applied sciences

MDPI

Review

A Systematic Review of Intelligent Systems and Analytic Applications in Credit Card Fraud Detection

Ercan Oztemel [1] and Muhammed Isik [2,*]

[1] Department of Industrial Engineering, Faculty of Engineering, Marmara University, Istanbul 34854, Turkey; eoztemel@marmara.edu.tr
[2] Department of Industrial Engineering, Institute of Pure and Applied Sciences, Marmara University, Istanbul 34722, Turkey
* Correspondence: muhammedisik@marun.edu.tr

Abstract: The use of credit cards plays a crucial role in cash management and in meeting the needs for individual and commercial customers due to the spread of risks to the future by making monthly instalments instead of cash transactions. The use of credit cards therefore provides benefits not only to the customers but also to the banks as it enables and sustains a long-term relationship in between them. Despite the increase in the use of credit cards, there is also a significant increase in fraud transactions. To detect and prevent possible fraud operations, banks generally use rule-based techniques or analytical models. In this respect, analytical models have an important place due to their effectiveness, performance, and fast response. The main aim of this paper is therefore to enhance the theoretical and practical understanding of credit card fraud operations, review basic approaches, and propose a more comprehensive approach utilizing the agents. Note that in this study, static analytic modelling (existing approaches) and dynamic analytic modelling (emerging approaches) techniques are compared in terms of methodology, performance, and respective approaches. Since fraud methods and transactions are constantly changing over time, it is thought that there will be an increase in the use of agent-based models with dynamic analytical capabilities. Additionally, in this paper, a proposed model and empiric study are presented for an agent-based intelligent credit card fraud detection system.

Keywords: credit card fraud detection; imbalanced learning; feature selection; equation-based modelling; agent-based modelling

check for updates

Academic Editor: André Sales Mendes

Received: 23 November 2024
Revised: 23 January 2025
Accepted: 24 January 2025
Published: 28 January 2025

Citation: Oztemel, E.; Isik, M. A Systematic Review of Intelligent Systems and Analytic Applications in Credit Card Fraud Detection. *Appl. Sci.* **2025**, *15*, 1356. https://doi.org/10.3390/app15031356

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With technological progress and the digital transformation of business in the financial world, the use of credit cards is significantly increasing. Due to their fast operation and ease of use, credit cards are frequently preferred by customers as a means of payment [1]. Although huge amounts of card transaction data are collected and kept in the databases of the banks, not much attention is given to automatically interpreting these data. It is important to organize, manage, and apply a suitable pre-processing process and generate analysis methodologies for the sake of better interpretation. By applying appropriate analytical methods, it is possible to discover specific data patterns and provide this information to respective units or systems for the sake of risk management, marketing, and credit allocation. It is now obvious that the banks may frequently face some risks, especially depending on card utilization [2]. Illegal actions, such as fraud, can create severe financial problems and destroy the reputation of financial enterprises. Note that some fraud models have already been developed in order to detect and prevent undesired situations [3]. It

is proven that it is possible to prevent cash and reputational losses caused by fraudulent transactions. However, there are some issues such as balancing the data set, identifying the qualified features, etc., that still need to be sorted. A review of the literature as well as an explanation of the general training process is provided below.

Note that when dealing with fraud transactions using credit cards, the data sets generated are mainly imbalanced due to target variability [4]. This necessitates some pre-processing methods such as resampling to be employed before use and then imbalanced learning (IL) and training methods should be employed to balance the data. The qualified features of data sets are also presented as input to the classification algorithms forming the basis of supervised learning (SL) in order to identify the data patterns.

The literature provides several models used in training as well as a comparison with respect to performance metrics such as accuracy, recall, precision, f1-score, lift curve, etc. [5]. This comparison naturally highlights the so-called "champion model" in respective training performance as it can be used to identify whether the transactions are fraudulent or not. Similarly, some hybrid versions have been created by combining both oversampling and undersampling techniques in order to regulate the imbalanced data set [6]. With hybrid approaches such as oversampling followed by undersampling, the raw data set is converted in order to resample and use in generating the training model.

The reason for using the hybrid approach is that the oversampling followed by undersampling approaches contribute to the model development process by removing noise on the raw data set [7]. In addition, overfitting problems resulting from oversampling and loss of information through undersampling can be solved with hybrid models. Note that these approaches are mainly used in several anomaly detection studies, including fraudulent transactions.

The literature indicates some SL algorithms that are used to identify fraud transactions. Generally, equation-based modelling (EBM) is applied for this purpose. The dynamic nature of the data creates difficulty in learning that takes the attention of the research community to implement agent-based modelling (ABM), as stated in [8]. Due to the nature of intelligent agents, it is now obvious that the alerts and interactions of autonomous agents can provide the required flexibility and dynamism in credit card data processing [9]. It is also well known that the agents can respond to the changes in the data and generate/recommend immediate actions. This may well increase the performance of the fraud detection systems. In this paper, that is the main reason for proposing an ABM-based detection system instead of pure SL algorithms.

The main aim of this paper is therefore to enhance the theoretical and practical understanding of credit card fraud operations, review the basic approaches, and propose a more comprehensive approach utilizing the agents. In this paper, methods and applications from traditional approaches to contemporary approaches are discussed. In the first part of this paper, theoretical information about anomaly detection and financial fraud detection is given. In the following part, information about the modelling processes and techniques with existing applications is provided. Additionally, in this paper, the attention of the reader is drawn to the benefits of the ABM techniques as emerging approaches to credit card fraud modelling where fraud methods and behaviors are constantly changing. It is believed that the learning agents can quickly create fraudster patterns based on card transactions. In the last part of this paper, the new proposed agent-based model is detailed with a conceptual analysis beyond existing approaches and fraud prevention processes are also discussed. It is emphasized that fraud prevention efforts cannot be separated from fraud detection efforts and that these two processes constitute card fraud management with the contributions of the systematic data governance process and learning. In this section of the paper, we attempt to provide information about the research questions. Our

first research question is whether new approaches can be designed instead of existing approaches in the fraud detection model. In this process, the usability of the learning agent technology in card fraud detection was tested by moving away from classical approaches. In addition, in this study, whether the results obtained from the fraud detection model can be used in prevention processes and action plans will be examined. The usability of the new card action plan and its consistency on the basis of fraud flags will also be examined.

2. Theoretical Background

In the theoretical parts of this paper, the topic of anomaly detection is examined, and the studies on financial fraud detection are discussed. Note that the topic of credit card fraud detection (CCFD) is also exhaustively studied as part of the financial fraud detection in this section.

2.1. Anomaly Detection

Anomaly is a general term which is defined as recordings or transactions that differ from the common behavior of the data transactions. Identifying the abnormal behavior of the data is called anomaly detection. As mentioned in [10], anomaly detection is widely used in many areas such as credit card fraud, insurance fraud, application fraud, and intrusion detection. In these studies, there may be contextual anomaly behaviors as well as collective anomaly behaviors on the data sets [11]. The literature provides some studies employing analytical techniques such as machine learning and deep learning for analyzing anomalous and respective data patterns [12].

2.2. Financial Fraud Detection

Financial fraud is a serious anomaly situation that is rapidly increasing around the world. It seems that the financial fraud cases are being increased by the increase in the number of financial transactions and the change in fraudster methods [13]. It is therefore very important to detect financial fraud and prevent fraudster cases in the financial system before severe loss of cash and trust. In financial fraud studies, individual and commercial information is taken into account [14]. Customer information such as account and previous payment information is used for individual segments. On the other hand, balance sheets, income statements, activity reports, cheques, and promissory notes are considered in the commercial segment. As stated in [15], artificial intelligence algorithms can be used to develop fraud models for both individual and commercial segment customers. This is one of the main motivations for this study explained in this paper. It seems that the research along this line will increase every day.

2.3. Credit Card Fraud Detection

As implied above, technological progress and digitalization have brought many fraud concepts, particularly credit card fraud in banking causing negative situations such as cash damage and loss of trust, into consideration [16]. According to the Federal Trade Commission report, card fraud attacks were recorded as 277.739 in 2019, 399.721 in 2020, 395.391 in 2021, 448.459 in 2022, and 425.977 in 2023. The report estimates that 2024 will also be an increasing year. In relation to credit cards, fraudsters use many different channels for fraud attempts. Credit card fraud types are depicted in Figure 1. Card fraud attempts that are carried out specifically for physical cards such as counterfeits, lost, stolen, or non-receipt have been used for a long time. In addition, application and account takeover fraud methods are frequently used by fraudsters in digital environments.

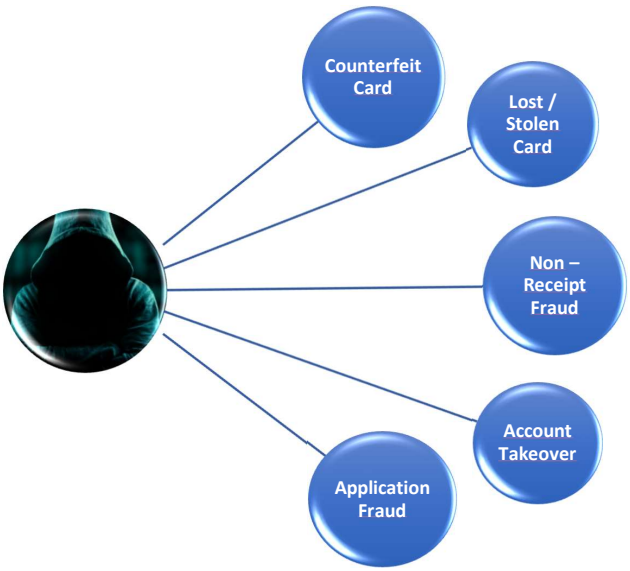

Figure 1. Credit card fraud attacks.

Although there are some attempts to create a solution to this problem, it is still very difficult to analyze, model, detect, and prevent credit card-related fraud situations. In [17], it is reported that the fraud-related credit card transactions do not make up even 1% of all credit card transactions, and therefore model patterns are difficult to distinguish as compared to regular balanced transactions. In order to prevent credit card misuse, semi-manual decision systems consisting of rules based on the expert opinion are to be employed. However, it is known that there are some patterns that cannot be noticed with rules created by experience and intuition. More intelligent systems capable of detecting misuse of credit cards through utilization of other artificial intelligence methodologies are necessary [18].

When generating intelligent systems, it should be taken into account that the credit card fraud studies are based on two important structures. The first structure is the process of managing the data that will be used in fraud studies. In this context, card-level transactions are combined with customer information and credit bureau information to develop a fraud data mart. In the second structure, enough samples are taken from the fraud data mart within the appropriate time interval to create training, testing, and validation of the data sets. This process is run on three successive operations as given below:

a. Imbalanced Learning (balancing the imbalanced card fraud data set);
b. Feature Selection (detecting the important variables on the card fraud data set);
c. Predictive Model (development of card fraud models for possible prediction).

At the end of several runs (trials), the card fraud detection models developed are evaluated in terms of a set of performance metrics. By benchmarking the trials, the most appropriate one is determined as the "champion fraud detection model". In developing the champion model, SL or semi-supervised learning (SSL) are used.

Fraud flag information must be fed completely, fully, and accurately into all card fraud data sets, especially in data marts for the sake of better learning. Once defining and running the champion model, the output of the model can be fed into a prevention model defining respective action plans against fraudulent data. Note that the existing credit card fraud modelling approaches as well as emerging credit card fraud modelling approaches are reviewed in this paper. In addition, the existing modelling approaches such as classification are mainly based on equation-based traditional techniques whereas the emerging models are agent-based techniques, as proposed in this paper. ABM techniques are also elaborated below for validating the proposed model.

3. Existing Fraud Detection Techniques

In recent years, different resampling approaches, feature selection (FS)/dimensionality reduction (DR) techniques, and classification algorithms have been studied on card fraud data processing. As explained above, the CCFD studies consist of successive operations such as creating balanced fraud data sets with IL, selecting important features for model generation and developing the appropriate fraud model. These operations are crucial and need to be analyzed very carefully to sustain the learning performance of the models employed. In this study, credit card fraud research studies between 2020 and 2024 are reviewed and 34 distinguished papers have been taken as the reference to support and validate the proposed model.

3.1. Solutions of Imbalanced Data in CCFD

In the first operation mentioned above, the data sets with an imbalanced structure are converted into pre-processed data with various resampling approaches. Several approaches are applied at cost-sensitive, algorithm-level, data-level, and ensemble of classifiers to generate balanced fraud data sets. Some of the resampling approaches and respective abbreviations are given in Table 1.

Table 1. Imbalance learning approaches used in credit card fraud studies.

Resampling Type	Resampling Method	Abbreviation
Undersampling	Random Undersampling	RUS
	One-Sided Selection	OSS
	Condensed Nearest Neighbor	CDNN
	Edited Nearest Neighbors	ENN
	Repeated Edited Nearest Neighbors	RENN
	All k-Nearest Neighbors	AllKNN
	Instance Hardness Threshold	IHT
	Near Miss Sampling	NMS
	Neighborhood Cleaning Rule	NCR
	TomekLinks	TMLK
	Cluster Centroid Sampling	CCS
	Sequence Aware Undersampling	SAUS
Oversampling	Random Oversampling	ROS
	Synthetic Minority Oversampling Technique	SMOTE
	Borderline Synthetic Minority Oversampling Technique	Borderline SMOTE
	k-Means Synthetic Minority Oversampling Technique	k-Means SMOTE
	Support Vector Machine Synthetic Minority Oversampling Technique	SVM SMOTE
	Adaptive Synthetic Sampling	ADASYN
Oversampling followed by Undersampling	Synthetic Minority Oversampling Technique + Edited Nearest Neighbors	SMOTEENN
	Synthetic Minority Oversampling Technique + TomekLinks	SMOTETomek

Ref. [19] highlighted some approaches that reference the neighborhood, boundaries, and distribution that are used as resampling approaches in both undersampling and oversampling. Additionally, there is a hybrid version of oversampling followed by undersampling. In this approach, the minority class is first brought closer to the major class with the oversampling approach, and then the balance between the classes is created with the undersampling approach [see [20] for more information]. Note that the different resampling techniques contribute to the knowledge discovery process in terms of feature selection and training performance.

3.2. Feature Selection and Dimensionality Reduction in CCFD

In the IL process, pre-processing is performed on the basis of the target variable to avoid overlapping problems. FS studies are then carried out for feature reduction

by identifying important features in accordance with the data and directing important features into the analysis and modelling process [21,22]. Since the training model cannot be executed with raw data, depending on the data set and variables, different FS approaches are applied. Although the FS process is quite costly, it is very important in terms of reducing the dimensionality and identifying important features. In dimensionality reduction (DR), there is a transition from a high-dimensional solution space to a low-dimensional solution space on the data with linear and non-linear processors to eliminate the complexity from dimensionality [23,24]. Both FS and DR studies enable the identification of important features and the discovery of patterns for respective fraud models.

3.3. Supervised Learning Models in CCFD

In CCFD studies, it is also very important to develop model patterns with important features. During the development of the fraud models, SL techniques are frequently used due to the labels of fraud transaction (legal/fraud) [25]. In these studies, SL techniques are employed due to generating predictive results and presenting differential knowledge. Additionally, the performances of SL models can be easily examined with different metrics and approaches with several advantages. As stated in [26], SL techniques give very effective results in terms of model performance in CCFD as opposed to unsupervised learning (USL) algorithms that are using unlabeled data which are also used for fraud detection [27]. Note that some examples of the SL methods and abbreviations are listed in Table 2.

Table 2. Supervised learning methods used in credit card fraud studies.

Supervised Learning Method	Abbreviation
Adaptive Boosting	AdaBoost
Adaptive Boosting and Light Gradient Boosting Machine	AdaBoost-LGBM
Classification and Regression Tree	CART
Category Boosting	CatBoost
Convolutional Neural Network	CNN
Decision Tree	DT
Ensemble Learning	EL
Extreme Learning Machine	ELM
Extra Tree Classifier	ETC
Genetic Algorithm and Support Vector Machine	GA-SVM
Generative Adversarial Network	GAN
Gradient Boosting Machines	GBM
Gaussian Naive Bayesian	GNB
Gated Recurrent Unit	GRU
K-Nearest Neighbors	KNN
Linear Discriminant Analysis	LDA
Light Gradient Boosting Machine	LGBM
Logistic Regression	LR
Long Short-Term Memory	LSTM
Long Short-Term Memory and Conditional Random Fields	LSTM-CRF
Latent Dirichlet Allocation	LTDA
Multilayer Perceptron	MLP
Multinominal Naive Bayesian	MNB
Naive Bayesian	NB
Passive Aggressive Classifier	PAC
Particle Swarming Organization and Weighted k Means	PSO-Weighted k-Means
Random Forest	RF
Radius Neighbors Classifier	RNC
Support Vector Machine	SVM
eXtreme Gradient Boosting	XGBoost
eXtreme Gradient Boosting on Spark	XGBoost-Spark

In classification models employing SL, a well-known confusion matrix is taken as the reference to measure and evaluate training performances. In data mining models, many performance metrics, especially accuracy ratio, are calculated using the confusion matrix. The *Accuracy Ratio* is calculated as given in Equation (1) below. Note that in the equations, *TP*, *TN*, *FP*, and *FN* represent true positive, true negative, false positive, and false negative [28].

$$Accuracy\ Ratio = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

In addition to the accuracy ratio, it may be useful to calculate and evaluate the sensitivity (known as true positive rate or recall) and specificity (known as true negative rate) metrics. The *Sensitivity* and *Specificity* are calculated as given in Equations (2) and (3) below:

$$Sensitivity = \frac{TP}{TP + FN} \quad (2)$$

$$Specificity = \frac{TN}{TN + FP} \quad (3)$$

In CCFD training, Type I and II errors (false positive and false negative) indicate the negative effects on the bank and the bank customer. Model performance is evaluated by calculating the Matthews correlation coefficient (*MCC*) to handle Type I and II errors. When the *MCC* value is close to 1, the success of the model increases. The *MCC* is calculated as given in Equation (4) below:

$$MCC = \frac{(TP \times TN) - (FP \times FN)}{\sqrt{(TP + FP)\ (TP + FN)(TN + FP)(TN + FN)}} \quad (4)$$

In addition to the *MCC*, the binning method is also recommended to eliminate Type 1 and Type 2 errors. For CCFD, the alternative technique with the binning approach has been explained under the emerging fraud detection techniques below. Similarly, the existing fraud detection techniques reviewed (IL, FS and SL) are listed in Table 3.

Table 3. Different modelling approaches used in credit card fraud detection studies.

Reference	Solutions for Imbalance Data	Feature Selection Methods	Classification Methods	The Best Model
[29]	RUS, ROS, SMOTE, and ADASYN	PCA	LR, SVM, NB, RF, DT, and KNN	RF Model with ROS
[30]	ROS and CBM	PCA	MLP, DT, LR, RF, and SVM	RF Model with RUS
[31]	ROS	PCA	GAN, NB, and MLP	MLP Model with ROS
[32]	SMOTE	PCA	LR, RF, DT, XGBoost, and SXGBoost	SXGBoost
[33]	SMOTE	PCA	MLP and ELM	MLP
[34]	CCS	PCA	RF, LR, NB, and GA-SVM	GA-SVM
[35]	SMOTE	PCA	RF, LR, MLP, SVM, NB, and KNN	RF
[36]	SMOTE	GA	DT, RF, LR, MLP, and NB	RF
[20]	SMOTEENN	PCA	SVM, MLP, DT, AdaBoost, and LSTM	LSTM
[37]	ADASYN	PCA	CNN	CNN Model with ADASYN

Table 3. *Cont.*

Reference	Solutions for Imbalance Data	Feature Selection Methods	Classification Methods	The Best Model
[38]	SMOTE, Borderline SMOTE, ADASYN, SMOTEENN, and SMOTETomek	PCA	KNN, LR, LTDA, CART, and NB	CART Model with Borderline SMOTE
[39]	SMOTE	RFE	PAC, LDA, RNC, BNB, GNB, and ETC	ETC
[40]	SMOTE, ADASYN, ROS, RUS, TMLK, CCS, AIIKNN, SMOTETomek, and SMOTEENN	PCA	AdaBoost, XGBoost, RF, SVM, LR, GNB, MNB, KNN, and DT	AdaBoost, XGBoost, and RF
[41]	SMOTE, Borderline SMOTE, k-Means SMOTE, and ADASYN	PCA, AE, and VAE	CNN and SVM	CNN Model with ADASYN
[42]	SMOTEENN	CRA	LR, SVM, NB, RF, LGBM, XGBoost, AdaBoost, and DT	AdaBoost + LGBM (Hybrid Model)
[43]	RUS	PCA	LR, XGBoost, and MLP	MLP
[44]	SMOTE	PCA	LR, LDA, NB, and XGBoost	XGBoost
[45]	RUS, TMLK, OSS, CDNN, ENN, AllKNN, RENN, NCR, NMS, IHT, ROS, ADASYN, SMOTE, SVM SMOTE, Borderline SMOTE, SMOTEENN, and SMOTETomek	PCA	LR, DT, KNN, RF, NB, GBM, CatBoost, LGBM, and XGBoost	CatBoost Model with AllKNN
[46]	RUS	PCA	DT, LR, NB, and EL	EL
[19]	SMOTE, Borderline SMOTE, and ADASYN	PCA and MRMR	DT, RF, and ETC	ETC Model with Borderline SMOTE
[47]	SMOTE	PCA	SVM, ELM, and XGBoost	XGBoost
[48]	RUS, SAUS, ROS, ADASYN, and SMOTE	PCA	MLP, GRU, LSTM, and LSTM-CRF	LSTM-CRF
[49]	RUS	t-SNE, PCA, and SVD	LR, KNN, DT, and SVM	LR
[28]	ROS	PCA and AE	LGBM, KNN, and RF	LGBM
[50]	SMOTE	PCA, AE, and OCSVM	LR, KNN, DT, RF, NB, AdaBoost, and XGBoost	XGBoost
[51]	RUS and ROS	PCA	LR	LR
[52]	SMOTEENN	Shapiro	LR, KNN, DT, RF, NB, AdaBoost, and XGBoost	RF
[25]	RUS	CRA	LR, GNB, KNN, DT, and RF	RF
[53]	RUS, ROS, and SMOTE	PCA	LR, DT, XGBoost, and MLP	XGBoost Model with ROS
[54]	SMOTE	PCA	ETC, GBM, DT, and RF	GBM Model with AdaBoost and RF Model with AdaBoost
[27]	SMOTEENN	PCA	k-Means, Weighted k-Means, and PSO-Weighted k-Means	PSO-Weighted k-Means Hybrid Model

Table 3. *Cont.*

Reference	Solutions for Imbalance Data	Feature Selection Methods	Classification Methods	The Best Model
[55]	RUS, ROS, SMOTE, ADASYN, Borderline SMOTE, and SVM SMOTE	Mutual Information	RF, KNN, LGBM, XGBOOST, and DT	RF
[56]	SMOTE	PCA	Voting, Stacking, CNN, and LSTM	Stacking
[57]	RUS	PCA	RF, GBM, NB, KNN, DT, and LR	RF

When reviewing 34 distinguished papers, it is realized that advanced level undersampling and oversampling approaches have been used in addition to the basic level random over sampling (ROS) and random under sampling (RUS) approaches. As can be seen in Table 3, the SMOTE oversampling approach has been the most used method in resampling for CCFD between 2020 and 2024. It is also shown that the use of the ADASYN oversampling approach has increased for the balancing of imbalance fraud data sets. In recent years (2022 and 2024), it seems that the use of oversampling followed by undersampling approaches such as SMOTEENN and SMOTETomek known as hybrid resampling approaches have increased. Note that hybrid approaches reduce the overfitting problem of the minority class from the oversampling process [34]. In addition, hybrid approaches minimize the loss of information resulting from the undersampling process in all data [38]. It is thought that the use of a hybrid approach will increase in the resampling process and different hybrid approaches could be developed.

With the progress in data science, many different approaches such as heuristic and meta-heuristic algorithms for FS are also used and some of those are listed in Table 3. As can also be seen in Table 3, singular value decomposition (SVD), correlation analysis (CRA), mutual information (MI), nearest neighborhood (relief feature elimination (RFE) and t-distributed stochastic neighbor embedding (t-SNE)) approaches, latent vector-based approaches (auto encoder (AE) and variational auto encoder (VAE)), one class support vector machine (OCSVM) with USL for fraudsters and minimum redundancy maximum relevance (MRMR) have been used among the papers (years 2020–2024) in CCFD. Moreover, it can be seen that the genetic algorithm (GA) is very effective in determining crucial features in card fraud data [36]. Due to the limitations of linearity assumptions, t-SNE, one of the manifold learning approaches, has been used for pattern discovery in fraud FS processing [49].

The basic-level SL techniques such as LR, DT, SVM, and MLP have frequently been used in CCFD. Additionally, ensemble SL methods such as RF, XGBoost, and AdaBoost have frequently been used, and they have outperformed other SL methods employed for CCFD. Similarly, the training performances of deep learning algorithms are very good in CCFD. In CCFD, SL models have been widely used to discover patterns in predictive studies. However, SL models create offline structure in CCFD studies, and these models may be insufficient to capture the changes in the fraudulent behavior. In this context, the usability of existing approaches such as SL models have been examined as well as different approaches supported by agent technology.

4. Emerging Fraud Detection Techniques

In traditional CCFD studies, models are developed with processes consisting of IL, FS, and SL algorithms. In addition to the traditional modelling approach on the card fraud data set, agent-based models as emerging approaches are developed instead of SL algorithms. In an environment where card fraud behavior is constantly changing, the use of autonomous

agents can be very beneficial for fraud decision systems. ABM and autonomous agents can perform dynamic learning processes to learn fraud behaviors through learning abuse actions in a repetitive process. They build a dynamic learning structure by compiling what they have learned. In python programming language, libraries such as Mesa, Tensorforce, TF-Agents, KerasRL, and ImbDRL have been developed to be used in ABM studies. In learning-based modelling approaches, the use of agent technology will benefit several areas, especially in fraud analysis.

4.1. Agent-Based Modelling in CCFD

In addition to EBM, ABM approaches have been recently used in several financial areas such as risk management, credit scoring, credit pricing, early warning, and macro economy. There are several ABM studies especially on the effects of credit risk [58,59]. Also, as stated in [60,61], there are some studies on how credit transactions affect banks, customers, and financial indicators. All stakeholders on credit network systems are brought together and the macro/micro effects are examined with the ABM [62–64]. For example, agent-based macroeconomic models have been developed in order to see the financial effects [65,66]. Due to this capability, it is thought that agent-based approaches can be employed to contribute to the modelling of CCFD studies. With the ABM approach, fraudulent behaviors can be depicted by examining interactions on the credit card fraud data sets. Table 4 shows the studies on ABM in the financial world. The use of ABM modelling approaches in different financial issues is increasing day by day. In the financial world, the use of ABM approaches is increasing in studies on analyzing behavioral information and evaluating impacts. In financial modelling studies, hybrid structures can be developed by combining different sub-branches of the ABM approach with predictive algorithms. The reinforcement learning approach, which is a sub-branch of ABM, can be combined with the deep learning process to produce predictive outputs such as SL.

Table 4. Studies on agent-based modelling in the financial world.

Reference	Title	Topic	Comment
(Jonsson, 2014) [58]	Credit Risk—an Agent Model of Post Credit Decision Actions and Credit Losses in Banks	Finance–Banking–Credit Risk	In the study, an agent model was developed to examine the effect of bankers' post credit decisions on bank credit losses caused by lending to corporate customers. The model results show that post credit decisions have significant effects on bank loan losses.
(Liu et al., 2016) [61]	Credit Rationing and the Simulation of Bank—Small- and Medium-Sized (SMEs) Firm Artificial Credit Market	Finance–Banking–Credit Transactions	In the study, the financing difficulties faced by SMEs were analyzed and an artificial credit market was created with agent-based computational to imitate credit transactions. The model results show that the number of collaterals, the average probability of success of the projects, and the principal interest ratio have an important effect on the average profit of the bank, the bank capital, the total interest ratio, the number of borrowers, the size of the credit, and the degree of the credit score.

Table 4. *Cont.*

Reference	Title	Topic	Comment
(Catullo et al., 2018) [62]	Early Warning Indicators and Macro Prudential Policies—a Credit Network Agent-Based Model	Finance–Banking–Credit Network System	In the study, an agent model was developed that renews an artificial credit network according to the leverage options of firms and banks. The study aimed to identify and analyze both early warning indicators and policy precautionary measures in the credit network.
(Erlingsson et al., 2014) [64]	Housing Market Bubbles and Business Cycles in an Agent Credit Economy	Finance–Banking–Credit Network System	In the study, housing and mortgage markets were examined with an agent-based macroeconomic model. A series of computational experiments were conducted to investigate the effects of different households' credibility conditions on the credit network system. In the study, it is seen that easy access to credit increases housing prices and uncertainty in the economy.
(Dosi et al., 2013) [65]	Income Distribution, Credit and Fiscal Policies in an Agent Keynesian Model	Economics–Financial Impact–Macroeconomic Model	In the study, the relationships between income distribution and monetary and fiscal policies were examined using a different version of the agent-based Keynesian model. With the help of the developed model, it was attempted to explain the effect of financial factors on the real economy and income distribution. In addition, the model shows that unstable economies are subject to severe business cycle fluctuations, high unemployment rates, and high crisis probabilities.
(Russo et al., 2016) [66]	Increasing Inequality, Consumer Credit, and Financial Fragility in an Agent Macroeconomic Model	Economics–Financial Impact–Macroeconomic Model	The study examined the interaction between increasing inequality and consumer credit in a multiplex macroeconomic system of households, banks and firms. The simulation results show that there are positive and negative effects to implementing consumer credit. A fiscal policy might be needed as the increase in financial profits triggers the decline in the real wealth of the household.
(Catullo et al., 2021) [63]	Macro and Micro Prudential Policies—Sweet and Lowdown in a Credit Network Agent Model	Finance–Banking–Credit Network System	In the study, an agent-based model was presented that reproduces a credit network formed by firms, banks, and individual customers. Simulation trials show that a combination of micro and macro prudential strategies decreases systemic risk but also increases banks' capital volatility. The results support the argument that meso prudential policy can reduce systemic risk without affecting the stability of banks' capital structure.

Table 4. *Cont.*

Reference	Title	Topic	Comment
(Alexandre and Lima, 2020) [60]	Macroeconomic Impacts of Trade Credit—an Agent Modelling Exploration	Finance–Banking–Credit Transactions	In the study, the effects of macroeconomic changes on commercial loans were examined by evaluating the macroeconomic effects in various dimensions. Two different types of agent-based model were developed in the study (down-stream firms and up-stream firms). The results show that there is a potential relationship between the ratio of non-performing loans and the average product of firms.
(Jonsson, 2015) [59]	The Effects of Reward System on Bank Credit Losses—an Agent Model	Finance–Banking–Credit Risk	In the study, an agent model was used to examine how reward system design affects bank credit losses. The model results show that a collaborative reward system has the potential to decrease bank credit losses.

In agent-based card fraud modelling studies, while some of the samples are used for training, testing, and validation, some of them can be used for scoring, monitoring, and reporting. In the first stage of the card fraud model development, the model pattern is determined by taking the training data set as a reference. The performance of the agent-based fraud training model can be examined on different data sets such as testing. The agent-based model should also be tested on out-of-time data sets, such as validation and scoring data sets. In credit card fraud studies, the performances of agent-based models and benchmarking models should be evaluated with the help of key performance indicators (KPIs).

Training models are recorded in the process known as machine learning operations (MLOps), which is a continuation of the model development process. In card fraud modelling, the pattern of the model is printed on the model template in an appropriate format. The pattern of the agent-based fraud model can be used in different times and environments to produce score values on a transaction basis. In bank decision systems where credit card fraud results are used, real-time scores can be produced by positioning the model pattern appropriately and smoothly in the system.

4.2. Reinforcement Learning in CCFD

Reinforcement learning (RL) is an ABM technique in which the learning process is carried out by being influenced by the actions of an agent and its environment [67,68]. In RL, agents evaluate information in the environment (situation), and they affect the environment (action) with their obtained information [69,70]. Unlike SL, RL uses positive and negative behaviors as rewards and punishments by providing feedback between input and output [71]. Therefore, RL is very successful in detecting, evaluating, and using the behavior of information in data sets. The RL approach is frequently used in several financial areas such as card fraud, credit allocation, credit pricing, credit scoring, and investment and portfolio management. As stated in [72,73], RL has recently been used instead of SL, especially in fraud studies carried out via POS or digital transactions. In addition, the model performance of the RL models has been found to be very high compared to the supervised learning models [74].

RL models attract attention not only with their performance and impact in financial matters but also with their speed in processing and response. In terms of processing time,

financial fraud models with RL are considerably lower than financial fraud models with supervised learning [75]. In credit allocation and credit pricing studies, RL models have been found to positively affect processes in terms of scaling, computational efficiency and fast training [76]. As mentioned in [77,78], in credit scoring, RL has also been used in subjects such as testing the model effects and determining the optimal threshold value. Cutoff strategies, which are an important issue in the credit scoring, can also be easily carried out with RL approach studies. In addition to credit-based studies, RL approaches are also used in studies such as investment and portfolio management for the buying and selling of financial assets. RL has frequently begun to be used in the fields of investment and portfolio management from decision processes to optimal policies [79,80]. It is thought that the RL approach will make a great contribution to several different financial issues [81]. It is anticipated that financial modelling studies using the RL approach will increase. Table 5 depicts the studies on RL applications in the financial world.

Table 5. Studies on reinforcement learning in the financial world.

Reference	Title	Topic	Comment
(Mead et al., 2018) [73]	Detecting Fraud in Adversarial Environments: A Reinforcement Learning Approach	Finance–Banking–Credit Card Fraud	In the study, it was stated that credit card fraud is a costly problem for banks. In addition, it was stated that this abuse creates a great concern for consumers. The disadvantages of supervised learning methods used are mentioned in credit card fraud. It has been stated that supervised learning leads to a static approach and in this case, it creates weakness in recognizing the changing conditions. In addition, the reinforcement learning approach is more effective than static approaches in modelling. In the study, a hybrid structure was developed by adding the Markov decision process (MDP) to the reinforcement learning approach.
(Dang et al., 2021) [72]	Machine Learning based on Resampling Approaches and Deep Reinforcement Learning for Credit Card Fraud Detection Systems	Finance–Banking–Credit Card Fraud	The study focused on the imbalanced data set problem and its solution. In the study, the raw data set and the data sets obtained because of resampling (SMOTE and ADASYN) were used. Machine learning algorithms and the deep reinforcement learning approach were applied to these data sets. Models obtained with different approaches (raw data-machine learning, resampled data sets-machine learning and raw data-deep reinforcement learning) were compared in terms of performance. The deep reinforcement learning model using the raw data set did not meet the expectations in terms of performance.

Table 5. *Cont.*

Reference	Title	Topic	Comment
(Tekkali and Natarajan, 2023) [75]	RDQN: Ensemble of Deep Neural Network with Reinforcement Learning in Classification based on Rough Set Theory for Digital Transactional Fraud Detection	Finance–Banking–Digital Fraud	In the study, it was stated that several machine learning algorithms can detect whether the digital transaction is fraudulent, but these algorithms fail to reduce the processing time. Hybrid models are being developed to detect movements quickly and efficiently. A new approach (RDQN) was obtained by combining the rough set theory approach and the deep reinforcement learning approach. The study consists of three main titles: data preprocessing process, determination of structural relations with rough set theory, and establishment of hybrid system (DQN) by determining properties. In particular, with the improvement in the reward function, the processing time is considerably reduced.
(Vimal et al., 2021) [74]	Application of Deep Reinforcement Learning to Payment Fraud	Finance–Banking–Digital Fraud	In the study, it was mentioned that the models developed with standard machine learning algorithms could not give optimum results in the desired solutions. A decision model was created by adding the benefit maximization to the reward function in the reinforcement learning approach. The developed model was compared with other standard classifiers. The developed model gave very successful results in terms of performance compared to other classification models except for XGBoost.
(Handhika et al., 2021) [76]	Reinforcement Learning on the Credit Risk-Based Pricing	Finance–Banking–Credit Pricing	In the study, credit prices were created on an individual basis by using individual customer information such as credit scores, maturity, and number of applications. While creating the credit scorecard used in pricing, the past information of individual customers was used. It was attempted to create a model pattern with the deep reinforcement learning approach.
(Hassani, 2021) [77]	Societal Biases Reinforcement through Machine Learning—a Credit Scoring Perspective	Finance–Banking–Credit Scoring	The study tested whether social biases affect credit scorecards. Reinforcement learning approach was used in the analysis of factors and evaluation of results in this test process. When the results of the study were examined, it was seen that social biases affected credit scorecards and made them biased.
(Herasymovych et al., 2019) [78]	Using Reinforcement Learning to Optimize the Acceptance Threshold of a Credit Scoring Model	Finance–Banking–Credit Scoring	In the study, the reinforcement learning approach was used to determine the optimal threshold values of credit scores. It was concluded that the optimal threshold values obtained with the reinforcement learning will be better than the threshold values obtained with the traditional approach (in terms of profit).

Table 5. *Cont.*

Reference	Title	Topic	Comment
(Zeynullahu et al., 2022) [80]	Applications of Reinforcement Learning in Finance-Trading with a Double Deep Q-Network	Finance–Banking–Investment Management	The study focused on improving the buying and selling of individual financial assets in the investment decision process. In the study, the agent is trained in buying/selling transactions, and its behavior is tested on new data.
(Li et al., 2021) [81]	FinRL-Podracer: High Performance and Scalable Deep Reinforcement Learning for Quantitative Finance	Finance–Banking–Investment Management	The study offered a deep reinforcement learning approach cloud solution with high performance and high scalability in investment decisions. The deep reinforcement learning approach has a constantly renewing mechanism to improve investment performance.
(Hu and Lin, 2019) [79]	Deep Reinforcement Learning for Optimizing Finance Portfolio Management	Finance–Banking–Portfolio Management	In the study, the use and results of deep reinforcement learning approach, which is a combination of deep learning and reinforcement learning approaches, were evaluated in portfolio management. In the first stage, GRUs, one of the deep neural network models, were used to examine the effects. Then, it was attempted to determine the risk adjustable reward function. In the last stage, a model was developed by combining deep and reinforcement learning approaches to determine the optimal policy in the portfolio.
(Wu and Li, 2024) [70]	Reinforcement learning for continuous-time mean-variance portfolio selection in a regime-switching market	Finance–Banking–Portfolio Management	In the study, the RL approach was used to solve the continuous-time mean-variance portfolio selection problem in a market-facing regime change. It is seen that the model with an RL approach is quite useful in the long-term investment problem of portfolio management.

4.3. Proposed Conceptual Model

In this study, RL approaches are recommended instead of SL approaches and a conceptual model is proposed utilizing deep RL, deep Q learning, and a deep Q network for more effective CCFD, as depicted in Figure 2. As illustrated, it is proposed to develop an end-to-end analytical structure for card fraud. The proposed model includes many processes, from adding and editing data to databases to evaluating the real-time activity of the end user. In the first stage, credit card transactions, customer information, and external knowledge are managed in a data mart. The information of different data marts are brought together on a transaction/customer basis to create samples for training, testing, validation, and scoring. When creating these samples, data sets should be created that can reflect the population. Also, in this process, samples should not differ from each other at a high level.

The new training data set is balanced by applying IL (oversampling, undersampling, and hybrid approaches) techniques to the training data set. During the balancing process, transactions are made on rows in the training data set. Important features are determined on a column basis by applying different FS (filter, wrapper, and combined techniques) methods on training fraud data set balanced by resampling. After these two pre-processing stages are completed, the agent-based training process is started with learning agents. Specifically, learning agents are run on training data sets, which are organized both on

row and column basis, to analyze card transactions. Learning agents maximize the total rewards by determining the patterns of abnormal behavior on the fraud training data set using deep learning. In this paper, equation-based and agent-based model trials were conducted. Model trials with SVM, RF, and double deep Q network (DDQN) approaches were conducted to support the proposed conceptual model. The European Credit Cardholder (2013) raw data set was used in model trials. On the raw data set, SMOTEENN was applied as the IL approach and ANOVA F test was applied as the FS approach. It is seen that the DDQN model, which is an ABM approach, is more successful than benchmarking models (SVM and RF).

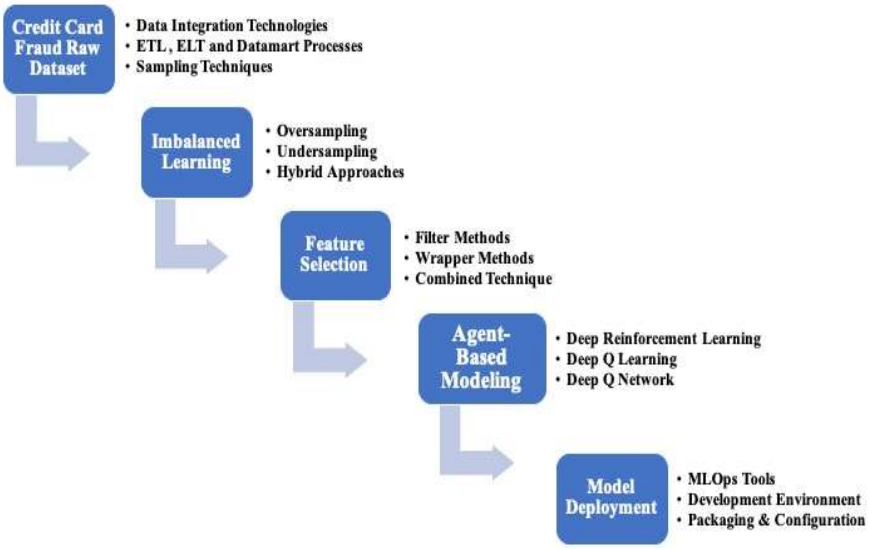

Figure 2. Proposed conceptual RL model in detecting credit card fraud.

The performance results of the card fraud model trials are shown in Table 6.

Table 6. The performances of the models developed using the IL and FS methods.

Approach	Partition	Recall	Precision	GMean	F1-Score
DDQN Model	Train	1.000000	0.987671	0.993816	0.993797
DDQN Model	Test	1.000000	0.987617	0.993789	0.993770
SVM Model	Train	0.993123	0.991848	0.992485	0.992485
SVM Model	Test	0.993450	0.991721	0.992585	0.992585
RF Model	Train	0.979660	0.998757	0.989162	0.989116
RF Model	Test	0.978902	0.998480	0.988643	0.988594

When the models presented above are examined, it is seen that the training model with the highest f1-score value is the DDQN model. This model is defined as the champion model and the deployment process is started based on this model. Through the model deployment methods, fraud/legal patterns are recorded on the model template with learning agents. Python libraries such as pickle and mlflow can be used during the model saving process. After the saving process, the model template can be loaded and made ready for scoring. With the model template, real-time transactions can be evaluated, and instant and effective decisions can be made. Once running the deployment system, Q values, which are the function output values, are obtained from the DDQN model developed. When the DDQN model detects transactions containing fraudulent information, the Q value increases through deviating from the average. At the same time, risk groups have begun to be created using Q values and actual fraud flag. In this section, the Q value has been subjected to binning and divided into risk groups. In particular, for card fraud prevention process, the creation of example risk groups is shown in Table 7).

Table 7. The implementing of example binning approach for risk groups.

Risk Group	Binning	Legal Rate	Fraud Rate
1	Q Value < 0.2831	99.97%	0.03%
2	0.2831 $\leq$ Q Value < 0.2899	99.94%	0.06%
3	0. 2899 $\leq$ Q Value < 0. 2945	99.90%	0.10%
4	0. 2945 $\leq$ Q Value < 0. 2985	99.88%	0.12%
5	0. 2985 $\leq$ Q Value < 0.3031	99.64%	0.36%
6	0.3031 $\leq$ Q Value	99.52%	0.48%

While the actual fraud rate of risk group 1 is lower compared to the other groups, the actual fraud rate of risk group 5 is higher compared to the other groups. In SL approaches, labelling card transactions as fraudulent or legitimate can lead to Type 1, Type 2, and Type 3 errors. Instead, determining the risk group according to the Q value and applying security protocols specific to the risk group can benefit for card fraud processes in banking. Different security protocols at the transaction can benefit bank processes in fraud management. For example, for those with a risk group assignment of 4, 5, or 6, mobile application approvals, personal inquiries, and additional passwords may be requested. In this way, the management of risks encountered as a result of incorrect label assignments of models (Type 1 (*FP*—not assigning fraud label to an action that is actually fraud) or Type 2 (*FN*—assigning fraud label to an action that is not actually fraud)) will be facilitated.

5. Conclusions and Future Works

Due to increasing card fraud transactions, banks are faced with cash and reputational losses. In order to minimize fraud-related losses in banks, detection models are developed. These fraud models should evaluate abnormal transactions immediately. In implementation with real time, CCFD models are expected to be fast, effective, and consistent. CCFD models should not only be high-performance models but also contribute to the prevention process.

In this paper, many distinguished papers on the modelling of credit card fraud transactions have been examined. The methods used in CCFD studies have been classified and evaluated as existing techniques and emerging techniques. The approaches of existing techniques, which are frequently used in CCFD studies, have been examined in detail and the results have been interpreted. Furthermore, the benefits of modern emerging techniques to CCFD studies are also revealed in this paper. On the card fraud data set, it is thought that the use of hybrid approaches, which are a combination of oversampling and undersampling approaches, will increase in the process of dealing with imbalanced data. In imbalanced data sets, RL-based models give very successful results compared to other classification models. It is also thought that the DDQN approach, which is one of the RL approaches, will be effective on the card fraud data set. It is very important that the developed model patterns are usable in real-time and do not cause Type I or Type II errors. In particular, during the examination of model performance, the emergence and ungovernableness of Type I and Type II errors can cause important problems in card fraud management. To solve possible problems in Type I and Type II, the Q value can be divided into many groups and examined with binning methods such as bucket and quantile. The binning process can be divided into groups by considering the Q value and the actual fraud flag. Actions for the prevention process can be determined by making risk-free, low-risk, and risky assignments to groups developed according to the level of risk. Model deployment and online scoring studies are among the most important issues in the credit card fraud detection and prevention process. The system deployment process of models is a very difficult issue for the credit card fraud topic. Model deployment is among the issues awaiting a solution regarding credit card fraud. Apart from the model deployment topic, online scoring studies on credit card fraud should also be carried out on a transaction basis.

In the world of credit card fraud, online scoring is one of the issues awaiting solutions to take quick action.

This paper has many potential benefits for the card fraud process. This paper offers suggestions in many different areas, from the data governance process to the action determination processes. It is suggested that the card data set in the big data category can be managed via cloud platforms. In the model development process, it is suggested that ABM approaches can be used effectively as well as EBM approaches. Integrating CCFD studies with prevention processes will benefit card fraud management processes. There are some limitations in this paper. The performance of the developed models could have been examined on different fraud data sets. However, the reluctance of banks to share data limits this study. In future works, the CCFD models will be carried out together with credit card prevention systems in line with the business requirements. It is thought that in the future, CCFD studies will evolve into card fraud management studies. It is also expected that different methodologies will be developed for the management of card fraud risk.

Author Contributions: E.O., conceptualization, methodology, idea proposal, writing—original draft preparation, and supervision; M.I., conceptualization, methodology, writing—original draft preparation, writing—review and editing, funding acquisition, and submission. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data used in this paper is publicly available. The data can be accessed from the this address: https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud (accessed on 20 January 2025).

Conflicts of Interest: The authors have no competing interests to declare that are relevant to the content of this paper.

References

1. Alarfaj, F.K.; Malik, I.; Khan, H.U.; Almusallam, N.; Ramzan, M.; Ahmed, M. Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms. *IEEE Access* **2022**, *10*, 39700–39715. [CrossRef]
2. Jain, V.; Kavitha, H.; Mohana Kumar, S. Credit Card Fraud Detection Web Application using Streamlit and Machine Learning. In Proceedings of the 2022 IEEE International Conference on Data Science and Information System (ICDSIS), Hassan, India, 29–30 July 2022; IEEE: Hassan, India, 2022; pp. 1–5. [CrossRef]
3. Arun, G.K.; Rajesh, P. Design of Metaheuristic Feature Selection with Deep Learning Based Credit Card Fraud Detection Model. In Proceedings of the 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 23–25 February 2022; IEEE: Coimbatore, India, 2022; pp. 191–197. [CrossRef]
4. Al-Faqeh, A.-W.K.; Zerguine, A.; Al-Bulayhi, M.A.; Al-Sleem, A.H.; Al-Rabiah, A.S. Credit Card Fraud Detection via Integrated Account and Transaction Submodules. *Arab. J. Sci. Eng.* **2021**, *46*, 10023–10031. [CrossRef]
5. Lenard, M.J.; Watkins, A.L.; Alam, P. Effective Use of Integrated Decision Making: An Advanced Technology Model for Evaluating Fraud in Service-Based Computer and Technology Firms. *J. Emerg. Technol. Account.* **2007**, *4*, 123–137. [CrossRef]
6. Roseline, J.F.; Naidu, G.; Pandi, V.S.; Rajasree, S.A.; Mageswari, N. Autonomous credit card fraud detection using machine learning approach. *Comput. Electr. Eng.* **2022**, *102*, 108132. [CrossRef]
7. Berkmans, T.J.; Karthick, S. Credit Card Fraud Detection with Data Sampling. In Proceedings of the 2022 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), Chennai, India, 8–9 December 2022; IEEE: Chennai, India, 2022; pp. 1–6. [CrossRef]
8. Li, Y.; Chen, Z.; Zha, D.; Zhou, K.; Jin, H.; Chen, H.; Hu, X. Automated Anomaly Detection via Curiosity-Guided Search and Self-Imitation Learning. *IEEE Trans. Neural Netw. Learn. Syst.* **2022**, *33*, 2365–2377. [CrossRef]
9. Patra, M.R.; Jayasingh, B.B. A Software Agent Based Approach for Fraud Detection in Network Crimes. In *Applied Computing. AACC 2004*; Manandhar, S., Austin, J., Desai, U., Oyanagi, Y., Talukder, A.K., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3285. [CrossRef]
10. Boutaher, N.; Elomri, A.; Abghour, N.; Moussaid, K.; Rida, M. A Review of Credit Card Fraud Detection Using Machine Learning Techniques. In Proceedings of the 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech), Marrakesh, Morocco, 24–26 November 2020; IEEE: Marrakesh, Morocco, 2020; pp. 1–5. [CrossRef]

11. Al Smadi, B.; Min, M. A Critical review of Credit Card Fraud Detection Techniques. In Proceedings of the 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 28–31 October 2020; IEEE: New York, NY, USA, 2020; pp. 0732–0736. [CrossRef]
12. Karthik, V.S.S.; Mishra, A.; Reddy, U.S. Credit Card Fraud Detection by Modelling Behavior Pattern using Hybrid Ensemble Model. *Arab. J. Sci. Eng.* **2022**, *47*, 1987–1997. [CrossRef]
13. Ravisankar, P.; Ravi, V.; Raghava Rao, G.; Bose, I. Detection of Financial Statement Fraud and Feature Selection using Data Mining Techniques. *Decis. Support Syst.* **2011**, *50*, 491–500. [CrossRef]
14. Saeed, S.K.; Hagras, H. Adaptive Type-2 Fuzzy Logic Based System for Fraud Detection in Financial Applications. In Proceedings of the 2018 10th Computer Science and Electronic Engineering (CEEC), Colchester, UK, 19–21 September 2018; IEEE: Colchester, UK, 2018; pp. 15–18. [CrossRef]
15. Hilal, W.; Gadsden, S.A.; Yawney, J. Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. *Expert Syst. Appl.* **2022**, *193*, 116429. [CrossRef]
16. Lahmiri, S.; Bekiros, S.; Giakoumelou, A.; Bezzina, F. Performance assessment of ensemble learning systems in financial data classification. *Intell. Syst. Account. Financ. Manag.* **2020**, *27*, 3–9. [CrossRef]
17. Itoo, F.; Meenakshi Singh, S. Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. *Int. J. Inf. Technol.* **2021**, *13*, 1503–1511. [CrossRef]
18. Alharbi, A.; Alshammari, M.; Okon, O.D.; Alabrah, A.; Rauf, H.T.; Alyami, H.; Meraj, T. A Novel text2IMG Mechanism of Credit Card Fraud Detection: A Deep Learning Approach. *Electronics* **2022**, *11*, 756. [CrossRef]
19. Own, R.M.; Salem, S.A.; Mohamed, A.E. TCCFD: An Efficient Tree-based Framework for Credit Card Fraud Detection. In Proceedings of the 2021 16th International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt, 15–16 December 2021; IEEE: Cairo, Egypt, 2021; pp. 1–6. [CrossRef]
20. Esenogho, E.; Mienye, I.D.; Swart, T.G.; Aruleba, K.; Obaido, G. A Neural Network Ensemble with Feature Engineering for Improved Credit Card Fraud Detection. *IEEE Access* **2022**, *10*, 16400–16407. [CrossRef]
21. Kumbure, M.M.; Lohrmann, C.; Luukka, P.; Porras, J. Machine learning techniques and data for stock market forecasting: A literature review. *Expert Syst. Appl.* **2022**, *197*, 116659. [CrossRef]
22. Zhang, W.; He, H.; Zhang, S. A Novel Multi-Stage Hybrid Model with Enhanced Multi-Population Niche Genetic Algorithm: An Application in Credit Scoring. *Expert Syst. Appl.* **2019**, *121*, 221–232. [CrossRef]
23. Işık, M.; Sennaroğlu, B.; Genç, M. Predicting the Probability of Default with the Help of Macroeconomic Indicators in IFRS 9 Provision Calculations. In *Post Covid Era: Future of Economies and World Order*; Istanbul University Press: Istanbul, Turkey, 2023; pp. 181–194. [CrossRef]
24. Xu, J.; Zhou, C.; Xu, S.; Zhang, L.; Han, Z. Feature selection based on multi-perspective entropy of mixing uncertainty measure in variable-granularity rough set. *Appl. Intell.* **2024**, *54*, 147–168. [CrossRef]
25. Afriyie, J.K.; Tawiah, K.; Pels, W.A.; Addai-Henne, S.; Dwamena, H.A.; Owiredu, E.O.; Ayeh, S.A.; Eshun, J. A Supervised Machine Learning Algorithm for Detecting and Predicting Fraud in Credit Card Transactions. *Decis. Anal. J.* **2023**, *6*, 100163. [CrossRef]
26. Bequé, A.; Lessmann, S. Extreme Learning Machines for Credit Scoring: An Empirical Evaluation. *Expert Syst. Appl.* **2017**, *86*, 42–53. [CrossRef]
27. Sharma, N.; Ranjan, V. Credit Card Fraud Detection: A Hybrid of PSO and K-Means Clustering Unsupervised Approach. In Proceedings of the 2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 19–20 January 2023; IEEE: Noida, India, 2023; pp. 445–450. [CrossRef]
28. Du, H.; Lv, L.; Guo, A.; Wang, H. AutoEncoder and LightGBM for Credit Card Fraud Detection Problems. *Symmetry* **2023**, *15*, 870. [CrossRef]
29. Ahmed, F.; Shamsuddin, R. A Comparative Study of Credit Card Fraud Detection Using the Combination of Machine Learning Techniques with Data Imbalance Solution. In Proceedings of the 2021 2nd International Conference on Computing and Data Science (CDS), Stanford, CA, USA, 28–29 January 2021; IEEE: Stanford, CA, USA, 2021; pp. 112–118. [CrossRef]
30. Sahu, A.; Gm, H.; Gourisaria, M.K. A Dual Approach for Credit Card Fraud Detection using Neural Network and Data Mining Techniques. In Proceedings of the 2020 IEEE 17th India Council International Conference (INDICON), New Delhi, India, 10–13 December 2020; IEEE: New Delhi, India, 2020; pp. 1–7. [CrossRef]
31. Ali, I.; Aurangzeb, K.; Awais, M.; ul Hussen Khan, R.J.; Aslam, S. An Efficient Credit Card Fraud Detection System using Deep learning-based Approaches. In Proceedings of the 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 5–7 November 2020; IEEE: Bahawalpur, Pakistan, 2020; pp. 1–6. [CrossRef]
32. Chen, H.; Ai, H.; Yang, Z.; Yang, W.; Ye, Z.; Dong, D. An Improved XGBoost Model Based on Spark for Credit Card Fraud Prediction. In Proceedings of the 2020 IEEE 5th International Symposium on Smart and Wireless Systems Within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), Dortmund, Germany, 17–18 September 2020; IEEE: Dortmund, Germany, 2020; pp. 1–6. [CrossRef]

33. El hlouli, F.Z.; Riffi, J.; Mahraz, M.A.; El Yahyaouy, A.; Tairi, H. Credit Card Fraud Detection Based on Multilayer Perceptron and Extreme Learning Machine Architectures. In Proceedings of the 2020 International Conference on Intelligent Systems and Computer Vision (ISCV), Fez, Morocco, 9–11 June 2020; IEEE: Fez, Morocco, 2020; pp. 1–5. [CrossRef]
34. Cui, Y.; Song, Z.; Hu, J. Research on Credit Card Fraud Classification Based on GA-SVM. In Proceedings of the 2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE), Changsha, China, 26–28 March 2021; IEEE: Changsha, China, 2021; pp. 1076–1080. [CrossRef]
35. Aung, M.H.; Seluka, P.T.; Fuata, J.T.R.; Tikoisuva, M.J.; Cabealawa, M.S.; Nand, R. Random Forest Classifier for Detecting Credit Card Fraud based on Performance Metrics. In Proceedings of the 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Gold Coast, Australia, 16–18 December 2020; IEEE: Gold Coast, Australia, 2020; pp. 1–6. [CrossRef]
36. Ileberi, E.; Sun, Y.; Wang, Z. A Machine Learning based Credit Card Fraud Detection using the GA Algorithm for Feature Selection. *J. Big Data* **2022**, *9*, 24. [CrossRef]
37. Gambo, M.L.; Zainal, A.; Kassim, M.N. A Convolutional Neural Network Model for Credit Card Fraud Detection. In Proceedings of the 2022 International Conference on Data Science and Its Applications (ICoDSA), Bandung, Indonesia, 6–7 July 2022; IEEE: Bandung, Indonesia, 2022; pp. 198–202. [CrossRef]
38. Abd El-Naby, A.; Hemdan, E.E.-D.; El-Sayed, A. An Efficient Fraud Detection Framework with Credit Card Imbalanced Data in Financial Services. *Multimed. Tools Appl.* **2023**, *82*, 4139–4160. [CrossRef]
39. Karthika, J.; Senthilselvi, A. Credit Card Fraud Detection based on Ensemble Machine Learning Classifiers. In Proceedings of the 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 17–19 August 2022; IEEE: Coimbatore, India, 2022; pp. 1604–1610. [CrossRef]
40. Singh, A.; Ranjan, R.K.; Tiwari, A. Credit Card Fraud Detection under Extreme Imbalanced Data: A Comparative Study of Data-level Algorithms. *J. Exp. Theor. Artif. Intell.* **2022**, *34*, 571–598. [CrossRef]
41. Zioviris, G.; Kolomvatsos, K.; Stamoulis, G. Credit Card Fraud Detection using a Deep Learning Multistage Model. *J. Supercomput.* **2022**, *78*, 14571–14596. [CrossRef]
42. Malik, E.F.; Khaw, K.W.; Belaton, B.; Wong, W.P.; Chew, X. Credit Card Fraud Detection Using a New Hybrid Machine Learning Architecture. *Mathematics* **2022**, *10*, 1480. [CrossRef]
43. Negi, S.; Das, S.K.; Bodh, R. Credit Card Fraud Detection using Deep and Machine Learning. In Proceedings of the 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 9–11 May 2022; IEEE: Salem, India, 2022; pp. 455–461. [CrossRef]
44. Abdulghani, A.Q.; Ucan, O.N.; Alheeti, K.M.A. Credit Card Fraud Detection using XGBoost Algorithm. In Proceedings of the 2021 14th International Conference on Developments in eSystems Engineering (DeSE), Sharjah, United Arab Emirates, 7–10 December 2021; IEEE: Sharjah, United Arab Emirates, 2021; pp. 487–492. [CrossRef]
45. Alfaiz, N.S.; Fati, S.M. Enhanced Credit Card Fraud Detection Model Using Machine Learning. *Electronics* **2022**, *11*, 662. [CrossRef]
46. Tomar, P.; Shrivastava, S.; Thakar, U. Ensemble Learning based Credit Card Fraud Detection System. In Proceedings of the 2021 5th Conference on Information and Communication Technology (CICT), Kurnool, India, 10–12 December 2021; IEEE: Kurnool, India, 2021; pp. 1–5. [CrossRef]
47. Jovanovic, D.; Antonijevic, M.; Stankovic, M.; Zivkovic, M.; Tanaskovic, M.; Bacanin, N. Tuning Machine Learning Models Using a Group Search Firefly Algorithm for Credit Card Fraud Detection. *Mathematics* **2022**, *10*, 2272. [CrossRef]
48. Forough, J.; Momtazi, S. Sequential credit card fraud detection: A joint deep neural network and probabilistic graphical model approach. *Expert Syst.* **2022**, *39*, e12795. [CrossRef]
49. Razaque, A.; Frej, M.B.H.; Bektemyssova, G.; Amsaad, F.; Almiani, M.; Alotaibi, A.; Jhanjhi, N.Z.; Amanzholova, S.; Alshammari, M. Credit Card-Not-Present Fraud Detection and Prevention Using Big Data Analytics Algorithms. *Appl. Sci.* **2022**, *13*, 57. [CrossRef]
50. Ghosh, S.; Bilgaiyan, S.; Gourisaria, M.K.; Sharma, A. Comparative Analysis of Applications of Machine Learning in Credit Card Fraud Detection. In Proceedings of the 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 3–4 March 2023; IEEE: Mathura, India, 2023; pp. 1–7. [CrossRef]
51. Mahajan, A.; Baghel, V.S.; Jayaraman, R. Credit Card Fraud Detection using Logistic Regression with Imbalanced Dataset. In Proceedings of the 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 15–17 March 2023; IEEE: New Delhi, India, 2023; pp. 339–342.
52. Alabrah, A. An Improved CCF Detector to Handle the Problem of Class Imbalance with Outlier Normalization Using IQR Method. *Sensors* **2023**, *23*, 4406. [CrossRef]
53. Gupta, P.; Varshney, A.; Khan, M.R.; Ahmed, R.; Shuaib, M.; Alam, S. Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques. *Procedia Comput. Sci.* **2023**, *218*, 2575–2584. [CrossRef]
54. Jose, S.; Devassy, D.; Antony, A.M. Detection of Credit Card Fraud Using Resampling and Boosting Technique. In Proceedings of the 2023 Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA), Ernakulam, India, 20–21 January 2023; IEEE: Ernakulam, India, 2023; pp. 1–8. [CrossRef]

55. Tanapanichkan, S.; Kosolsombat, S.; Luangwiriya, T. Credit Card Fraud Detection Using Machine Learning. In Proceedings of the 2024 IEEE International Conference on Cybernetics and Innovations (ICCI), Chonburi, Thailand, 29–31 March 2024; IEEE: Chonburi, Thailand, 2024; pp. 1–5. [CrossRef]
56. Menon, P.P.; Sachdeva, A.; M, G.V. Fraud Shield: Credit Card Fraud Detection with Ensemble and Deep Learning. In Proceedings of the 2024 4th International Conference on Pervasive Computing and Social Networking (ICPCSN), Salem, India, 3–4 May 2024; IEEE: Salem, India, 2024; pp. 224–230. [CrossRef]
57. Mostafa, N.; Helmy, M.M.; Hatem, F.; Hani, J.; Nabil, L.M.; AbdElminaam, D.S. ML_MastercardFraud | Machine Learning's Mastery in Credit Card Fraud Detection. In Proceedings of the 2024 Intelligent Methods, Systems, and Applications (IMSA), Giza, Egypt, 13–14 July 2024; IEEE: Giza, Egypt, 2024; pp. 259–266. [CrossRef]
58. Jonsson, S. Credit risk: An agent-based model of post-credit decision actions and credit losses in banks. In *Agent-Based Modeling and Simulation*; Taylor, S.J.E., Ed.; Palgrave Macmillan: London, UK, 2014; pp. 185–207. [CrossRef]
59. Jonsson, S. The Effects of Reward System on Bank Credit Losses—An Agent-Based Model. *Manag. Financ.* **2015**, *41*, 908–924. [CrossRef]
60. Alexandre, M.; Lima, G.T. Macroeconomic Impacts of Trade Credit: An Agent-Based Modeling Exploration. *EconomiA* **2020**, *21*, 130–144. [CrossRef]
61. Liu, X.; Zhang, W.; Xiong, X.; Shen, D.; Zhang, Y. Credit rationing and the simulation of bank-small and medium sized firm artificial credit market. *J. Syst. Sci. Complex.* **2016**, *29*, 991–1017. [CrossRef]
62. Catullo, E.; Palestrini, A.; Grilli, R.; Gallegati, M. Early Warning Indicators and Macro-Prudential Policies: A Credit Network Agent Based Model. *J. Econ. Interact. Coord.* **2018**, *13*, 81–115. [CrossRef]
63. Catullo, E.; Giri, F.; Gallegati, M. Macro and Microprudential Policies: Sweet and Lowdown in a Credit Network Agent-Based Model. *Macroecon. Dyn.* **2021**, *25*, 1227–1246. [CrossRef]
64. Erlingsson, E.J.; Teglio, A.; Cincotti, S.; Stefansson, H.; Sturluson, J.T.; Raberto, M. Housing Market Bubbles and Business Cycles in an Agent-Based Credit Economy. *Economics* **2014**, *8*, 20140008. [CrossRef]
65. Dosi, G.; Fagiolo, G.; Napoletano, M.; Roventini, A. Income Distribution, Credit and Fiscal Policies in an Agent-Based Keynesian Model. *J. Econ. Dyn. Control* **2013**, *37*, 1598–1625. [CrossRef]
66. Russo, A.; Riccetti, L.; Gallegati, M. Increasing Inequality, Consumer Credit and Financial Fragility in an Agent Based Macroeconomic Model. *J. Evol. Econ.* **2016**, *26*, 25–47. [CrossRef]
67. Cornalba, F.; Disselkamp, C.; Scassola, D.; Helf, C. Multi-objective reward generalization: Improving performance of Deep Reinforcement Learning for applications in single-asset trading. *Neural Comput. Appl.* **2024**, *36*, 619–637. [CrossRef]
68. Kochliaridis, V.; Kouloumpris, E.; Vlahavas, I. Combining deep reinforcement learning with technical analysis and trend monitoring on cryptocurrency markets. *Neural Comput. Appl.* **2023**, *35*, 21445–21462. [CrossRef]
69. Tahvonen, O.; Suominen, A.; Malo, P.; Viitasaari, L.; Parkatti, V.-P. Optimizing high-dimensional stochastic forestry via reinforcement learning. *J. Econ. Dyn. Control* **2022**, *145*, 104553. [CrossRef]
70. Wu, B.; Li, L. Reinforcement learning for continuous-time mean-variance portfolio selection in a regime-switching market. *J. Econ. Dyn. Control* **2024**, *158*, 104787. [CrossRef]
71. Liu, W.; Xiang, S.; Zhang, T.; Han, Y.; Guo, X.; Zhang, Y.; Hao, Y. Judgmentally adjusted Q-values based on Q-ensemble for offline reinforcement learning. *Neural Comput. Appl.* **2024**, *36*, 15255–15277. [CrossRef]
72. Dang, T.K.; Tran, T.C.; Tuan, L.M.; Tiep, M.V. Machine Learning based on Resampling Approaches and Deep Reinforcement Learning for Credit Card Fraud Detection Systems. *Appl. Sci.* **2021**, *11*, 10004. [CrossRef]
73. Mead, A.; Lewris, T.; Prasanth, S.; Adams, S.; Alonzi, P.; Beling, P. Detecting Fraud in Adversarial Environments: A Reinforcement Learning Approach. In Proceedings of the 2018 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 27 April 2018; IEEE: Charlottesville, VA, USA, 2018; pp. 118–122. [CrossRef]
74. Vimal, S.; Kayathwal, K.; Wadhwa, H.; Dhama, G. Application of Deep Reinforcement Learning to Payment Fraud. *arXiv* **2021**. [CrossRef]
75. Tekkali, C.G.; Natarajan, K. RDQN: Ensemble of Deep Neural Network with Reinforcement Learning in Classification based on Rough Set Theory for Digital Transactional Fraud Detection. *Complex Intell. Syst.* **2023**, *9*, 5313–5332. [CrossRef]
76. Handhika, T.; Sabri, A.; Murni, M. Reinforcement Learning on Credit Risk-Based Pricing. In Proceedings of the 2021 2nd International Conference on Computational Methods in Science & Technology (ICCMST), Mohali, India, 17–18 December 2021; IEEE: Mohali, India, 2021; pp. 233–236. [CrossRef]
77. Hassani, B.K. Societal Bias Reinforcement through Machine Learning: A Credit Scoring Perspective. *AI Ethics* **2021**, *1*, 239–247. [CrossRef]
78. Herasymovych, M.; Märka, K.; Lukason, O. Using Reinforcement Learning to Optimize the Acceptance Threshold of a Credit Scoring Model. *Appl. Soft Comput. J.* **2019**, *84*, 105697. [CrossRef]

79. Hu, Y.-J.; Lin, S.-J. Deep Reinforcement Learning for Optimizing Finance Portfolio Management. In Proceedings of the 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 4–6 February 2019; IEEE: Dubai, United Arab Emirates, 2019; pp. 14–20. [CrossRef]
80. Zejnullahu, F.; Moser, M.; Osterrieder, J. Applications of Reinforcement Learning in Finance—Trading with a Double Deep Q-Network. *arXiv* **2022**. [CrossRef]
81. Li, Z.; Liu, X.-Y.; Zheng, J.; Wang, Z.; Walid, A.; Guo, J. FinRL-Podracer: High Performance and Scalable Deep Reinforcement Learning for Quantitative Finance. In Proceedings of the ICAIF '21: Proceedings of the Second ACM International Conference on AI in Finance, Virtual, 3–5 November 2021; Cornell University: Ithaca, NY, USA, 2021; pp. 1–9. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.