ISSN: 0067-2904

Credit Card Fraud Detection Challenges and Solutions: A Review

Sumaya S. Sulaiman[1,3] *, Ibraheem Nadher[2], Sarab M. Hameed[3]
[1] *Computer Science Department, Collage of Science, Al-Mustansiriya University, Baghdad, Iraq*
[2] *Faculty of Basic Education, AL- Mustansiriya University, Baghdad, Iraq*
[3] *Computer Science Department, Collage of Science, University of Baghdad, Baghdad, Iraq*

Received: 26/1/2023 Accepted: 28/4/2023 Published: 30/4/2024

Abstract

Credit card fraud has become an increasing problem due to the growing reliance on electronic payment systems and technological advances that have improved fraud techniques. Numerous financial institutions are looking for the best ways to leverage technological advancements to provide better services to their end users, and researchers used various protection methods to provide security and privacy for credit cards. Therefore, it is necessary to identify the challenges and the proposed solutions to address them. This review provides an overview of the most recent research on the detection of fraudulent credit card transactions to protect those transactions from tampering or improper use, which includes imbalance classes, concept drift, and verification latency problems using machine learning and deep learning. It also provides valuable information for academic and industrial researchers and opens new avenues for research aimed at developing robust fraud detection systems.

Keywords: Credit card fraud detection, fraudster, class imbalance, concept drift, verification latency.

تحديات وحلول الكشف عن الاحتيال لبطاقات الائتمان

سميه سعد سليمان[13]*,ابراهيم نظير[2],سراب مجيد حميد[3]
[1]قسم علوم الحالسوب, كلية العلوم, الجامعة المستنصرية, بغداد, العراق
[2]كلية التربية الاساسية, الجامعة المستنصرية, بغداد, العراق
[3]قسم علوم الحاسوب, كلية العلوم, جامعة بغداد, بغداد, العراق

الخلاصة

أصبح الاحتيال على بطاقات الائتمان مشكلة متزايدة بسبب الاعتماد المتزايد على أنظمة الدفع الإلكترونية والتقدم التكنولوجي الذي أدى إلى تحسين تقنيات الاحتيال. تبحث العديد من المؤسسات المالية عن أفضل الطرق للاستفادة من التقدم التكنولوجي لتقديم خدمات أفضل لمستخدميها النهائيين ، واستخدم الباحثون أساليب حماية مختلفة لتوفير الأمان والخصوصية لبطاقات الائتمان. لذلك من الضروري تحديد التحديات والحلول المقترحة لمواجهتها. تقدم هذه المراجعة نظرة عامة على أحدث الأبحاث حول مشكلة الكشف عن معاملات

* Email: sumasaad@uomustansiriyah.edu.iq

بطاقات الائتمان الاحتيالية لحماية معاملات بطاقات الائتمان من العبث أو الاستخدام غير السليم الذي يتعامل مع مشاكل عدم التوازن في البيانات وانحراف المفهوم ومشكلات زمن الوصول للتحقق باستخدام التعلم الآلي والتعلم العميق. كما يوفر معلومات قيمة للباحثين الأكاديميين والصناعيين ويفتح آفاقًا جديدة للبحث الذي يهدف إلى تطوير أنظمة قوية للكشف عن الاحتيال.

1. Introduction

The huge advancement in technology and communication systems led to the improvement of electronic payment services, such as e-commerce and mobile payments, to facilitate online money transactions and save the customer time [1, 2]. Most of these e-services accept credit cards issued by a bank or non-banking financial institution to the cardholder to purchase goods [3, 4]. Figure 1 depicts e-commerce as a percentage of global retail sales from 2015 to 2020, with forecasts from 2021 to 2025[5].

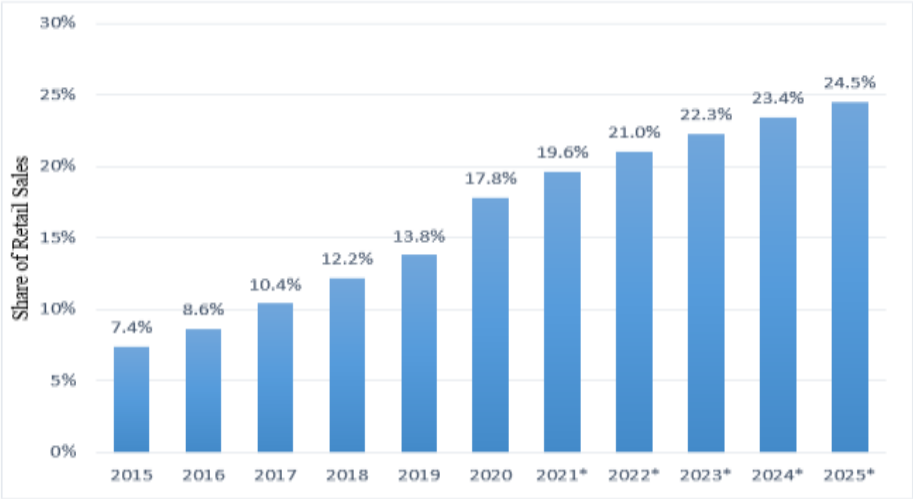

Figure 1: Worldwide retail e-commerce sales (in billion U.S. dollars) [5].

This increased reliance on credit cards leads to an increment in fraudulent transactions, as shown in Figure 2 [6, 7]. Fraudsters have been developing techniques to create fraudulent transactions that are undetectable. As stated by the European Central Bank, billions of dollars are lost each year as a result of credit card fraudulent transactions [1, 8].

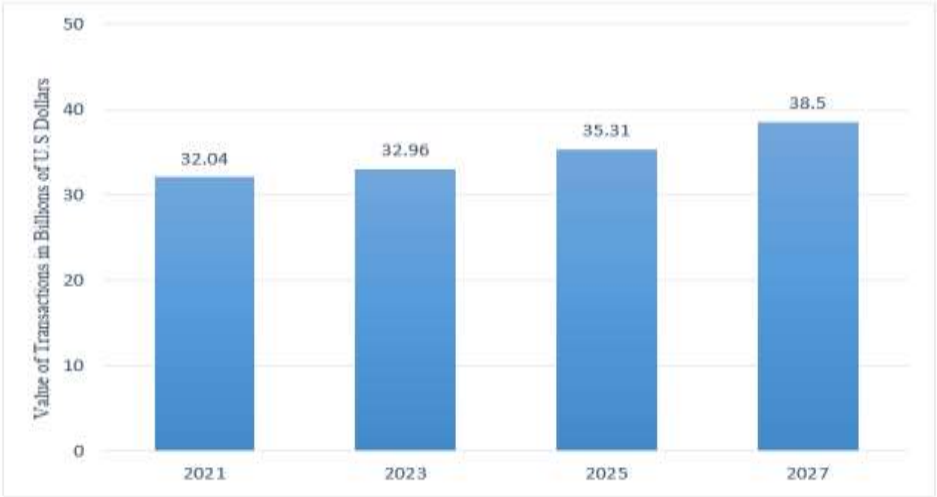

Figure 2: Worldwide fraudulent card transactions payment value from 2021 to 2027 [5].

It is vital for both users and businesses to use sustainable tools or techniques to reduce fraudulent activity and protect themselves from potential negative consequences. Many Credit Card Fraud Detection Systems (CCFDS) were proposed to detect and prevent fraud as soon as a fraudulent transaction is detected. These CCFDS face numerous challenges, including dataset class imbalance, concept drift, and verification latency [9, 10].

CCFDS needs to be improved to avoid loopholes exploited by fraudsters. To do this, it is key to determine the factors and challenges that impact the performance of CCFDS, such as imbalance classes (high number of fraud-free transactions compared to the low number of fraudulent), concept drift (card holder's spending nature changes), and verification latency (where a small transaction amount are timely tested by investigators) [11, 12, 13]. To this end, this paper presents a review of the challenges of CCFDS and how various techniques can be used to solve CCFD problems. The main contribution of the paper can be summarized as follows:

- Present a review of some of the CCFDS challenges and key research in this area, with a brief discussion of these challenges.
- Investigate the most recent advances in research in machine learning (ML) and deep learning (DL) methods for solving the CCFD problems in the literature.
- Show the datasets most used by researchers that can be more beneficial for analysis and comparison.

This paper is organized as follows: Section 2 introduces the credit card fraud detection classification. Section 3 presents the credit card fraud detection challenges and their solutions. Section 4 summarizes some of the CCFD techniques used till now. Finally, section 5 includes the paper's conclusion.

2. Credit Card Fraud Detection

Fraud Detection Systems (FDS) are critical for securing financial institutions and reducing the risk of financial loss. Avoiding credit card fraud can be achieved in two ways: prevention and detection. Prevention is intended to add an extra layer of protection to thwart fraudulent attacks and eliminate the possibility of fraud before it happens. This is primarily used for terminal authentication, such as ATMs and payment websites[12, 14]. Detection, on the other hand, occurs when prevention fails and it helps identify and alert financial institutions when fraudulent transactions are identified [12].

According to the nature of credit card fraudulent activity, Credit Card Fraud (CCF) can be classified as [9, 15]:

- Application fraud: a fraudster controls the application and steals the credentials of the cardholder to create a fake account and conduct transactions
- Counterfeit fraud / Electronic or manual card imprints: a fraudster copies card details through its magnetic strip by using skimmers. Then the credentials are used to carry out fraudulent transactions.
- Behavioural fraud / cardholder-not present fraud: when the cardholder pays online, transactions are made remotely so the details of an authentic credit card are needed. These card details can be obtained by skimming or shoulder surfing.
- Lost/stolen fraud: occurs when a card is lost by the cardholder or stolen from the cardholder. This is the simplest form of credit card fraud and is easily detected.
- Card identity theft: occurs when a fraudster steals the card details and uses them to create a fake account with the cardholder's id.
- Mail non-received card fraud: the fraudster deceives the cardholder through phishing or defrauding the credit card issuing mail.

- Account Takeover: the fraudster takes control of the account holder.
- Fake fraud in website: malicious code in a website is used to do fraudster work.
- Merchant collision: the merchant shares cardholder details without cardholder authorization.
- Internal fraud bank employees act as fraudsters and steal card details for remote use.

3. Credit Card Fraud Detection Challenges and Solutions

Fraudsters always find new loopholes no matter what CCFDS implements. Therefore, the need to continue to improve and invest in CCFDS is a challenge and is imperative for all financial institutions. Therefore, it is necessary to detect the factors and challenges that influenced the performance of CCFDS and devise strategies for improving the detection process [1].

Figure 3 depicts the distribution of papers published between 2015 and 2022 in various journals concerning challenges to CCFDS indexed by the digital database Scopus. The following subsections present how these challenges add varying levels of difficulty to CCFD.

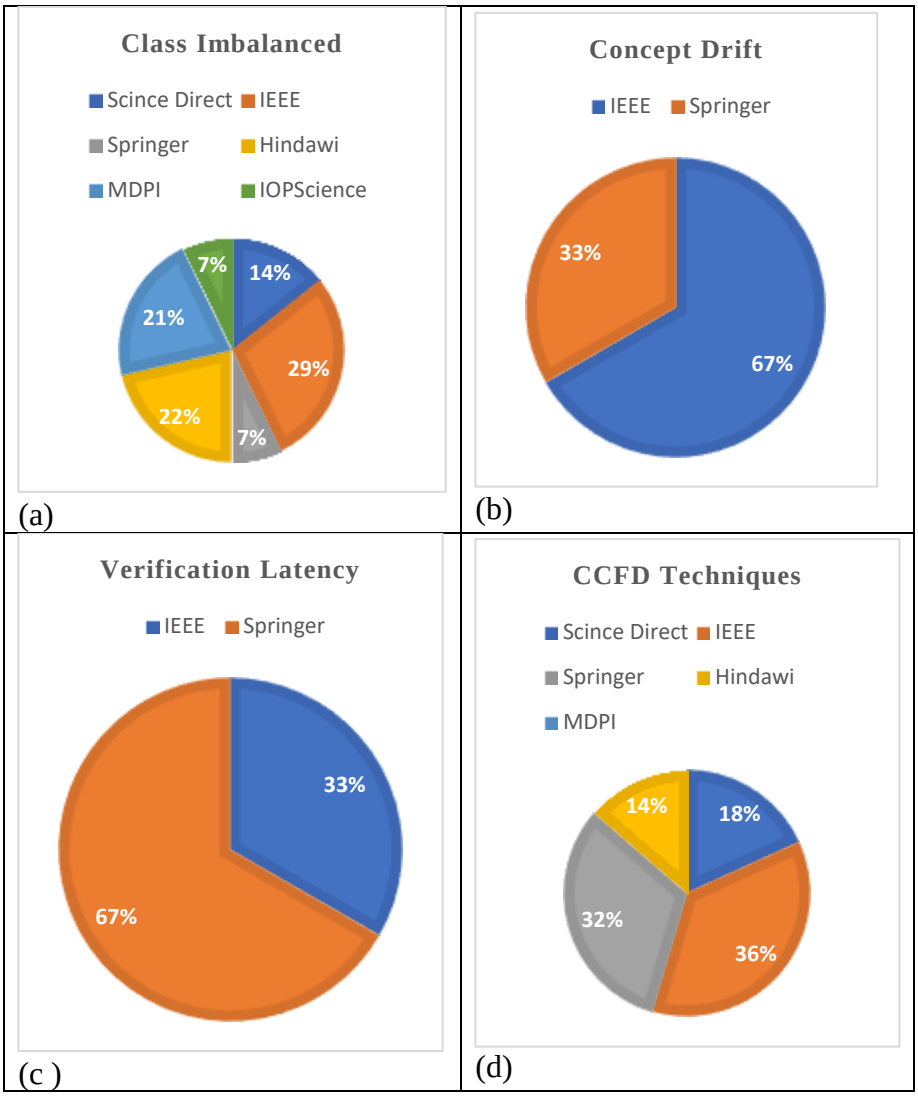

Figure 3: Distribution of the published papers in different journals according to publishers (a) Class Imbalance (b) Concept Drift (c) Verification Latency (d) CCFD techniques.

3.1 Class Imbalance challenge

One of the major challenges in CCFD that greatly affects the efficiency of classification models is the problem of imbalanced classes. The class is considered imbalanced because it is not uniformly denoted in the credit card dataset, which has a much lower number of fraudulent transactions than normal transactions [1, 16]. In real cases, 98% of transactions are legal, but 2% are fraudulent. As a result [17], many traditional classifiers are unable to detect minority class objects for these skewed datasets causing the classification solutions to be biased towards the majority class and obtain a prediction with a high misclassification rate [18, 19, 20, 21].

Many preprocessing approaches have been proposed to solve the class imbalance problem, as shown in Figure 4, including Data- Based (sampling), algorithmic-based (cost-based), or a combination of both ensemble learning techniques and cost-sensitive classification [22, 23].

The sampling approach requires the class distributions in the training set to be balanced before running the learning algorithm. Two types of sampling methods are Undersampling and Oversampling. Undersampling involves removing samples from the majority class in the training set to balance the class proportions, whereas oversampling involves replicating samples from the minority class to balance the class proportions [11, 15].

The cost-based approach modifies the learning algorithm to account for the minority class's higher misclassification cost (fraud class) [24]. Missed fraud is frequently assumed to have a cost proportional to the transaction amount, which assigns a high misclassification cost to fraud and instructs classifiers to prioritize false alerts over the risk of missing fraud. As a result, these algorithms can produce a large number of false positives [11, 25, 26]. Table 1 provides a brief description of the pre-processing techniques used most by researchers.

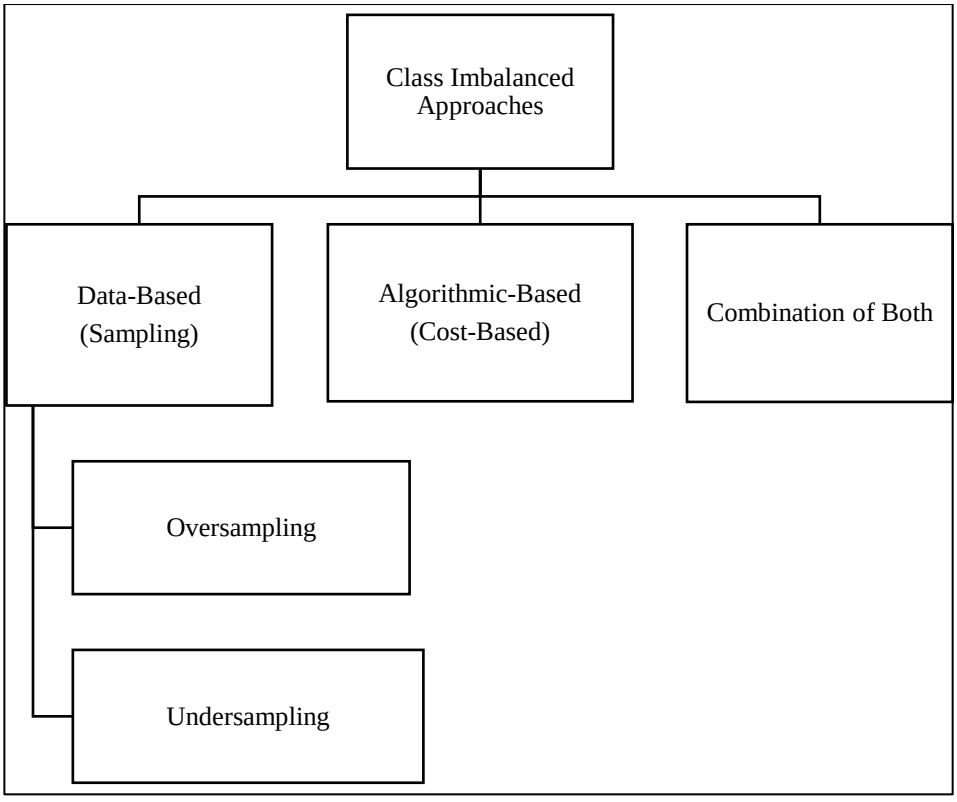

Figure 4: Imbalanced dataset pre-processing techniques.

To address the effects of class imbalance on real-world data streams, a new learning strategy was suggested in [11]. A supervised balanced bootstrap mechanism using Randomly Undersampling (RUS) was proposed to feed Random Forest (RF) in such a way that each tree in RF is trained on arbitrarily chosen transactions and identical fraud samples.
In [3] the Synthetic Minority Oversampling Technique (SMOTE) and the Matthew Coefficient Correlation (MCC) were applied to several machine learning algorithms, including Support Vector Machines (SVM), Logistic Regression (LR), RF, and Decision Trees (DT) to improve its performance. The results show that only the performance of the RF algorithm improved with an accuracy of 99.98%.

In [15] several techniques were used to avoid the drawbacks of using undersampling that handles class imbalance. The first technique employed Random Oversampling (RO) as a preprocessing step, whereas the second was a One-Class Classification technique (OCC). Since OCC is based solely on fraud observations, the results show that the OCC technique has a significant impact on the algorithm`s accuracy and sensitivity due to data overfitting. Furthermore, the results show that SVM outperforms OCC SVM in terms of accuracy, with 96% and 87%, respectively.

To compensate for the smaller number of fraudulent transactions, [21] proposed a mechanism that uses SMOTE to reduce majority occurrences while increasing minority occurrences using Condensed Nearest Neighbor (CNN) and RUS. The LR, Naïve Biased (NB), and SVM algorithms were used in this study. The acquired results in terms of accuracy for LR, NB, and SVM were 74%, 83%, and 91%, respectively.

In [22], a new approach called CtRUSBoost was used. It involved customizing the RUS algorithm and combining boosting using DT as in the standard RUSBoost algorithm with a bagging process using SVM. CtRUSBoost can be deployed at the Credit Card Interchange or Credit Card Provider Computer Controller System stage. The proposed approach produces more accurate results with large datasets, with precision reaching 95.7% when compared to RUSBoost`s 85.9%, DT's 49.5%, and SVM's 67.8%

Researcher in [20] improved detection performance in a large-scale imbalance dataset using a hybrid data-point approach that combined feature selection with a Near Miss-based undersampling technique. Near Miss was chosen because it avoids replicating sensitive financial data, which means only genuine financial records were included in the experiment. According to the results, the hybrid data-point approach enhanced the predictive accuracy of the four ML algorithms, namely SVM, RF, LR, and DT, by 73%, 90%, 90%, and 100%, respectively.

A novel approach was proposed in [13] that combines Spark with a deep learning AE approach. Spark accomplishes two tasks: it combines historical transactions to achieve design engineering, and online classifies transactions to return the estimated risk of fraud. Different parameters and ML techniques, including RF, LR, ANN, DT, and SVM, were used in a comparative analysis. An accuracy of over 96 % was achieved on both the training and test datasets.

A new framework was proposed by [1] that uses fuzzy C-means clustering to group instances based on similar features, followed by the RUS sampling technique to select and combine instances with similar features based on preferred ratios. Fuzzy c-means provide robust sampling steps for improving detection process accuracy and performance. This

reduces the RUS elimination of relevant and important data. The new framework employs four ML algorithms: KNN, LR, ANN, and NB, and the results indicate that ANN outperforms the other ML approaches with 96.6% accuracy.

On the other hand, the approach proposed by [27] combines the All K-Nearest Neighbors (AllKNN) undersampling technique with category boosting (CatBoost) to improve CCFD without compromising fraud detection as much as possible. The AllKNN-CatBoost model was compared with other algorithms, such as RF, LR, and KNN. The results indicate that the proposed model was superior to previous models with an accuracy of 99.96%.

To address the issues of potentially useful instances being removed during undersampling and overfitted during oversampling, [27-29] used a hybrid technique known as Synthetic Minority Oversampling Technique with Edited Nearest Neighbors (SMOTE-ENN). They first applied SMOTE in the oversampling phase, then used ENN as a data cleaning method to reduce overlapping instances between classes and get a better-defined class cluster. This technique experimented on several ML algorithms with different datasets and the result shows precision increasing up to 90%.

Another hybrid technique was proposed to overcome undersampling and oversampling techniques limitations coined as a SMOTE-Tomek. The class clusters may overlap with each other`s space after applying SMOTE technique. This causes the model of the classifier to overfit. Tomek links corresponding instances of the opposite class that are the nearest neighbors to each other to provide better class separation to the decision borders. The results were improved to 99% compared with 94% in RUS [27, 30].

Table 1: Description of different dataset imbalance pre-processing techniques

Reference	Preprocessing technique	Dataset	Advantage	Disadvantage.
[11]	Random undersampling	European Credit Cardholder	Provide balanced distribution to trees, find each subset of the majority class, and make training times reasonably low.	Relevant training samples may accidentally remove from the data set.
[3]	SOMTE+ MMC	European Credit Cardholder	It includes all the true and false values so it is considered as a balanced measure to be used even if there are different classes.	SOMTE alone is not enough to solve the imbalance problem.
[15]	RO, OCC	Credit Cardholder Dataset	Improvement in the classifier's performance and considerable fraud cases detection.	OCC technique alone may have unwanted costs when the imbalance is extreme, as the amount of false alarms generated is more than the number of detected frauds.
[21]	SOMTE+CNN+ RUS	Financial Institution	An API module with predictive analytics is used to alert users over the GUI when a transaction is identified as fraud.	Imposes additional cost and time to the prediction process
[22]	CtRUSBoost	European Credit Cardholder,	The proposed methodology is more reliable, authentic and	Less accurate with small datasets.

		UCI-ML, Abstract	can detect fraudster transactions more robustly.	
[20]	Near Miss-based undersampling	European Credit Cardholder, UCI-ML	Improve detection performance in large-scale imbalance data sets by providing robust and clear class distribution boundaries	Using undersampling led to ignoring most of the majority classes.
[13]	Spark+AE	European Credit Cardholder	Framework ability to do analyses in batch and stream to resolve the class imbalanced problem.	The system is not able to prevent fraud.
[1]	Fuzzy C-means + RUS	European Credit Cardholder	Decreasing the elimination of relevant and important data that occurred with the RUS method. Assure the feature instances' similarity and integrity.	Better in algorithms with an enormous amount of weights, free parameters, and biases among interconnected neurons and other variables.
[27]	AllKNN-CatBoost	European Credit Cardholder	Increasing recall value by decreasing the number of fraudulent transactions that classifies as valid transactions.	the work is inadequate in allowing for only one dataset
[27-29]	SMOTE-ENN	European Credit Cardholder, German, Taiwan	Overall performance efficiency is improved by reducing the error rate using a hybrid method.	Limited dealing with noise and missing values.
[27, 30]	SMOTE-Tomek	European Credit Cardholder	increase class separation around the decision borders	The classifier model may overfit.

3.2 Concept Drift

Customer spending patterns and fraudster patterns change with time as the market and technology evolve. These changes are referred to as concept drift. So, fraudsters and card investigators need to adapt to these pattern changes [15, 31]. To successfully handle concept drift problems, a CCFD model must be updated regularly. An irregular update of the FD model may be caused by a poorly handled concept drift problem that leads to poor-quality fraud detection [32].

Depending on the action, CCFDS can be categorized into an Expert-Driven Model (EDM) and a Data-Driven Model (DDM). In the first category, EDM employs rules written by domain experts and investigators to predict the true state of a transaction, with investigators frequently updating the EDM by adding transaction blocks or scoring rules to thwart the start of new fraudulent activities, and eliminating rules that generate too many false alarms. On the other hand, DDM is the development of models based on ML and DL techniques for detecting fraudulent patterns in data [14]. The DDM cannot be modified by investigators because it is uninterpretable and can only be modified using recent supervised information. This update needs a large amount of labeled transactions but the investigators can only provide a small set

of supervised instances through alerts; while the vast label of transactions can be available only a few days later, when cardholders may report unauthorized transactions [11, 33]. This review paper will focus primarily on DDM, and Table 2 shows a description of the ML methods used.

To handle the concept drift problem, [33] proposed two FDS based on an ensemble and a sliding-window approach. The results are then combined. The experiment used a real-world transaction stream to demonstrate how alert-feedback interaction provides more precise alerts and adapts more smoothly in concept-drifting environments.

To increase the alert precision of the previous study, a large importance was assigned to feedback (investigator alerts). However, [11] suggested a sliding window active approach providing delayed supervised instances gradually to train and update the RF classifier by training each classifier on instances of a different day and then ensemble their result. Each RF adopted has 100 trees and each tree is trained on a balanced bootstrap sample.
To respond in real-time, an Auto-Encoder (AE) and Restricted Boltzmann Machine (RBM) were proposed in [34] to find anomalies from the reconstructed normal patterns by applying backpropagation. The results show the Area Under Curve (AUC) for AE and RBM were 96.03 and 95.05 respectively.

Sequential modeling of data proposed in [18] combines the power of three sub-methods; the Uniform Manifold Approximation and Projection (UMAP) for selecting the most suitable predictive features, the Long Short Term Memory (LSTM) networks for incorporating transaction sequences, and the Attention Mechanism (AM) to enhance LSTM performance. The model is composed of 6 layers: an attention layer then two LSTM network layers that take the output of the attention layer as the input with the activation function assumed to be tanh. A dense layer is added at the end of the two LSTM layers to obtain the prediction classes (genuine and fraud transactions). Finally, the Batch Normalization layer is applied after the dense layer.

In addition, a multi-classifier system was designed in [35] by combining a hierarchical agent-based framework with the Behavior-Knowledge Space (BKS) as a decision-making method to classify CC transactions into normal or fraudulent. The hierarchical agent-based framework involves three agents RF, Generalized Linear Model (GLM), and Gradient Boosting Machine (GBM). This combination allows the accumulation of knowledge and yields robust and more effective accuracy of over 99%.

Table 2: Description of different concept drift techniques

Reference	Method	Dataset	advantage	disadvantage	Performance (%)
[36]	RUS+ RF	European Credit Cardholder	Separately handle late feedback to reduce the delay effect, increase FD precision	Delay in obtaining accurate label transaction	-
[11]	RF + bootstrap	European Credit Cardholder	Guarantee larger relevance to the trained supervised samples, and alert only about those transactions that are considered most probably frauds	Unidealistically assuming that investigators can determine the correct label for each transaction every day.	-

[34]	AE	European Credit Cardholder, German, Australian	Can accurately succeed in fraud detection with a massive dataset with no previous history, find fraudulent patterns, and respond in real-time to the system as a fraud or legitimate transaction.	It is more difficult to choose the appropriate techniques to detect anomalous behavior.	AUC= 96.03
	RBM				AUC= 95.05
[18]	LSTM+ AM	European Credit Cardholder,	The model can extract valuable patterns within cardholder behavior to differentiate legitimate from fraudulent transactions. The model shows good results in terms of efficiency and effectiveness.	-	Accuracy = 96.72
		BankSim			Accuracy = 97.48
[35]	BKS	Southeast Asia financial firm	The proposed BKS-based framework is efficient in identifying fraudulent transactions.	If there are many classifiers then the empty cells in BKS table may lead to no prediction. In addition, noise in class labels, causes incorrect information in the BKS cells, leading to false predictions.	Accuracy = 99%

3.3 Verification Latency

The third challenge is verification latency, which occurs when investigators can't examine all transactions in a real-world FDS.

Many transactions are treated as legitimate because they cannot be verified until a cardholder reports them as fraudulent, or a reasonable period has passed with no dispute. Therefore, most of the supervised samples used to update the classifier are significantly delayed by the interaction of alarm feedback. Many papers in the literature omit verification latency and the alert-feedback interaction, and they assume that the FDS receives a label for each transaction daily. When concept drift occurs, validation latency can be a serious issue, and the interaction of alarms and feedback can affect Sample Selection Bias (SSB) when classifiers are trained or updated [11, 37].

Class-prior bias, feature bias (also known as covariate shift), and complete bias are the three types of SSB. A basic way to deal with SSB is to assign higher weights to the training samples that are more like the data distribution in the test set to reduce the influence of the biased samples in the learning process, this technique is named importance weighting or semi-supervised reweighting. However, its efficiency decreases when there are many overlaps.
For the interaction of alarms and feedback, importance weighting may be ineffective as it reduces the impact of fraudulent transactions on feedback and reduces accuracy. Table 3 displays a description of different verification latency techniques.

In [11], the authors proposed a method for dealing with the feature bias problem by training a classifier exclusively on feedback using a weight-sensitive implementation of the RFs based on conditional inference trees while another classifier is trained on delayed

supervised transactions. The probabilities are then aggregated to determine which transactions to alert.

In [19], a very promising research direction was undertaken to improve the labeling process in FDS by combining traditional active learning strategies, such as High-Risk Querying (HRQ), with ML techniques such as Stochastic Semi-Supervised Labeling (SSSL). The idea is to compute the average weight of two classifiers, the delayed classifier, and the feedback classifier using a logarithmic function to obtain scores. The result shows the increment in fraudulent labels in the dataset from 0.13% to 23.33% for scores higher than 0.95 and 61.90% for scores past 0.99.

In [38], a diversity-based ensemble learning method was proposed. The method preserves and reuses previous concepts for faster adaptation to changes. Balanced Random Forest of ten trees, with each tree training on a different balanced dataset subsample. The framework starts with a single model and no updates are applied before generating a single model every day using a moving set of batches and a sliding time window. The most recent seven sliding window models are saved in an ensemble, and their average is used for prediction. Following that, one member is randomly removed at each iteration to add the new model to the ensemble model by maximizing a diversity measure computed on unseen data.

Table 3: Comparison of different verification latency techniques.

Reference	Algorithm (approaches)	Dataset	advantage	disadvantage
[19]	HQR+ (SR-SU)	credit card transactions provided by industrial partner Worldline	New instances are Discovered from the minority class to improve the training dataset balance and positively affect the accuracy.	The selection step in the querying strategy depends on the classifier accuracy which may be incorrect and affect the detection accuracy.
[11]	RF+ bagging	European Credit Cardholder	Proposes a novel learning strategy that effectively analyzes a large number of transactions processed every day and gets precise alerts by assigning larger importance to feedback during the learning process.	Processing labeled transactions individually adds a layer of complication to the CCFD problem.
[38]	diversity-based ensemble balanced RF classifier	credit card transactions provided by industrial partner Worldline	Ensemble-based models overcome single models because they support the value of historical knowledge and decrease focus on recent data.	Performing several models increases memory and computation costs. Also, if the selection criteria of which model to store are based on recentness, it might lead to unnecessary redundancy.

4. Credit Card Fraud Detection Techniques

Many techniques based on ML and DL can be used to enforce CCFD [61]. Table 4 provides a summary of the DL and ML approaches used in the CCFD domain. The datasets used in the literature are obtained from three repositories. Kaggle [39-43], UCI machine learning repository [44, 45], Credit Card Datasets, Github [45], and Credit Card Dataset. Most

ML techniques are supervised such that training is made on a labeled dataset [62, 63]. LR and DT show the best performance among ML techniques due to their ability to build a more robust anomaly detector that finds anomalies directly without profiling all the regular transactions. Preprocessing techniques, such as ROS, RU, and hybrid sampling were used to improve the results. However, to manage the high daily volume of transactions, DL techniques such as AE, CNN, and LSTM were used to improve production efficiencies and reduce false alarms [64, 65].

Table 4: A comparative analysis of CCFD applications.

Reference	Dataset	Techniques	Performance (%)	Purpose
[46]	German Credit Card Dataset	LR	-	Increase effectiveness
[47]	Real-world Credit Card Dataset	CNN	-	Identify sophisticated fraud patterns
[11]	European Credit Card Dataset	RF	-	Decrease the effect of feedback in the learning process
[48]	European Credit Card Dataset	RUS + RO	Accuracy= 97.9	Determine the best attribute efficiently
[7]	European Credit Card Dataset	Majority Voting+ Adaboost	MCC= 0.95	The best result is obtained using the MCC metric
[34]	German, Australian, and European Credit Card Datasets	AE +RBM	AUC based on AE= 0.9603 AUC based on RBM= 0.9505	Recreate genuine transactions to fraudulent from these patterns
[49]	PagSeguro Transactions Dataset	Bayesian network classifier (BNC)		Accuracy and efficiency increment
[3]	European Credit Card Dataset	SMOTE + ML	Accuracy=99.9	Solve the problem of concept drift and predict fraud transaction
[15]	Credit Card Fraud Labeled Data	RO + SVM	Accuracy=95	Resolve the data imbalance problem.
[50]	European Credit Card Dataset	Condensed Nearest Neighbor (CNN)	-	Reduce the number of features to enhance the processing time
[51]	European Credit Card Dataset	SMOTE	Accuracy=99.96	Determine the best features to reduce class overfitting
[52]	German Credit Card Dataset	NB	Accuracy=90.61	Model performance is improved
[53]	German Credit Card Dataset	Filter RF	Accuracy=76.4	Enhancing accuracy with less classification time.
[31]	IEEE- CIS Credit Card Dataset	RO +BilLSTM-MaxPooling -BiGRU	AUC= 91.37	DL results overcome ML.
[22]	Abstract, Default, European Credit Card Dataset	CtRUSBoost	Precision= 0.957 F1 score= 0.976	Robust results in detecting fraudster transactions.
[54]	European Credit Card Dataset	Light gradient Boosting (LGB)	Accuracy=98.4	Reduce training time.
[55]	European Credit Card Dataset	SVM-recursive feature elimination and hyper-parameters optimization	Accuracy=99	Eliminate class imbalance
[56]	European Credit Card Dataset	RO + LR	Accuracy=95.9	Enhancing accuracy by reducing the classification time.
[57]	NetGuardians SA	ARIMA model		

	Credit Card Dataset		-	
[18]	European, BankSim Credit Card Datasets	LSTM- Attention Mechanism	Accuracy=96.7	Improve the prediction efficiency during the identification of fraudulent transaction
[58]	German, Australian Credit Card Datasets	SA- ANN	Accuracy=85.71	Verify an improvement in the result.
		HTM-CLA	Accuracy=80	
		LSTM-ANN	Accuracy=80	
[20]	European, UCI Credit Card Datasets	Near Miss	Accuracy=90	Enhancement in the ability to forecast normal classes
[9]	European Credit Card Dataset	RUS +ANN	Accuracy=99.9	Increases fraud prediction rate.
[13]	European Credit Card Dataset	Deep AE	Accuracy=96.5	Resolve the class imbalanced problem
[59]	European Credit Card Dataset	Enhanced Stacking Classifiers System (ESCS)	Accuracy=98.37	Credit card fraud detection can be improved by applying an additional level to the stacking classifier.
[60]	European Credit Card Datasets	Ensemble stacking	Accuracy=93.4	Expose frauds efficiently with high performance
[28]	European Credit Card Dataset	SMOTE-ENN and LSTM	Accuracy=99	-

5. Conclusion

The use of electronic payment in digital commerce is becoming increasingly problematic. Various financial institutions are looking for the best ways to leverage technological advancements in order to provide better services to their end users. However, the widespread use of credit cards has led to the introduction of various forms of fraud, in which fraudsters use technological advancements and FDS gaps to conduct illegal transactions, resulting in significant losses. Understanding the challenges faced by the CCFD and the key solutions used to address these challenges is key to reduce the threat posed by fraudsters and improve cardholder performance.

There are many CCFD issues that can be addressed, such as changes in cardholder behavior, imbalanced datasets where fraudulent transactions make up a small portion of the dataset, and the inability to provide alert feedback to update the CCFDS in a short period of time. This review introduced and analyzed the state-of-the-art solutions to these challenges and their impact on the CCFD problem. According to the findings of the review, extensive studies are addressing the challenges of an imbalanced class. These studies used hybrid preprocessing techniques, such as combining features of RO or RUS with ML and DL algorithms, to get better results and deeply search for the best relevant features to minimize the class imbalanced effect on the CCFD problem. Also, several works of literature proposed methods to solve the problem of concept drift, but only few addressed the problem of validation latency, which supports the value of historical knowledge over recent data during the learning process. Furthermore, credit cardholder changing behavior influence can be reduced through the use of DL approaches due to their ability to extract valuable patterns from large amounts of transactions.

6. Acknowledgment

The authors would like to thank Al-Mustansiriyah University in Bagdad, Iraq, for their cooperation with this study (http://uomustansiriyah.edu.iq).

7. Disclosure and conflict of interest

Conflict of Interest: The authors declare that they have no conflicts of interest.

References

[1] H. Ahmad, B. Kasasbeh, B. Aldabaybah, and E. Rawashdeh, "Class balancing framework for credit card fraud detection based on clustering and similarity-based selection (SBS)," *International Journal of Information Technology, Springe*r, vol. 15, pp. 325–333, 2022.

[2] A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, "Credit card fraud detection in the era of disruptive technologies: A systematic review," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 1, pp.145-174, 2022.

[3] V. N. Dornadula and S. Geetha, "Credit card fraud detection using machine learning algorithms," *Procedia computer science*, vol. 165, pp. 631-641, 2019.

[4] N. Sivakumar and R. Balasubramanian, "Fraud detection in credit card transactions: classification, risks, and prevention techniques," *International Journal of Computer Science and Information Technologies*, vol. 6, no. 2, pp. 1379-1386, 2015.

[5] Statista. https://www.statista.com/ (accessed 2022).

[6] T. A. Olowookere and O. S. Adewale, "A framework for detecting credit card fraud with cost-sensitive meta-learning ensemble approach," Scientific African, vol. 8, p. e00464, 2020.

[7] 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, doi: 10.1109/ACCESS.2018.2806420.

[8] H. Wang, P. Zhu, X. Zou, and S. Qin, "An ensemble learning framework for credit card fraud detection based on training set partitioning and clustering," in IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Guangzhou, China, 2018, pp. 94-98, doi: 10.1109/SmartWorld.2018.00051.

[9] R. Asha and S. K. KR, "Credit card fraud detection using artificial neural network," Global Transitions Proceedings, vol. 2, no. 1, pp. 35-41, 2021.

[10] R. Van Belle, B. Baesens, and J. De Weerdt, "CATCHM: A novel network-based credit card fraud detection method using node representation learning," Decision Support Systems, vol. 164, pp. 113866, 2023.

[11] 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.

[12] R. M. Dantas, R. Firdaus, F. Jaleel, P. Neves Mata, M. N. Mata, and G. Li, "Systemic Acquired Critique of Credit Card Deception Exposure through Machine Learning," Journal of Open Innovation: Technology, Market, and Complexity, vol. 8, no. 4, pp. 192, 2022.

[13] S. Sanober, I. Alam, S. Pande, F. Arslan, K. P. Rane, B. K. Singh, A. Khamparia, and M. Shabaz, "An enhanced secure deep learning algorithm for fraud detection in wireless communication," Wireless Communications and Mobile Computing, vol. 2021, pp. 1-14, 2021.

[14] S. Rajora, D. Li, C. Jha, N. Bharill, O. P. Patel, S. Joshi, D. Puthal, M. Prasad, "A comparative study of machine learning techniques for credit card fraud detection based on time variance," in 2018 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 1958-1963, 2018.

[15] 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.

[16] N. Boutaher, A. Elomri, N. Abghour, K. Moussaid, and M. Rida, "A Review of Credit Card Fraud Detection Using Machine Learning Techniques," in 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech), pp. 1-5, 24-26 Nov. 2020, doi: 10.1109/CloudTech49835.2020.9365916.

[17] P. Juszczak, N. M. Adams, D. J. Hand, C. Whitrow, and D. J. Weston, "Off-the-peg and bespoke classifiers for fraud detection," Computational Statistics & Data Analysis, vol. 52, no. 9, pp. 4521-4532, 2008.

[18] I. Benchaji, S. Douzi, B. E. Ouahidi, and J. Jaafari, "Enhanced credit card fraud detection based on attention mechanism and LSTM deep model," Journal of Big Data, vol. 8, pp. 1-21, 2021.

[19] F. Carcillo, Y.-A. L. Borgne, O. Caelen, and G. Bontempi, "Streaming active learning strategies for real-life credit card fraud detection: assessment and visualization," International Journal of Data Science and Analytics, vol. 5, pp. 285-300, 2018.

[20] N. M. Mqadi, N. Naicker, and T. Adeliyi, "Solving misclassification of the credit card imbalance problem using near miss," Mathematical Problems in Engineering, vol. 2021, 2021.

[21] A. Thennakoon, C. Bhagyani, S. Premadasa, S. Mihiranga, and N. Kuruwitaarachchi, "Real-time credit card fraud detection using machine learning," in 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), IEEE, pp. 488-493, 2019.

[22] V. Arora, R. S. Leekha, K. Lee, and A. Kataria, "Facilitating user authorization from imbalanced data logs of credit cards using artificial intelligence," Mobile Information Systems, vol. 2020, pp. 1-13, 2020.

[23] B. Pes, "Learning From High-Dimensional Biomedical Datasets: The Issue of Class Imbalance," IEEE Access, vol. 8, pp. 13527-13540, 2020, doi: 10.1109/ACCESS.2020.2966296.

[24] C. Elkan, "The foundations of cost-sensitive learning," in International joint conference on artificial intelligence: Lawrence Erlbaum Associates Ltd vol. 17, no. 1, pp. 973-978, 2001.

[25] A. C. Bahnsen, D. Aouada, and B. E. Ottersten, "Example-dependent cost-sensitive decision trees," Expert Syst. Appl., vol. 42, pp. 6609-6619, 2015.

[26] N. Mahmoudi and E. Duman, "Detecting credit card fraud by modified Fisher discriminant analysis," Expert Systems with Applications, vol. 42, no. 5, pp. 2510-2516, 2015.

[27] N. S. Alfaiz and S. M. Fati, "Enhanced Credit Card Fraud Detection Model Using Machine Learning," Electronics, vol. 11, no. 4, pp. 662, 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/4/662.

[28] 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.

[29] E. F. Malik, K. W. Khaw, B. Belaton, W. P. Wong, and X. Chew, "Credit Card Fraud Detection Using a New Hybrid Machine Learning Architecture," Mathematics, vol. 10, no. 9, pp. 1480, 2022.

[30] K. Praveen Mahesh, S. Ashar Afrouz, and A. Shaju Areeckal, "Detection of fraudulent credit card transactions: A comparative analysis of data sampling and classification techniques," Journal of Physics: Conference Series, vol. 2161, no. 1, pp. 012072, 2022.

[31] H. Najadat, O. Altiti, A. A. Aqouleh, and M. Younes, "Credit card fraud detection based on machine and deep learning," in 2020 11th International Conference on Information and Communication Systems (ICICS), IEEE, pp. 204-208, 2020.

[32] I. Mekterović, M. Karan, D. Pintar, and L. Brkić, "Credit card fraud detection in card-not-present transactions: Where to invest?," Applied Sciences, vol. 11, no. 15, pp. 6766, 2021.

[33] A. D. Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit card fraud detection and concept-drift adaptation with delayed supervised information," in 2015 International Joint Conference on Neural Networks (IJCNN), pp. 1-8, 12-17 July 2015 doi: 10.1109/IJCNN.2015.7280527.

[34] A. Pumsirirat and Y. Liu, "Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine," International Journal of advanced computer science and applications, vol. 9, no. 1, 2018.

[35] A. K. Nandi, K. K. Randhawa, H. S. Chua, M. Seera, and C. P. Lim, "Credit card fraud detection using a hierarchical behavior-knowledge space model," Plos one, vol. 17, no. 1, p. e0260579, 2022.

[36] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit card fraud detection and concept-drift adaptation with delayed supervised information," in 2015 international joint conference on Neural networks (IJCNN), 2015: IEEE, pp. 1-8, 2015.

[37] A. Dal Pozzolo, R. Johnson, O. Caelen, S. Waterschoot, N. V. Chawla, and G. Bontempi, "Using HDDT to avoid instances propagation in unbalanced and evolving data streams," in 2014 International Joint Conference on Neural Networks (IJCNN), IEEE, pp. 588-594, 2014.
[38] G. M. Paldino et al., "The role of diversity and ensemble learning in credit card fraud detection," Advances in Data Analysis and Classification, pp. 1-25, 2022.
[39] "Credit Card Dataset." https://www.kaggle.com/datasets/shubhamjoshi2130of/abstract-data-set-for-credit-card-fraud-detection (accessed 2022).
[40] BankSim. "Credit Card Dataset." https://www.kaggle.com/datasets/ealaxi/banksim1 (accessed 2022).
[41] I. CIS. "Credit Card Dataset." https://www.kaggle.com/c/ieee-fraud-detection (accessed 2022).
[42] Default. "Credit Card Dataset." https://www.kaggle.com/datasets/uciml/default-of-credit-card-clients-dataset (accessed 2022).
[43] European. "Credit Card Dataset." https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud (accessed 2022).
[44] Australian. "Credit Card Dataset." https://archive.ics.uci.edu/ml/datasets/statlog+(australian+credit+approval) (accessed 2022).
[45] German. "Credit Card Dataset." https://archive.ics.uci.edu/ml/datasets/statlog+(german+credit+data) (accessed 2022).
[46] P. Kulkarni and R. Ade, "Logistic regression learning model for handling concept drift with unbalanced data in credit card fraud detection system," in Proceedings of the Second International Conference on Computer and Communication Technologies, Springer, pp. 681-689, 2016.
[47] K. Fu, D. Cheng, Y. Tu, and L. Zhang, "Credit card fraud detection using convolutional neural networks," in International conference on neural information processing, Springer, pp. 483-490, 2016.
[48] J. O. Awoyemi, A. O. Adetunmbi, and S. A. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis," in 2017 international conference on computing networking and informatics (ICCNI), IEEE, pp. 1-9, 2017.
[49] A. G. de Sá, A. C. Pereira, and G. L. Pappa, "A customized classification algorithm for credit card fraud detection," Engineering Applications of Artificial Intelligence, vol. 72, pp. 21-29, 2018.
[50] P. R. Vardhani, Y. I. Priyadarshini, and Y. Narasimhulu, "CNN data mining algorithm for detecting credit card fraud," in Soft Computing and Medical Bioinformatics: Springer, pp. 85-93, 2019.
[51] D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, "Credit card fraud detection-machine learning methods," in 18th International Symposium INFOTEH-JAHORINA (INFOTEH), IEEE, pp. 1-5, 2019.
[52] P. Kumari and S. P. Mishra, "Analysis of credit card fraud detection using fusion classifiers," in Computational Intelligence in Data Mining: Springer, pp. 111-122, 2019.
[53] A. Singh and A. Jain, "Adaptive credit card fraud detection techniques based on feature selection method," in Advances in computer communication and computational sciences: Springer, 2019, pp. 167-178.
[54] 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.
[55] N. Rtayli and N. Enneya, "Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization," Journal of Information Security and Applications, vol. 55, pp. 102596, 2020.
[56] F. Itoo and S. Singh, "Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection," International Journal of Information Technology, vol. 13, no. 4, pp. 1503-1511, 2021.
[57] G. Moschini, R. Houssou, J. Bovay, and S. Robert-Nicoud, "Anomaly and fraud detection in credit card transactions using the arima model," Engineering Proceedings, vol. 5, no. 1, p. 56, 2021.
[58] 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, pp. 100080, 2021.

[59] N. A. Ishak, K.-H. Ng, G.-K. Tong, S. N. Kalid, and K.-C. Khor, "Mitigating unbalanced and overlapped classes in credit card fraud data with enhanced stacking classifiers system," F1000Research, vol. 11, no. 71, pp. 71, 2022.

[60] R. Soleymanzadeh, M. Aljasim, M. W. Qadeer, and R. Kashef, "Cyberattack and Fraud Detection Using Ensemble Stacking," AI, vol. 3, no. 1, pp. 22-36, 2022.

[61] S. J. Muhamed, "Detection and Prevention WEB-Service for Fraudulent E-Transaction using APRIORI and SVM," Al-Mustansiriyah J. Sci., vol. 33, no. 4, pp. 72–79, Dec. 2022, doi: 10.23851/mjs.v33i4.1242.

[62] D. I. . Mahmood and S. M. . Hameed, "A Multi-Objective Evolutionary Algorithm based Feature Selection for Intrusion Detection", Iraqi Journal of Science, vol. 58, no. 1C, pp. 536–549, Jan. 2022.

[63] M. Haqi Al-Tai, B. M. Nema, and A. Al-Sherbaz, "Deep Learning for Fake News Detection: Literature Review," Al-Mustansiriyah J. Sci., vol. 34, no. 2, pp. 70–81, Jun. 2023, doi: 10.23851/mjs.v34i2.1292.

[64] S. Salman and J. H. Soud, "Deep Learning Machine using Hierarchical Cluster Features," Al-Mustansiriyah J. Sci., vol. 29, no. 3, pp. 82–93, Mar. 2019, doi: 10.23851/mjs.v29i3.625.

[65] N. H. Ali, M. E. Abdulmunem and A. E. Ali, "Learning Evolution: a Survey," Iraqi Journal of Science, vol. 62, no. 12, pp. 4978-4987 , 2021.