



Financial Data Analysis for Financial Management Based on Cloud Computing Using Deep Reinforcement Learning Model

Parviz Gurbanov^{1,*}, Mansur Matkarimov², Nilufar Sapayeva³, Alexey Nedelkin⁴, Andrey Kulik⁵, Olga Zanina⁶

¹Department of Economics, Baku Eurasian University, Baku, AZ1110, Azerbaijan

²Department of Economics, Mamun University, Khiva, 220900, Uzbekista

³Department of Business and Management, Urgench State University, Urgench, 220100, Uzbekistan

⁴Department of Computer Science, Plekhanov Russian University of Economics, Moscow, 117997, Russia

⁵Department of Management, Kuban State Agrarian University named after I.T. Trubilin, Krasnodar, 350044, Russia

⁶Kursk Branch, Financial University under the Government of the Russian Federation, Moscow, 125167, Russia

Emails: gurbanov.p.a@mail.ru; matkarimov_mansur1@mamunedu.uz; sapayeva.n.k@mail.ru; aem735@mail.ru; kulik.andrey.a@mail.ru; ovzanina@fa.ru

Abstract

Maintainable financial fraud detection includes the usage of viable and decent performs in the recognition of fraudulent actions in financial region. A credit card is susceptible to cyber threats, which leads to a fraud of credit card. The fraudster does dishonest action by attaining illegal access to credit card information and this action affects an economic loss for the user as well as company. At present, deep learning (DL) and machine learning (ML), systems were deployed in financial fraud detection owing to their features' ability of making a great device to find out fraudulent dealings. This paper presents a Financial Data Analysis for Financial Management Based on Cloud Computing Using Deep Reinforcement Learning Model (FDAFM-CCDRLM). The main intention of FDAFM-CCDRLM model is to improve analysis of financial data in the economic management. Initially, the min-max normalization is employed in the data normalization stage to convert a data of input into a suitable format. Besides, the proposed FDAFM-CCDRLM model designs a black-winged kite algorithm (BKA) for the subset of feature selection process. For the classification process, the double deep Q-network (DDQN) algorithm has been executed. At last, the artificial bee colony (ABC) algorithm-based hyperparameter range method is done for improving the classification outcomes of the DDQN model. The experimental evaluation of the FDAFM-CCDRLM system can be tested on a benchmark database. The extensive outcomes highlight the significant solution of the FDAFM-CCDRLM approach to the financial data analysis classification process

Keywords: Financial Data Analysis; Min-Max Normalization; Financial Management; Cloud Computing; Deep Reinforcement Learning

1. Introduction

Financial fraud might be deliberated as some criminal action linked to payment processes, or some fraud targeted economic organizations like lending institutions, banks, fintechs, and crypto exchanges [1]. Financial fraud recognition denotes as set of rules in place to evade the harm led by fraudulent actions take place in economic service providers. It could contain money laundering, credit card fraud, theft identity, and other payment fraud types [2]. Unless any risk or the user knowledge, a substantial quantity of money might be withdrawn in a smaller amount of period. The fraudster functions by attempting to create every succeeding transaction valid, and

recognizing this could be a highly challenging and complicate job. A credit card is susceptible to cybercrime, inducing credit card fraud [3].

Several financial frauds leads enormous wounds to global financial institutions and companies [4]. Without the authenticated user knowledge, credit card theft, unauthorized debit and credit card transactions and multiple other such fraudulent actions are alarming the global governance, banking sector and clients [5]. The financial fraud recognition methods have the capability to recognize unauthorized access and unusual threats. These fraud recognition systems are continually upgraded by economic organizations [6]. Recently, fraud recognition has been facing severe challenges owing to the unprecedented evolution in the online transactions [7]. Consequently, Machine Learning (ML) and Artificial Intelligence (AI) methodologies has been widely utilized in payment fraud recognition methods. Scientific workers are endeavouring to build fraud detection method over Deep Learning (DL), ML methodologies and Data Mining (DM) to recognize the transaction is either fraudulent or genuine, depend on a database that contains transaction particulars [8]. Therefore, ML or statistical learning models are often utilized to automatically recognize fraudulent transactions [9]. Semi-supervised, unsupervised, supervised learning, Decision Tree (DT), Deep Neural Network (DNN), and hybrid methodologies has been widely discovered to employ in the fraud recognition method [10].

This paper presents a Financial Data Analysis for Financial Management Based on Cloud Computing Using Deep Reinforcement Learning Model (FDAFM-CCDRLM). Initially, the min-max normalization is employed in the data normalization stage to convert a data of input into a suitable format. Besides, the proposed FDAFM-CCDRLM model designs a black-winged kite algorithm (BKA) for the subset of feature selection process. For the classification process, the double deep Q-network (DDQN) algorithm has been executed. At last, the artificial bee colony (ABC) algorithm-based hyperparameter selection method is done to improve the classification results of the DDQN model. The experimental evaluation of FDAFM-CCDRLM algorithm can be verified on a benchmark database.

2. Literature of Works

Huang et al. [11] presented a ML-based K-means clustering approach for improving an efficiency and precision of financial fraud recognition. By collecting huge quantities of financial transaction data, they might recognize abnormal patterns and behaviours in an appropriate time, thus identifying possible fraud. In comparison with conventional rule-based detection models, ML-based techniques well adjust to constantly changing fraud methods and designs however increasing accuracy and flexibility during detection. Furthermore, K-means clustering additionally helps in enhancing resource allocation by improving concentrated prevention and monitoring efforts in higher-risky regions, therefore successfully alleviating the influence of fraud on the complete financial management. In [12], the original GNN-CL method introduced in this study marks an innovation in the domain of financial fraud detection by collaboratively joining the benefits of CNN, LSTM, and GNN systems. These convergences allows multi-layered investigation of composite transaction designs, refining detection precision and flexibility alongside composite fraudulent actions. A main innovation of this study is the usage of multilayer perceptron (MLPS) to approximation similarity of the node, successfully removing neighborhood noise, which may results in false positives. Innan et al. [13] developed a new model to detect financial fraud utilizing Quantum Graph Neural Networks (QGNNs). It is kind of neural networks, which may handle graph-structured data and utilize the Quantum Computing (QC) power to carry out computations more effectively than traditional NNs. Our method utilizes Variational Quantum Circuits (VQC) to improve the QGNN performance.

Khodabandehlou and Golpayegani [14] recommend FiFrauD that is a scalable, unsupervised method, which represents the manipulators behavior in the stream of transaction. During this model, real-world transactions among traders were transformed into a stream of graphs and, rather than utilizing semi- and supervised learning techniques, fraudulent traders are identified accurately by developing density signals in graphs. Ismail and Haq [15] objective is to enhance the financial fraud detection in organizations over the use of artificial intelligence (AI) algorithms. The architecture uses ML model and data analytics to precisely recognize designs, differences, and signs of false action. They utilized investigative data study methods to recognize examples of lost values and demanding data. The choice of the RF Classifier is depending on its capability to constantly seizure complex designs and powerfully address the multi-collinearity problem.

The authors [16] concentrations on design an intellectual credit card fraud recognition and classification method using the Garra Rufa Fish optimizer technique with an ensemble-learning (CCFDC-GRFOEL) algorithm. This method defines the occurrence of non-and fraudulent credit card transactions through feature selection and an ensemble procedure. A novel GRFO-based feature subset selection (GRFO-FSS) technique is used to select a features set. An ensemble-learning procedure, consist of auto-encoder (AE), ELM, and Bi-LSTM, has been applied for the fraud transactions detection. Lastly, the pelican optimizer algorithm (POA) has been applied for parameter tuning. Aftabi et al. [17] implemented a new technique derived from the ensemble and generative adversarial

networks (GAN) models, which can not only solve the absence of non-fraudulent instances but also furthermore process the higher-dimensionality of feature space.

3. Proposed Methods

In this paper, we provide a FDAFM-CCDRLM model. The main intention of FDAFM-CCDRLM model is to improve analysis of financial data in the economic management. To accomplish that, the proposed FDAFM-CCDRLM model involves various stages such as data normalization, feature selection, classification, and hyperparameter tuning models. Fig. 1 represents the overall working procedure of FDAFM-CCDRLM model.

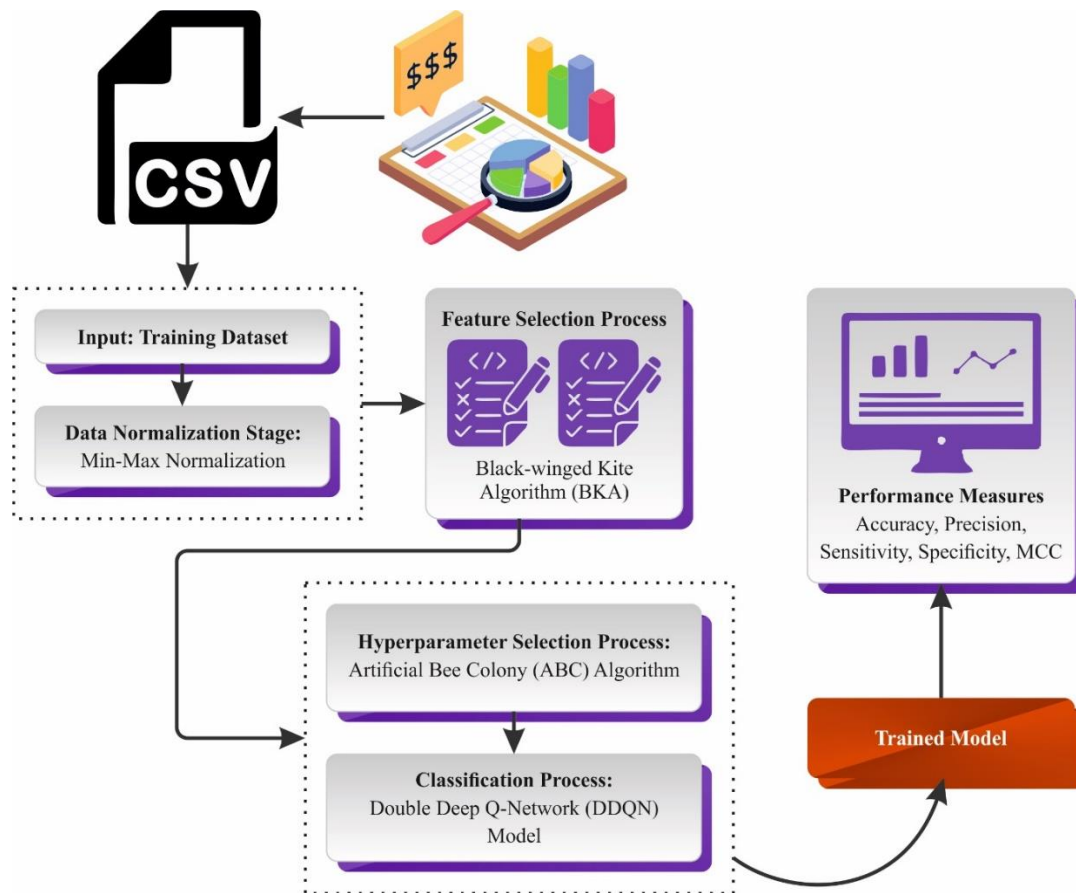


Figure 1. Overall Workflow of FDAFM-CCDRLM model

A. Data Normalization

Initially, the min-max normalization is employed to convert a data of input into a suitable format. It is a method used in financial data study to measure data into a within the range of [0, 1]. This technique aids normalize economic variables, like stock prices, returns, or economic ratios, creating them similar despite variances in their original measures [18]. By converting the data, min-max normalization removes the influence of outliers and permits for more precise contrasts and trend study. In financial management, it is valuable for range of optimization, performance evaluation, and risk assessment. This method ensures that every variable donates respectively to the complete analysis, enhancing the decision-making and predicting.

B. BKA-based Feature Selection Process

Besides, the proposed FDAFM-CCDRLM model designs a BKA for the subset of feature selection process. The BKA is an optimizer model, which is stimulated by the higher flexibility and intellectual behavior shown by black-winged kites (BK) throughout their migrations, assaults, and hunting procedures [19]. These exclusive natural features stimulated scholars to progress a novel swarm intellect optimizer model, which meant at better handle intricate issues. The algorithm captures the fight and black-winged kites hunting behaviours and intensely fakes their higher flexibility to ecological variations and target positions. This donates the model with robust progressive abilities, quick search velocity, and outstanding capability to discover an optimum solution. The distinctive bioinspired feature of the model deliver it with strong dynamic search abilities and let to efficiently manage with fluctuating optimizer settings.

Initialization of population

An initialization set of random solution has been made, with every BK. Its mathematical formulation is expressed below:

$$BK = \begin{bmatrix} BK_{1,1} & BK_{1,2} & \cdots & BK_{1,d} \\ BK_{2,1} & BK_{2,2} & \cdots & BK_{2,d} \\ \vdots & \vdots & \ddots & \vdots \\ BK_{p,1} & BK_{p,2} & \cdots & BK_{p,d} \end{bmatrix} \quad (1)$$

Here, p signifies the amount of latent solutions and d represents the dimension of problem. Then, every BK is evenly spread as defined in Eq. (2).

$$Y_i = BK_{lb} + rand(BK_{ub} - BK) \quad (2)$$

Whereas, i represents a number among 1 and p , lb and ub signify the lower and upper bounds, correspondingly, $rand$ refers to a randomly generated number among 0 and 1. Throughout the initial process, the BKA picks the finest fitness value as Y_L . The mathematical formulation is shown in Eqs. (3) and (4).

$$f_{best} = \min(f(Y_i)) \quad (3)$$

$$Y_L = Y(find(f_{best} == f(Y_i))) \quad (4)$$

Aggressive Behavior

As hunters of small animals and creatures on the grasses, BK alter their tail and wing directions as per to speed of wind throughout the flight. They float in order to detect their target before jumping to attack. This procedure comprises numerous attack patterns for hunting the prey, which is termed in Eqs. (5) and (6).

$$b_{t+1}^{i,j} = \begin{cases} b_t^{i,j} + n(1 + \sin(r)) \times b_t^{i,j}, & p < r \\ b_t^{i,j} + n \times (2r - 1) \times b_t^{i,j}, & else \end{cases} \quad (5)$$

$$n = 0.05e^{-2(\frac{t}{T})^2} \quad (6)$$

While, p means a constant, which is set to 0.9, $b_t^{i,j}$ signifies the location of i th BK in j th dimension at t th iteration, r refers to a randomly generated amount among 0 and 1, (T) refers to an amount of iterations finished up to now.

Behavior of Migration

Bird migration is a difficult behavior impelled by seasonal variations, weather, and food accessibility, which naturally led by a leader. This tactic of dynamic leader selection certifies effective migration. Its mathematical formulation is given in Eqs. (7) and (8).

$$b_{t+1}^{i,j} = \begin{cases} b_t^{i,j} + C(0,1) \times (b_t^{i,j} - L_t^j), & F_j < F_{ri} \\ b_t^{i,j} + C(0,1) \times (L_t^j - m \times b_t^{i,j}), & else \end{cases} \quad (7)$$

$$m = 2 \times \sin\left(r + \frac{\pi}{2}\right) \quad (8)$$

In the above formulation, L_t^j signifies the leader of j th dimension for t th iteration, F_i represents the fitness of any BK in j th size at the t th iteration. $C(0,1)$ denotes the Cauchy mutation. If $\delta = 1$ and $\mu = 0$, then it changes to the normal method. Its formulation is given below:

$$f(x, \delta, \mu) = \frac{1}{\pi} \frac{\delta}{\delta^2 + (x - \mu)^2} = \frac{1}{\pi} \frac{1}{x^2 + 1} \quad -\infty < x < \infty \quad (9)$$

The fitness function (FF) reveals the accuracy of classifier and the quantity of chosen features. It exploits the accuracy of classification and decreases the set dimension of chosen features. Therefore, the below mentioned FF is utilized for estimating a distinct solution. Its formulation is given in Eq. (10).

$$Fitness = \alpha * ErrorRate + (1 - \alpha) * \frac{\#SF}{\#All_F} \quad (10)$$

Here, $ErrorRate$ is the classification rate of error. $ErrorRate$ is computed as the ratio of improper which is classified to an amount of classifications set amongst 0 and 1. $\#SF$ denotes the amount of chosen features and $\#All_F$ is the complete quantity of features. α is employed for controlling the impact of classification excellence and sub-set length. The value of α is 0.9 in this experiment.

C. DDQN-based Classification Process

For the classification process, the DDQN algorithm has been executed. DDQN is an enhanced form of DQN intended to deal with the over-estimation issues characteristic in DQN. The over-estimation problem can result in biased learning that adversely influences the implementation of the strategy DDQN determines this by separating the maximizing procedure in the targeted network into dual portions [20]. Though the dual networks have dissimilar architectures in the task of reinforcement learning (RL), they sharing the similar output and input kinds of data, make it promising to incorporate them into a united method. The targeted value computation equation is presented in Eq. (11).

$$y_t = r_t + \gamma Q(s_{t+1}, \arg \max_{a'} Q(s_t, a'; \theta); \theta^-) \quad (11)$$

Whereas $\arg \max_{a'} Q(s_t, a'; \theta)$ refers to action selection by the present online network for s_{t+1} , $Q(s_{t+1}, a'; \theta^-)$ signifies Q -value output for s_{t+1} and the action selection a' , γ denotes factor of discount, normally within the interval of $[0,1]$, and r_t refers to instant reward obtained at time step t . This objective value expression decreases over-estimation bias by utilizing the online system for selecting the action and the targeted network to assess it. Fig. 2 represents the infrastructure of DDQN model.

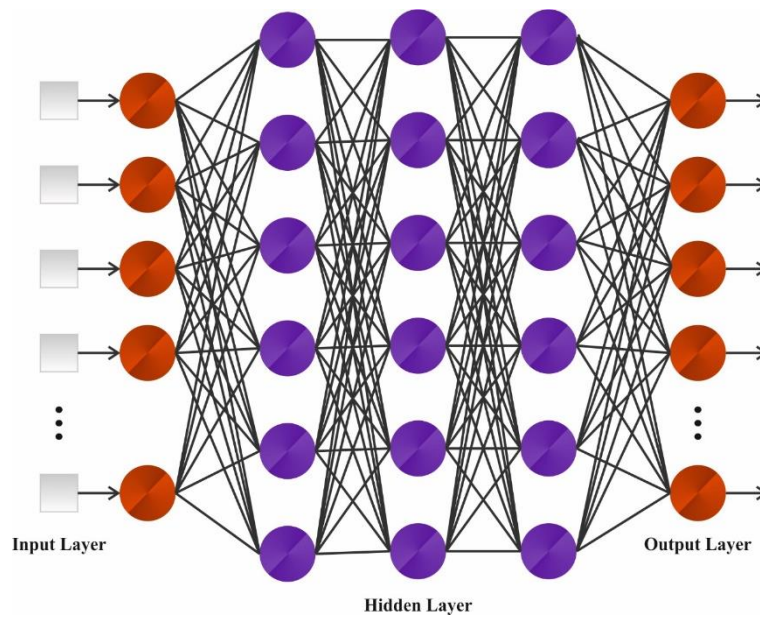


Figure 2. Structure of DDQN method

D. ABC-based Hyperparameter Tuning Model

Eventually, the ABC algorithm-based parameter tuning method is done to improve the classification results of DDQN model. The ABC model is in combination with a crossover operator for enhancing the substituting directions at numerous motor speeds. Then, the resultant optimum data are combined into the torque distribution element, instituting an optimum element intended at further decreasing torque ripple [21].

The ABC system is a swarm intellect technique. When equated with the generally employed genetic algorithm (GA), the ABC system comes with few parameters, lesser intricacy, a decreased possibility of receiving trapped in local goals, quicker convergence velocity, and improved steadiness. In the model of ABC, the amount of leader bees is fixed equivalent to the quantity of follower bees. If a novel, solution has a greater fitness value than a present one, it substitutes the old solution; or else, the old solution is kept. If a solution fails to enhance after a pre-defined maximum amount of upgrades, the food resource is wild, and scout bees were organized to make a novel food resource at random. This iterative procedure endures until the optimum solution is attained.

The ABC system sets its parameters with the amount of food resources SN , the maximum amount of upgrades permitted for a distinct food resource limit. The maximum iteration amount is $MaxIt$, and α is signified as acceleration coefficient. Firstly, SN food resources are made at random, and an exact feasible solution was arbitrarily produced below:

$$v_{ij} = x_{ij} + r(x_{ij} - x_{kj}) \quad (12)$$

Here, v_{ij} signifies the novel location; x_{ij} denotes the original location; x_{kj} is the location of a chosen neighboring food resource at random; r denotes a randomly generated amount which is evenly spread among $[1, 1]$; $k = \{1, 2, \dots, BN\}$ (means a size of population); and $j = \{1, 2, \dots, n\}$ (n refers to a size).

The leader bees distribute data about food resources to the follower bees and then use Eqs. (13) and (14) for selecting a food resource by employing a mechanism of roulette wheel. Eq. (12) is employed for generating a novel food resource location at random in closeness to the present one.

$$p_i = \frac{fit_i}{\sum_{n=1}^{BN} fit_n} \tag{13}$$

$$fit_i = \begin{cases} \frac{1}{1 + f_i}, & f_i \geq 0 \\ 1 + |f_i|, & f_i < 0 \end{cases} \tag{14}$$

Here, fit_i signifies the fitness value. If a food resource shows no development in fitness after a definite amount of generations, then it is measured wild. Furthermore, at the present food resource, the leading bee changes into a scout bee, which utilizes Eq. (14) to discover novel food resources at random:

$$x_{ij} = x_j^{\min} + rand[0,1](x_j^{\max} - x_j^{\min}) \tag{15}$$

Here, x_j^{\min} and x_j^{\max} signify the lower and upper limits of j th dimensional module, correspondingly. The search procedure comprises three bees such as follower, leader, and scout, which is iterated till the model finishes either upon attaining the maximum iterations count.

For enhancing the global optimizer ability of ABC model, this paper presents a crossover operator into the ABC structure. It simplify the switch of values within paternal encoding to generate novel individual. This procedure allows a more complete spread of solutions across the searching space. In this model, a uniform randomly generated number from 0 to 1 is made for every module. If a randomly generated number is under a pre-defined value cr , then the novel value is known; or else, the present value is kept. The ABC system originates a FF for getting an enhanced performance of classification. It determines an optimistic number to imply the better outcome of candidate solution. Here, the classification rate of error reduction is dignified as FF. Its formulation is expressed in Eq. (16).

$$\begin{aligned} fitness(x_i) &= ClassifierErrorRate(x_i) \\ &= \frac{no. of misclassified samples}{Total no. of samples} * 100 \end{aligned} \tag{16}$$

4. Performance Analysis

The performance analysis of the FDAFM-CCDRLM system can be tested utilizing Credit Card Fraud Detection database from Kaggle repository [22]. It includes 900 samples with dual class labels are depicted in Table 1. It holds 30 features in total, out of which 23 features were chosen.

Table 1: Details on Dataset

Class	Samples
Financial_Fraud	450
Financial_Non-Fraud	450
Total	900

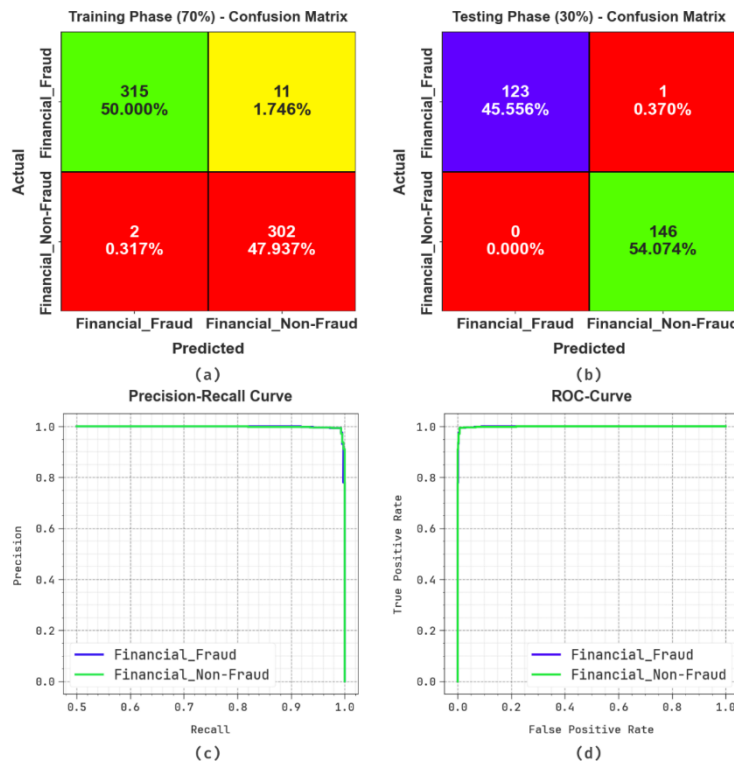


Figure 3. (a-b) Confusion matrix and (c-d) curves of PR and ROC

Fig. 3 represents the classifier outcomes of the FDAFM-CCDRLM methodology on the test dataset. Figs. 3a-3b show the confusion matrices with correct recognition and identification of each 2 classes on a 70%:30% TRASE/TESSE. Fig. 3c displays the PR analysis, signifying superior performance over every classes. Followed by, Fig. 3d demonstrates the ROC values, representing capable outcomes with better ROC analysis for different class labels.

In Table 2 and Fig. 4, the financial fraud detection outcomes of the FDAFM-CCDRLM system is clearly depicted under 70%:30% TRASE/TESSE. The results meant that the FDAFM-CCDRLM approach correctly documented the two samples. With 70%TRASE, the FDAFM-CCDRLM technique gains average $accu_y$ of 97.94%, $prec_n$ of 97.93%, $sens_y$ of 97.98%, $spec_y$ of 97.98%, and MCC of 95.91%. In addition, with 30%TESSE, the FDAFM-CCDRLM methodology achieves average $accu_y$ of 99.63%, $prec_n$ of 99.66%, $sens_y$ of 99.60%, $spec_y$ of 99.60%, and MCC of 99.261%.

Table 2: Detection outcome of FDAFM-CCDRLM technique below 70%:30% TRASE/TESSE

Classes	$Accu_y$	$Prec_n$	$Sens_y$	$Spec_y$	MCC
TRASE (70%)					
Financial_Fraud	97.94	99.37	96.63	99.34	95.91
Financial_Non-Fraud	97.94	96.49	99.34	96.63	95.91
Average	97.94	97.93	97.98	97.98	95.91
TESSE (30%)					
Financial_Fraud	99.63	100.00	99.19	100.00	99.26
Financial_Non-Fraud	99.63	99.32	100.00	99.19	99.26
Average	99.63	99.66	99.60	99.60	99.26

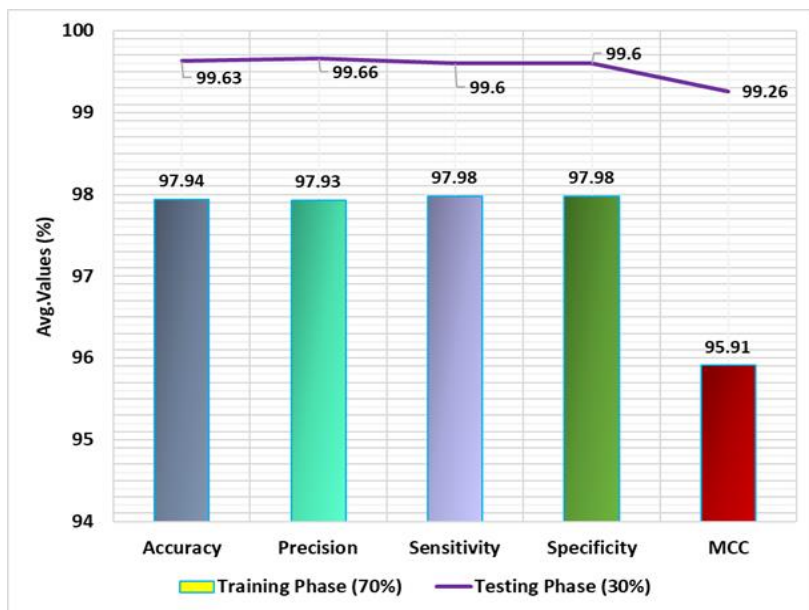


Figure 4. Average outcome of FDAFM-CCDRLM methodology under 70%:30% TRASE/TESTE

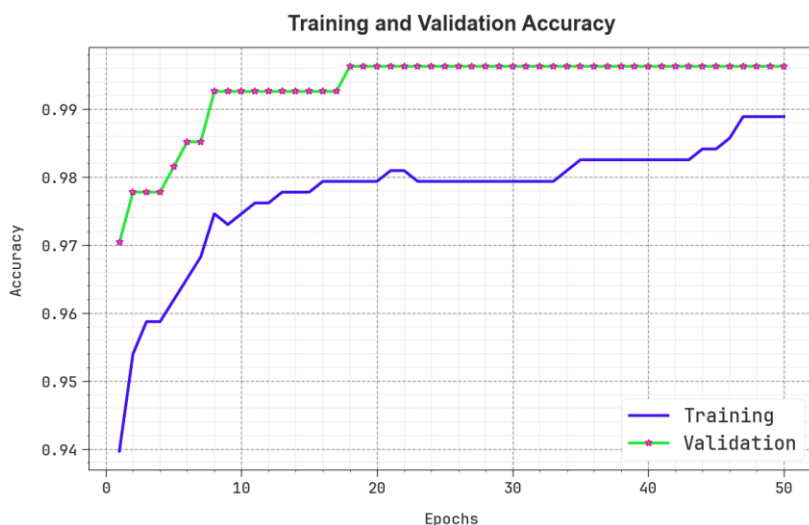


Figure 5. $Accu_y$ Curve of the FDAFM-CCDRLM method

In Fig. 5, the TRA $accu_y$ (TRAAY) and validation $accu_y$ (VLAAY) analysis of the FDAFM-CCDRLM technique is illustrated. The $accu_y$ analysis are computed across the range of 0-50 epochs. The figure highlighting that the TRAAY and VLAAY analysis exhibitions a raising trend which informed the capacity of the FDAFM-CCDRLM approach with superior performance across multiple iterations. In addition, the TRAAY and VLAAY leftovers closer across the epochs, which identifies inferior overfitting and shows maximal outcomes of the FDAFM-CCDRLM system.

In Fig. 6, the TRA loss (TRALO) and VLA loss (VLALO) curve of FDAFM-CCDRLM technique is showed. The values of loss are computed across within the range of 0-50 epochs. It is denoted that the TRALO and VLALO analysis exemplify a reducing trend, which notified the capability of the FDAFM-CCDRLM algorithm in balancing a trade-off. The continuous reducing in values of loss besides assurances the high outcome of the FDAFM-CCDRLM system.

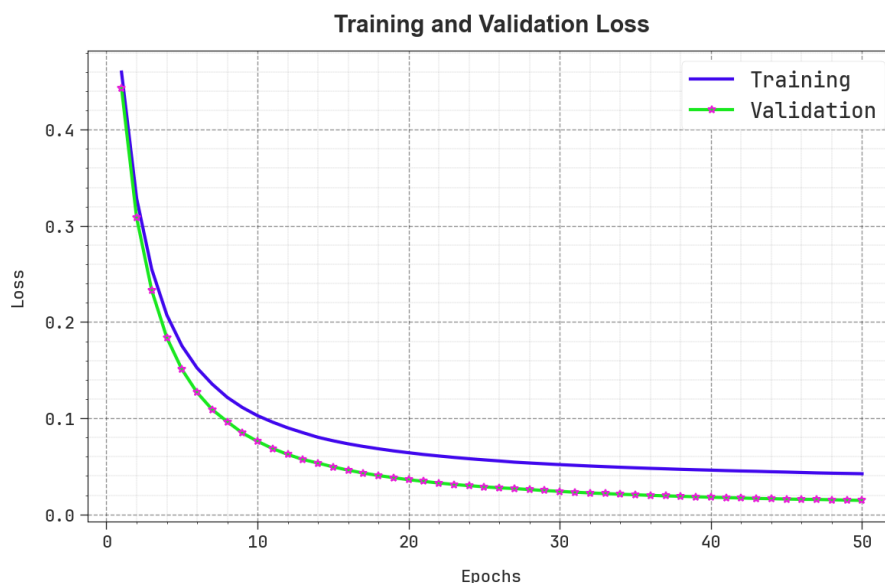


Figure 6. Loss graph of the FDAFM-CCDRLM algorithm

In Table 3 and Fig. 7, a comparison study of the FDAFM-CCDRLM methodology is obviously exemplified [23]. The outcomes specify that the DSGBT technique has displayed unsuccessful performance. Along with that, the DTNB, RFGBT, and DTDS algorithms have showed somewhat boosted outcomes. Meanwhile, the DTGBT, OCSODL-CCFD, and CCFDC-GRFOEL techniques have illustrated reasonably closer outcomes. However, the FDAFM-CCDRLM methodology outperforms the other methods with increased $accu_y$ of 99.63%, $prec_n$ of 99.66%, $sens_y$ of 99.60%, and $spec_y$ of 99.60%.

Table 3: Comparative outcomes of FDAFM-CCDRLM methodology with current techniques

Framework	$Accu_y$	$Prec_n$	$Sens_y$	$Spec_y$
FDAFM-CCDRLM	99.63	99.66	99.60	99.60
CCFDC-GRFOEL	99.47	96.24	97.61	97.27
OCSODL-CCFD	99.12	96.63	96.38	97.12
DSGBT Method	98.15	98.62	96.16	98.64
DTGBT Model	98.88	95.67	98.80	97.24
DTDS Method	98.81	98.63	96.53	98.38
RFGBT Model	98.81	97.44	95.73	98.91
DTNB Model	98.18	96.97	98.91	98.70

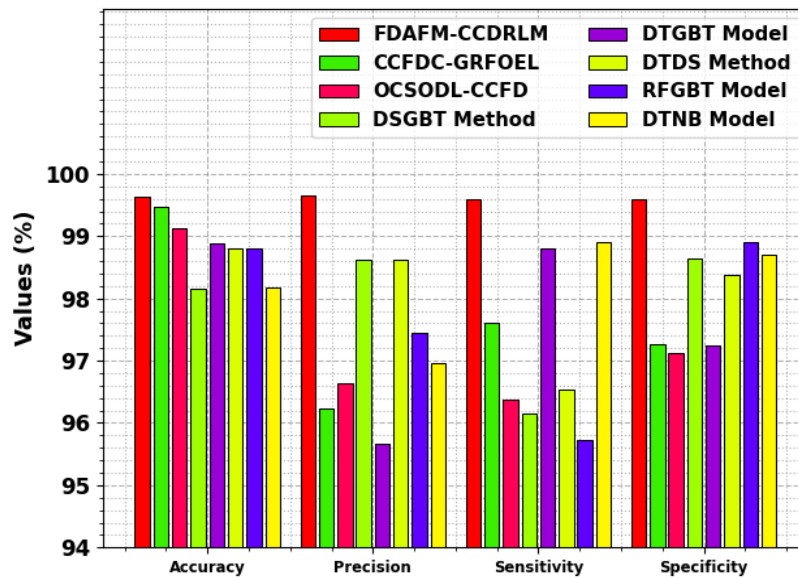


Figure 7. Comparative analysis of FDAFM-CCDRLM methodology with recent approaches

The processing time (PT) outcomes of the FDAFM-CCDRLM system is equated with existing DL techniques in Table 4 and Fig. 8. The table values presented that the FDAFM-CCDRLM approach reaches inferior PT of 20min. On the other hand, the CCFDC-GRFOEL model, OCSODL-CCFD method, DSGBT system, DTGBT technique, DTDS algorithm, RFGBT methodology, and DTNB system attain maximal PT values of 68min, 70min, 67min, 36min, 51min, 56min, and 41min, respectively. Thus, the SEHDL-OSCCR approach can be used for the recognition of financial fraud.

Table 4: PT outcomes of FDAFM-CCDRLM system with recent approaches

Methods	Processing Time (min)
FDAFM-CCDRLM	20
CCFDC-GRFOEL	68
OCSODL-CCFD	70
DSGBT Method	67
DTGBT Model	36
DTDS Method	51
RFGBT Model	56
DTNB Model	41

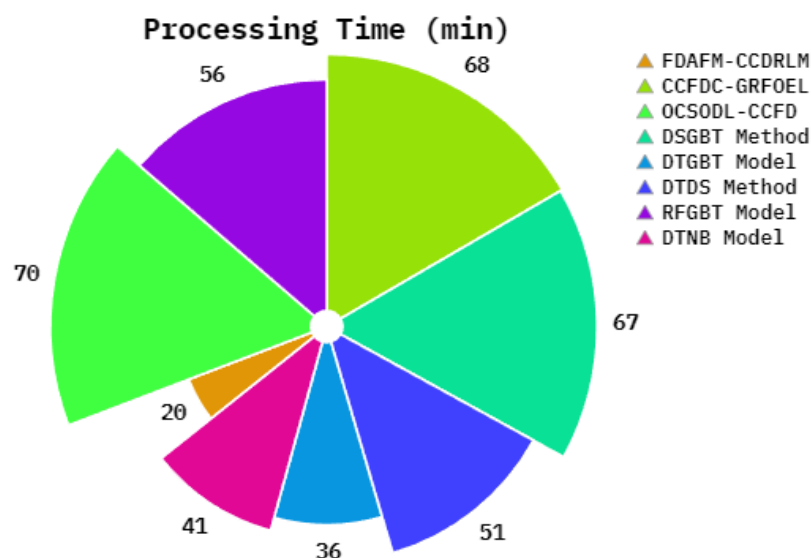


Figure 8. PT analysis of FDAFM-CCDRLM methodology with recent approaches

5. Conclusion

This paper presents a FDAFM-CCDRLM model. The main intention of FDAFM-CCDRLM model is to improve analysis of financial data in the economic management. Initially, the min-max normalization is employed in the data normalization stage for converting a data of input into a suitable format. Besides, the proposed FDAFM-CCDRLM model designs a BKA for the subset of feature selection process. For the classification process, the DDQN algorithm has been executed. At last, the ABC algorithm-based parameter tuning method is done to improve the classification outcomes of the DDQN model. The experimental evaluation of FDAFM-CCDRLM system can be verified on a benchmark database. The extensive outcomes highlight the significant solution of the FDAFM-CCDRLM approach to the financial data analysis classification process.

Funding: “This research received no external funding”

Conflicts of Interest: “The authors declare no conflict of interest.”

References

- [1] E. Strelcenia and S. Prakoonwit, "Improving Classification Performance in Credit Card Fraud Detection by Using New Data Augmentation," *AI*, vol. 4, pp. 172–198, 2023.
- [2] S. Han, K. Zhu, M. Zhou, and X. Cai, "Competition-driven multimodal multiobjective optimization and its application to feature selection for credit card fraud detection," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 52, pp. 7845–7857, 2022.
- [3] 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," *Inf. Sci.*, vol. 557, pp. 302–316, 2021.
- [4] G. Kumar, C. B. Muckley, L. Pham, and D. Ryan, "Can alert models for fraud protect the elderly clients of a financial institution?" *The European Journal of Finance*, vol. 25, no. 17, pp. 1683–1707, 2019.
- [5] H. O. Bello, C. Idemudia, and T. V. Iyelolu, "Integrating machine learning and blockchain: Conceptual frameworks for real-time fraud detection and prevention," *World Journal of Advanced Research and Reviews*, vol. 23, no. 1, pp. 056–068, 2024.
- [6] B. R. Chirra, "AI-Driven Fraud Detection: Safeguarding Financial Data in Real-Time," *Revista de Inteligencia Artificial en Medicina*, vol. 11, no. 1, pp. 328–347, 2020.
- [7] H. Fanai and H. Abbasimehr, "A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection," *Expert Syst. Appl.*, vol. 217, p. 119562, 2023.
- [8] W. Utami, L. Nugroho, R. Mappanyuki, and V. Yelvionita, "Early warning fraud determinants in banking industries," *Asian Economic and Financial Review*, vol. 10, no. 6, p. 604, 2020.

- [9] N. Shonhadji and A. Maulidi, "The roles of whistleblowing system and fraud awareness as financial statement fraud deterrent," *International Journal of Ethics and Systems*, vol. 37, no. 3, pp. 370–389, 2021.
- [10] M. A. Al-Khasawneh, M. Faheem, D. M. Alsekait, A. Abubakar, and G. F. Issa, "Hybrid Neural Network Methods for the Detection of Credit Card Fraud," *Security and Privacy*, vol. 8, no. 1, Jan. 2025. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.500>.
- [11] Z. Huang, H. Zheng, C. Li, and C. Che, "Application of machine learning-based k-means clustering for financial fraud detection," *Academic Journal of Science and Technology*, vol. 10, no. 1, pp. 33–39, 2024.
- [12] Y. Cheng, J. Guo, S. Long, Y. Wu, M. Sun, and R. Zhang, "Advanced financial fraud detection using GNN-CL model," in *2024 International Conference on Computers, Information Processing and Advanced Education (CIPAE)*, 2024, pp. 453–460.
- [13] N. Innan, A. Sawaika, A. Dhor, et al., "Financial fraud detection using quantum graph neural networks," *Quantum Machine Intelligence*, vol. 6, no. 1, p. 7, 2024.
- [14] S. Khodabandehlou and A. H. Golpayegani, "FiFrauD: Unsupervised financial fraud detection in dynamic graph streams," *ACM Transactions on Knowledge Discovery from Data*, vol. 18, no. 5, pp. 1–29, 2024.
- [15] M. M. Ismail and M. A. Haq, "Enhancing Enterprise Financial Fraud Detection Using Machine Learning," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 14854–14861, 2024.
- [16] M. Maashi, B. Alabdullah, and F. Kouki, "Sustainable financial fraud detection using garra rufa fish optimization algorithm with ensemble deep learning," *Sustainability*, vol. 15, no. 18, p. 13301, 2023.
- [17] S. Z. Aftabi, A. Ahmadi, and S. Farzi, "Fraud detection in financial statements using data mining and GAN models," *Expert Systems with Applications*, vol. 227, p. 120144, 2023.
- [18] L. Munkhdalai, T. Munkhdalai, K. H. Park, et al., "Mixture of activation functions with extended min-max normalization for forex market prediction," *IEEE Access*, vol. 7, pp. 183680–183691, 2019.
- [19] Y. Deng, L. Xiao, and Y. Shi, "Enhanced Hyperspectral Forest Soil Organic Matter Prediction Using a Black-Winged Kite Algorithm-Optimized Convolutional Neural Network and Support Vector Machine," *Applied Sciences*, vol. 15, no. 2, p. 503, 2025.
- [20] Y. Liu, T. Yang, L. Tian, and J. Pei, "SGD-TripleQNet: An Integrated Deep Reinforcement Learning Model for Vehicle Lane-Change Decision," *Mathematics*, vol. 13, no. 2, p. 235, 2025.
- [21] H. Wang, J. Wu, C. Xie, and Z. Guo, "Vehicle-Mounted SRM DITC Strategy Based on Optimal Switching Angle TSF," *World Electric Vehicle Journal*, vol. 16, no. 1, p. 26, 2025.
- [22] Kaggle Dataset, "Credit Card Fraud Detection," [Online]. Available: <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud>.
- [23] M. Maashi, B. Alabdullah, and F. Kouki, "Sustainable financial fraud detection using garra rufa fish optimization algorithm with ensemble deep learning," *Sustainability*, vol. 15, no. 18, p. 13301, 2023.