IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 26, Issue 1, Ser. 1 (Jan. – Feb. 2024), PP 11-18
www.iosrjournals.org

Deep Learning Ensemble Approach For Financial Fraud Detection

Md. Arifuzzaman[1], Md. Anisuzzaman Siddique[2]
[1]*(Deputy General Manager, Rajshahi Krishi Unnayan Bank, Bangladesh)*
[2]*(Department Of Computer Science And Engineering, University Of Rajshahi, Bangladesh)*

Abstract
Security has become a major challenge with the significant increase in online and offline transactions; various financial fraud crimes occur daily. Fraud detection is a critical measure in today's digitalized world and on e-commerce platforms. Financial fraud has seriously affected the health of economies and damaged the welfare of consumers, investors, as well as financial institutions. Considering the significant advantages that Deep Learning (DL) methods bring to the world of machine learning, it seems necessary to examine their potential usage in the field of fraud detection. This is especially important for e-commerce transactions, where we need to assess whether DL methods can be good candidates as effective classifiers. In this paper, we propose a DL based ensemble method for fraud detection in the e-commerce domain. We implement several well-known Convolutional Neural Network (CNN) methods on e-commerce customer data and compare it results using different performance criteria. We combined four classical CNN techniques such as GoogLeNet (also known as Inception), DenseNet (Densely Connected Convolutional Networks), VGG (Visual Geometry Group) Net, and ResNet (Residual Network) to create an ensemble model. Then compare its performance with each individual model. The performance comparison shows that proposed DL-ensemble method outperforms other CNN methods for fraud detection. The results of this study can be helpful for scholars willing to optimize their fraud detection systems with DL methods. Additionally, the present study shows which classification algorithms can be best used in a CNN framework for application in fraud detection for online payments. In future, we will conduct a series of experiments to evaluate the effectiveness of CNN approaches with other state-of-the-art methods on several real datasets.

Key Word: *Deep Learning; CNN; GoogLeNet; DenseNet; VGG, ResNet, Ensemble.*

Date of Submission: 01-01-2024 Date of Acceptance: 09-01-2024

I. Introduction

In recent years, E-commerce has experienced substantial growth and advancement, driven by digital transformation, sophisticated e-commerce platforms, and enhanced communication capabilities, which have shifted consumers towards increased online shopping[1]. Utilizing E-commerce platforms offers numerous benefits for both businesses and customers, including expedited buying processes, reduced costs, and heightened flexibility. Customers can easily compare prices and product quality, while also having access to a variety of payment options[2]. However, this surge in online business activities has also led to a rise in cyber threats, particularly targeting banks and financial institutions. Cyber-attacks such as fraud, phishing, hacking, and ransomware have become more prevalent, undermining public confidence in online services and impeding the growth of online banking[3,4]. Recognizing the severity of the situation, financial institutions are heavily investing in cyber security to prevent cyber-attacks and attempts at online bank robbery[5]. The consequences of cyber-attacks on bank security are significant, impacting reputation and resulting in substantial financial losses[6].

The rapid expansion of online business platforms and the escalating volume of transactions naturally attract fraudsters and opportunists, leading to an increase in fraud cases. Exploiting potential vulnerabilities and loopholes in electronic payment processes, fraudsters stand to gain substantial sums of money. Consequently, it is imperative to implement robust and intelligent fraud detection solutions to safeguard against these financial and economic losses. Fraud detection typically employs fundamental approaches that analyze customer data to recognize patterns associated with fraudulent activities. Key data points investigated include online navigation tracks, historical activities, and customer payment behavior. In domains like credit card and financial fraud, data mining and machine learning emerge as highly effective methods[7,8,9]. The problem is commonly framed as a two-class classification, where each input transaction is categorized as normal or fraudulent. Machine learning techniques play a crucial role by learning from training data and applying acquired patterns to production data.

Various popular classification algorithms, including Logistic Regression, K-nearest neighbor[10], Artificial Neural Networks[11], Support Vector Machines[12], and Random Forests[13], have been proposed for fraud detection. However, the growing number and complexity of fraudulent attempts in e-commerce transactions, coupled with issues like skewed and noisy data for detection, pose challenges for traditional methods. These methods may struggle to capture multiple characteristics and the underlying structure of the data. Consequently, there is a need for more sophisticated and robust approaches to effectively combat fraud in the modern era. Recent studies in machine learning applications for fraud detection have increasingly focused on the development of hybrid and flexible systems[14,15].

Ensemble methods stand out as powerful solutions for enhancing classification accuracy[16]. The core concept behind ensemble learning involves amalgamating diverse classifiers with varying learning mechanisms or training samples to enhance the final prediction outcomes[17,18]. Essentially, ensemble learning seeks to unify a range of supervised or unsupervised classification algorithms through a combination method or voting system to elevate the overall system performance. To construct an ensemble model, several different (typically weak) classifiers are initially trained on the training data to discern data patterns using their respective algorithms. Subsequently, predictions from each classifier are combined using a combination or voting method to generate a conclusive prediction. This framework offers several advantages for machine learning methods, such as adaptability to diverse techniques, enhanced detection performance, and versatile applicability[16,19]. Consequently, ensemble methods find application in various domains, including network intrusion detection[20], bioinformatics[21], time-series forecasting, and risk analysis[22].

Given the overall advantages offered by ensemble methods, it is imperative to explore their application in the realm of fraud detection, particularly in the context of e-commerce transactions, and assess their effectiveness as potential solutions. Surprisingly, there has been a dearth of comprehensive research examining the enhancement and efficacy of these methods specifically in the domain of fraud detection. This paper aims to fill this gap by evaluating the suitability of ensemble learning methods for application in fraud detection within the e-commerce domain. We conducted experiments applying various well-known ensemble methods to e-commerce customer data and scrutinized their outcomes using diverse performance criteria. The findings of this study are intended to assist scholars seeking to optimize their fraud detection systems through the integration of ensemble methods. Additionally, this research identifies which classification algorithms are most effective within an ensemble framework for detecting fraud in online payments. This study makes the following contributions:

- ✓ Introduction of an ensemble method designed for detecting fraud in bank payments. The model leverages ensembling techniques by integrating algorithms such as GoogLeNet, DenseNet, VGG Net, and ResNet.
- ✓ Comprehensive capture of both global and local transaction patterns, ensuring adaptability over time.
- ✓ Evaluation and validation of the proposed model through extensive experiments, revealing a remarkable 98% detection accuracy.

The subsequent sections of this paper are structured as follows: Section II furnishes a background on existing methods for fraud detection, along with an introduction to the structures of certain ensemble methods. Section III outlines our methodology, encompassing the implementation of diverse ensemble methods on fraud data, the experimental process, and the subsequent evaluation phase. Section IV is dedicated to the presentation and analysis of the evaluation results. Finally, Section V concludes the paper and outlines potential future directions for research in this domain.

II. Related Work

In this section, we explore past methodologies utilized in detecting fraud and present an overview of ensemble learning systems. Additionally, we provide insights into how these ensemble learning systems are applied in the context of fraud detection.

Past Methods

Financial fraud detection is a very hot research issue that has been studied by many researchers from both academic circles and industrial fields for decades. Recently, decision trees, bayesian networks, and support vector machines (SVM) have been applied in studying this issue more frequently[23]. For example, Kirkos et al. compared the financial fraud detection performance of decision trees, neural networks and bayesian belief networks[24]. Abbasi et al. and West et al. summarized the existing classification methods for financial fraud detection comprehensively[23,25]. West et al. provided a review on key performance of classification metrics that used for financial fraud detection[26]. There are also some researchers tried to look this problem in a combinatorial perspective. Chan et al. tried to use scalable techniques to analyse massive amount of transaction data and they proposed a combining multiple learned fraud detectors under "cost model"[27]. Bhattacharyya et al. discussed three techniques that employed in fraud detection study namely Logistic Regression, Support Vector Machines, and Random Forest[28]. Another part of researchers tried to seek a novel method. For instance, Padmaja et al. proposed a new method for fraud detection, which using extreme outlier elimination and k Reverse Nearest Neighbours[29].

Ensemble Learning for Fraud Detection

Given the diverse advantages offered by ensemble methods in enhancing detection and classification performance, researchers have explored their application in the realm of fraud detection. Many proposed methods incorporate ensemble learning as a component within the detection algorithm, forming hybrid structures with other elements. Notably, Random Forest has emerged as a prominent choice for fraud detection, with several researchers successfully employing it[30,31,32]. Particularly in credit card fraud detection, Random Forest stands out as one of the most effective methods according to the literature. Sohony et al. introduced an ensemble approach for credit card fraud detection, leveraging a combination of Random Forest and neural network techniques[33]. This hybrid model capitalizes on the strengths of both methods, enhancing the accuracy of detecting both normal and fraudulent instances.

Haider et al. introduced an ensemble-based approach for detecting impression fraud in mobile advertising[34]. Employing bagging and boosting ensemble methods, the authors classified each ad display (impression) as either fraudulent or non-fraudulent, achieving high accuracy, precision, and recall rates. In a different domain, Xu et al. proposed a neural network ensemble method based on random rough subspaces for insurance fraud detection[35]. Their methodology involved utilizing rough set reduction to generate a set of reductions ensuring data information consistency. Subsequently, these reductions were randomly chosen to create a subset, and each selected reduction was employed to train a neural network classifier within an ensemble framework. Additionally, Bagga et al. enhanced the performance of credit card fraud detection by applying the bagging method in conjunction with pipelining[36].

While ensemble methods exhibit promise in the realm of fraud detection, there is still a need for a more systematic exploration of their extensive potential to enhance detection performance. The following section outlines our methodology for evaluating the performance of several key ensemble methods in the context of fraud detection.

III. Research Methodology

The method for developing an ensembling fraud detection model involved several steps, including data collection, pre-processing, feature engineering, model selection, and ensembling.

Dataset

In this study, Table no 1 presents the features utilized for online payment fraud analysis. The dataset, sourced from the Kaggle community, encompasses 6,362,620 records capturing historical details of customer transactions. This dataset serves as a benchmark for evaluating various fraud detection solutions. The predictive target variable, denoted as “isFraud” classifies transactions into class 0 for “normal” transactions and class 1 for fraudulent transactions.

Data Preprocessing

Given the inherent class imbalance in such datasets, 70% of the data was allocated for training the models, 20% was allocated for validation the models and the remaining 10% reserved for testing. During the training phase, a 10-fold cross-validation approach was employed. Additionally, all methods underwent optimization using cross-validation and grid search techniques to identify the optimal set of hyper parameters, ensuring robust results. The reported outcomes stem from the utilization of optimized methods, with a focus on comparing the best results achieved by ensemble methods. Typically, fraud detection systems assign labels to transaction instances, indicating their classification as fraud or normal. While most algorithms generate probabilities for each case to signify the system's confidence in detecting fraud, these probabilities are rounded to obtain binary values {0, 1}.

Table no 1: The online fraud dataset

Feature	Description
step	represents a unit of time where 1 step equals 1 hour
type	type of online transaction
Amount	the amount of the transaction
nameOrig	customer starting the transaction
oldbalanceOrg	balance before the transaction
newbalanceOrg	balance after the transaction
nameDest	recipient of the transaction
oldbalanceDest	initial balance of the recipient before the transaction
newbalanceDest	the new balance of the recipient after the transaction
isFraud	class label

DL-Ensemble Methods

Within the field of cyber-attack identification and classification, ensemble learning stands out as a significant methodology in machine learning. Broadly, these methods involve the integration of multiple machine learning classifiers to address common challenges, and their outcomes are consolidated using various voting techniques. Our DL-ensemble methodology incorporates four CNN methods: GoogLeNet, DenseNet, VGG, and ResNet. The following section provides an in-depth exploration of each of these methods.

GoogLeNet: It is a deep CNN architecture designed for classification tasks. Developed by researchers at Google[37]. Key features of GoogLeNet include the use of inception modules, which are blocks containing multiple parallel convolutional layers of different filter sizes. These modules enable the network to capture features at various scales simultaneously, promoting richer representations of the input data. The inception modules are designed to balance the trade-off between computational efficiency and expressive power. GoogLeNet incorporated global average pooling and significantly fewer parameters than traditional deep networks, making it computationally efficient. The architecture also introduced the concept of auxiliary classifiers at intermediate layers during training, aiding in mitigating the vanishing gradient problem and improving convergence.

DenseNet: A DL architecture designed to address challenges related to information flow and feature reuse in neural networks. In DenseNet, each layer receives direct inputs from all preceding layers, and in turn, contributes to the feature maps of all subsequent layers[38]. This dense connectivity facilitates the efficient flow of information throughout the network, enhances feature reuse, and helps alleviate the vanishing gradient problem. DenseNet architecture promotes parameter efficiency, encourages feature propagation, and has shown to achieve competitive performance with fewer parameters compared to other DL architectures. The dense connections in DenseNet result in compact models that are easier to train and often exhibit improved accuracy.

VGG: A convolutional neural network architecture proposed by the Visual Geometry Group in the 2014 ImageNet Large Scale Visual Recognition Challenge[39]. VGG is characterized by its simplicity and uniform architecture. Unlike other contemporary models that used a variety of layer types and complex architectures, VGG maintained a consistent structure throughout its design. It primarily used 3x3 convolutional filters and stacked multiple convolutional layers with small filter sizes, making the network deeper. The key variations of VGG architecture include VGG16 and VGG19, representing the number of weight layers in each variant. VGG16 has 16 weight layers, and VGG19 has 19 weight layers. VGG influence can be seen in subsequent architectures that aimed to strike a balance between depth, complexity, and computational efficiency in deep learning models for image recognition.

ResNet: ResNet is a deep learning architecture that introduced the concept of residual learning. Developed by researchers at Microsoft Research[40]. The key innovation of ResNet lies in the use of residual blocks. Traditional deep neural networks faced challenges in training very deep architectures due to issues like vanishing gradients and degradation in accuracy. Residual learning addresses these problems by introducing shortcut connections, or skip connections, that allow the network to skip one or more layers during forward and backward propagation. A residual block consists of a "shortcut" connection and two paths for information flow: one path involves standard convolutional layers, and the other is a direct shortcut that adds the original input to the processed output. This architecture facilitates the training of extremely deep networks, as the gradient can be directly propagated through the shortcut connections, mitigating the vanishing gradient problem. ResNet architectures come in various depths, such as ResNet-18, ResNet-34, ResNet-50, ResNet-101, and ResNet-152, with the numbers indicating the total number of layers in the network. These architectures have demonstrated outstanding performance in various computer vision tasks, including classification, object detection, and image segmentation.

DL-Ensemble Model Framework

This study utilized a fusion strategy leveraging deep learning to integrate the classifications of multiple models, generating a single conclusive classification for each new transaction. Figure no 1 shows the proposed method DL-ensemble model framework. This approach facilitates the combination of diverse model strengths, leading to increased accuracy and resilience compared to individual models. Furthermore, it can adapt to evolving patterns in transaction data by undergoing retraining with new data. The procedural steps of the deep learning ensemble method are outlined as follows:

1. *Partition the dataset into training, validation, and testing subsets.*
2. *Split the training set into k-folds.*
3. *Train every base model using k-1 folds and predict the remaining fold.*
4. *Iterate step 3 for each fold.*
5. *Utilize the classification from all base models as input features for the final decision.*
6. *Train and validate the DL-ensemble model on the training set and evaluate on the testing set.*
7. *Repeat steps 1-6 for each new transaction.*

The ensemble methodology combines the strengths of various models, surpassing the accuracy and resilience of individual models. Additionally, it exhibits adaptability to changing patterns in transaction data through retraining with new data.

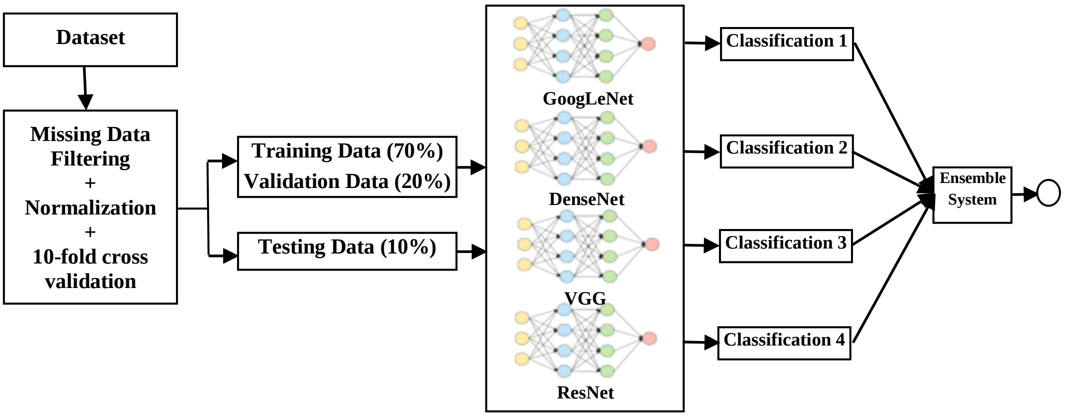

Figure no 1: DL-ensemble classification framework.

Evaluation

We use a set of criteria for evaluating the performance and comparing the ensemble method and other four individual methods together. We consider four important detection metrics as True Negative (TN), True Positive (TP), False Negative (FN), and False Positive (FP). True Positives are the instances that are positive and were also classified as positive. Similarly, True Negatives are the actual negatives and were classified as negative. False Positives are cases that are negative but are classified as positives. Similarly, False Negatives are cases that are positive but are classified as negative. According to these metrics, the performance criteria are as follows:

Accuracy: Accuracy is a measure of the overall correctness of the classifier. It is calculated as the ratio of correctly predicted instances (both true positives and true negatives) to the total number of instances.

$$Accuracy = (TP + TN) / (TP + TN + FP + FN)$$

Precision: Precision is a measure of the accuracy of the positive predictions made by a classifier. It is calculated as the ratio of true positive predictions to the total number of positive predictions made by the classifier.

$$Precision = TP / (TP + FP)$$

High precision indicates that the classifier has a low false positive rate, meaning that when it predicts the positive class, it is often correct.

Recall: Recall is a measure of the ability of the classifier to capture all the positive instances. It is calculated as the ratio of true positive predictions to the total number of actual positive instances.

$$Recall = TP / (TP + FN)$$

High recall indicates that the classifier is good at identifying positive instances, but it may have a higher false positive rate.

F1-Score: F1-score is the harmonic mean of precision and recall. It provides a balance between precision and recall. It is calculated using the following formula:

$$F1\text{-}score = 2 * (Precision * Recall) / (Precision + Recall)$$

F1-score ranges from 0 to 1, where 1 indicates perfect precision and recall, and 0 indicates poor performance in both.

IV. Results and Discussion

In this segment, we showcase the outcomes of our fraud detection model experiments conducted on the online fraud dataset. The model underwent evaluation through a 10-fold cross-validation, and the average performance across all folds was documented. The objective of this study was to assess diverse candidate algorithms and ensemble methods for the fraud detection model, ultimately selecting the optimal combination based on performance metrics such as accuracy, precision, recall, and F1-score. This comprehensive process encompasses multiple stages, including model training, validation, and testing, coupled with the utilization of relevant performance measures to gauge model effectiveness. Following the completion of experiments, we extracted and organized the results in accordance with the performance criteria introduced in the preceding section.

Table no 2 and Figure no 2 portray the performance results of all methods employed in this inquiry. Each model demonstrated commendable accuracy scores, ranging from 0.92 to 0.98, indicating their proficiency in making accurate predictions in the majority of cases. However, relying solely on accuracy might not offer a comprehensive understanding of model efficacy, as it overlooks the balance between correctly classified positive and negative cases. Precision, representing the proportion of true positive predictions among all positive predictions, varied among the models. The DL-ensemble model exhibited the highest precision score of 0.84, showcasing its adeptness in correctly identifying fraudulent cases among those labeled as such. In contrast, VGG displayed the lowest precision, scoring 0.73, highlighting the trade-off between precision and recall. This trade-off underscores that higher precision often accompanies lower recall, and vice versa. Conversely, recall, indicating the model's capability to identify all relevant instances in the dataset, displayed relatively consistent values among the models, ranging from 0.76 to 0.90. The DL-ensemble model achieved the highest recall at 0.9, signifying its effectiveness in capturing a substantial proportion of relevant instances. The F1-score, representing the harmonic mean of precision and recall, furnishes a balanced evaluation of a model's overall performance by considering both false positives and false negatives. The DL-ensemble model secured the highest F1-score of 0.87, solidifying its status as a robust performer in this classification task.

Table no 2: Performance comparison of different models.

Model	*Accuracy*	*Precision*	*Recall*	*F1-Score*
GoogLeNet	0.94	0.80	0.85	0.83
DenseNet	0.95	0.82	0.86	0.84
VGG	0.92	0.73	0.76	0.75
ResNet	0.96	0.77	0.84	0.81
DL-ensemble	0.98	0.84	0.90	0.87

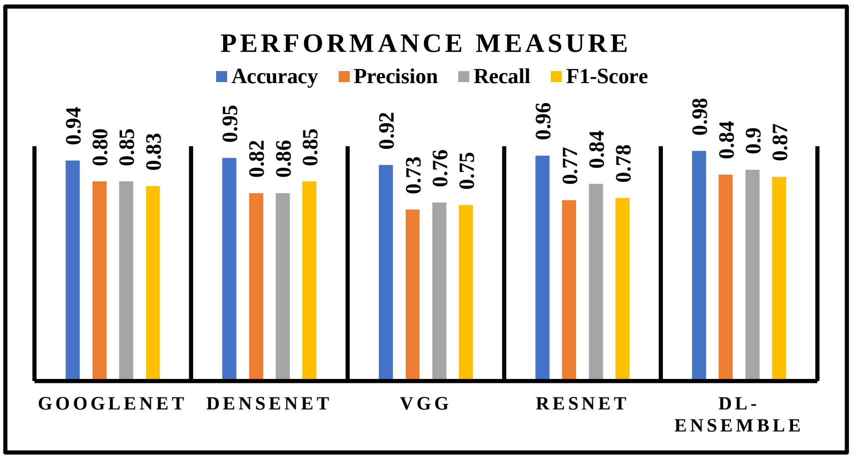

Figure no 2: Overall performance comparison between models

The trade-off between precision and recall is evident in the results. Models with higher precision tend to generate fewer false positives but may overlook some relevant cases, resulting in lower recall. Conversely, models with higher recall correctly capture more instances but may produce more false positives, leading to lower precision. The choice of a model should be guided by the specific requirements and consequences associated with false positives and false negatives in the given application. Consistently standing out as a notable performer across multiple metrics, the DL-ensemble model demonstrates its effectiveness in achieving a high F1-score, emphasizing its ability to strike a balanced trade-off between precision and recall an essential consideration for fraud detection tasks. While the presented models show promise, the results also indicate opportunities for further exploration and improvement. The ongoing challenge in the field of fraud detection lies in achieving higher levels of accuracy, precision, and recall while maintaining an optimal balance. This study lays the groundwork for the development of more sophisticated and comprehensive solutions to enhance the resilience of fraud detection systems. The proposed fraud detection model, employing an ensemble method, offers several advantages over alternative approaches. By leveraging the strengths of multiple models, the ensemble method can improve accuracy and robustness, mitigate the risk of overfitting, and adapt to evolving patterns in the data over time. This is particularly crucial in identifying sophisticated fraud patterns that may undergo changes over time.

V. Conclusion

This paper presents an innovative fraud detection model for bank payments, employing an ensemble method. The model demonstrates notable effectiveness in improving accuracy and robustness compared to individual models. By capturing patterns in transaction data and dynamically adapting to evolving patterns over time, the proposed model excels at detecting emerging fraud patterns. The ensemble approach, known as the DL-ensemble model, not only enhances accuracy but also strengthens model resilience and adaptability within fraud detection systems. This study pioneers an advanced ensemble-based fraud detection model that utilizes sophisticated techniques to enhance the precision and reliability of cyber threat classifications and countermeasures in financial transactions. The DL-ensemble model exhibits superior performance in identifying fraudulent activities, coupled with adaptability to evolving threat landscapes, marking a significant advancement in cybersecurity within financial sectors. The proposed model's versatility extends to diverse datasets and holds promise for integration into operational banking systems, promoting enhanced customer trust and financial security.

Through a comprehensive analysis of results and implications derived from the findings, this study identifies potential avenues for future research and proposes enhancements to the model. Recommending further exploration of alternative ensemble methods or combinations of algorithms to improve the DL-ensemble model's performance, the study also suggests investigating advanced feature engineering techniques, such as graph-based approaches, to capture more intricate patterns in transaction data. The proposal to incorporate additional data sources, such as social media or network information, aims to strengthen the model's ability to detect frauds and deepen the understanding of underlying patterns of fraudulent behavior.

References

[1]. Song Y., Escobar O., Arzubiaga U., And De Massis A. The Digital Transformation Of A Traditional Market Into An Entrepreneurial Ecosystem. Review Of Managerial Science. 2022; 16(1):65–88.

[2]. Rodrigues V. F., Policarpo L. M., Da Silveira D. E., Da Rosa Righi R., Da Costa C. A., Barbosa J. L. V., Antunes R. S., Scorsatto R., And Arcot T. Fraud Detection And Prevention In E-Commerce: A Systematic Literature Review. Electronic Commerce Research And Applications. 2022; 101207.

[3]. A. Darem, "Anti-Phishing Awareness Delivery Methods," Engineering, Technology & Applied Science Research. 2021; 11(6):7944–7949.

[4]. African Corporates Face Rising Cybercrime Risks. Emerald Expert Briefings. 2021; Https://Doi.Org/10.1108/Oxan-Db262652.

[5]. Best M., Krumov L., And Bacivarov I. Cyber Security In Banking Sector. International Journal Of Information Security And Cybercrime. 2019; 8(2): 39-52.

[6]. V. Ghodasara, Research On Importance Of Cyber Security Audit And Assessment In Bank. International Journal For Research In Applied Science And Engineering Technology. 2019; 7(5):1409–1416.

[7]. Abdallah A., Maarof, M. A. And Zainal A. Fraud Detection System: A Survey. Journal Of Network And Computer Applications. 2016; 68:90–113.

[8]. Diadiushkin A., Sandkuhl K., And Maiatin A. Fraud Detection In Payments Transactions: Overview Of Existing Approaches And Usage For Instant Payments. Complex Systems Informatics And Modeling Quarterly. 2019; 20:72–88.

[9]. Varmedja D., Karanovic M., Sladojevic S., Arsenovic M., And Anderla A. Credit Card Fraud Detection-Machine Learning Methods. 2019 18th International Symposium (Infoteh). 2019;1–5.

[10]. Itoo F., And Singh S. Comparison And Analysis Of Logistic Regression, Naïve Bayes, And Knn Machine Learning Algorithms For Credit Card Fraud Detection. International Journal Of Information Technology. 2021; 13(4):1503–1511.

[11]. Asha R. B., And Kr S. K. Credit Card Fraud Detection Using Artificial Neural Network. Global Transitions Proceedings 2021;2(1): 35– 41.

[12]. Gyamfi N. K., And Abdulai J.-D. Bank Fraud Detection Using Support Vector Machine. Ieee 9th Annual Information Technology, Electronics And Mobile Communication Conference (Iemcon), 2018; 37–41.

[13]. Xuan S., Liu G., Li Z., Zheng L., Wang S., And Jiang C. Random Forest For Credit Card Fraud Detection. 2018 Ieee 15th International Conference On Networking, Sensing And Control (Icnsc). 2018; 1–6.

[14]. Lin W., Sun L., Zhong Q., Liu C., Feng J., Ao X., And Yang H. Online Credit Payment Fraud Detection Via Structure-Aware Hierarchical Recurrent Neural Network. Ijcai, 2021; 3670–3676.

[15]. Nami S., And Shajari M. Cost-Sensitive Payment Card Fraud Detection Based On Dynamic Random Forest And K-Nearest Neighbors. Expert Systems With Applications. 2018; 110:381–392.

[16]. Polikar, R. Ensemble Learning. In Ensemble Machine Learning. Springer. 2012; 1–34.

[17]. Dietterich T. G. Ensemble Learning. The Handbook Of Brain Theory And Neural Networks. 2002; 2(1):110–125.

[18]. Dong X., Yu Z., Cao W., Shi Y., And Ma Q. A Survey On Ensemble Learning. Frontiers Of Computer Science. 2020; 14(2):241–258.

[19]. Kuncheva L. I. Combining Pattern Classifiers: Methods And Algorithms. John Wiley & Sons. 2014.

[20]. Amini M., Rezaeenour J., And Hadavandi E. A Neural Network Ensemble Classifier For Effective Intrusion Detection Using Fuzzy Clustering And Radial Basis Function Networks. International Journal On Artificial Intelligence Tools, 2016; 25(02):1550033.

[21]. Verma A., And Mehta S. A Comparative Study Of Ensemble Learning Methods For Classification In Bioinformatics. 7th International Conference On Cloud Computing, Data Science & Engineering-Confluence. 2017; 155–158.

[22]. Hamori S., Kawai M., Kume T., Murakami Y., And Watanabe C. Ensemble Learning Or Deep Learning? Application To Default Risk Analysis. Journal Of Risk And Financial Management. 2018; 11(1): 12.

[23]. Abbasi A., Albrecht C., Vance A., And Hansen J. Metafraud: A Meta-Learning Framework For Detecting Financial Fraud. Mis Quarterly. 2012; 36 (4): 1293-1327.

[24]. Kirkos E., Spathis C., And Manolopoulos Y. Data Mining Techniques For The Detection Of Fraudulent Financial Statements. Expert Systems With Applications. 2007; 32(4): 995-1003.

[25]. West J., And Bhattacharya M. Intelligent Financial Fraud Detection: A Comprehensive Review. Computers & Security. 2016; (57): 47-66.

[26]. West J., And Bhattacharya M. Some Experimental Issues In Financial Fraud Detection: An Investigation. In The Proceedings Of The 5th International Symposium On Cloud And Service Computing. 2016; Ieee Cs Press.

[27]. Chan P. K., Fan W., Prodromidis A. L., And Stolfo S. J. Distributed Data Mining In Credit Card Fraud Detection. Intelligent Systems And Their Applications. 1999; 14(6): 67-74.

[28]. Bhattacharyya S., Jha S., Tharakunnel K., And Westland J. C. Data Mining For Credit Card Fraud: A Comparative Study. Decision Support Systems. 2011; 50(3): 602-613.

[29]. Padmaja T. M., Dhulipalla N., Bapi R. S., And Krishna P. R. Unbalanced Data Classification Using Extreme Outlier Elimination And Sampling Techniques For Fraud Detection. International Conference On Advanced Computing And Communications (Adcom). 2007; 511-516.

[30]. Carneiro N., Figueira G., And Costa M. A Data Mining Based System For Credit-Card Fraud Detection In E-Tail. Decision Support Systems. 2017; 95: 91–101.

[31]. Dornadula V. N., And Geetha S. Credit Card Fraud Detection Using Machine Learning Algorithms. Procedia Computer Science. 2019; 165: 631–641.

[32]. Rai A. K., And Dwivedi R. K. Fraud Detection In Credit Card Data Using Machine Learning Techniques. International Conference On Machine Learning, Image Processing, Network Security And Data Sciences. 2020; 369–382.

[33]. Sohony I., Pratap R., And Nambiar U. Ensemble Learning For Credit Card Fraud Detection. Proceedings Of The Acm India Joint International Conference On Data Science And Management Of Data. 2018; 289–294.

[34]. Haider C. M. R., Iqbal A., Rahman A. H., And Rahman M. S. An Ensemble Learning Based Approach For Impression Fraud Detection In Mobile Advertising. Journal Of Network And Computer Applications. 2018; 112: 126–141.

[35]. Xu W., Wang S., Zhang D., And Yang B. Random Rough Subspace Based Neural Network Ensemble For Insurance Fraud Detection. Fourth International Joint Conference On Computational Sciences And Optimization. 2011; 1276–1280.

[36]. Bagga S., Goyal A., Gupta N., And Goyal A. Credit Card Fraud Detection Using Pipeling And Ensemble Learning. Procedia Computer Science 2020; 173: 104–112.

[37]. Szegedy C., Liu W., Jia Y., Sermanet P., Reed S., Anguelov D., Erhan D., Vanhoucke V., And Rabinovich A. Going Deeper With Convolutions. Ieee Conference On Computer Vision And Pattern Recognition (Cvpr). 2015; 1-9.

[38]. Huang G., Liu Z., Maaten L. V. D. And Weinberger K. Q. Densely Connected Convolutional Networks. Ieee Conference On Computer Vision And Pattern Recognition (Cvpr). 2017: 2261-2269.

[39]. Russakovsky O., Deng J., Su H., Krause J., Satheesh S., Ma S., Huang Z., Karpathy A., Khosla A., Bernstein M., Berg Alexander C., F. Li. International Journal Of Computer Vision. 2015; 115: 211-252.

[40]. He K., Zhang X., Ren S. And Sun J. Deep Residual Learning For Image Recognition. Ieee Conference On Computer Vision And Pattern Recognition (Cvpr). 2016; 770-778.