for their usage in contentious industries such as medical and banking, where great care must be taken with client data to avoid privacy concerns. Secondly, the same algorithm, XGBoost, was evaluated on the two datasets with the same settings because the datasets included a label that could be employed as the classifier. Based on the data, both approaches achieved comparable categorization precision levels. In conclusion, the study shows that deep learning techniques can be effectively deployed in synthetic data production. Further studies will investigate potential new adversarial network versions for this task, and experiment with different parameter settings to achieve optimal reliability.

Table 1. Comparison table of GAN-based methods. This tabular representation presents different studies conducted by researchers in more recent times to generate synthetic data. It provides a detailed tabular presentation of different datasets and methods, their merits and demerits, as well as the Accuracy, Precession, Recall and F-1 scores of multiple studies to provide a detailed description of their key findings.

Model	Accuracy	Precision	Recall	F-Measure
Duo-GAN	—	—	—	—
C-GAN	0.826	—	—	0.509
CT-GAN	21.51%	—	—	CTGAN = 0.274
SDG GAN	—	0.9863	0.8090	0.8889
OCAN	0.826	—	—	0.509
cWGAN	—	—	—	—
ScoreGAN	—	—	—	—
GAN-RF	99.83	GAN-RF = 99.88	GAN-RF = 99.9	GAN-RF = 99.90
Tuned GAN	0.99963	GAN = 0.93204	—	GAN = 0.82051
Majority–minority GAN	—	—	—	Bank B = 0.552

In the above table "—" refers to experiments that have not been done in previous studies.

Furthermore, Zhao et al. [89] employed various GAN models for synthetic data generation related to credit card transactions. The results from the research suggest using CTAB-GAN, a conditional GAN-based tabular data generator. By modeling mixed variables, CTAB-GAN surpassed the previous state-of-the-art approaches and offered superior generating capabilities for imbalanced categorical variables and continuous variables with complex distributions. In relation to this, CTAB-GAN has three main features: First, incorporating a classifier into the conditional GAN. Second, efficient data encoding for mixed variables. The third is a novel construction of conditional vectors. They compared CTAB-GAN to four other tabular data generators using various measures, including their statistical similarity, ML utility, and ability to defend user privacy. The CTAB-synthetic GAN's data outperformed the current state-of-the-art privacy guarantee in terms of similarity and utility methods. Compared to all other state-of-the-art algorithms, it enhanced the accuracy by as much as 17% when applied to complicated datasets. The CTAB-impressive GAN's findings showed its potential use in various applications that could benefit tremendously from data exchange, such as manufacturing, banking, and insurance.

Similarly, Lee and Park [40] employed the GAN model to detect fraud in credit card transactions with imbalanced data. The study used the GAN model to resample minority classes and accurately recreate them. The GAN was trained with ten times as many data from the uncommon classes of Infiltration, Heartbleed, and Bot to evaluate its classification efficacy. Compared to a standard Random Forest classification, the results of the tests demonstrate that GAN resampling achieved better results. In particular, the results demonstrate a superior categorization ability for the minority classes compared to normal and control classes. It appears that the normal class classification performance was enhanced through increased exposure to information concerning the minority class' features, which differed markedly from those of other classes. Additionally, the results prove that GAN-RF demonstrated superior performance by classifying the data resampled with SMOTE, a technique employed in earlier studies to resolve unbalanced data. While the basic idea behind both SMOTE and GAN is to generate new data, SMOTE had issues with overlapping noise and classes. As a result, the GAN model, which replicated the uncommon class and properly compared attributes, performed better in cases of data asymmetry. Based on the research results, GAN also performed very well in detecting intrusions in networks with skewed data. The deep learning model known as GAN is frequently employed for image and language processing because it does not rely on human oversight or labeling. The effectiveness of the training data before and after resampling was measured, and the efficacy of various algorithms was measured in separate experiments.

To resample the data, the study employed a GAN model, and the study used the Random Forest technique to classify the samples.

Additionally, Fiore et al. [5] used the synthetic data generation GAN model to identify irregularities in credit card transactions using imbalanced datasets. The study employed the GAN and SMOTE models. They described an approach for addressing the challenge of class imbalance that arises with the use of supervised classification in detecting fraud in the credit card domain. When a training set was provided, an augmented set was generated with more data from the minority class than the original set. In addition, a fine-tuned GAN was used to produce synthetic instances. As a result, the GAN's Discriminator could not distinguish between fake and accurate data. Recent research work by [13] constitutes the continuation of the research work by [5]. Langevin et al. [13] used GANs to generate synthetic sampling. Their case study investigated two cooperating party scenarios yielding four consumer distributions by credit quality. The authors selected GANs as a scalable and flexible approach to generating synthetic data for fraud detection related to credit card fraud. Furthermore, the authors got access to almost 80 million credit card transaction datasets, with different data types, through collaborating with a financial institution. Their findings show that organizations tilted more and more towards quality consumers are more prone to benefit from augmentations with GANs. In Refs. [96–103], studies are discussed addressing the different techniques used in generative adversarial networks to overcome class imbalance. Among them, SMOTE (Synthetic Minority Over-sampling Technique) is studied in [96], while Gulrajani et al. [97] proposed an improved training of Wasserstein GANs, and [98] proposed a Generative Adversarial Fusion Network for class imbalance credit scoring. Furthermore, Vijayaraghavan and Guan [99] discussed using GAN-based data augmentation to resolve class imbalance. Creswell et al. [53] discussed an overview of GANs, while Gui et al. [100] reviewed the algorithms, theories and applications of GANs. Pandey et al. [101] discussed the limitations and applicability of GANs in the banking domain, and Ramponi et al. [102] proposed using T-CGAN for data augmentation with irregular sampling. Finally, Vega-Márquez et al. [103] studied the creation of synthetic data with CGAN. These studies demonstrate that GANs can be effective in addressing class imbalance by using techniques such as oversampling or data augmentation. However, further research is necessary to evaluate the effectiveness of this approach in different scenarios, and to improve the accuracy of GANs. Moreover, it is necessary to investigate the effectiveness of combining GANs with other techniques to address class imbalance. Furthermore, it is important to develop approaches that are able to generate more accurate and diverse samples in order to improve the accuracy of classification models. Finally, further research should be undertaken on how to effectively combine generative adversarial networks and classifiers to tackle the class imbalance problem.

5. Conclusions and Future Recommendations

This report reviews the recent advancements made in GANs, starting from the basic principles according to which GANs are presented as the most modern architectures. Furthermore, the challenges that GANs can suffer from are addressed, and some of the most common evaluation metrics are discussed and elucidated. In addition, this survey reviewed the original GAN and introduced different GAN variants dealing with credit card-based fraud. Furthermore, this study shows that GAN can facilitate multiple practical approaches to credit card-based fraud detection. In addition, we have discussed multiple studies that have proposed novel training techniques. Moreover, we have also highlighted the merits and demerits of the generative techniques proposed by scholars to generate realistic data. Our work has shown that data augmentation using GANs has the ability to address the problems of imbalanced data in credit card-based fraud. To deal with this challenge, multiple GAN-based solutions have been introduced in recent years. However, there are many limitations that need to be considered in future work. To start with, recent studies lack standardization in the evaluation metrics used to assess the performance of synthetic data generated by GANs for credit card fraud detection. Other than that,

recent studies have shown that while GANs can generate high-quality synthetic data, the diversity of synthetic data can be improved. In general, there are many areas that should be focused on in future research on data augmentation using GANs for credit card fraud detection. Among these areas, addressing the limitations of GANs to improve their effectiveness in the credit card fraud domain is essential to protect credit card holders from monetary losses. The future research on GAN-based data augmentation should focus on setting up a taxonomy of augmentation methods, enhancing the overall quality of GAN samples, learning novel ways to build correlations between classifier frameworks and data augmentation, and widening the scope of GANs to other data types. This research work is focused on GAN-based data augmentation in credit card fraud detection. However, data augmentation is limited to this domain, and can be employed for breast cancer detection, imaging, insurance and so on. In future research, enhancing the quality of GAN samples and the effectiveness of their testing on multiple datasets is also an important area to explore. Researchers can also combine GAN samples with other data augmentation methods.

GANs have shown immense success in recent years in generating artificial data. However, there are limitations in the conventional architecture. Future studies should look into alternative GAN frameworks to generate high-quality and diverse artificial data to detect credit card fraud. In addition, GANs have the capacity for improvements in terms of the effectiveness of the synthetic data generated by GANs. Researchers can also focus on enhancing the quantity and quality of GAN-generated data. For instance, researchers can optimize the training phase or fine-tune GAN hyper-parameters. Moreover, future studies can also combine data augmentation using GANs with other techniques, such as active learning, to improve the performance of credit card fraud detection models. In addition, it is essential to check the generalization of synthetic data generated by GAN to see if the underlying data distribution represents the data or not. Potential future studies should explore methods to evaluate the generalization of data generated by GANs to assess their applicability in credit card fraud detection models. It is imperative to mention that GANs ensure the privacy of the credit card holder while generating synthetic data with similar traits to the original credit card data. However, researchers could examine other ethical considerations linked with data augmentation using GANs, such as making sure that the GAN-generated data are not discriminatory or biased.

The observations of this survey conclude that GANs are more effective and appropriate for use in handling the class imbalance challenge. Moreover, this survey also finds GANs are highly robust towards overfitting and overlapping, as GANs can understand the hidden patterns of data thanks to deep networks. In addition, GANs' characteristics, such as their architectural design, multiple variants, and application areas, make this method superior to other machine learning algorithms. Generative Adversarial Networks have achieved significant progress in credit card fraud detection. GANs can address an imbalanced class problem via data augmentation, as they approximate the distribution of real data and generate synthetic data for the minority class (fraudulent transactions). Furthermore, GANs have received much attention from researchers, and attained promising results in credit card fraud detection.

However, despite the enormous progress made in GAN techniques, these models still have shortcomings in dealing with credit card fraud. Therefore, future research should focus more on elaborating powerful additional GANs for existing models in the financial domain.

Author Contributions: Conceptualization, E.S. and S.P.; methodology, E.S. and S.P.; software, E.S.; validation, E.S.; formal analysis, E.S.; investigation, E.S. and S.P.; resources, S.P.; data curation, E.S.; writing—original draft preparation, E.S.; writing—review and editing, S.P.; visualization, E.S.; supervision, S.P.; project administration, S.P.; funding acquisition, S.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Bournemouth University, United Kingdom.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Adewumi, A.O.; Akinyelu, A.A. A survey of machine-learning and nature-inspired based credit card fraud detection tech-niques. *Int. J. Syst. Assur. Eng. Manag.* **2017**, *8*, 937–953. [CrossRef]
2. Bahnsen, A.C.; Aouada, D.; Stojanovic, A.; Ottersten, B. Feature engineering strategies for credit card fraud detection. *Expert Syst. Appl.* **2016**, *51*, 134–142. [CrossRef]
3. Srivastava, A.; Kundu, A.; Sural, S.; Majumdar, A. Credit card fraud detection using hidden Markov model. *IEEE Trans. Dependable Secur. Comput.* **2008**, *5*, 37–48. [CrossRef]
4. Tan, G.W.H.; Ooi, K.B.; Chong, S.C.; Hew, T.S. NFC mobile credit card: The next frontier of mobile payment? *Telemat. Inform.* **2014**, *31*, 292–307. [CrossRef]
5. Fiore, U.; De Santis, A.; Perla, F.; Zanetti, P.; Palmieri, F. Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. *Inf. Sci.* **2019**, *479*, 448–455. [CrossRef]
6. Zhang, F.; Liu, G.; Li, Z.; Yan, C.; Jiang, C. GMM-based Undersampling and Its Application for Credit Card Fraud Detection. In Proceedings of the 2019 International Joint Conference on Neural Networks (IJCNN), Budapest, Hungary, 14–19 July 2019; pp. 1–8. [CrossRef]
7. Haixiang, G.; Yijing, L.; Shang, J.; Mingyun, G.; Yuanyue, H.; Bing, G. Learning from class-imbalanced data: Review of methods and applications. *Expert Syst. Appl.* **2017**, *73*, 220–239. [CrossRef]
8. Guo, X.; Yin, Y.; Dong, C.; Yang, G.; Zhou, G. On the class imbalance problem. In Proceedings of the Fourth International Conference on Natural Computation, Jinan, China, 18–20 October 2008; Volume 4, pp. 192–201.
9. Malave, N.; Nimkar, A.V. A survey on effects of class imbalance in data pre-processing stage of classification problem. *Int. J. Comput. Syst. Eng.* **2020**, *6*, 63–75. [CrossRef]
10. Moreno-Barea, F.J.; Jerez, J.M.; Franco, L. Improving classification accuracy using data augmentation on small data sets. *Expert Syst. Appl.* **2020**, *161*, 113696. [CrossRef]
11. Al Olaimat, M.; Lee, D.; Kim, Y.; Kim, J.; Kim, J. A learning-based data augmentation for network anomaly detection. In Proceedings of the 29th International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, 3–6 August 2020; pp. 1–10.
12. Tamtama, A.S.; Arifudin, R. Increasing Accuracy of The Random Forest Algorithm Using PCA and Resampling Techniques with Data Augmentation for Fraud Detection of Credit Card Transaction. *J. Adv. Inf. Syst. Technol.* **2022**, *4*, 60–76.
13. Langevin, A.; Cody, T.; Adams, S.; Beling, P. Synthetic data augmentation of imbalanced datasets with generative adversarial networks under varying distributional assumptions: A case study in credit card fraud detection. *J. Oper. Res. Soc.* **2021**, 1–28. [CrossRef]
14. Wang, C.; Deng, C.; Wang, S. Imbalance-XGBoost: Leveraging weighted and focal losses for binary label-imbalanced classi-fication with XGBoost. *Pattern Recognit. Lett.* **2020**, *136*, 190–197. [CrossRef]
15. Johnson, J.M.; Khoshgoftaar, T.M. Survey on deep learning with class imbalance. *J. Big Data* **2019**, *6*, 27. [CrossRef]
16. Pouyanfar, S.; Sadiq, S.; Yan, Y.; Tian, H.; Tao, Y.; Reyes, M.P.; Shyu, M.L.; Chen, S.C.; Iyengar, S.S. A survey on deep learning: Algorithms, techniques, and applications. *ACM Comput. Surv. (CSUR)* **2018**, *51*, 92. [CrossRef]
17. Bauder RA, Khoshgoftaar TM, Hasanin, T. An empirical study on class rarity in big data. In Proceedings of the 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA, 17–20 December 2018; pp. 785–790. [CrossRef]
18. Kotsiantis, S.B.; Kanellopoulos, D.; Pintelas, P.E. Data preprocessing for supervised leaning. *Int. J. Comput. Sci.* **2006**, *1*, 111–117.
19. Yang, W.; Zhang, Y.; Ye, K.; Li, L.; Xu, C.-Z. FFD: A Federated Learning Based Method for Credit Card Fraud Detection. In Proceedings of the Big Data–BigData 2019: 8th International Congress, Held as Part of the Services Conference Federation, SCF, San Diego, CA, USA, 25–30 June 2019; pp. 18–32. [CrossRef]
20. Tanaka, F.H.K.D.S.; Aranha, C. Data augmentation using GANs. *arXiv* **2019**, arXiv:1904.09135v1.
21. Cordón, I.; García, S.; Fernández, A.; Herrera, F. Imbalance: Oversampling algorithms for imbalanced classification in R. *Knowledge-Based Syst.* **2018**, *161*, 329–341. [CrossRef]
22. Benchaji, I.; Douzi, S.; El Ouahidi, B. Using genetic algorithm to improve classification of imbalanced datasets for credit card fraud detection. In *Smart Data and Computational Intelligence: Proceedings of the International Conference on Advanced Information Technology, Services and Systems (AIT2S-18), 17–18 October 2018*; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; Volume 3, pp. 220–229.

23. Cai, Z.; Wang, X.; Zhou, M.; Xu, J.; Jing, L. Supervised class distribution learning for GANs-based im-balanced classification. In Proceedings of the IEEE International Conference on Data Mining (ICDM), Beijing, China, 8–11 November 2019; pp. 41–50.
24. Sayed, G.I.; Soliman, M.M.; Hassanien, A.E. A novel melanoma prediction model for imbalanced data using opti-mized SqueezeNet by bald eagle search optimization. *Comput. Biol. Med.* **2021**, *136*, 104712. [CrossRef]
25. Kuppa, A.; Aouad, L.; Le-Khac, N.A. Towards improving privacy of synthetic datasets. In *Privacy Technologies and Policy, Proceedings of the 9th Annual Privacy Forum, APF, Oslo, Norway, 17–18 June 2021*; Springer International Publishing: Cham, Switzerland; pp. 106–119.
26. Sakharova, I. Payment card fraud: Challenges and solutions. In Proceedings of the 2012 IEEE International Conference on Intelligence and Security Informatics, Washington, USA, 11–14 June 2012; pp. 227–234.
27. Triastcyn, A.; Faltings, B. Generating artificial data for private deep learning. *arXiv* **2018**, arXiv:1803.03148.
28. Goodfellow, I.J.; Pouget-Abadie, J.; Mirza, M.; Xu, B.; Warde-Farley, D.; Ozair, S.; Courville, A.; Bengio, Y. *Generative Adversarial Nets (Advances in Neural Information Processing Systems)*; Red Hook: New York, NY, USA, 2014. [CrossRef]
29. Chen, J.; Shen, Y.; Ali, R. Credit card fraud detection using sparse autoencoder and generative adver-sarial network. In Proceedings of the IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 1–3 November 2018; pp. 1054–1059.
30. Wei, W.; Li, J.; Cao, L.; Ou, Y.; Chen, J. Effective detection of sophisticated online banking fraud on extremely im-balanced data. *World Wide Web* **2013**, *16*, 449–475. [CrossRef]
31. Kajal, D.; Kaur, K. Credit card fraud detection using imbalance resampling method with feature selection. *Int. J.* **2021**, *10*, 2061–2071.
32. Makki, S.; Assaghir, Z.; Taher, Y.; Haque, R.; Hacid, M.-S.; Zeineddine, H. An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection. *IEEE* **2019**, *7*, 93010–93022. [CrossRef]
33. Dal Pozzolo, A.; Caelen, O.; Le Borgne, Y.-A.; Waterschoot, S.; Bontempi, G. Learned lessons in credit card fraud detection from a practitioner perspective. *Expert Syst. Appl.* **2014**, *41*, 4915–4928. [CrossRef]
34. Thennakoon, A.; Bhagyani, C.; Premadasa, S.; Mihiranga, S.; Kuruwitaarachchi, N. Real-time credit card fraud detection using machine learning. In Proceedings of the 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Uttar Pradesh, India, 10–11 January 2019; pp. 488–493.
35. Chaudhary, K.; Yadav, J.; Mallick, B. A review of fraud detection techniques: Credit card. *Int. J. Comput. Appl.* **2012**, *45*, 39–44.
36. Dong, Q.; Gong, S.; Zhu, X. Imbalanced Deep Learning by Minority Class Incremental Rectification. *IEEE Trans. Pattern Anal. Mach. Intell.* **2018**, *41*, 1367–1381. [CrossRef]
37. Assefa, S.A.; Dervovic, D.; Mahfouz, M.; Tillman, R.E.; Reddy, P.; Veloso, M. Generating synthetic data in finance: Opportunities, challenges and pitfalls. In Proceedings of the First ACM International Conference on AI in Finance, New York, NY, USA, 15–16 October 2020; pp. 1–8.
38. Wang, S.; Yao, X. Multiclass Imbalance Problems: Analysis and Potential Solutions. *IEEE Trans. Syst. Man Cybern. Part B (Cybernetics)* **2012**, *42*, 1119–1130. [CrossRef] [PubMed]
39. Herland, M.; Khoshgoftaar, T.M.; Bauder, R.A. Big Data fraud detection using multiple medicare data sources. *J. Big Data* **2018**, *5*, 29. [CrossRef]
40. Lee, J.; Park, K. GAN-based imbalanced data intrusion detection system. *Pers. Ubiquitous Comput.* **2021**, *25*, 121–128. [CrossRef]
41. Seiffert, C.; Khoshgoftaar, T.M.; Van Hulse, J.; Napolitano, A. Mining data with rare events: A case study. In Proceedings of the 19th IEEE International Conference on Tools with Artificial Intelligence (ICTAI), Patras, Greece, 29–31 October 2007; Volume 2, pp. 132–139.
42. Shorten, C.; Khoshgoftaar, T.M. A survey on Image Data Augmentation for Deep Learning. *J. Big Data* **2019**, *6*, 60. [CrossRef]
43. Pan, Z.; Yu, W.; Yi, X.; Khan, A.; Yuan, F.; Zheng, Y. Recent Progress on Generative Adversarial Networks (GANs): A Survey. *IEEE Access* **2019**, *7*, 36322–36333. [CrossRef]
44. Antipov, G.; Baccouche, M.; Dugelay, J.L. Face aging with conditional generative adversarial networks. In Proceedings of the 2017 IEEE international conference on image processing (ICIP), Beijing, China, 17–20 September 2017; pp. 2089–2093.
45. Dziugaite, G.K.; Roy, D.M.; Ghahramani, Z. Training generative neural networks via maximum mean dis-crepancy optimization. In Proceedings of the Thirty-First Conference on Uncertainty in Artificial Intelligence, Amsterdam, The Netherlands, 12–16 July 2015; pp. 258–267.
46. Lassner, C.; Pons-Moll, G.; Gehler, P.V. A generative model of people in clothing. In Proceedings of the IEEE international conference on computer vision, Venice, Italy, 22–29 October 2017; pp. 853–862.
47. Hwang, J.; Kim, K. An Efficient Domain-Adaptation Method using GAN for Fraud Detection. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 94–103. [CrossRef]
48. Cai, Z.; Xiong, Z.; Xu, H.; Wang, P.; Li, W.; Pan, Y. Generative adversarial networks: A survey toward private and secure applications. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–38. [CrossRef]

49. Yang, X.; Song, Z.; King, I.; Xu, Z. A survey on deep semi-supervised learning. *IEEE Trans. Knowl. Data Eng.* **2022**, *1*, 1–20. [CrossRef]
50. Wang, Z.; Wang, W.; Yang, Y.; Han, Z.; Xu, D.; Su, C. CNN-and GAN-based classification of malicious code families: A code visualization approach. *Int. J. Intell. Syst.* **2022**, *37*, 12472–12489. [CrossRef]
51. Jiang, J.; Liu, F.; Liu, Y.; Tang, Q.; Wang, B.; Zhong, G.; Wang, W. A dynamic ensemble algorithm for anomaly detection in IoT imbalanced data streams. *Comput. Commun.* **2022**, *194*, 250–257. [CrossRef]
52. Zhang, L.; Chen, W.; Wang, W.; Jin, Z.; Zhao, C.; Cai, Z.; Chen, H. Cbgru: A detection method of smart contract vulnerability based on a hybrid model. *Sensors* **2022**, *22*, 3577. [CrossRef] [PubMed]
53. Creswell, A.; White, T.; Dumoulin, V.; Arulkumaran, K.; Sengupta, B.; Bharath, A.A. Generative Adversarial Networks: An Overview. *IEEE Signal Process. Mag.* **2018**, *35*, 53–65. [CrossRef]
54. Park, S.-W.; Ko, J.-S.; Huh, J.-H.; Kim, J.-C. Review on Generative Adversarial Networks: Focusing on Computer Vision and Its Applications. *Electronics* **2021**, *10*, 1216. [CrossRef]
55. Cauli, N.; Recupero, D.R. Survey on Videos Data Augmentation for Deep Learning Models. *Futur. Internet* **2022**, *14*, 93. [CrossRef]
56. Ali-Gombe, A.; Elyan, E.; Savoye, Y.; Jayne, C. Few-shot classifier GAN. In Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, 8–13 July 2018; pp. 1–8.
57. Burks, R.; Islam, K.A.; Lu, Y.; Li, J. Data Augmentation with Generative Models for Improved Malware Detection: A Comparative Study. In Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 10–12 October 2019; pp. 0660–0665. [CrossRef]
58. Jain, S.; Seth, G.; Paruthi, A.; Soni, U.; Kumar, G. Synthetic data augmentation for surface defect detection and classi-fication using deep learning. *J. Intell. Manuf.* **2022**, *33*, 1007–1020. [CrossRef]
59. Torkzadehmahani, R.; Kairouz, P.; Paten, B. Dp-cgan: Differentially private synthetic data and label generation. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, Long Beach, CA, USA, 16–20 June 2019; pp. 1–7.
60. Alqahtani, H.; Kavakli-Thorne, M.; Kumar, G. Applications of Generative Adversarial Networks (GANs): An Updated Review. *Arch. Comput. Methods Eng.* **2021**, *28*, 525–552. [CrossRef]
61. Kim, J.; Jeong, K.; Choi, H.; Seo, K. GAN-based anomaly detection in imbalance problems. In Proceedings of the Computer Vision–ECCV 2020 Workshops, Glasgow, UK, 23–28 August 2020; pp. 128–145. [CrossRef]
62. Saqlain, A.S.; Fang, F.; Ahmad, T.; Wang, L.; Abidin, Z.-U. Evolution and effectiveness of loss functions in generative adversarial networks. *China Commun.* **2021**, *18*, 45–76. [CrossRef]
63. Ba, H. Improving Detection of Credit Card Fraudulent Transactions using Generative Adversarial Networks. *arXiv* **2019**, arXiv:1907.03355.
64. Sethia, A.; Patel, R.; Raut, P. Data augmentation using generative models for credit card fraud detection. In Proceedings of the 4th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 14–15 December 2018; pp. 1–6.
65. Liu, H.; Lang, B. Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. *Appl. Sci.* **2019**, *9*, 4396. [CrossRef]
66. Charitou, C.; Dragicevic, S.; Garcez, A.D.A. Synthetic Data Generation for Fraud Detection using GANs. *arXiv* **2021**, arXiv:2109.12546.
67. Ngwenduna, K.S.; Mbuvha, R. Alleviating class imbalance in actuarial applications using generative adversarial net-works. *Risks* **2021**, *9*, 49. [CrossRef]
68. Zhong, Z.; Zheng, L.; Kang, G.; Li, S.; Yang, Y. Random Erasing Data Augmentation. In Proceedings of the AAAI Conference on Artificial Intelligence, New York, NY, USA, 7–12 February 2020.
69. Eom, S.; Huh, J.-H. The Opening Capability for Security against Privacy Infringements in the Smart Grid Environment. *Mathematics* **2018**, *6*, 202. [CrossRef]
70. Eom, S.; Huh, J.-H. Group signature with restrictive linkability: Minimizing privacy exposure in ubiquitous environment. *J. Ambient. Intell. Humaniz. Comput.* **2018**, *1*, 1–11. [CrossRef]
71. Chen, J.; Tam, D.; Raffel, C.; Bansal, M.; Yang, D. An empirical survey of data augmentation for limited data learning in NLP. *arXiv* **2021**, arXiv:2106.07499.
72. Laddha, S.; Kumar, V. DGCNN: Deep convolutional generative adversarial network based convolutional neural net-work for diagnosis of COVID-19. *Multimed. Tools Appl.* **2022**, *81*, 31201–31218. [CrossRef] [PubMed]
73. Talavera, E.; Iglesias, G.; González-Prieto, Á.; Mozo, A.; Gómez-Canaval, S. Data Augmentation techniques in time series domain: A survey and taxonomy. *arXiv* **2022**, arXiv:2206.13508.
74. Mikołajczyk, A.; Grochowski, M. Data augmentation for improving deep learning in image classification problem. In Proceedings of the International Interdisciplinary PhD Workshop (IIPhDW), Swinoujscie, Poland, 9–12 May 2018; pp. 117–122. [CrossRef]

75. Antoniou, A.; Storkey, A.; Edwards, H. Data augmentation generative adversarial networks. *arXiv* **2017**, arXiv:1711.04340.
76. Saxena, D.; Cao, J. Generative adversarial networks (GANs) challenges, solutions, and future directions. *ACM Com-Puting Surv. (CSUR)* **2021**, *54*, 1–42.
77. Chen, H. Challenges and Corresponding Solutions of Generative Adversarial Networks (GANs): A Survey Study. *J. Physics: Conf. Ser.* **2021**, *1827*, 012066. [CrossRef]
78. Zhou, Z.; Zhang, B.; Lv, Y.; Shi, T.; Chang, F. Data Augment in Imbalanced Learning Based on Generative Adversarial Networks. In *Neural Information Processing, Proceedings of the 26th International Conference, ICONIP 2019, Sydney, NSW, Australia, 12–15 December 2019*; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; Part IV 26; pp. 21–30. [CrossRef]
79. Xia, X.; Pan, X.; Li, N.; He, X.; Ma, L.; Zhang, X.; Ding, N. GAN-based anomaly detection: A review. *Neurocomputing* **2022**, *493*, 497–535. [CrossRef]
80. Niu, X.; Wang, L.; Yang, X. A comparison study of credit card fraud detection: Supervised versus unsuper-vised. *arXiv* **2019**, arXiv:1904.10604.
81. Mullick, S.S.; Datta, S.; Das, S. Generative adversarial minority oversampling. In Proceedings of the IEEE/CVF Interntional Conference on Computer Vision, Seoul, Korea, 27 October–2 November 2019; pp. 1695–1704.
82. Kodali, N.; Abernethy, J.; Hays, J.; Kira, Z. On Convergence and Stability of GANs. *arXiv* **2017**, arXiv:1705.07215.
83. Kossaifi, J.; Tran, L.; Panagakis, Y.; Pantic, M. Gagan: Geometry-aware generative adversarial networks. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 18–22 June 2018; pp. 878–887.
84. Mangalam, K.; Garg, R. Overcoming mode collapse with adaptive multi adversarial training. *arXiv* **2021**, arXiv:2112.14406.
85. Wang, Z.; She, Q.; Ward, T.E. Generative adversarial networks in computer vision: A survey and taxonomy. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–38. [CrossRef]
86. Arjovsky, M.; Chintala, S.; Bottou, L. Wasserstein generative adversarial networks. In Proceedings of the International Conference on Machine Learning, Baltimore, MD, USA, 17–23 July 2017; pp. 214–223.
87. Mirza, M.; Osindero, S. Conditional generative adversarial nets. *arXiv* **2014**, arXiv:1411.1784.
88. Ferreira, F.; Lourenço, N.; Cabral, B.; Fernandes, J.P. When Two are Better Than One: Synthesizing Heavily Un-balanced Data. *IEEE Access* **2021**, *9*, 150459–150469. [CrossRef]
89. Zhao, Z.; Kunar, A.; Birke, R.; Chen, L.Y. Ctab-gan: Effective table data synthesizing. In Proceedings of the Asian Conference on Machine Learning, Online, 17–19 November 2021; pp. 97–112. Available online: https://proceedings.mlr.press/v157/zhao21a (accessed on 13 February 2023).
90. Engelmann, J.; Lessmann, S. Conditional Wasserstein GAN-based oversampling of tabular data for imbalanced learning. *Expert Syst. Appl.* **2021**, *174*, 114582. [CrossRef]
91. Choi, E.; Biswal, S.; Malin, B.; Duke, J.; Stewart, W.F.; Sun, J. Generating multi-label discrete patient records using generative adversarial networks. In Proceedings of the Machine learning for Healthcare Conference, Boston, MA, USA, 18–19 August 2017; pp. 286–305.
92. Xu, L.; Skoularidou, M.; Cuesta-Infante, A.; Veeramachaneni, K. Modeling tabular data using conditional gan. *Adv. Neural Inf. Process. Syst.* **2019**, *32*, 1–11.
93. Park, N.; Mohammadi, M.; Gorde, K.; Jajodia, S.; Park, H.; Kim, Y. Data synthesis based on generative adversarial networks. *arXiv* **2018**, arXiv:1806.03384. [CrossRef]
94. Zheng, P.; Yuan, S.; Wu, X.; Li, J.; Lu, A. One-class adversarial nets for fraud detection. In Proceedings of the AAAI Conference on Artificial Intelligence, Honolulu, HA, USA, 29–31 January 2019; Volume 33, pp. 1286–1293.
95. Shehnepoor, S.; Togneri, R.; Liu, W.; Bennamoun, M. ScoreGAN: A Fraud Review Detector Based on Regulated GAN With Data Augmentation. *IEEE Trans. Inf. Forensics Secur.* **2021**, *17*, 280–291. [CrossRef]
96. Chawla, N.V.; Bowyer, K.W.; Hall, L.O.; Kegelmeyer, W.P. SMOTE: Synthetic minority over-sampling technique. *J. Artif. Intell. Res.* **2002**, *16*, 321–357. [CrossRef]
97. Gulrajani, I.; Ahmed, F.; Arjovsky, M.; Dumoulin, V.; Courville, A.C. Improved training of wasserstein gans. *Adv. Neural Inf. Process. Syst.* **2017**, *30*, 1–11.
98. Lei, K.; Xie, Y.; Zhong, S.; Dai, J.; Yang, M.; Shen, Y. Generative adversarial fusion network for class imbalance credit scoring. *Neural Comput. Appl.* **2020**, *32*, 8451–8462. [CrossRef]
99. Vijayaraghavan, S.; Guan, T. GAN based Data Augmentation to Resolve Class Imbalance. *arXiv* **2022**, arXiv:2206.05840.
100. Gui, J.; Sun, Z.; Wen, Y.; Tao, D.; Ye, J. A Review on Generative Adversarial Networks: Algorithms, Theory, and Applications. *IEEE Trans. Knowl. Data Eng.* **2021**, *35*, 3313–3332. [CrossRef]
101. Pandey, A.; Bhatt, D.; Bhowmik, T. Limitations and Applicability of GANs in Banking Domain. In Proceedings of the Workshop on Applied Deep Generative Networks co-located with 24th European Conference on Artificial Intelligence (ECAI 2020), Santiago de Compostela, Spain, 29 August 2020.

102. Ramponi, G.; Protopapas, P.; Brambilla, M.; Janssen, R. T-cgan: Conditional generative adversarial network for data augmentation in noisy time series with irregular sampling. *arXiv* **2018**, arXiv:1811.08295.
103. Vega-Márquez, B.; Rubio-Escudero, C.; Riquelme, J.C.; Nepomuceno-Chamorro, I. Creation of synthetic data with conditional generative adversarial networks. In Proceedings of the 14th International Conference on Soft Computing Models in Industrial and Environmental Applications (SOCO 2019), Seville, Spain, 13–15 May 2019; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; pp. 231–240.