Review

JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)

Vol.32; No.2.| 2024

Survey of Fraud Detection Techniques for Credit Card Transactions

Ola Imran Obaid [1*], Ali Yakoob Al-Sultan [2]

1,2 College of Science for Women-Computer Science Dept, University of Babylon, Babylon, Iraq

[1]ola.alghazaly.gsci135@student.uobabylon.edu.iq, [2]ali.alsultan@uobabylon.edu.iq

***Corresponding author email:** ali.alsultan@uobabylon.edu.iq; mobile: 07832406409

تقنيات كشف الاحتيال لمعاملات بطاقات الائتمان: دراسة استقصائية

علا عمران عبيد[1]، علي يعكوب السلطان [2]

1،2 كلية العلوم للبنات، جامعة بابل، الحلة، بابل، العراق

[1]ola.alghazaly.gsci135@student.uobabylon.edu.iq, [2]ali.alsultan@uobabylon.edu.iq

Accepted: 30/4/2024 **Published:** 30/6/2024

ABSTRACT

With the rapid advancement of Internet technology in recent years, online financial transactions have become increasingly popular for purchasing a wide range of goods and services over the Internet, owing to their numerous advantages. The widespread adoption of credit cards has thus heightened the potential for abuse. Present a significant menace to users as a result of pervasive fraudulent operations. Credit card fraud has become an essential concern in today's digital era, posing substantial financial losses and security risks for financial institutions and consumers. In response to this growing challenge, researchers and industry experts have continuously developed and refined fraud detection techniques to safeguard against fraudulent activities. This survey paper aims to provide a comprehensive overview of the latest advances in fraud detection techniques for credit card transactions. Explore various methodologies, data sources, and machine learning algorithms used in fraud detection systems. Additionally, they discuss the challenges these systems face.

Keywords: Fraud Detection; Anomaly Detection; Credit Cards; deep learning; long short-term memory.

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

INTRODUCTION

Anomaly detection is a crucial component of data mining, wherein the primary aim is to discern atypical or aberrant data within a provided dataset. The field of anomaly detection is intriguing due to its ability to identify and uncover noteworthy and infrequent patterns within datasets autonomously [1]. The detection of anomalies is extensively employed in a diverse range of applications. Illustrative instances comprise the identification of fraudulent activities and the surveillance of medical conditions. One instance of a medical application is using heart rate monitors [2]. A further illustration can be found in the identification of irregularities within the transactional data of a credit card, which could potentially signify instances of theft [3].

The proliferation of websites and mobile applications has led to the widespread adoption of online financial transactions to acquire various goods and services via the Internet. This trend can be attributed to several advantages, including the convenience of use, the immediate purchasing process, and the ability to purchase at any time and from any location. The issue pertains to the proliferation of fraudulent online transactions resulting from the convenience of conducting financial activities on the Internet. Unauthorized individuals can pilfer financial credentials, leading to substantial monetary losses for users. This pervasive problem necessitates a concerted effort to address it by implementing cutting-edge programming methodologies [4].

The researchers implemented additional security measures to safeguard users' financial credentials on internet websites and applications. These security layers aim to ensure a secure and protected online purchasing experience for users. They impede attackers from illicitly obtaining users' financial credentials, including sensitive financial information such as credit card numbers, dates of expiration, and card security codes. Attackers may exploit these credentials to engage in unauthorized purchases or withdraw funds from banking accounts unlawfully [5].

Furthermore, a necessity has emerged to employ detection systems designed to identify potentially illicit activities while completing financial transactions via the Internet. Credit card companies have recently employed specialized investigators to examine fraudulent financial transactions. However, this process is perceived as time-consuming and necessitates analyzing each fraudulent transaction. Consequently, only a limited number of fraudulent transactions are scrutinized daily, leaving the majority unchecked. Conversely, credit card users promptly report instances of fraud to the credit card company upon detecting and acknowledging such illicit transactions [6].

In 2016, the aggregate value of fraudulent transactions inside the Single Euro Payments Area (SEPA) reached EUR 1.8 billion. Based on the findings of the Nilsson Report, an authoritative source that analyzes worldwide payment systems, the cumulative financial impact of fraudulent activities in 2018 was recorded at a substantial sum of USD 27.85 billion. Projections indicate that this figure is anticipated to escalate to USD 35.67 billion by 2023 [7], as shown in Figure 1.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

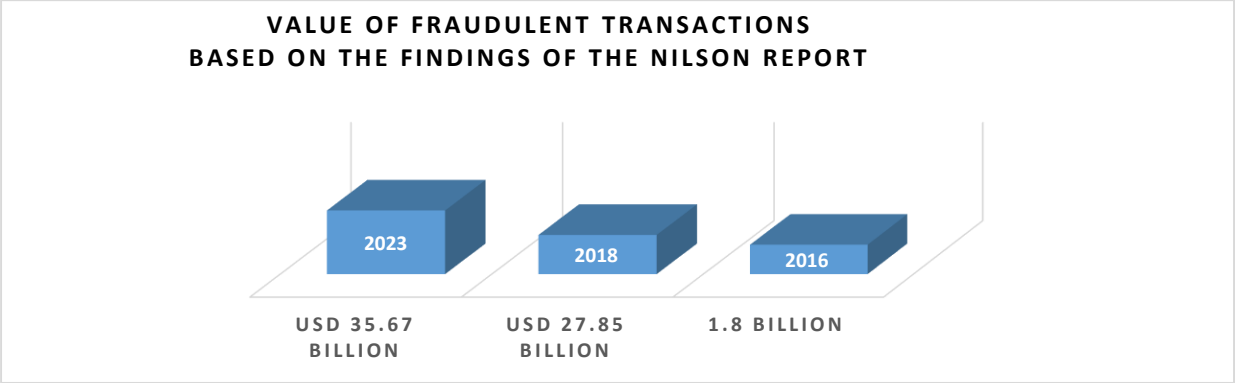

Figure 1: Value of fraudulent transactions inside the Single Euro Payments Area (SEPA)

In order to tackle this matter, financial institutions and digital payment providers employ anti-fraud mechanisms to identify fraudulent transactions. Due to their robust prediction capabilities, machine learning (ML) and deep learning (DL) have garnered significant interest as effective methods for fraud detection systems. In ML/DL-based approaches, the input characteristics of models often consist of card transaction data, including information such as the identity of cardholders and the amount of money involved. The outputs of these models are confidence scores, which establish a probability space used to determine whether a transaction is genuine or fraudulent [8].

RELATED WORKS

The present study light on the growing worry around the occurrence of credit card fraud due to routine financial activities. The advent of machine learning methodologies has facilitated the fraud detection processes, enabling fast identification of online fraudulent activities. The primary aim of this study is to determine the most efficient algorithm for the identification and detection of fraudulent activities related to credit card transactions.

The present study conducted a comparative analysis of two machine learning algorithms, namely Isolation Forest and Local Outlier Factor. This paper analyzes the Kaggle data set for European credit card transactions. Accuracy of 97% by Local Outlier Factor and 76% by Isolation Forest [9].

This paper studies deep learning methods (CNN, LSTM) for credit card fraud detection and compares their performance with machine learning algorithms (SVM, LR, DT) on three different datasets, European Card Data (ECD) contains 284,807 samples and 31 features, Small Card Data (SCD) containing 3075 samples and 12 features and Tall Card Data (TCD) containing 10 million samples (rows) and 9 features (columns). Experimental results show great performance against traditional models, suggesting their effectiveness in real-world systems. Sampling methods address the class imbalance problem, F1-Score 84.85% to LSTM [10].

This project proposes a model to detect credit card fraud using machine learning. Using a random forest algorithm and decision trees. The results show on dataset credit card transactions, with the best accuracy for RF being 98.6% [11].

This paper presents a model for predicting legitimate transactions or fraud on European dataset credit cards. The proposed model is OSCNN (Oversampling with Convolution Neural Network), which is based on oversampling preprocessing using SMOTE and CNN (convolution neural network). The proposed model achieved better results with 98.9% accuracy [12].

In this paper, a Deep Convolutional Neural Network (DCNN) is proposed for real-time credit card fraud detection, learning complex patterns dynamically on a 5 million transaction dataset with 6223 fraud records. Tested against other machine learning techniques, it achieved a 99% accuracy [13].

The objective of this study is to assess the effectiveness of three unsupervised machine learning methods: Local Outlier Factor, Isolation Forest Algorithm, and K-means clustering. The initial stage involves partitioning the dataset into three distinct proportions:1. 60 % train, 40 % test (accuracy of IF was 99.7787 %LOF 99.6752 % K -Means 53.9978 %) .2. 70 %train, 30 %test (accuracy of IF was 99.7799 %, LOF 99.6804 %, K- Means 53.8756 %). 3. 80 %train, 20 %test (accuracy of IF was 99.7928 %, LOF 99.6804 %, K-Means 53.9043 %). The results indicate that the Isolation Forest method exhibits superior performance compared to the other two algorithms on the European dataset credit card [14].

The primary objective of this paper is the reduction of both undetected fraudulent activities and false positive alarms. This is achieved by integrating the output scores from three independent deep learning models: convolutional neural networks (CNN), auto encoders (AE), and recurrent neural networks (RNN). The experimental results were conducted on a European dataset credit card, with an accuracy of 94.9% [5].

The objective of this study is to identify instances of fraudulent activity. Various machine learning methods, including a Decision Tree, Random Forest, Support Vector Machine, Logistic Regression, and XG Boost, have been employed in the domain of fraud detection. A comparative analysis was conducted on machine learning and convolutional neural network models comprising 20 layers. The analysis utilized the European card benchmark dataset. The proposed model exhibits superior performance compared to existing machine learning and deep learning methods in the context of credit card recognition challenges. The results showed improved accuracy, f1-score, and precision, 99.9%, 85.71%, and 93%, respectively [15].

This paper involves comparing the performance, accuracy, and efficiency of several Machine Learning techniques, namely Support Vector Machine, Random Forest, logistic regression, and K-Nearest Neighbor. These classifiers are applied to analyze prediction outcomes on both credit card European datasets from Kaggle. This study demonstrates that the K-nearest neighbors (KNN) algorithm is a superior classifier for the detection of credit card fraud accuracy of 0.958 [16].

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

This study discusses a system that effectively identifies fraud; the suggested system incorporates the Support Vector Machine (SVM) classification algorithm. This approach is utilized to effectively detect instances of fraud and mitigate the risk of overfitting. The findings indicate that the dataset used was obtained from the Kaggle platform. An accuracy 94.9%, precision 95.9%, Recall 95.1%, F1-score 95.1% [17].

This paper aims to examine two preprocessing strategies utilizing a European dataset credit card. Additionally, ensemble classifiers, namely Random Forest, CatBoost, and XGBoost, are employed. The findings indicate that employing the RUS approach in conjunction with the CAE method yields the most optimal outcomes in detecting credit card fraud. The F1 score achieved a value of 91.1%[18].

This study presents an unsupervised attentional anomaly detection-based credit card fraud detection network, referred to as UAAD-FDNet. The network comprises a generator and a discriminator. One of the methods employed in this study is the utilization of an auto encoder with Feature Attention. This technique is utilized to reconstruct the input transaction samples in order to generate synthetic transaction data that closely resembles real transaction data. Compared to machine learning techniques, including Support Vector Machines (SVM), Decision Trees (DT), XG Boost, K-Nearest Neighbors (KNN), and Random Forests (RF), as well as existing deep learning approaches, such as Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNN), Multilayer Perceptron (MLP), and Auto encoder (AE). The experimental findings UAAD-FD Net on IEEE Fraud Detection Dataset AUC 0.8556, Recall 0.6281 and on the Kaggle Credit Card Fraud dataset AUC 0.9515, Recall 0.7553 demonstrate that the proposed method successfully addresses the issue of data imbalance [19]. Table 1 presents the data type, methodology, and findings from related works.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Table 1. Results of fraud detection techniques

Cite	Database used	Method used	All Results
[9]	European dataset credit card	isolation forest and local outlier detection	accuracy of 97% by Local Outlier Factor and 76% by Isolation Forest
[10]	Three datasets: European Card Data, Small Card Data, and Tall Card Data.	(CNN, LSTM) and comparison with different machine learning algorithms (DT, LR, SVM)	F1-Score 84.85% to LSTM
[11]	dataset credit card transaction	RF	accuracy for RF 98.6%.
[12]	European dataset credit card	OSCNN (Oversampling with Convolution Neural Network), which is based on oversampling preprocessing, and CNN (convolution neural network)	Accuracy: 98.9%
[13]	dataset credit card transactions	The Deep Convolution Neural Network (DCNN) scheme	Accuracy: 99%.
[14]	European dataset credit card	Isolation forest (IF), Local Outlier (LO) and K-Means	1. 60 % train, 40 % test (accuracy of IF was 99.7787%, LO 99.6752 % K -Means 53.9978 %) 2.70% train, 30%test (accuracy of IF was 99.7799%, LO 99.6804 %, K-Means 53.8756 %). 3. 80% train, 20% test (accuracy of IF was 99.7928 %, LO 99.6804 %, K-Means 53.9043 %)
[5]	European dataset credit card	proposed a majority voting-based ensemble technique that combines three deep learning algorithms CNN, auto-encoder, and RNN	Accuracy (94.9%)
[15]	European dataset credit card	convolutional neural network with 20 layers	Accuracy 99.9%, F1-score 85.71% and precision 93%,
[16]	European dataset credit card	Several techniques used are Support Vector Machine, Random Forest, logistic regression, and K-Nearest Neighbor	KNN is a better classifier with an accuracy of 0.958
[17]	Data credit card	Support vector machine	Accuracy 94.9%
[18]	European dataset credit card	the RUS(random under sampling) method followed by CAE (Convolutional Auto encoder)	F1 score 91.1%
[19]	IEEE-CIS and European Fraud Detection Dataset.	a new Unsupervised Attentional Anomaly Detection Network-based Credit Card Fraud Detection framework (UAAD-FDNet)	UA AD-FD Net on IEEE Fraud Detection Dataset AUC 0.8556 and Credit Card Fraud Detection Dataset AUC 0.9515

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

DATASET

The dataset from Kaggle used for fraud detection in the IEEE-CIS has four files: train transaction, train identity, test transaction, and test identity [19]. These files include 394, 41, 393, and 41 columns of characteristics, respectively. European dataset credit card from Kaggle consists of a total of 284,807 transactions, out of which 492 transactions are identified as fraudulent [5,9,10,12,14,15,16,18]. Three different datasets from Kaggle, European Card Data (ECD) contains 284,807 samples and 31 features; Small Card Data (SCD) includes 3075 samples and 12 features; and Tall Card Data (TCD) contains 10 million samples (rows) and nine features (columns) [10]. Table 2 displays the various types of data utilized for the identification of financial fraud.

Table 2. Dataset used for credit cards fraud detection.

Dataset	Number of transactions	Fraud instances
IEEE-CIS Fraud Detection Dataset.	590,540	20,663
European dataset credit card	284.807	492
Three different datasets credit card fraud	Dataset 1 284.807, Dataset 2 3075 Dataset3 10 million	Dataset 3 28,000

Types of credit card fraud

In this paper, review the types of credit cards as shown below.

1. Application fraud occurs when an individual illicitly obtains control over an application system via unauthorized access to sensitive user information, such as passwords and usernames, to create a fraudulent account. It typically occurs in the context of identity theft. When an individual engaged in fraudulent activities submits an application for credit or a new credit card using the identity of a legitimate cardholder. The individual engaged in fraudulent activities appropriates the accompanying documentation to bolster or validate their deceitful application.
2. Card ID theft is a form of fraudulent activity resembling application scams. Identity theft is the unauthorized acquisition of personal information from an initial cardholder, which a fraudulent individual then utilizes to exploit an existing card or establish a new account. Identifying this particular form of fraudulent activity poses significant challenges.
3. The phenomenon of false merchant sites bears similarity to phishing attacks, wherein customers are ensnared by fraudulent individuals who develop deceptive web pages that closely mimic legitimate websites. This webpage potentially provides various discounts as a means to incentivize customers to make purchases of the available products. After the completion of the transaction, the fraudster collects all the relevant information pertaining to the transaction and thereafter utilizes it to engage in fraudulent trades [20].

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

The Challenges Associated with Credit Card Fraud Detection

The proposed paper aims to address several challenges in anomaly detection for financial transaction

1. The credit card fraud detection data exhibits an imbalance. The proportion of illegal transactions in credit card purchases is relatively tiny. The complexity and inaccuracy of identifying fraudulent operations are evident in this dataset.
2. The data indicates a potential interference: there may be an increase in transactions that could be mistakenly classified as illegal (false positives), as well as illegal purchases that may appear legitimate (false negatives). The issue of high false positive and false negative rates in fraud detection algorithms is a significant challenge in the field [21].
   One common challenge encountered by classification algorithms is the limited ability to detect novel normal or fraudulent patterns, thereby resulting in a lack of adaptability. The efficacy of supervised and unsupervised fraud detection systems in identifying novel patterns of normal and fraudulent behavior is limited [22].

Fraud Detection Techniques

Given the exponential growth of data, discerning significant patterns within datasets has become exceedingly challenging for human programmers and specialists. Due to this rationale, machine learning has been prevalent across several areas within the field of computer science, particularly in cases where the extraction of information from extensive datasets is necessary. The applications encompass a wide range of functionalities, such as filtering out spam, online searching, face and voice recognition, rating credit, and identifying fraud. Supervised learning and unsupervised learning are the two predominant machine learning approaches that have gained widespread adoption. Supervised learning involves training the algorithm using pre-existing labeled datasets, enabling it to learn from the provided annotations. On the other hand, unsupervised learning involves unlabeled training data to facilitate the algorithm's discovery of patterns and relationships inherent in the input data [23].

Logistic Regression (LR)

The technique is widely employed in previous studies focused on detecting instances of fraud at an early stage. Despite their ease of implementation, these methods have low efficacy in addressing non-linear data, rendering them inadequate for complicated fraud detection challenges [23]. The logistic regression algorithm leverages the sigmoid function to perform binary classification by considering several factors in the dataset. The sigmoid function is depicted in the following manner as shown in equation1; the function is linear as shown in equation 2 [24] :

$$Y^i = \frac{1}{1+e^{-(z)}} \quad (1)$$

$$z = b + m1x1 + m2x2 + \cdots mnxn \quad (2)$$

The Sigmoid function is employed to determine the probability of binary classification. In the given equation, the variable y represents the probability associated with the output. In linear regression, m represents the weighted values, b represents the bias, and x represents the highlighted values. The probability of a specific outcome is estimated using the sigmoid function [24]. Logistic regression is commonly employed for binary classification tasks, where the outcome variable can take on one of two values, typically denoted as 1 or 0. In this context, a threshold of 0.5 is typically utilized to determine the predicted class. Specifically, any predicted value exceeding this threshold is assigned the class label 1, while any value falling below the threshold of 0.5 is assigned the class label 0 [25].

Decision Tree (DT)

Researchers have used the Decision Tree (DT) classifier to construct fraud detection models. The methods can be readily implemented, visualized, and comprehended. Although decision trees (DTs) offer flexibility and interpretability, they can exhibit instability and high sensitivity when confronted with imbalanced class distributions [23]. The decision tree is a form of supervised learning that requires training on a dataset consisting of fraudulent transaction data. The dataset is partitioned based on decision nodes, while the tree leaves hold the ultimate result. In the case of this specific dataset, the decision tree is structured such that the leaf nodes store the ultimate class label while the pathways represent the corresponding outcomes. In the context of decision trees, partitioning data is carried out recursively, employing either breadth-first or depth-first search [24].

Support Vector Machine (SVM)

Support Vector Machines (SVMs) represent a type of supervised algorithm utilized in the domain of supervised learning, specifically for addressing classification and regression problems [25]. Support Vector Machines (SVMs) have demonstrated their efficacy in various classification tasks, such as fraud detection, due to their capacity to operate effectively in high-dimensional feature spaces without incurring additional computing complexity. The inherent characteristic of Support Vector Machines (SVMs) allows for the resolution of non-linear classification issues, such as those encountered in fraud detection scenarios [23]. The objective of this technique is to identify an optimal hyperplane that can effectively separate a given dataset (specifically, a transaction dataset) into distinct classes. These classes consist of a group of fraudulent transactions and a group of legitimate transactions. The hyperplane is determined by a set of support vectors, which are the points closest to the hyperplane. These support vectors are then utilized to predict the class to which a new data point belongs. The Support Vector Machine (SVM) model is constructed through the process of training it with historical datasets in order to

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

acquire the anticipated output. After achieving the intended outcome, the trained model is applied to a new dataset in order to achieve the output. Therefore, it can be utilized to categorize fraudulent or legitimate transactions [26].

The K-Nearest Neighbor (KNN)

The K-nearest neighbor (KNN) algorithms are employed to identify instances of credit card fraud. The technique is classified as a supervised learning technique [27]. This strategy was initially employed by Aha, Albert, and Kibler in 1991. The outcomes of the K-nearest neighbors (KNN) algorithm is contingent upon two primary factors:

1. The selection of an appropriate distance metric to determine the nearest neighbors.
2. The number of neighboring instances considered for classifying the new sample.

The K-nearest neighbors (KNN) algorithm for credit card fraud detection relies on two critical estimations: the calculation of distance or similarity measures between pairs of data instances. In the K-nearest neighbors (KNN) algorithm, each incoming transaction is evaluated to determine its proximity to the nearest point of the new incoming transaction. If the incoming transaction is fraudulent, the algorithm will classify it as such. Various approaches can be employed to calculate the distance between two data instances, with the most utilized one being the Euclidean distance. This approach involves including authentic and deceptive instances to train the datasets. This approach has a high level of efficiency, characterized by rapid processing time and a low incidence of erroneous notification [28].

Random Forest (RF)

The random forest algorithm is widely recognized as a supervised learning technique that can effectively address classification and regression problems. The system comprises numerous decision trees. This approach demonstrates improved performance when the forest has a more significant number of trees, mitigating the risk of overfitting in the model. Each decision tree within the forest yields specific outcomes. The merging of these results is performed to enhance the accuracy and stability of the forecast [29].

Neural networks (NN)

The neural network is a technique also used to detect unauthorized credit card usage. The neural network is a method based on the functioning concept of the human brain. Like the human brain, neural network likewise retains the existing knowledge and utilizes that information when needed. In identifying illicit credit card usage, neural networks split the input into distinct categories. It depends on the credit card holder's wages, career, and payment data frequency and counting of significant transactions. This detail will evaluate the future transaction, whether the transaction is fraudulent or authentic. It has three unique types of layers [30].

1. Input Layer: Input nodes are used to identify the cardholder details, and using this information will validate the uniqueness of the transaction.

2. Hidden Layer: It performs neural network operation to identify whether the transaction is authenticated.
3. Output Layer: After analyzing the transaction, output nodes give the outcome value between 0 and 1 [30].

K means

Clustering is a widely recognized unsupervised method commonly employed in fraud detection. One example of a clustering method is K-Means (KM), known for its simplicity and efficiency. KM can divide unlabeled samples into K distinct clusters. Despite their simplicity and ease of implementation, KM clustering methods are highly susceptible to the initial selection of cluster centers, which is done randomly. KM algorithms are susceptible to outliers [14]. The K-means clustering algorithm is widely employed as a primary approach for distinguishing between fraudulent and legitimate transactions. Certain variables are often declared during a transaction; examples of sensitive information that may be involved in a transaction include the total amount of the transaction, the credit card number used, the date and identification number of the transaction, the country in which the transaction occurred, and the merchant category identification. It is necessary to provide a credit card number. The provided information will be stored in the transaction dataset. The subsequent step involves assigning a cluster designation to each transaction type, categorizing them as either a small cluster, a big cluster, and a dangerous cluster. The k-means algorithm will utilize the transaction details. A notice is displayed when a transaction is determined to be fraudulent or legitimate [30].

Self-Organizing Map (SOM)

The SOM is a sort of neural network adopting unsupervised learning that configures the network's neurons according to the input data's topological structure. This process is known as self-organization, which iteratively optimizes the weights of neurons to resemble the input data, resulting in clustering. The neurons in a SOM are arranged in a matrix structure that maps inputs from a high-dimensional space to the two-dimensional array of neurons. This mapping is designed to model similar input vectors as neurons closer together in the final matrix, offering visualization of the input. Various distance measures can be used throughout the iterative training phase to group the nodes, such as Euclidean and Manhattan distances. After training, the data in the data set becomes sorted into legitimate or fraudulent sets by self-organization, and all new transaction after that similarly experiences the same process before being sent into the SOM [31].

Isolation Forest (IF)

The isolation forest is a tree-based model that has been designed for the purpose of detecting outliers. The technique is founded on the principle that anomalies are characterized by their rarity and distinctiveness within the dataset. These characteristics give rise to a sensitive system to irregularities, commonly referred to as Isolation. This method exhibits basic differences from

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

all other established methods and possesses significant utility. In order to identify abnormalities, this approach differs from traditional distance and density assessments and instead includes the concept of isolation, which proves to be a more efficient and successful method [9].

Deep Learning-Based Fraud Detection

Deep learning has emerged as a prominent paradigm in machine learning, characterized by utilizing several hidden layers to yield better outcomes than other machine learning methods. The hidden layers of the system possess a significant computational capacity, enabling them to attain a notable level of precision [32]. The data contained within online payment records is classified as big data due to its vast volume, including millions of transactions [33]. Traditional machine learning techniques may be insufficient in effectively processing and analyzing large volumes of data. Additionally, several algorithms exhibit a saturation phenomenon when their performance reaches a maximum at a specific data quantity and does not improve further with additional data size. In contrast, deep learning exhibits a distinct characteristic whereby its performance consistently improves as the volume of data is expanded. Therefore, it is possible to analyze and categorize this extensive volume of transactions into legitimate and fraudulent transactions. Several examples of neural networks commonly used in deep learning include Convolutional Neural Networks (CNNs), Auto encoders, and Recurrent Neural Networks (RNN) [34].

Convolutional Neural Networks (CNN)

Convolutional neural networks (CNNs) have primarily been employed for tasks involving pattern identification in images, as the input data is typically represented in matrix format, making CNNs particularly suitable for such tasks. Nevertheless, it has been empirically shown that these techniques can be effectively utilized in other disciplines and areas by manipulating the input data structure [35]. The Convolutional Neural Network (CNN) is a kind of deep learning architecture initially proposed in the 1990 [31]. It is defined by its multi-layered structure, which can be classed into distinct levels: input, convolution, pooling, fully connected, and output. The convolution process is executed within the convolutional layer to extract features obtained from the input data. Various filters are employed in the convolution operation, serving as detectors of features. The max pooling layer is employed to decrease the dimensionality of the feature maps generated by the convolutional layer while preserving the most critical data. The fully connected and output layers are components of a conventional densely connected feedforward neural network, also known as a multi-layer perceptron [36]. These layers receive input from the convolutional and max pooling layers and are responsible for classifying the data, explicitly distinguishing between valid and fraudulent transactions [37].

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Auto encoder

The Auto-Encoder is an unsupervised deep learning technique [31]. This model has been designed to acquire knowledge from a dataset that possesses a high number of dimensions while utilizing features that have a lower dimensionality. The proposed model employs an encoder to encode the input data and a decoder to decode and reproduce the data. It ensures that the number of input instances is equivalent to the number of output instances. An auto encoder consists of two primary components, namely the Encoder and the Decoder. The input, which corresponds to the number of features, is compression by the Encoder. This compression results in a reduction of the input size and the generation of a corresponding representation. This representation is then used in the decoder model at a later stage. The Decoder, as the second component, reconstructs the input utilizing the provided representation. The Auto-Encoder model has acquired knowledge of the characteristics included in legal records, resulting in a case where the input closely resembles the output upon execution. However, in the context of fraudulent transactions (anomalies), the input and output may differ when unexpected data is involved [5].

Long Short-Term Memory (LSTM)

Long Short-Term Memory Networks (LSTM) represent an expansion of recurrent neural networks (RNN), a deep neural network predominantly employed for analyzing time series data. Every neuron within a Long Short-Term Memory (LSTM) model is characterized as a cell that can retain information, preserving its internal state. The memory capacity of Long Short-Term Memory (LSTM) models can be attributed to the introduction of input and output "gates" into the cell structure. These gates were subsequently accompanied by the development of the forget gate [31]. The forget gate determines which information is kept from the preceding phase, while the input gate determines which information is added from the current step. Lastly, the output gate controls the choice of information from the current cell state that is utilized in generating the output [10].

In contrast to recurrent neural networks (RNNs), which operate by preserving the valuable output of a particular layer and reintroducing it as input for further processing within current data, hence aiding in the prediction of the layer's output [5]. Long Short-Term Memory (LSTM) models are presently considered the most advanced techniques in various practical domains, including text analysis, writing and speech recognition, and natural language processing. The application of Long Short-Term Memory (LSTM) models for fraud detection has emerged in recent years [38].

Performance Metrics

This section discusses the performance metrics employed to assess the efficiency and effectiveness of classification algorithms.

1. Accuracy is a metric that assesses the ratio of accurate predictions to the overall number of cases that have been assessed, as shown in equation 3 [39].

$$\boldsymbol{Accuracy} = \frac{\boldsymbol{TP+TN}}{\boldsymbol{TP+FP+FN+TN}} \quad \textbf{(3)}$$

2. Precision is a measure that computes the proportion of actual positive forecasts in relation to the overall count of positive predictions, as shown in equation 4 [39].

$$\boldsymbol{precision} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FP}} \quad \textbf{(4)}$$

3. Recall (Sensitivity): This metric is defined as the proportion of correctly anticipated positive cases in regard to the overall number of positive cases. The subsequent equation (5) is employed for the computation of recall [40].

$$\boldsymbol{recall} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FN}} \quad \textbf{(5)}$$

4. F1-score: is a performance metric that calculates the weighted arithmetic mean, considering each recall and precision, as shown in equation 6 [40].

$$\boldsymbol{F1-score} = \boldsymbol{2} * \frac{\boldsymbol{precision * recall}}{\boldsymbol{precision+recall}} \quad \textbf{(6)}$$

5. Specificity refers to the accuracy of correctly identifying negative cases, as shown in equation 7 [41].

$$\boldsymbol{Specificity} = \frac{\boldsymbol{TN}}{\boldsymbol{TN+FP}} \quad \textbf{(7)}$$

6. The Area Under the Curve (AUC) is a graphical representation that compares the true positive rate (sensitivity) to the false positive rate (specificity), as shown in equation 8 [42].

$$\boldsymbol{AUC} = (\textbf{Sensitivity} + \textbf{Specificity})/\,\boldsymbol{2} \quad \textbf{(8)}$$

Discussion and analysis of related work

Given the importance and volume of financial transactions, there can be a rise in transactions misclassified as illicit (false positives) and instances of illicit purchases that appear legal (false negatives). Accurately identifying fraud trends in real-time requires the use of complex mathematical calculations. Current situation. Deep learning has emerged as a prominent paradigm in machine learning and is characterized by multiple hidden layers to achieve better and relevant results in fraud detection and risk reduction; compared to previous related works, they were more accurate in identifying fraudulent transactions.

The primary goal of this study is to evaluate system robustness using metrics such as accuracy, precision, F1 score, recall, and AUC. A review of relevant prior research papers. In the Ref. [5,9-19] which focus on the detection of credit card fraud, is used to support this assessment. The research was conducted using a variety of machine-learning algorithms, and the results are shown in Figure 2 and Table 3, with an overall accuracy range between 94.90% and 99.90%.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Table 3. Reference with performance metrics [5, 9-19]

Ref. No.	Accuracy	Precision	F1-score	AUC	Recall
[5]	94.90	-	-	-	-
[9]	97	-	-	-	-
[10]	-	-	84.85	-	-
[11]	98.60	-	-	-	-
[12]	98.90	-	-	-	-
[13]	99	-	-	-	-
[14]	99.79	-	-	-	-
[15]	99.90	93	85.71	-	-
[16]	95.80	-	-	-	-
[17]	94.90	95.90	95.10		95.10
[18]	-	-	91.10	-	-
[19]	-	-	-	95.10	75.50

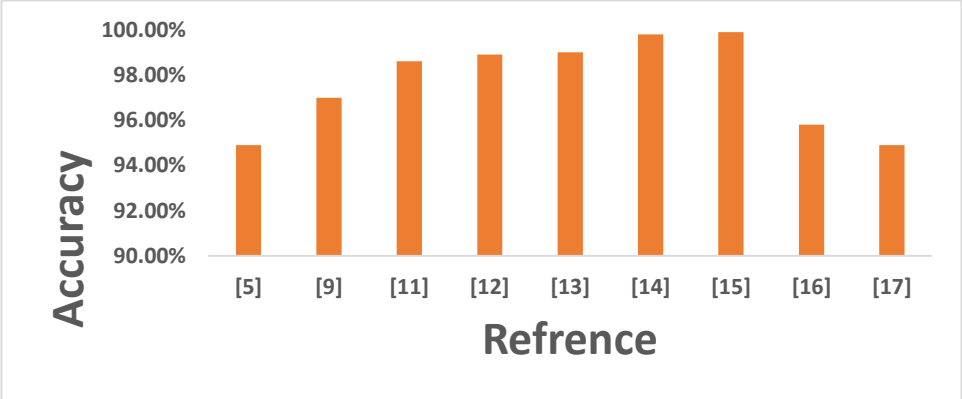

Figure 2. Reference with Accuracy metric [5,9, 11-17]

The overall precision, recall, AUC and F1-score range, as shown in Figure 3, between 75.50% and 95.90% to pertinent past study papers [10,15,17,18,19].

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

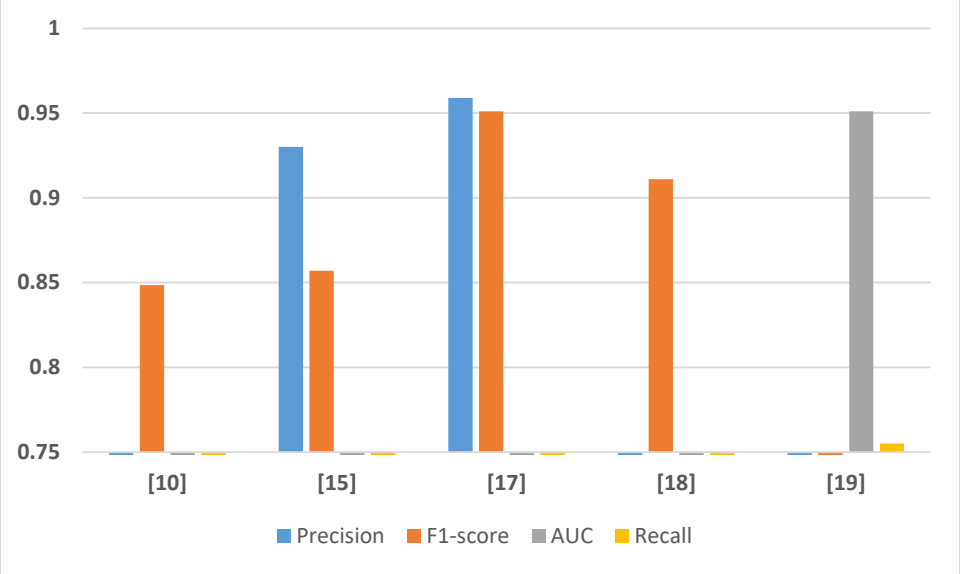

Figure 3. Reference with Performance metrics [10, 15, 17-19]

CONCLUSIONS:

This study provides a thorough analysis of machine learning techniques for credit card fraud detection issues. This study emphasized the importance of identifying fraud and its negative impacts on the financial sector. Thus, it is essential to create a model that can manage data rapidly and effectively. By lowering computational complexity and enhancing detection accuracy, these techniques have been shown to increase the efficacy of fraud detection systems.

ACKNOWLEDGEMENT

This study is supported by computer science department, college of science for women, University of Babylon.

Conflict of interests.

There are non-conflicts of interest.

References

[1] M. Ahmed, A. N. Mahmood, and M. R. Islam, "A survey of anomaly detection techniques in financial domain," *Futur. Gener. Comput. Syst.*, vol. 55, pp. 278–288, Feb. 2016, doi: 10.1016/j.future.2015.01.001.

[2] T. Schlegl, P. Seeböck, S. M. Waldstein, U. Schmidt-Erfurth, and G. Langs, "Unsupervised anomaly detection with generative adversarial networks to guide marker discovery," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10265 LNCS, pp. 146–147, 2017, doi: 10.1007/978-3-319-59050-9_12.

[3] A. B. Nassif, M. A. Talib, Q. Nasir, and F. M. Dakalbab, "Machine Learning for Anomaly Detection:

A Systematic Review," *IEEE Access*, vol. 9, pp. 78658–78700, 2021, doi: 10.1109/ACCESS.2021.3083060.
[4] Y. Lu, "Deep neural networks and fraud detection," *U.U.D.M. Proj. Rep.*, pp. 1–39, 2017.
[5] S. Al-Faqir and O. Ouda, "Credit Card Frauds Scoring Model Based on Deep Learning Ensemble," *J. Theor. Appl. Inf. Technol.*, vol. 100, no. 14, pp. 5223–5234, 2022.
[6] S. Sanober *et al.*, "An Enhanced Secure Deep Learning Algorithm for Fraud Detection in Wireless Communication," *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021, doi: 10.1155/2021/6079582.
[7] G. Moschini, R. Houssou, J. Bovay, and S. Robert-Nicoud, "Anomaly and Fraud Detection in Credit Card Transactions Using the ARIMA Model †," *Eng. Proc.*, vol. 5, no. 1, pp. 1–11, 2021, doi: 10.3390/engproc2021005056.
[8] T. Y. Wu and Y. T. Wang, "Locally Interpretable One-Class Anomaly Detection for Credit Card Fraud Detection," *Proc. - 2021 Int. Conf. Technol. Appl. Artif. Intell. TAAI 2021*, pp. 25–30, 2021, doi: 10.1109/TAAI54685.2021.00014.
[9] H. John and S. Naaz, "Credit Card Fraud Detection using Local Outlier Factor and Isolation Forest International Journal of Computer Sciences and Engineering Open Access Credit Card Fraud Detection using Local Outlier Factor and Isolation," no. April, 2019, doi: 10.26438/ijcse/v7i4.10601064.
[10] T. T. Nguyen, H. Tahir, M. Abdelrazek, and A. Babar, "Deep Learning Methods for Credit Card Fraud Detection," 2020.
[11] M. Computing, A. Nimisha, and A. Jyothsna, "CREDIT CARD FRAUD DETECTION," vol. 10, no. 4, pp. 71–79, 2021, doi: 10.47760/ijcsmc.2021.v10i04.011.
[12] A. Abd, "Deep Learning Approach for Credit Card Fraud Detection," 2021, doi: 10.1109/ICEEM52022.2021.9480639.
[13] J. I. Chen, "Deep Convolution Neural Network Model for Credit-Card Fraud Detection and Alert," vol. 03, no. 02, pp. 101–112, 2021, doi: 10.36548/jaicn.2021.2.003.
[14] A. Joshi, P. A. Limited, and V. Jain, "An Experimental Study using Unsupervised Machine Learning Techniques for Credit Card Fraud Detection An Experimental Study using Unsupervised Machine Learning Techniques for Credit Card Fraud Detection," no. July, 2021.
[15] M. Ramzan and M. Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," *IEEE Access*, vol. 10, pp. 39700–39715, 2022, doi: 10.1109/ACCESS.2022.3166891.
[16] M. J. Madhurya, H. L. Gururaj, B. C. Soundarya, K. P. Vidyashree, and A. B. Rajendra, "Exploratory analysis of credit card fraud detection using machine learning techniques," vol. 3, no. April, pp. 31–37, 2022, doi: 10.1016/j.gltp.2022.04.006.
[17] V. K. Gunjan, M. D. Ansari, G. N. Institutions, and R. Pathak, "Credit Card Fraud Detection Using Support Vector Machine," no. July, 2022, doi: 10.1007/978-981-16-6407-6.
[18] Z. Salekshahrezaee, J. L. Leevy, and T. M. Khoshgoftaar, "The effect of feature extraction and data sampling on credit card fraud detection," *J. Big Data*, vol. 10, no. 1, 2023, doi: 10.1186/s40537-023-00684-w.
[19] S. Jiang, R. Dong, J. Wang, and M. Xia, "Credit Card Fraud Detection Based on Unsupervised Attentional Anomaly Detection Network," *Systems*, vol. 11, no. 6, pp. 1–14, 2023, doi: 10.3390/systems11060305.
[20] Y. Jain, N. Tiwari, S. Dubey, and S. Jain, "A comparative analysis of various credit card fraud detection techniques," *Int. J. Recent Technol. Eng.*, vol. 7, no. 5, pp. 402–407, 2019.
[21] R. H. Alwan, M. M. Hamad, and O. A. Dawood, "A comprehensive survey of fraud detection methods in credit card based on data mining techniques A Comprehensive Survey of Fraud

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Detection Methods in Credit Card Based on Data Mining Techniques," vol. 020006, no. October, 2022, doi: 10.1063/5.0112422.

[22] Z. Zojaji, R. E. Atani, and A. H. Monadjemi, "A survey of credit card fraud detection techniques: Data and technique oriented perspective," *arXiv Prepr. arXiv1611.06439*, 2016.

[23] N. Yousefi, M. Alaghband, and I. Garibay, "A comprehensive survey on machine learning techniques and user authentication approaches for credit card fraud detection," *arXiv Prepr. arXiv1912.02629*, 2019.

[24] A. Kumar, G. S. Mishra, P. Nand, M. S. Chahar, and S. K. Mahto, "Financial Fraud Detection in Plastic Payment Cards using Isolation Forest Algorithm," *Int. J. Innov. Technol. Explor. Eng.*, vol. 10, no. 8, pp. 132–136, 2021, doi: 10.35940/ijitee.g8873.0610821.

[25] O. Adepoju, J. Wosowei, and H. Jaiman, "COMPARATIVE EVALUATION OF CREDIT CARD FRAUD DETECTION USING MACHINE," no. October, 2019, doi: 10.1109/GCAT47503.2019.8978372.

[26] P. K. Sadineni, "Detection of Fraudulent Transactions in Credit Card using Machine Learning Algorithms," no. October, 2020, doi: 10.1109/I-SMAC49090.2020.9243545.

[27] A. Pumsirirat and L. Yan, "Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine," vol. 9, no. 1, pp. 18–25, 2018, doi: 10.14569/IJACSA.2018.090103.

[28] N. Malini and M. Phil, "Analysis on Credit Card Fraud Identification Techniques based on KNN and Outlier Detection," pp. 3–6, 2017, doi: 10.1109/AEEICB.2017.7972424.

[29] D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, "Credit Card Fraud Detection - Machine Learning methods," *2019 18th Int. Symp. INFOTEH-JAHORINA*, no. October, pp. 1–5, 2019, doi: 10.1109/INFOTEH.2019.8717766.

[30] G. Suresh and R. J. Raj, "A Study on Credit Card Fraud Detection using Data Mining Techniques," no. 21, pp. 21–24, 2018, doi: 10.20894/ijdmta.102.007.001.004.

[31] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial Fraud : A Review of Anomaly Detection Techniques and Recent Advances," *Expert Syst. Appl.*, vol. 193, p. 116429, 2022, doi: 10.1016/j.eswa.2021.116429.

[32] N. F. Sahib and A. Y. Al-Sultan, "Diagnosis of COVID-19 in CT Images Based on Convolutional Neural Network (CNN)," *AIP Conf. Proc.*, vol. 2394, no. November, 2022, doi: 10.1063/5.0121126.

[33] J. A. Lopez, "FEDERAL RESERVE BANK OF SAN FRANCISCO Monitoring Banking System Connectedness with Big Data Monitoring Banking System Connectedness with Big Data," 2018, doi: 10.24148/wp2018-01.

[34] I. Conference and I. Engineering, "A Survey of Deep Learning based Online Transactions Fraud Detection Systems," 2020, doi: 10.1109/ICIEM48762.2020.9160200.

[35] A. Y. Yousif, "Convolutional Neural Network (CNN) for diagnosing age-related macular degeneration (AMD) in retinal images Speaker localization and identification View project Speaker localization using enhanced beamforming View project," *Artic. Int. J. Mech. Eng. Educ.*, no. October, 2022, [Online]. Available: https://www.researchgate.net/publication/364811092

[36] S. M. Hussein, E. H. Al-Saadi, and A. Y. Al-Sultan, "Automatic Classification of AMD in Retinal Images," *AIP Conf. Proc.*, vol. 2394, no. November, 2022, doi: 10.1063/5.0121323.

[37] N. Fahem Sahib and A. Y. Al-Sultan, "Design Engineering Lung Segmentation and Detection of COVID-19 in CT Images based on Deep Learning (CNN)," no. October, 2022.

[38] M. Ala'raj, M. F. Abbod, and M. Majdalawieh, "Modelling customers credit card behaviour using bidirectional LSTM neural networks," *J. Big Data*, vol. 8, no. 1, 2021, doi: 10.1186/s40537-021-00461-7.

[39] E. Ileberi, Y. Sun, and Z. Wang, "Performance Evaluation of Machine Learning Methods for Credit

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Card Fraud Detection Using SMOTE and AdaBoost," *IEEE Access*, vol. 9, pp. 165286–165294, 2021, doi: 10.1109/ACCESS.2021.3134330.

[40] V. Sushma, S. Neelamma, Y. Machaiah, and S. Fathima, "Credit Card Fraud Detection using Machine Learning," *14th Int. Conf. Adv. Comput. Control. Telecommun. Technol. ACT 2023*, vol. 2023-June, no. 2, pp. 861–864, 2023, doi: 10.48175/ijarsct-9488.

[41] L. Moumeni, M. Saber, I. Slimani, I. Elfarissi, and Z. Bougroun, "Machine Learning for Credit Card Fraud Detection," *Lect. Notes Electr. Eng.*, vol. 745, no. 24, pp. 211–221, 2022, doi: 10.1007/978-981-33-6893-4_20.

[42] O. Ata and L. Hazim, "Comparative analysis of different distributions dataset by using data mining techniques on credit card fraud detection," *Teh. Vjesn.*, vol. 27, no. 2, pp. 618–626, 2020, doi: 10.17559/TV-20180427091048.

الخلاصة

مع التطور السريع لتكنولوجيا الإنترنت في السنوات الأخيرة، أصبحت المعاملات المالية عبر الإنترنت شائعة بشكل متزايد لشراء مجموعة واسعة من السلع والخدمات عبر الإنترنت، نظرًا لمزاياها العديدة. وانتشار استخدام بطاقات الائتمان بشكل واسع زاد بالتالي من إمكانية الاستغلال، مما يشكل تهديدًا كبيرًا للمستخدمين نتيجة للعمليات الاحتيالية المنتشرة. لقد أصبح احتيال بطاقات الائتمان قضية أساسية في عصر الرقمي الحالي، مما يشكل خسائر مالية كبيرة ومخاطر أمنية للمؤسسات المالية والمستهلكين. واستجابةً لهذا التحدي المتزايد، طور الباحثون وخبراء الصناعة بشكل مستمر وحددوا تقنيات كشف الاحتيال لحماية ضد الأنشطة الاحتيالية. يهدف هذا الورق البحثي إلى تقديم نظرة شاملة على آخر التطورات في تقنيات كشف الاحتيال لمعاملات بطاقات الائتمان. يستكشف المنهج المتبع في هذا البحث مختلف الطرق ومصادر البيانات والخوارزميات التعلم الآلي المستخدمة في أنظمة كشف الاحتيال. بالإضافة إلى ذلك، يناقش البحث التحديات التي تواجه هذه الأنظمة.

الكلمات المفتاحية: كشف الاحتيال، كشف الشذوذ، بطاقات الاعتماد، التعلم العميق، طويلة المدى على المدى القصير

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com