International Journal of Communication Networks and Information Security
ISSN: 2073-607X, 2076-0930
Volume 15 Issue 04 Year 2023

A Novel Deep Learning-Based Identification of Credit Card Frauds in Banks for Cyber Security Applications

Damodharan Kuttiyappan
Research Scholar, Computer Science & Engineering, SRMIST, Vadapalani, Chennai, Tamilnadu, India
dt3388@srmist.edu.in
Rajasekar V*
Associate Professor, Computer Science & Engineering, SRMIST, Vadapalani, Chennai, Tamil Nadu, India
rajasekv2@srmist.edu.in

Article History

Received: 09 November 2023
Revised: 19 December 2023
Accepted: 31 January 2024

Abstract

Due to the widespread use of constantly evolving internet technology and the increased frequency of cyber-attacks and crimes, cyber security is crucial for the banking sector. One of the biggest dangers confronting the banking sector globally is credit card (CC) fraud. It is becoming a serious issue and is growing rapidly, especially as the number of financial transactions utilizing CC keeps rising. The prevalence and growth of Internet banking have enhanced CC fraud identification. Finding fraudulent transactions of CC has become a major issue for internet buyers. In this study, an entirely novel deep learning (DL) algorithm is suggested for use in cyber security applications to identify CC thefts in the banking industry. We use a collection of significantly skewed CC fraud data sets to apply the proposed Multi-Gradient Whale Optimized Convolutional Neural Network (MW-CNN). The efficacy of the suggested methodis assessed depending on the performance evaluation criteria and comparing it with traditional techniques.

Keywords: Cyber Security, Cyber-Attacks, Credit Card (CC), Banking, Deep Learning(DL)

1. Introduction

In the contemporary era, widespread technological advancements and online accessibility have democratized access to statistics. Organizations store vast amounts of critical data on the cloud, sourced from various channels such as social networks, consumer behavior, and online interactions. The escalating threat of white-collar crime, including scams, presents a major obstacle for the banking sector, companies, as well as governments [1]. Credit card transactions have become the predominant method for both online and offline payments, amplifying the incidence of card fraud amid society's increasing reliance on communication technologies [2].

DL, a revolutionary advancement of this century, has transformed modern approaches, excelling in handling extensive datasets beyond human capacity. DL techniques are categorized into unsupervised and supervised learning, with fraud detection strategies depending on the accessibility of datasets [3]. Supervised learning identifies anomalies based on historical patterns, and numerous procedures have been employed over time to detect credit card fraud. However, the primary challenge lies in dealing with highly unbalanced databases, where a small fraction of transactions is

fraudulent compared to the majority being legitimate. The crucial issue faced by investigators is designing a precise and efficient strategy for fraud prevention, minimizing false positives while accurately identifying fraudulent activities [4]. In general, the contemporary usage of credit cards, individuals often resort to them for purchasing essential goods they cannot afford immediately. However, this trend has led to a surge in associated fraud. Hence, there is a pressing need to develop a robust model that not only fits well but also predicts with higher accuracy. This underscores the importance of addressing the specific challenges faced in credit card fraud detection, providing a more explicit context for the proposed solution.

This study introduces an effective DL-based approach designed to enhance CC fraud detection by incorporating a feedback system to elevate overall performance and detection rates. A comprehensive assessment was conducted, comparing the performance of various classification techniques, including artificial neural networks, tree-based algorithms, support vector machines, Naive Bayes, random forest, logistic regression, and gradient boosting classifier. The evaluation utilized a highly imbalanced CC fraud database. The research report encompasses key components such as the introduction, related studies, fraud obfuscation methods, application of DL approaches, performance evaluation, and conclusive findings. The report concludes with insightful recommendations for future enhancements in the proposed solution, emphasizing a holistic perspective on improving CC fraud detection methodologies.

The following parts: An overview of related works is given in Section 2, a more thorough explanation of the methodology is given in Section 3, and simulation results and discussion are presented in Section 4. Section 5 concludes the study and offers suggestions for more research.

2. Related Works

The goal of the study [5] was to find instances of fraud that cannot be found using supervised learning or historical data. It suggested a model that combinesa deep Auto-encoder to reconstruct typical transactions and a restricted Boltzmann machine (RBM). Unsupervised training with backpropagation was used in the DL method. For DL, the implementation makes use of the tensor library and H2O.Organizations and financial institutions are both at great financial risk from fraud. Several strategies are used in the article [6] to reduce the danger, including 3D secured authentication, chip and PIN technology and fraud detection methods. These controls are designed to increase security and stop fraud in financial transactions.In the engine for detecting CC fraud described in the paper [7], genetic algorithms, and ML (machine learning)were used to select features. Following that, the enhanced features are input into a variety of ML classifiers, such as Decision Tree, Random Forest, Logistic Regression, Artificial Neural Network, and Naive Bayes. Using a dataset created from European cardholders, the performance of the suggested detection engine is assessed, proving its superiority to current methods.The fields of data science and ML are essential to the identification of fraud. In order to identify fraudulent activity, the study [8] was created to use ML algorithms and data science methodologies. The study illustrates the use of several modeling techniques in fraud detection. The study attempts to improve the efficacy and accuracy by integrating the power of data science and ML.Research [9] suggested a ML-based solution for detecting CC fraud. Customers use CCs 24/7. Thus, the bank's server can continuously watch and monitor all transactions using ML techniques. The goal was to use ML techniques to detect and foresee instances of fraudulent behavior in real time.

The paper [10] presented a brand-new deep network technique for fraud detection. A log transform approach was used to address problems with data skew in the dataset. The network also focused on loss to efficiently train on difficult examples. Experimental findings show that in terms of performance and accuracy for fraud detection, their suggested neural network model outperforms more established models like logistic regression and support vector machines.Article [11] presented a novel fraud detection technique created especially for streaming transaction data. The method focused on deriving consumer behavioral patterns from past transaction records. The suggested method intends to identify and prevent fraud in streaming transaction data by analyzing these patterns and detecting fraudulent activity in real time.The goal of the study [12] was to develop a thorough understanding of typical user behavior with a focus on identifying identity fraud. Each person has unique trading habits, uses particular operating systems, finishes transactions in particular lengths of time, and has a tendency to spend money in particular quantities and ranges. The identification of identity fraud was made easier by using neural networks to locate and identify

these distinctive transaction patterns linked to certain users. In the study [13], seven blended ML models for identifying fraudulent behaviors are introduced and investigated using data from the real world. Modern ML algorithms are used to detect CC fraud in the first phase of the hybrid models. Then, depending upon the best-performing engine from the first phase, hybrid techniques are developed. According to the results, the combination of Adaboost and LGBM performs better than the others and has the highest level of proficiency in spotting fraud.The study [14] introduces a revolutionary paradigm for fraud detection called Federated Meta-Learning. Our platform enables banks to create fraud detection models using their own locally distributed training data, in contrast to conventional methods that train models using centrally stored data in the cloud. With this decentralized strategy, data privacy was guaranteed while yet allowing for efficient fraud detection.The paper [15] generally served high-value individuals or businesses. On-demand, a small sum is given to the debtor in cash or by electronic transfer. However, some borrowers fail to pay back the funds within the allotted time, which causes problems for the bank. Then, using historical data, potential loan defaults are predicted, assisting in the mitigation of such issues.The study [16] introduced FFD (Federated learning for Fraud Detection), a framework for federated learning-based training of a fraud detection model utilizing behavior features. The article [17] provided a method to feature engineering based on rules that take into account both individual and group behavior, portraying individual behavior as group features. The ability to distinguish between legitimate and fraudulent transactions was improved by this technique. Our test results show that our strategy is advantageous and effective. This study [18] proposes a novel approach to early detection and diagnosis of oral cancer, utilizing deep neural networks, specifically the Inception-V3 algorithm. Leveraging transfer learning techniques, the model enhances its performance by identifying intricate patterns associated with the disease. The study highlights the value of routine dental exams and demonstrates the way DL can be used to overcome the difficulties associated with oral cancer diagnosis. The article [19] suggested a novel hybrid solution to the overlapped class imbalance problem. A divide and conquer strategy is used in the plan. Initially, a model for anomaly detection is trained using the minority samples. This model can be used to remove a number of outliers from the minority class as well as a significant fraction of the overall samples from the original dataset.

Existing fraud detection systems face difficulties in detecting complicated fraud cases, causing the need for developments beyond conventional supervised learning. Extensive tests on a variety of datasets are necessary to determine the robustness of the novel models that research suggest. The significance of consistently developing fraud detection techniques exceeding existing measures is highlighted by organizational risk. Some models are difficult to implement since they are not explainable, which means that interpretable solutions are needed to satisfy with regulations. Federated learning has benefits in terms of privacy, but its applicability in a variety of financial institutions needs to be thoroughly investigated. The persistence of class imbalance requires hybrid techniques that can more effectively identify fraud by addressing possible overlap difficulties and unbalanced datasets.

3. Methodology

3.1 Data Set

The dataset consists of European cardholder credit card transactions from September 2013. With 492 frauds out of 284,807 transactions over a two-day period, the dataset is incredibly skewed, with approximately 0.172% of transactions proving fraudulent. 'Time' and 'Amount' are the only non-transformed features in the dataset; all other numerical input variables were derived through PCA transformation. For cost-sensitive learning, 'Amount' denotes the transaction amount, while 'Time' shows the seconds that have passed since the first transaction. In response, the variable "Class" is assigned a value of 1 in cases of fraud and 0 in cases of non-fraud. Original features and other background information are not available due to confidentiality. Because confusion matrix accuracy is meaningless in unbalanced classification circumstances, the Area under the Precision-Recall Curve (AUPRC) is the best measure of accuracy given the class imbalance. It is accessible at https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud.

3.2 Min-Max Normalization

The process of scaling numerical data to a particular range is known as minimum-maximum normalization, sometimes referred to as Min-Max scaling or scaling of features. It is frequently employed in the preparation of data for techniques using DL.

Making the data fall inside a predetermined range, usually between 0 and 1, is the aim of minimum-maximum normalization. Equations 1 and 2 represent the min-max normalization formula.

$$Normalized\ Value\ = \frac{(Value - Minimum\ Value)}{(Maximum\ Value - Minimum\ Value)} \quad (1)$$

$$W_{norm} = \frac{W - W_{min}}{W_{max} - W_{min}} \quad (2)$$

Where W represents the feature's original value, W_{norm} its normalized value, W_{max} is the maximum attribute value within the dataset, and W_{min} is the minimum attribute value within the dataset.

3.3 Multi-Gradient Whale Optimized Convolutional Neural Network (MW-CNN)

3.3.1 Multi-gradient Whale Optimization Algorithm

The Multi-gradient Whale Optimization Algorithm (MW) is a natural-inspired single-objective problem optimizer based on the fundamental hunting instincts of humpback whales. When this metaheuristic approach is applied to an optimization issue, it produces a collection of randomly selected solutions that are then continually refined in accordance with preset standards and criteria. MW distinguishes itself from prior population-based metaheuristic algorithms by including humpback whale-inspired problem-solving strategies, such as the bubble net trap mechanism. This modification increases the algorithm's efficacy and efficiency in identifying the most appropriate responses. Equations (3), (4), (5), and (6) are the fundamental equation that drives the Multi-gradient Whale Optimization Algorithm. These equations govern the iterative modifications made to the solutions throughout each iteration.

Equation (3) represents the updating of the whale's (W) position in the search space. When an arbitrary number (o) is less than 0.5, the new location (W(s+1)) is calculated by subtracting the current ideal place (W*(s)) from a factor (B.C). This approach mimics the whale's regular hunting style.

$$W(s+1) = W*(s) - B.C; o < 0.5 \quad (3)$$

When the arbitrary number (o) equals or exceeds 0.5, the whale's location is modified in accordance with equation (4). Here the ideal place (W*(s)) is multiplied by a constant C'^{fak} to generate a cosine function that affects the new position (W(s+1)). This equation exemplifies the algorithm's adaptive behaviour.

$$W(s+1) = C'^{f^{ak}} \cos(2\pi s) + W*(s)) ; o \geq 0.5 \quad (4)$$

Equation (5) computes the distance (C) between the whale's present position (w) and a randomly chosen point (w_{rand}), indicating the whale's exploration of the search space.

$$C = |D.w_{rand} - w| \quad (5)$$

Equation (6) describes the procedure for updating the exploration location (w), which entails subtracting a factor (BC) from a randomly picked position(w_{rand}).

$$w(s+1) = w_{rand} - BC \quad (6)$$

The current iteration of these equations is represented by the coefficient vector A, the estimated distance C, the position vectors of the ideal solution W*, and the random integer s in the interval [0, 1]. MW distinguishes itself from other optimization algorithms by its capacity to tackle complex optimization issues. Its regular spacing of exploration and exploitation phases and lack of gradient information needs are due to its stochastic character. In the context of Deep Learning (DL) network training, researchers are investigating the possibilities of MW. When the appropriate target function is utilized, the method's properties make it a good choice for Convolutional Neural Network (CNN) training. According to this idea, integrating CNNs' great deep learning skills with MW's excellent optimization powers should improve training processes and provide higher accuracy in DL applications. To sum up, the Multi-gradient Whale Optimization Algorithm is a unique optimization technique that draws inspiration from humpback whale behavior. Equations (3) through (6), which explain its various strategies, aid in the efficient traversal of difficult search domains.

3.3.2 Convolutional Neural Network

Convolutional Neural Networks (CNNs) are sophisticated technologies commonly employed in computer vision applications. Photographs and movies perform exceptionally well when arranged

and resemble a grid. CNNs are modelled after the human visual brain and contain layers such as pooling, fully connected layers, and convolutional. Convolutional layers, which perform convolutions on incoming data using learnable filters to extract significant features, are the fundamental building blocks of CNNs. Patterns and indications in input images are used to teach these qualities. After that, they obtained feature maps are down sampled using pooling layers like mean or max pooling to reduce complexity and extract relevant properties. The final fully connected layers translate top-level information into desired results by performing classification or regression procedures. A CNN's architecture is shown in Figure 1.

CNNs are useful not only for computer vision but also for other sorts of data, such as transaction amounts, merchant details, transaction timestamps, and user profiles. The CNN acquires the ability to recognize patterns and anomalies suggestive of fraud by receiving instruction on a sizable dataset comprising both legitimate and fraudulent transactions. CNNs are effective because they can detect complex relationships and correlations across several variables, which can help identify suspicious patterns that are undetected by more conventional rule-based approaches. This feature helps to identify fraud more accurately and effectively, which lowers false positives and raises overall detection rates. The architecture of CNN is shown in Figure 1.

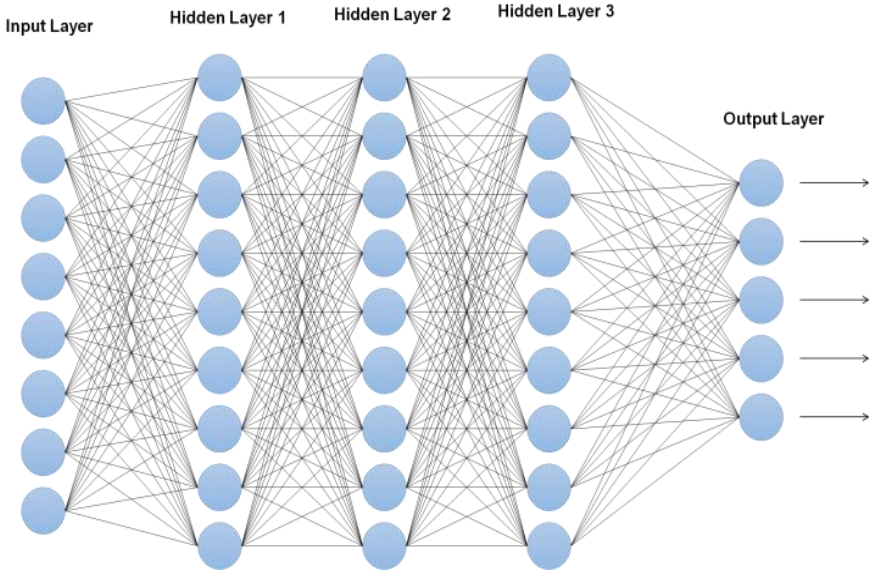

Figure 1. CNN Architecture

The MW-CNN method combines the resilient structure of a convolutional neural network with the novel Multi-gradient Whale Optimization method (MW). By integrating MW, CNN's optimization process is improved, resulting in more effective and efficient feature learning for the detection of credit card fraud. The MW-CNN technique uses filters that adapt as well as learn pertinent information linked to fraudulent patterns in order to execute convolution processes on the input data in the first layers of the CNN. To enhance the overall performance of the network, the convolutional filters are dynamically adjusted by the MW optimization, which is included into the training process. The learnt features are subsequently down sampled by the pooling layers, which improve the model's generalization capacity while retaining important data. The MW-CNN algorithm's completely linked layers serves as the central hub for decision-making, converting high-level information taken from lower layers into a result for fraud detection. By optimizing the weights and biases of these completely linked layers, the MW optimization process makes classification more precise and effective. The study recognizes the significance of additional investigation into approaches to deal with this particular problem, even if the MW-CNN algorithm performs exceptionally well in negotiating the challenging environment of unbalanced and dynamic credit card fraud detection datasets. A more thorough examination of methods and techniques meant to handle imbalanced datasets ought to be provided in order to enhance the article's content and offer readers a better knowledge of viable remedies for enhanced fraud detection performance.

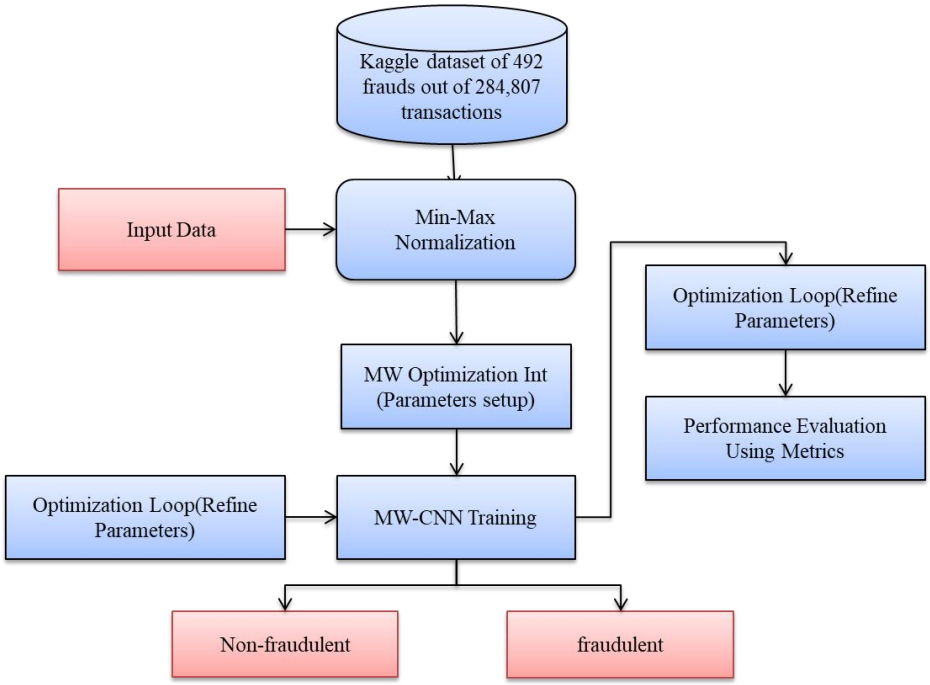

Figure 2. Working Principal of MW-CNN Architecture

Figure 2 depicts the wide range of transactions that the model is subjected to in order to train the MW-CNN algorithm to detect complex patterns indicative of fraud. The CNN is guaranteed to be able to effectively explore the solution space and stay away from convergence to poor solutions through the Multi-gradient Whale Optimization Algorithm. As a result, the model performs better and can generalize to unique and untested data. To summarize, the synergistic MW-CNN strategy combines the Multi-gradient Whale Optimization method's optimization powers with Convolutional Neural Networks' tremendous feature learning capabilities. As a result of this integration, a useful tool was produced that can recognize complex patterns, detect fraud with extreme efficiency and accuracy, and change with the dataset.

4. Results and Discussion

The way deep learning detects credit card fraud depends on a number of factors, including the size and quality of the dataset, the neural network's architecture and parameters, the pre-processing techniques utilized, and the assessment metrics applied. Recall, accuracy, precision, and F1-score are critical criteria for assessing credit card fraud detection technologies' effectiveness.

The following formulae can be used to calculate the various assessment metrics, including accuracy, recall, F1-score, and precision. To evaluate the effectiveness of credit card fraud detection systems, it is necessary to comprehend the nuances of the data. A more in-depth examination of these issues could enhance the research findings' overall readability and importance by giving readers with critical insights into the merits and downsides of the proposed MW-CNN approach. The assessment criteria for credit card fraud detection include True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN). The following important measures are required to determine the efficacy of the detection algorithms.

True Positive (TP): The MW-CNN system accurately classifies fraudulent transactions as such on certain instances.

True Negative (TN): The MW-CNN system accurately classifies fraudulent transactions as non-fraudulent on certain circumstances.

False Positive (FP): Non-fraudulent transactions are wrongly categorized as fraudulent by the MW-CNN algorithm.

False Negative (FN): Non-fraudulent transactions are mistakenly categorized as non-fraudulent by the MW-CNN algorithm.

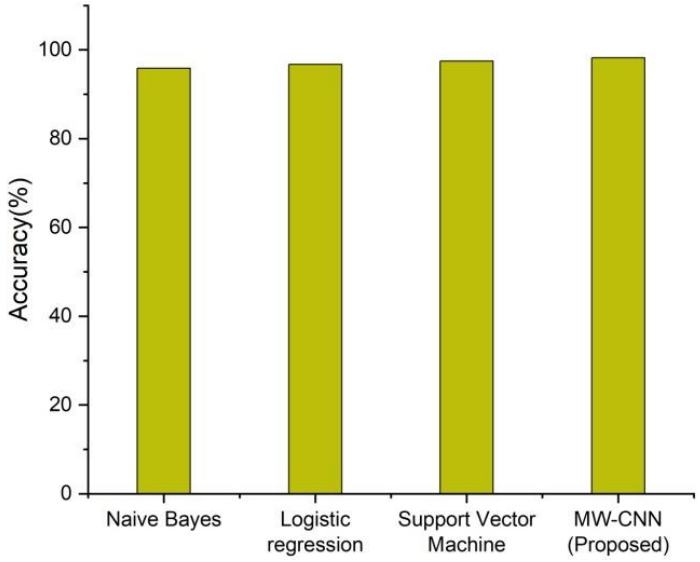

Figure 3. Accuracy

$$Accuracy = \frac{TP+TN}{(TP+TN+FP+FN)} \quad (7)$$

Figure 3 shows that MW-CNN surpasses established approaches such as NB (95.85%), LR (96.75%), and SVM (97.50%), with an accuracy of 98.25%. To balance both fraudulent and non-fraudulent transactions, this implies a higher percentage of correct classifications. The ability of MW-CNN to reduce false positives and false negatives indicates its usefulness and demonstrates that it is more accurate at detecting fraudulent behavior from lawful transactions.

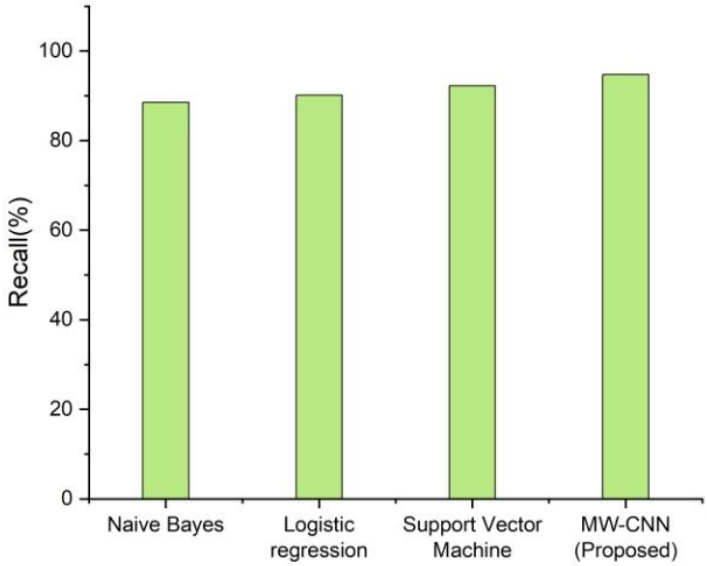

Figure 4. Recall

$$Recall = TP/(TP + FN) \quad (8)$$

Recall is an important metric for assessing the effectiveness of a prediction model or diagnostic test. Equation (8) contains the recall formula. The recall of the model, also known as the true positive rate, is a measure of how often it recognizes genuine positive cases. In the banking business, a greater recall score indicates efficiency in detecting credit card fraud. When compared to prior approaches such as NB (88.35%), LR (90.15%), and SVM (92.25%), Figure 4 shows how well our proposed method, MW-CNN, performs in detecting credit card fraud (94.75%). This demonstrates MW-CNN's efficacy in identifying credit card fraud by properly capturing a large number of true positive cases.

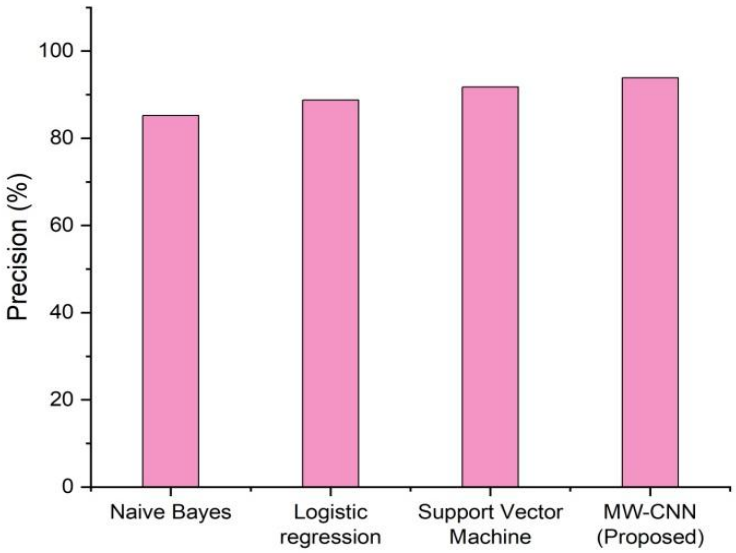

Figure 5. Precision

$$precision = TP/(TP + FP) \quad (9)$$

Precision, which is calculated using equation (9), demonstrates the accuracy of affirmative sample identifications. Figure 5 depicts the accuracy findings, which emphasize the 93.85% precision of our proposed technique, MW-CNN, as well as its improved performance. This performs better than conventional methods such as SVM (91.75%), LR (88.75%), and NB (85.25%). MW-CNN's ability to correctly detect positive samples is highlighted by its increased accuracy, which demonstrates its effectiveness in identifying credit card fraud.

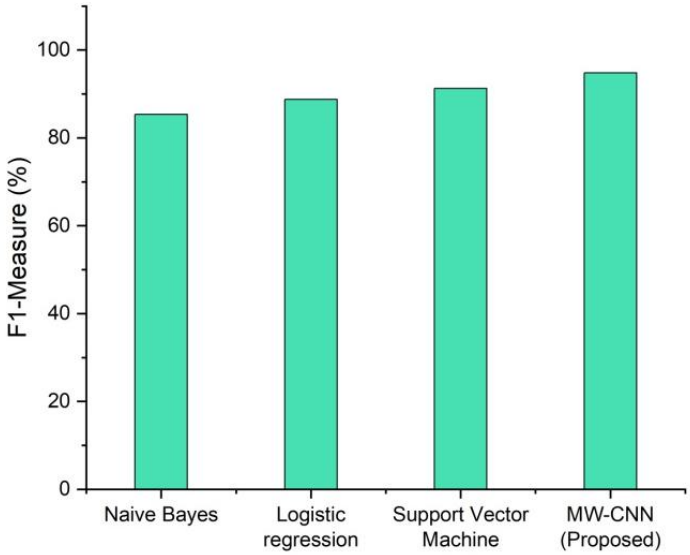

Figure 6. F1 Measure

$$\text{F1 measure} = 2 * \frac{(\text{specificity} * \text{sensitivity})}{(\text{specificity} + \text{sensitivity})} \quad (10)$$

The F1 metric, which represents the harmonic mean of accuracy and recall, is commonly employed in average rate estimates. Equation (10) is utilized to assess the F1-measure, and Figure 6 displays the outcomes. Specifically, our proposed approach, MW-CNN, surpasses existing methods such as NB (85.35%), LR (88.75%), and SVM (91.25%), with an F1 score of 94.83%. This emphasizes MW-CNN's excellent recall and accuracy, as well as its efficacy in balancing recall and precision to increase fraud detection performance.

The MW-CNN model incorporates convolutional neural networks with the Multi-gradient Whale Optimization Algorithm for robust feature learning and optimization. This integration handles the model's complexity. However, disadvantages include the requirement for meticulous parameter adjustment and possible susceptibility to changes in dataset properties. It could take a lot

of testing and careful evaluation of certain dataset aspects to get the best results. It is necessary to do further study to investigate methods for improving model adaptability to a variety of datasets and automating parameter adjustment.

5. Conclusion

The study presented a MW-CNN method for CC fraud detection. Internet banking provides a wealth of transactional data that helps in the detection and prevention of credit card fraud. For fraud detection systems, the availability of certain data such as transaction timestamps, IP addresses, device specifications, and user activity patterns provides insightful information. Effectively preventing credit card fraud is crucial, as it is a serious offense. To address these problems, artificial intelligence and DL technologies are needed. To increase the recognition level and efficacy of the classifier, this research focused on creating an effective fraud detection system utilizing DL techniques. Utilizing the evaluation metrics like accuracy, precision, recall, and F1-score, the study compared a variety of DL techniques, such as SVM, NB, and LR.Our suggested method MW-CNN performed the best and produced the most efficient results. However, it's important to acknowledge certain limitations in this study. The performance of the proposed MW-CNN technique may vary across different datasets and real-world scenarios. Additionally, the interpretability of the model and handling imbalanced and evolving datasets remain challenges that warrant further investigation. Future work in credit card fraud detection should prioritize improving interpretability in DL models for enhanced user trust and regulatory compliance. Advances in handling imbalanced datasets and evolving fraud patterns are crucial for developing more robust and adaptable detection systems. Exploration of federated learning approaches, enabling model training across distributed datasets without centralized data sharing, could contribute to privacy-preserving advancements in the banking sector. Continuous research in deep learning architectures and multimodal data integration is essential for achieving precision and effectiveness in the evolving landscape of financial cybersecurity.

References

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

[2] X. Zhang, Y. Han, W. Xu, and Q. Wang, “HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture,” *Information Sciences*, vol. 557, pp. 302-316, 2021.

[3] N. Kousika, G. Vishali, S. Sunandhana, and M. A. Vijay, “Machine Learning based Fraud Analysis and Detection System,” *Journal of Physics: Conference Series,* vol. 1916, no. 1, p. 012115, May.2021.

[4] G. K. Kulatilleke, “Challenges and complexities in machine learning based credit card fraud detection,” *arXiv preprint arXiv:2208.10943*, 2022.

[5] A. Pumsirirat and L. Yan, “Credit Card Fraud Detection Using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine,” *International Journal of advanced computer science and applications*, vol. 9, no.1, 2018.

[6] N. V. Krishna Rao, Y. Harika Devi, N. Shalini, A. Harika, V. Divyavani, and N. Mangathayaru, “Credit card fraud detection using spark and machine learning techniques,” in *Machine Learning Technologies and Applications: Proceedings of ICACECS 2020*, 2021, pp. 163-172.

[7] E. Ileberi, Y. Sun, and Z. Wang, “A machine learning based credit card fraud detection using the GA algorithm for feature selection,” *Journal of Big Data*, vol. 9, no. 1, pp.1-17, Feb. 2022.

[8] R. Almutairi, A. Godavarthi, A. R. Kotha, and E. Ceesay, “Analyzing CC Fraud Detection based on Machine Learning Models,” in *2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, Jun. 2022, pp. 1-8.

[9] K. Vengatesan, A. Kumar, S. Yuvraj, V. D. Ambeth Kumar, and S. S. Sabnis, “ CREDIT CARD FRAUD DETECTION USING DATA ANALYTICS TECHNIQUES,” *Advances in Mathematics: Scientific Journal,* vol. 9, no. 3, pp. 1177-1188, Jun. 2020.

[10] X. Yu, X. Li, Y. Dong, and R. Zheng, "A Deep Neural Network Algorithm for Detecting Credit Card Fraud," *IEEE Xplore,* pp. 181-183, Jun. 01, 2020.

[11] V. N. Dornadula, and S. Geetha, "Credit Card Fraud Detection using Machine Learning Algorithms," *Procedia computer science*, vol. 165, pp. 631-641, 2019.

[12] O. Voican, " CC Fraud Detection using DL Techniques," *Informatica Economica*, vol. 25, no. 1, 2021.

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

[14] W. Zheng, L. Yan, C. Gou, and F. Y. Wang, " Federated Meta-Learning for Fraudulent Credit Card Detection," *International Joint Conference on Artificial Intelligence*, Jul. 2020, doi: https://doi.org/10.24963/ijcai.2020/642.

[15] S. Arora, S. Bindra, S. Singh, and V. K. Nassa, " Prediction of credit card defaults through data analysis and machine learning techniques," *Materials Today: Proceedings*, vol. 51, pp. 110-117, 2022.

[16] W. Yang, Y. Zhang, K. Ye, L. Li, and C. Z. Xu, " FFD: A Federated Learning Based Method for Credit Card Fraud Detection," *Lecture Notes in Computer Science,* pp. 18-32, 2019.

[17] Y. Xie, G. Liu, R. Cao, Z. Li, C. Yan, and C. Jiang, "A Feature Extraction Method for Credit Card Fraud Detection," *IEEE Xplore,* Feb. 01, 2019.

[18] P. Ashok Babu et al., "An Explainable Deep Learning Approach for Oral Cancer Detection," *Journal of Electrical Engineering & Technology*, pp. 1-12, Oct. 2023.

[19] Z. Li, M. Huang, G. Liu, and C. Jiang, "A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection," *Expert Systems with Applications*, vol. 175, p. 114750, Aug. 2021.