scientific reports

Check for updates

OPEN

Hybrid Big Bang-Big crunch with cuckoo search for feature selection in credit card fraud detection

Mohd Shukri Ab Yajid[1], Nilesh Bhosle[2], Gadug Sudhamsu[3], Ali Khatibi[1], Sahil Sharma[4], Rubal Jeet[5], R. Sivaranjani[6], A. Bhowmik[7,8] & A. Johnson Santhosh[9]✉

The technological advancements of financial applications and the expansion of e-commerce platforms have increased the daily volume of credit card transactions. Consequently, there has been a substantial rise in instances of credit card fraud that leads to monetary losses for both individuals and financial institutions. The fraudsters continuously develop new technologies to breach security and acquire the credit card credentials of users through fraudulent activities such as scamming, phishing, or exploiting data breaches. There are numerous machine learning and deep learning techniques for detecting credit card frauds. However, due to the higher dimensionality and the imbalance between fraud and legitimate transactions, it becomes challenging to determine credit frauds with effective performance. To address the aforementioned issues, the current work has presented a novel hybrid Big Bang-Big crunch with cuckoo search (HB^{3}C^{2}S) method for feature selection prior to performing the classification process. Here, both the Big Bang-Big crunch (BB-BC) and cuckoo search (CS) are metaheuristic algorithms, with BB-BC being a physics-inspired algorithm derived from the theory of universe evolution and CS being an inspiration from the cuckoo bird's brood parasitism behavior. In the HB^{3}C^{2}S method, the BB-BC algorithm is utilized for exploiting the solution space locally and CS to explore the solutions globally. Here, the CS algorithm uses the Levy flight attribute to help the BB-BC agents escape from stagnation and premature convergence. After feature selection, classification is performed using Deep Convolutional Neural Networks (DCNN) and Enhanced DCNN (EDCNN) to improve detection accuracy. The efficacy of the proposed framework is accessed through experiments conducted on the ECC (European Credit Cardholders) dataset. The HB^{3}C^{2}S-based system achieves 94.59% accuracy with DCNN and 95.61% with EDCNN, outperforming individual BB-BC and CS feature selection techniques. The experimental evaluations also confirm the efficacy of the proposed framework to detect credit card frauds, surpassing state-of-the-art approaches.

Keywords Big Bang-Big crunch, Cuckoo search, Metaheuristic, Deep neural networks, Credit card frauds

In the age of rapid advancements in technology, the fusion of payments and digitization has sparked remarkable transformations in the manner in which consumers and organizations engage with money. This combination of technology and money is the foundation of modern economic systems. There are numerous technology-based payment methods, such as payment cards, wallet payments, QR code payments, cryptocurrencies, etc[1,2]. In these technology-based transactions, credit card payments serve a crucial role in a wide range of commercial operations, both online and offline, due to their widespread presence as well as their accessibility and adaptability.

[1]Management and Science University, Shah Alam, Malaysia. [2]Department of Computing Science and Artificial Intelligence, NIMS Institute of Engineering & Technology, NIMS University Rajasthan, Jaipur, India. [3]Department of Computer Science and Engineering, School of Engineering and Technology, JAIN (Deemed to be University), Bangalore, Karnataka, India. [4]Department of Computer Science and Engineering, Vivekananda Global University, 303012 Jaipur, Rajasthan, India. [5]Department of Computer Science Engineering, Chandigarh Engineering College, Chandigarh Group of Colleges-Jhanjeri, 140307 Mohali, Punjab, India. [6]Department of Computer Science and Engineering, Raghu Engineering College, 531162 Visakhapatnam, Andhra Pradesh, India. [7]Assistant Professor, Department of Additive Manufacturing, Mechanical Engineering, SIMATS, Saveetha Institute of Medical and Technical Sciences, Thandalam, 602105 Chennai, India. [8]Centre for Research Impact & Outcome, Chitkara University Institute of Engineering and Technology, Chitkara University, 140401 Rajpura, Punjab, India. [9]Faculty of Mechanical Engineering, Jimma Institute of Technology, Jimma University, Jimma, Ethiopia. ✉email: johnson.antony@ju.edu.et

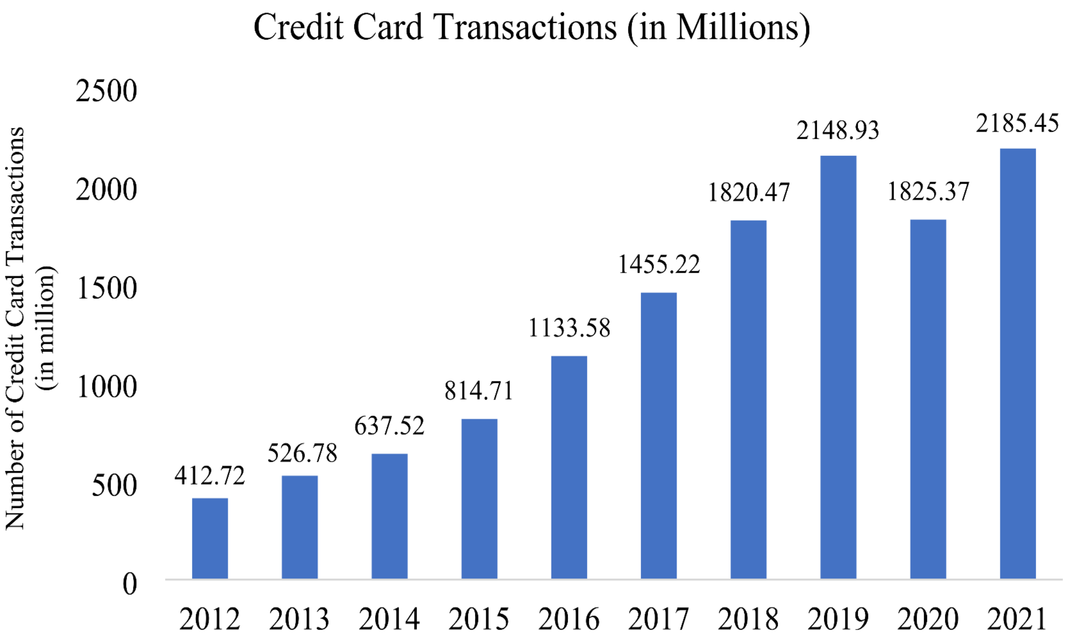
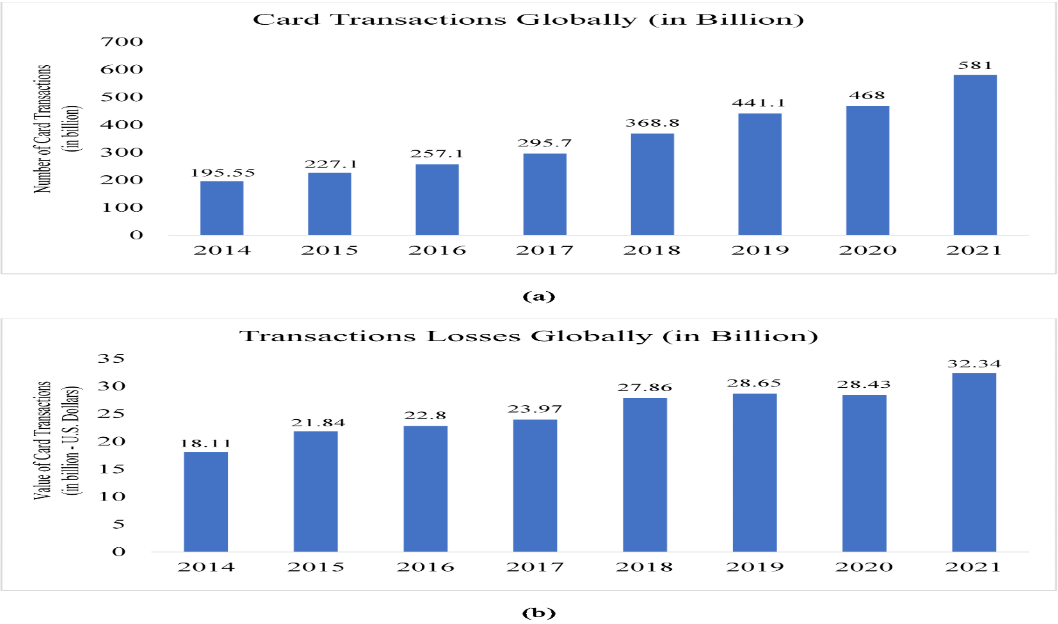


Fig. 1. Annual credit card transactions in India (2012–2021).



(a)

(b)

Fig. 2. (**a**) Annual card transactions globally (2014–2021), (**b**) Value of card transactions loses globally (2014–2021).

However, this widespread presence also brings along a specific set of shortcomings, as credit card transactions continue to be attractive targets for fraudulent operations carried out by highly skilled cybercriminals.

The first credit card was issued in 1958 in the USA, and the same was issued in 1981 in India[3]. In India, the annual number of credit card transactions were 412.72 million in 2012, which increased to 2,185.45 million in 2021[4]. Although there were the issues of credit card payment decline during the Corona virus pandemic years, the annual transactions still increased exponentially afterwards. The change in annual transactions from 2012 to 2021 is shown in Fig. 1.

The sustainable growth of credit card transactions is successful due to the emergence of digital payment systems, mobile banking applications, the growth of e-commerce platforms, and enhanced security of online transactions. As per the financial Statista reports, global card transactions were 195.55 billion in 2014, which is further increased to 581 billion in 2021[5]. The change in global card transactions is depicted in Fig. 2a. However, with the growth of card transactions, there are also transactional losses due to fraud. In 2014, there were transaction losses of 18.11 billion US dollars, which increased to 32.34 billion in 2021 and is expected to increase to 38.5 billion in 2027[6]. The financial card transaction losses from 2014 to 2021 are illustrated in Fig. 2b[7].

Since the inception of credit cards, fraud activities have led to billions of dollars in losses and escalating on a daily basis. Despite advancements in security, fraudsters continually develop sophisticated techniques, making detection increasingly challenging. One of the key reasons, especially for credit card fraud, among the other digital payment methods, is the higher credit limit assigned by financial institutions to users[3]. As technology is growing, so do the tactics of the fraudsters to make the frauds which makes it difficult for the traditional rule-based systems to adapt. The dynamic nature of fraudulent activities, combined with imbalanced transaction datasets, high-dimensional features, and the need for real-time detection, presents significant challenges for fraud detection systems. The increasing credit card fraud activities with the increasing adoption of digital payments can hinder the economic growth of businesses and the country.

Credit card fraud can occur either by obtaining the physical card illegally or by obtaining the card information[3]. The former category includes various attack instances such as account takeover, fake cards, doctored cards, assumed identity fraud, and stolen cards, all of which require physical access to the card or personal information. The latter category, which is more prevalent in digital fraud, the fraudster can acquire the card information illegally through numerous means, such as card ID theft, card imprints, clean frauds with user confidence, friendly frauds, etc. Among the aforementioned frauds, the former category frauds are a bit difficult to attempt as the actual identity of the fraudster may get revealed. On the other hand, the latter category of frauds is more feasible as the fraudsters can easily attain the credit card holder's data on internet websites via phishing, shoulder surfing, trojan, pharming attacks, etc[8]. Modern fraudsters employ machine learning-based adversarial attacks to bypass security measures, making traditional fraud detection methods ineffective. In the year 2020, there were a total of 3,93,207 instances of credit card fraud among the total reported 1.4 million incidents of identity theft[9]. These statistics highlight the urgency for robust and adaptive fraud detection mechanisms.

Therefore, it is imperative for financial institutions to adopt intelligent fraud detection mechanisms capable of handling dynamic and evolving fraud strategies. There are numerous research methods based on machine learning and deep learning for detecting credit card frauds, as discussed in the next section. However, detecting automated credit card fraud remains challenging due to data imbalance, high dimensionality, and the evolving nature of fraudulent activities. Traditional methods often suffer from high false positives, low recall rates, and scalability issues. To address these challenges, this research proposes an efficient HB^{3}C^{2}S method, which effectively enhances feature selection for fraud detection. This method integrates the exploratory strengths of the BB-BC algorithm[10] with the diversity-enhancing properties of the CS algorithm[11], ensuring better feature selection and improved classification accuracy. The BB-BC algorithm is a Big Bang-Big crunch theory-based algorithm with two successive steps of big bang and big crunch[12]. The big bang step generates the initial population and explores the solutions. The big crunch step acts on the convergence of the solutions by calculating the center of mass. During the initial exploration, the candidates may get trapped in the small subdomain during the process of determining the optimal solutions. The proposed HB^{3}C^{2}S method handles the situation using the attributes of the CS algorithm. The CS algorithm is derived from the special aggressive reproduction strategy of some species of cuckoo birds[13]. It uses Levy flight attributes for randomness, long-range exploration, and diverse search trajectories[14]. These attributes facilitate the BB-BC algorithm by avoiding premature convergence. The features selected using the HB^{3}C^{2}S method are used for the classification of fraud transactions by incorporating the deep neural network methods of Deep Convolutional Neural Networks (DCNN)[15,16] and Extended Deep Convolutional Neural Networks (EDCNN)[17,18].

The process of credit card fraud detection includes the modules of dataset input, data pre-processing, feature selection, and classification. Figure 3 illustrates the proposed framework to detect credit card frauds. In this research work, the experimental evaluations are conducted for the ECC dataset. As depicted in Fig. 3, the dataset is pre-processed with the RandomUnderSampler method to address the imbalance of fraud and legitimate transactions in the dataset. Further, the data is processed for the feature selection and classification modules using the proposed HB^{3}C^{2}S method and deep neural networks, respectively.

The remaining portion of the paper is ordered as follows: Section "Literature review" reviewed the research conducted for detecting the credit card frauds, specifically focusing on the utilization of different machine learning and deep learning methods. Section "Preliminaries" presents the fundamental concepts of the BB-BC and CS algorithms, which are employed in the proposed HB^{3}C^{2}S method. Section "Dataset and preprocessing" discusses the dataset and the preprocessing of the data for fraud detection. Section "Proposed method for feature selection" describes a detailed explanation of the proposed HB^{3}C^{2}S method for selecting features in card fraud detection. Section "Classification" demonstrates the classification module of the proposed framework to detect frauds. Section "Experimental assessment" presents the results and analysis of the conducted experiments, as well as a discussion on the significance of feature selection to detect credit card fraud. Section "Conclusion and future scope" provides the conclusion of the work along with future suggestions.

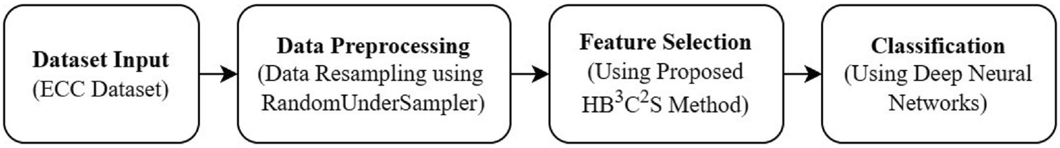


Fig. 3. Proposed framework for credit card fraud detection.

Literature review

Credit card fraud activities in businesses and the global financial sector results in financial losses and legal expenses. In the past decade, researchers have significantly increased their efforts to combat credit card fraudulent activities. The safety of financial operations depends on an efficient fraud detection system. The researchers have made substantial contributions to developing novel and innovative techniques for detecting credit card fraud. This literature review specially examines the four critical aspects to detect credit card fraud: machine learning methodologies, deep learning methodologies, strategies for data balancing, and techniques for feature selection.

Researchers have extensively explored different machine learning techniques to address credit card fraud detection. Saheed et al.[19,20] incorporated different machine learning methods for the credit card fraud detection. The authors have also performed the feature selection prior to fed the data for classification. Saheed et al.[19] utilized the genetic algorithm (GA) for feature selection and performed the experiments on German credit card using the machine learning methods such as Naïve Bayes (NB), Random Forest (RF) and Support Vector Machine. Further, Saheed et al.[20] incorporated the principal component analysis (PCA) for feature selection, experiments on the German credit card and Taiwan credit card datasets, and classification using supervised machine learning methods. Sailusha et al.[21] used the Adaboost and random forest algorithms for detecting credit card frauds. The authors performed the experiments for the ECC dataset and indicated the better performance of random forest algorithm in comparison with Adaboost. Rajora et al.[22] presented a comparison of the distinct machine learning techniques for detecting credit card frauds. The authors conducted the experiments for the dataset of ECC, and the effective performance was noted for the random forest (RF) and k-nearest neighbor (KNN) algorithms. Randhawa et al.[23] implemented the Adaboost and majority voting methods, along with the utilization of different machine learning techniques, for detecting fraudulent activities in the transactions of credit cards. The authors illustrated the better performance results of the majority voting classifier for experiments on the ECC dataset. Sulaiman et al.[24] presented a review for detecting credit card frauds using different machine learning techniques. In order to enhance the effectiveness of the available machine learning methods, the authors hybridized these methods with artificial neural networks. The overall model has attained an effective performance to detect credit card frauds. Kumar et al.[25] employed the support vector machine (SVM) to detect credit card frauds with experiments on the dataset extracted from Kaggle. The authors have compared the results with state-of-the-art machine learning methods to detect frauds in credit card transactions. The dataset included the feature attributes of transaction class, transaction country, risk factor of the country, number of transactions declines per day, transaction amount, merchant ID, etc. The performance comparison indicated the effective performance of the SVM algorithm compared to other methods. Khan et al.[26] adapted the methods of decision tree (DT), naïve bayes (NB), logistic regression (LR), fuzzy c-means (FCM), and principal component analysis (PCA) for comparing the performance of these methods in detecting credit card frauds. The authors have tested the various combinations of these methods with experiments on the ERC dataset and determined the effective performance for the combination of PCA, FCM, and LR. Alfaiz and Fati[27] experimented with the 66 machine learning methods to determine credit card frauds in two stages. The initial stage determines the top three methods, which are tested with another 19 resampling in the second stage. Among all the methods, the authors combined the All-KNN Category Boost (CatBoost) and determined the All-KNN-CatBoost as the efficient method for detecting credit card frauds.

In recent years, deep learning algorithms, particularly neural networks, have emerged as effective techniques for detecting credit card frauds. Jurgovsky et al.[28] incorporated the long short-term memory (LSTM) for detecting credit card frauds by considering it a sequence of classification tasks. The authors conducted the experiments for the real-time dataset and determined the results with a random forest algorithm as well to analyze the performance of LSTM compared to other techniques. Fiore et al.[29] employed generative adversarial networks for detecting credit card frauds with experiments on the ECC dataset. The authors have attained effective results with improved sensitivity but suffered from a slight increase in false positive values. Zioviris et al.[30] presented a multistage model using the deep learning method to detect credit card frauds. The authors have incorporated the method of deep convolutional neural networks (DCNN) for classifying the fraudulent activities. Forough and Momtazi[31] utilized the advantages of probabilistic graphical model and deep neural network for detecting credit card frauds. In particular, authors have used conditional random fields (CRF) and LSTM with experiments on the ECC and the Brazilian datasets. The authors noted the superiority in efficiency of the proposed LSTM-CRF technique compared to other deep learning techniques. Kasasbeh et al.[32] implemented multilayer perceptron (MLP) for detecting the frauds of credit cards. The authors conducted the experiments by adding one, two, and three hidden layers and analyzed the performance of MLP by performing experiments on the ECC dataset. The experimentation accuracy indicates the higher performance of MLP with two hidden layers compared to one and three layers based MLP. Karthika and Senthilselvi[33] presented the one-dimensional Dilated Convolutional Neural Network model (OD-DiCNN) for detecting credit frauds by training the model with both temporal and spatial features. Here, the OD-DiCNN model is designed by embedding the convolutional neural networks (CNN) with the dilated convolutional layer (DiCL). The authors stated to improve the weight function of the presented method to better analyze fraudulent activities.

Furthermore, addressing data imbalances is also crucial in order to improve the efficacy of the systems able to detect credit card fraud. Traditional machine learning and deep learning methods face challenges while dealing with imbalanced data, as the number of legitimate transactions will always be higher in the case of credit card transactions. There are numerous research techniques, including undersampling, oversampling, etc., that have been explored to address this problem. Ileberi et al.[34] used the Synthetic Minority Oversampling TEchnique (SMOTE) for balancing the unbalanced ECC dataset for detecting credit card frauds. The authors initially analyzed the classification using different machine learning methods. Further, the AdaBoost algorithm was adapted in addition to the mentioned machine learning methods to improve the efficacy of methods for detecting fraudulent activities. The experimental results indicate the effective performance after balancing the data. Khalid et al.[35] balanced the imbalanced ECC dataset using undersampling and SMOTE methods. The authors determined the effective performance of the machine learning and ensemble learning classifiers for the processed balanced data using the incorporated methods. Singh et al.[36] balanced the imbalanced German and European credit card dataset using the different techniques of SMOTE, SMOTE-Edited Nearest Neighbor (SMOTE-ENN), All-KNN, and random undersampling. The fraudulent activities were analyzed using the local outlier factor (LOF) and isolation forest (IF) algorithms. Mim et al.[37] presented the soft voting ensemble learning technique to detect financial credit card frauds. The authors used different types of dataset balancing techniques, such as ADASYN (Adaptive Synthetic Sampling Approach), SMOTE, random undersampling, SMOTE-Edited Nearest Neighbor (SMOTE-ENN), and SMOTE-Tomek. The authors conducted numerous experiments using different machine learning classifiers as well as soft voting ensemble learning methods. The authors indicated the superior performance of the ADASYN oversampling method along with the voting classifier combination of MLP, XGBoost, and RF methods. Mienye and Sun[38] hybridized the SMOTE method with ENN for dataset resampling. The balanced class distributed data was utilized for the classification using an ensemble of gated recurrent unit (GRU), LSTM, and MLP techniques. The performance evaluations indicated the effective performance of the presented fraud detection model compared to individual machine learning and deep learning techniques.

Moreover, feature selection plays a vital role in enhancing the efficiency and interpretability of credit card fraud detection models. Selecting pertinent features using the different techniques from the pool of extracted transaction features helps streamline the detection process and reduce computational complexity. Ileberi et al.[39] employed the genetic algorithm (GA) for feature selection in the application of credit card fraud detection. The optimized features were utilized to effectively classify the credit card transactions using different machine learning classifiers. Additionally, the random forest (RF) algorithm was incorporated to evaluate the fitness function as well as to handle the missing values and large input variables. Among the presented methods, GA-RF and GA-DT have attained superior performance results for the ECC and synthetic datasets, respectively. Geetha and Dheepa[40] incorporated the swarm intelligence-based artificial bee colony optimization (ABC) algorithm to select features and enhanced neural networks (ENN) for the classification of credit card frauds. The authors have also used the Logical Graph of Behavior Profile (LGBP) method to graph the transaction records for detecting credit card frauds. The authors declared the superiority of the LGBP-ENN method compared to the existing methods of Transaction Aggregation Technique (TAS) and LGBP. Further, Geetha and Dheepa[41] improved the feature selection criteria using the Modified Butterfly Optimization Algorithm (MBOA) method. Here, the dataset features were structured using the LGBP approach prior to selecting the features using the MBOA method. The classification performance was improved using the hybridization of the CNN model with the RNN (recurrent neural network). The performance evaluations show the effectiveness of the presented framework compared to Geetha and Dheepa[40] and the individual methods of TAS and LGBP. Arun and Rajesh[42] utilized the binary emperor penguin optimization (BEPO) algorithm for the selection of features, the optimal gated recurrent unit (OGRU) for classification, and Harris Hawks optimization to optimize the gated recurrent unit (GRU) method. The overall framework attained optimal results for the credit card fraud and German datasets. Karthika and Senthilselvi[43] presented the Hunter-prey optimization (HPO) algorithm for feature selection and the Inception-ResNet-v2 method for classification in credit card transactional frauds. The experimental evaluations were conducted for the ECC dataset and determined efficient results. Rawashdeh et al.[44] conducted the process of detecting credit card frauds in three steps. The initial step involves the information gain (IG) method for the raking of dataset features; the second step incorporates the competitive swarm optimization (CSO) method to select the optimal features from the complex search space; and the third step employs the random weight network (RWN) for the classification of fraud detection. The experimental findings demonstrate the effectiveness of the presented approach compared to traditional machine learning classifiers.

In summary, the literature on credit card fraud detection emphasizes the significance of utilizing advanced methodologies, addressing data imbalances, and employing effective feature selection techniques to develop robust and accurate fraud detection systems. However, existing approaches often struggle with issues such as high false positive rates, suboptimal feature selection methods, and inadequate handling of class imbalance, which can significantly impact detection performance. Furthermore, the lack of a holistic framework integrating advanced techniques limits the overall effectiveness of fraud detection systems. Our proposed framework aligns closely with these insights, as it incorporates advanced feature selection methods, tackles data imbalance issues, and integrates cutting-edge methodologies. Unlike existing hybrid metaheuristic approaches that primarily emphasize either local or global search, the proposed HB^{3}C^{2}S method strategically balances both aspects by utilizing the BB-BC algorithm for local exploitation and the CS algorithm for global exploration. The BB-BC phase refines the search within promising regions, while the CS phase enhances diversity through Levy flight-based perturbations that prevents premature convergence. This hybridization improves feature selection effectiveness, leading to enhanced classification performance. Additionally, the framework employs RandomUnderSampler for data balancing, and deep neural networks for classification. By synthesizing these elements into a cohesive framework, we aim to enhance the effectiveness and reliability of credit card fraud detection.

Preliminaries

The section describes the preliminaries for the BB-BC and CS algorithms that are employed for the proposed HB^{3}C^{2}S method. The fundamentals of these algorithms are discussed as follows.

Big Bang-Big crunch

The BB-BC algorithm is a computational optimization algorithm based on the physics theories of big bang and big crunch in cosmology[12]. Big bang and big crunch are the phases of the algorithm in which big bang phase initializes with the generation of the candidate solutions in the defined search space. These candidate solutions explore the space by moving away from each other. Then, the solutions converge towards the favorable regions during the big crunch phase. The output for the big crunch phase is determined by evaluating the center of mass based on the multiple inputs of the candidate solutions. Further, the new solutions for the next generation are generated using the calculated center of mass. The process continues until the termination criteria of maximum iterations met or the required solution is obtained.

Cuckoo search

The CS algorithm is a metaheuristic algorithm that utilizes swarm intelligence and is derived by imitating the brood parasitism attribute observed in certain cuckoo species[13,45]. The algorithm begins by stochastically producing the population of cuckoos as the solutions in the defined space. Cuckoo birds use Levy flight attributes to incorporate randomness and explore the search space for the cuckoo to lay eggs as the new solution. These laid solution eggs are evaluated to replace it with the inferior eggs of the nest (solution population) so that a better solution can be determined. Here, the nest is selected by calculating the fitness function. Nests (solutions) with better fitness functions are stored as it can provide better survival and offspring production chances. The process continues until the termination criteria are met. The CS algorithms work on the basis of the following three principles:

1. Every cuckoo lays a single egg each time and deposits it into a nest chosen randomly.
2. Nests with the best eggs continue to exist into subsequent generations, as the best eggs are indications of high-quality solutions.
3. The quantity of available host nests remains constant, and each nest has the probability to come across an alien egg, p_a, within the range of [0, 1]. Upon discovery, the host bird may either abandon the egg or vacate the nest entirely, opting to construct an entirely new nest at a changed location.

Dataset and preprocessing

The section describes the dataset utilized for the experiments of the credit card fraud detection. Additionally, the preprocessing module is elucidated, as it is essential to ensure the quality of the data and the optimized performance of the proposed framework for detecting credit card frauds.

Dataset

In this research work, the ECC dataset is incorporated for the research experiments, which is a dataset of two days of credit card transactions carried out by European cardholders in September 2013[46]. The dataset exclusively consists of numerical variables that have been obtained by a PCA transformation. There are a total of 30 feature attributes in the dataset, of which 28 features (V1, V2, …, V28) are PCA-based primary components, and two more features are time and amount. These 28 features are the transformed features due to confidentiality concerns. The time feature is the time interval, measured in seconds, between the initial transaction and other transactions in the dataset. The amount feature denotes the financial worth of a transaction. A response variable 'class' is also available in the dataset, which represents the ground truth value of a transaction by assigning value 1 to fraud activities and 0 to legitimate activities. The statistics of the dataset are depicted in Table 1.

Data preprocessing

Data preprocessing is a crucial step in detecting credit card frauds, as the dataset is highly imbalanced. The dataset statistics illustrated in Table 1 indicate that the proportion of fraud transactions is much lower compared to legitimate transactions. This data imbalance can affect the overall performance of the fraud detection system. Here, the data under the sampling approach is adapted to balance the data. The RandomUnderSampler from the Imbalanced-learn (imblearn) library is applied to the dataset for undersampling[47]. It is specifically employed to rectify class imbalances by randomly eliminating instances from the majority class. Unlike oversampling techniques such as SMOTE, which generate synthetic samples and may introduce noise or increase the risk of overfitting, RandomUnderSampler retains only real transactions, ensuring the model learns from actual fraudulent patterns. Additionally, RandomUnderSampler reduces the dataset size, improving training efficiency and lowering computational costs, making it well-suited for large-scale fraud detection tasks. Here, the RandomUnderSampler reduces the number of legitimate transactions to 492, which is equivalent to the number of fraudulent transactions. It ensures the accurate prediction of the classifier after balancing the data with equal classes.

Dataset attribute	Value
Transaction days	02
Fraud transactions	492
Legitimate transactions	2,84,315
Total transactions	2,84,807
Fraud transaction proportion	0.172%
Original features	Time and amount
Transformed features	V1, V2, …, V28

Table 1. Statistics of ECC dataset.

Proposed method for feature selection

Feature selection is the focused module of the proposed framework for detecting credit card frauds. The feature selection module improves the performance of the system by selecting the appropriate set of features. The availability of selected features reduces the computational time and, hence, the processing cost as well. The feature selection is conducted for the 28 transformed features, as the time and amount are the necessary features that cannot be excluded during the selection process. The methodology presented for feature selection is the proposed HB^{3}C^{2}S method. This section elaborates on the HB^{3}C^{2}S method, which is the hybridization of the BB-BC and CS algorithms. At the initial stage, for the BB-BC algorithm, the population size is set to 50, with a maximum count of 100 iterations and a convergence threshold of 10^{-6}. The big bang phase utilizes an expansion factor (β) of 0.5 to maintain a balanced search. For the CS algorithm, the discovery rate of new solutions (p_a) is set to 0.25, and the step size scaling factor (α) is chosen as 0.01. The Levy flight parameter (λ) is set to 1.5 to ensure effective global exploration. These values are selected empirically to optimize the tradeoff between exploration and exploitation in feature selection.

The HB^{3}C^{2}S method strategically utilizes the distinct strengths of the BB-BC and CS algorithms. To determine an efficient solution, an exploitation-exploration tradeoff is necessary. Here, the BB-BC algorithm is utilized for local exploitation and the CS algorithm for global exploration. The solution agents of the BB-BC algorithm can thoroughly analyze the complexities and subtle patterns within the local search space using the big bang and big crunch phases of the algorithm. Further, the CS algorithm excels at conducting global exploration, analyzing the whole search space to detect overarching patterns and connections.

The process of the HB^{3}C^{2}S method begins by initializing the candidate solutions $X = \{x_1, x_2, ?, x_N\}$ by the Big Bang-Big crunch algorithm. The BB-BC algorithm mimics the cosmology process, in which the big bang phase of the algorithm follows the universe expansion principle and the big crunch phase follows the universe contraction principle. In feature optimization, the objective function $f(x)$ with respect to the solutions' population is evaluated to analyze the quality of each solution. Further, the solutions are updated to explore the search space as per the universe expansion principle of the big bang phase. The update process for each solution (x_i) is described by Eq. (1).

$$x_i\left(t+1\right) = x_i\left(t\right) + r.\mathit{\Delta}\, x_i \tag{1}$$

Where, $\mathit{\Delta}\, x_i$ is the displacement vector, and *r* represents the random number within the range [0, 1].

The fitness of the newly generated population is evaluated for selecting the best solutions among the participated solutions. The solutions determined as fittest are proceed to the next big crunch phase. In the big crunch phase, the center of mass (C) is evaluated using Eq. (2) for the selected solutions.

$$C = \frac{\sum{}_{i=1}^{M} w_i.x_i}{\sum{}_{i=1}^{M} w_i} \tag{2}$$

Where, *M* is the number of selected solutions from the previous phase of big bang. w_i is the weight vector based on the fitness value with respect to selected solutions x_i.

After obtaining the value of the center of mass (C), all the available solutions are updated towards the center of mass using Eq. (3).

$$x_i\left(t+1\right) = x_i\left(t\right) - r.\mathit{\Delta}\, x_i \tag{3}$$

Further, the fitness function of the new optimized solutions is calculated. The process continues for the next iteration. The convergence can be attained by generating the population around the center of mass, which also retains the knowledge of previous iterations. The BB-BC algorithm can optimize features, but the solutions may be limited if candidates become confined to a small search space during the initial big bang phase. This scenario can lead to candidates being confined to specific local subdomains, hindering effective feature optimization. While increasing the number of candidates can address this issue, it simultaneously escalates computational costs and the number of function evaluations. To tackle this challenge, the CS algorithm is incorporated, which uses the Levy flight attribute to escape the candidates of the BB-BC algorithm from premature convergence. The global exploration is performed using the CS algorithm, as it possesses the brood parasitism behavior to effectively explore the solution space globally.

The CS algorithm incorporates the candidate solutions of BB-BC and disperses them randomly across the search space to facilitate global exploration. These incorporated solutions are checked for the fitness function as per the parameters of the CS algorithm for feature optimization. Subsequently, the new solutions (eggs) are generated by applying random perturbations to existing solutions. In the optimization process, the cuckoo perturbation allows the population to explore the different regions of search space beyond the immediate vicinity of current solutions, encouraging global exploration. It also ensures the escape of candidates from local optima and better diversity of solutions. The CS algorithm executes the update of solutions using Eq. (4).

$$x_i{}^{new}\left(t+1\right) = x_i\left(t\right) + \alpha\,.L.\left(x_i(\,t) - x_j(t\,)\right) \tag{4}$$

Where, $x_i\left(t\right)$ is the current position of the i^{th} solution, $x_j\left(t\right)$ is a randomly selected solution from the population different from $x_i\left(t\right)$, α is the step size parameter that lies in the range (0, 1], and L is the Levy flight distribution, which is evaluated using Eq. (5). In Eq. (4), the subtraction of $x_j\left(t\right)$ from the current solutions

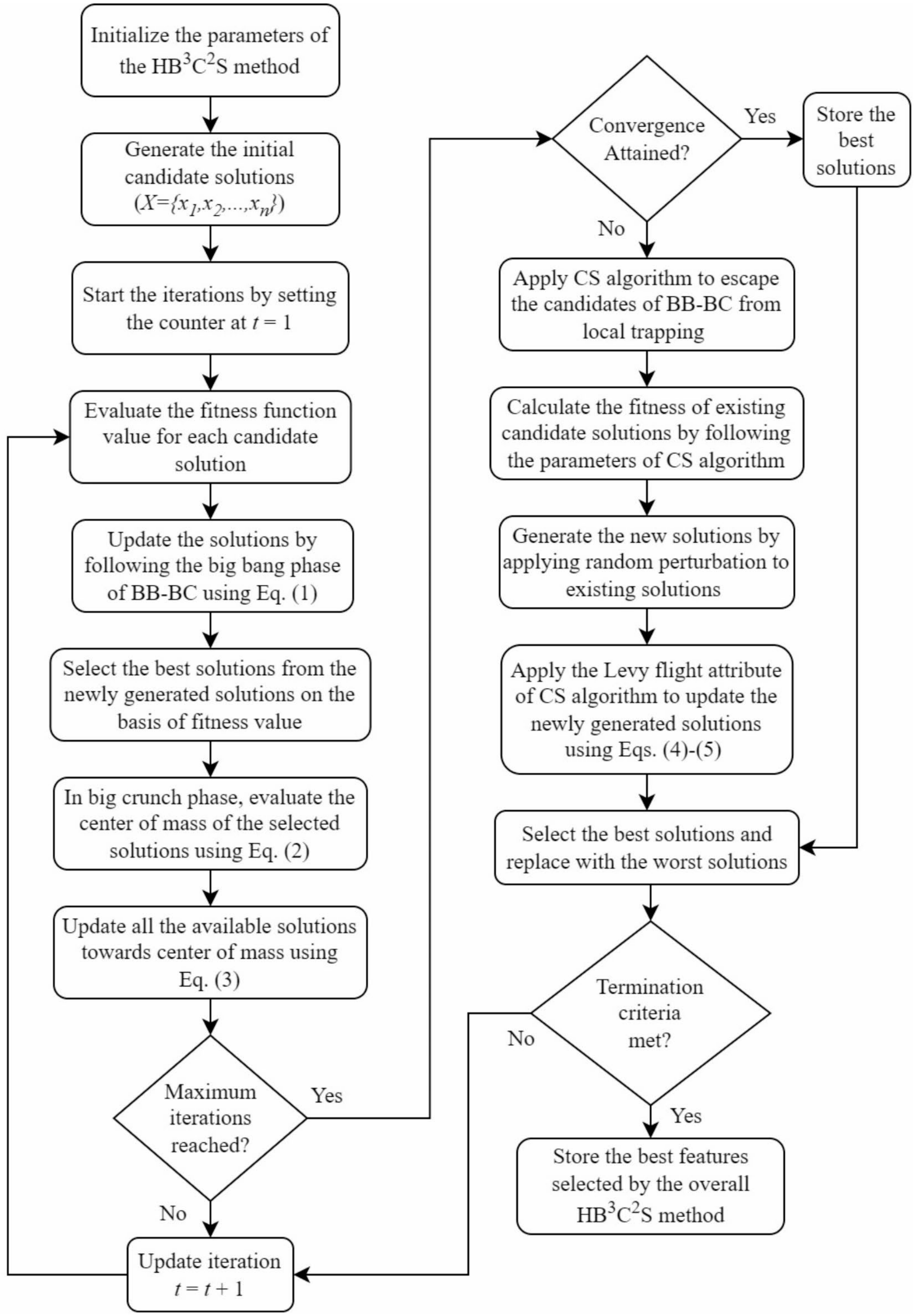

Initialize the parameters of the HB^{3}C^{2}S method
Generate the initial candidate solutions ($X=\{x_1,x_2,...,x_n\}$)
Start the iterations by setting the counter at $t = 1$
Evaluate the fitness function value for each candidate solution
Update the solutions by following the big bang phase of BB-BC using Eq. (1)
Select the best solutions from the newly generated solutions on the basis of fitness value
In big crunch phase, evaluate the center of mass of the selected solutions using Eq. (2)
Update all the available solutions towards center of mass using Eq. (3)
Maximum iterations reached?
Yes
No
Update iteration $t = t + 1$
Convergence Attained?
Yes
No
Store the best solutions
Apply CS algorithm to escape the candidates of BB-BC from local trapping
Calculate the fitness of existing candidate solutions by following the parameters of CS algorithm
Generate the new solutions by applying random perturbation to existing solutions
Apply the Levy flight attribute of CS algorithm to update the newly generated solutions using Eqs. (4)-(5)
Select the best solutions and replace with the worst solutions
Termination criteria met?
No
Yes
Store the best features selected by the overall HB^{3}C^{2}S method

Fig. 4. Process of feature selection using the proposed HB^{3}C^{2}S method.

($x_i\left(t\right)$) introduces a direction for the perturbation, which ensures better global exploration with diversified solutions.

$$L = \frac{\sigma}{\sqrt{U}} \tag{5}$$

Method	Selected features from dataset	Count of selected features
HB^{3}C^{2}S	V1, V4, V7, V8, V9, V10, V11, V14, V15, V17, V18, V22, V28	13
BB-BC	V2, V4, V5, V6, V8, V9, V11, V12, V13, V15, V18, V20, V21, V22, V25, V26, V27	18
CS	V1, V2, V3, V4, V7, V8, V10, V11, V12, V14, V16, V17, V18, V21, V22	15

Table 2. Features obtained using the feature selection methods.

Where, σ indicates the scale representation and U represents the random number derived from the uniform distribution with $U \in (0, 1]$.

Here, the Levy flight L controls the magnitude of the random perturbation that is applied to each solution during the exploration phase. The best solutions are selected and replaced with the worst solutions, ensuring that the size of the population is constant. The process persists until the maximum number of iterations is reached, and the optimized features, considered as the best solutions, are obtained. The process of feature selection using the proposed HB^{3}C^{2}S method is illustrated in Fig. 4.

In the overall process, the features selected using the proposed HB^{3}C^{2}S method are mentioned in Table 2. Additionally, to assess the efficacy of the proposed HB^{3}C^{2}S method compared to individual BB-BC and CS algorithms, feature selection is also performed using these individual algorithms. The selected features using BB-BC and CS algorithms are described in Table 2.

The results in Table 2 indicate that the HB^{3}C^{2}S method selects a more optimal feature subset (13 features) compared to the 18 and 15 features selected by the BB-BC and CS algorithms, respectively. This reduction demonstrates improved feature selection efficiency, as HB^{3}C^{2}S effectively eliminates redundant features while retaining the most discriminative ones for credit card fraud detection. The HB^{3}C^{2}S method integrate the strengths of both BB-BC and CS to achieve superior feature selection efficiency, which not only reduces computational cost but also enhances model performance in later stages of fraud detection.

Classification

The credit card fraud data is classified using deep neural networks based on the DCNN and EDCNN methods. The dataset is preprocessed and balanced using RandomUnderSampler (discussed in Sect. 4), comprising 492 instances of fraudulent transactions and an equal number of legitimate transactions. For classification, only the features selected by different feature selection methods from the dataset are considered (discussed in Sect. 5). These selected features serve as input to the classification methods, enabling them to learn discriminative representations and make accurate predictions.

The classification method of DCNN employs three layer types: convolutional, pooling, and fully connected layers. EDCNN extends DCNN by incorporating residual blocks, which introduce four layer types: convolutional, pooling, residual, and fully connected. The EDCNN method utilizes two residual blocks, each of which internally comprises four convolutional layers.

In both networks, the convolution operation is the initial operation of the network to analyze the features. After the convolution operation, both the DCNN and EDCNN methods are employed with the Rectified Linear Unit (ReLU) activation function for fully connected layers. This activation function introduces non-linearity into the network, enabling it to capture complex relationships and make accurate predictions, thus enhancing the overall performance of the models in fraud detection. Equation (6) defines the ReLU activation function.

$$ReLU\left(x\right)=\max(0,\ x) \tag{6}$$

The ReLU function adds non-linearity to the network by replacing negative values with zeros. Dropout regularization is subsequently applied to the output of the ReLU activation function. These operations help in preventing overfitting by randomly dropping out neurons during the training process. The dropout operation is described by Eq. (7).

$$Dropout\left(x\right)=\left\{\begin{array}{l}0,\ with\,probability\,p\\ \frac{x}{1-p},\ otherwise\end{array}\right. \tag{7}$$

Where, *x* is the input to the dropout layer and *p* is the dropout rate.

Further, the pooling layer reduces spatial dimensions while retaining significant features. The max pooling function is described by Eq. (8), which selects the maximum values from a small spatial region.

$$MaxPooling\left(x,y\right)=\max(x,\ y) \tag{8}$$

Where, *x* and *y* are the input values (activations) within a small spatial region.

After the max pooling operation, the operations of fully connected layers are performed. It retains the high-level features and incorporates a softmax layer for the classification.

In the EDCNN method, residual blocks after the convolution operations are added. Each residual block is composed of four convolutional layers. These convolutional layers are followed by a skip connection, which bypasses the multiple layers and adds the original input to the output of the convolutional layers. Equation (9) describes the output of the residual block.

$$H\left(x\right)=F\left(x\right)+x \tag{9}$$

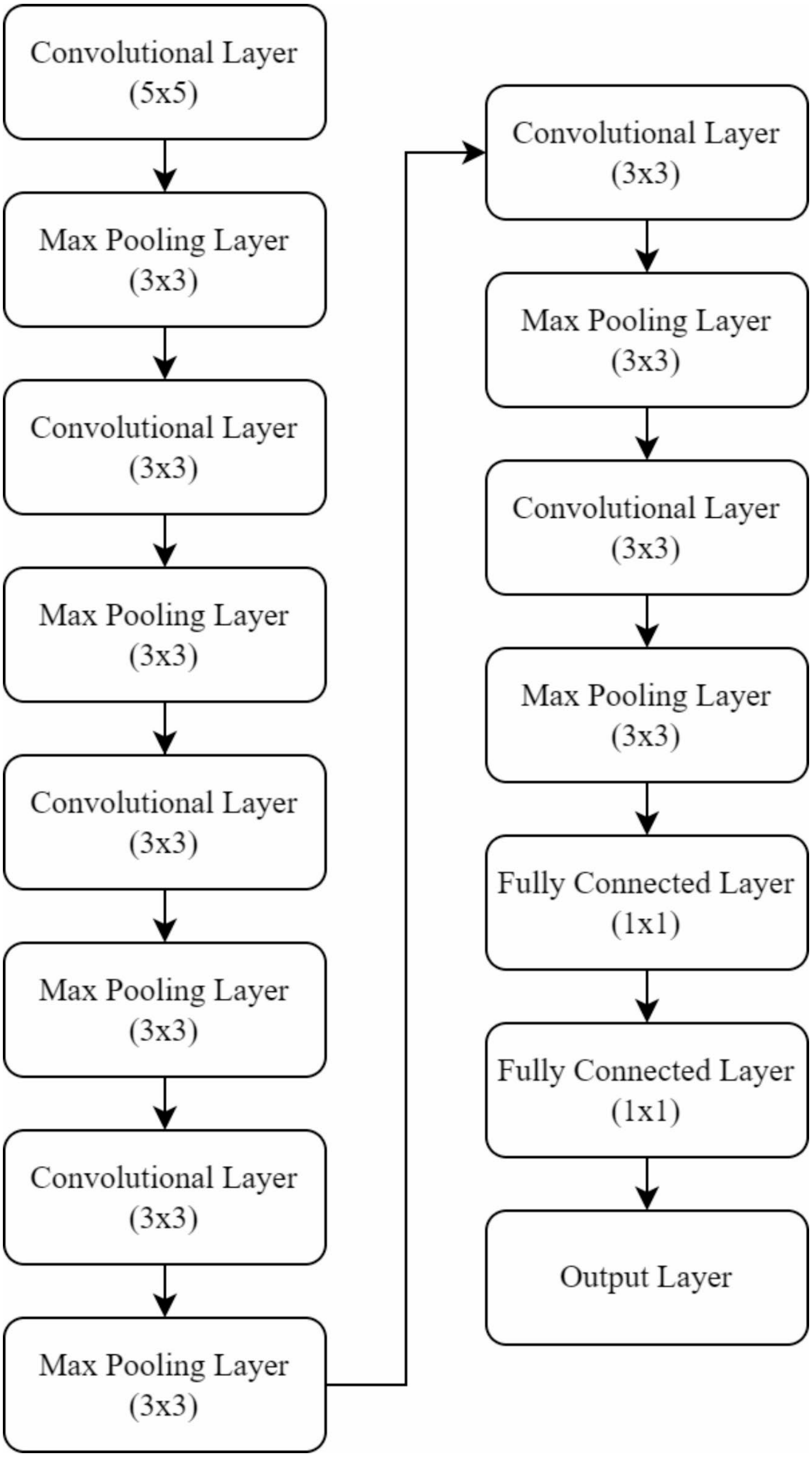

Convolutional Layer (5x5)
Max Pooling Layer (3x3)
Convolutional Layer (3x3)
Max Pooling Layer (3x3)
Convolutional Layer (3x3)
Max Pooling Layer (3x3)
Convolutional Layer (3x3)
Max Pooling Layer (3x3)
Convolutional Layer (3x3)
Max Pooling Layer (3x3)
Convolutional Layer (3x3)
Max Pooling Layer (3x3)
Fully Connected Layer (1x1)
Fully Connected Layer (1x1)
Output Layer

Fig. 5. Architecture of the DCNN methodology.

Where, x is the input to the block and $F(x)$ is the output to convolutional layers.

Figures 5 and 6 illustrate the network architectures of the DCNN and EDCNN methods, respectively.

Experimental assessment

This section presents the outcomes of the experimental assessment and provides an in-depth analysis of the obtained results. The proposed framework is assessed for the evaluation measures of precision, recall, f-measure, and accuracy as these metrics effectively capture both the predictive capability and overall performance of the

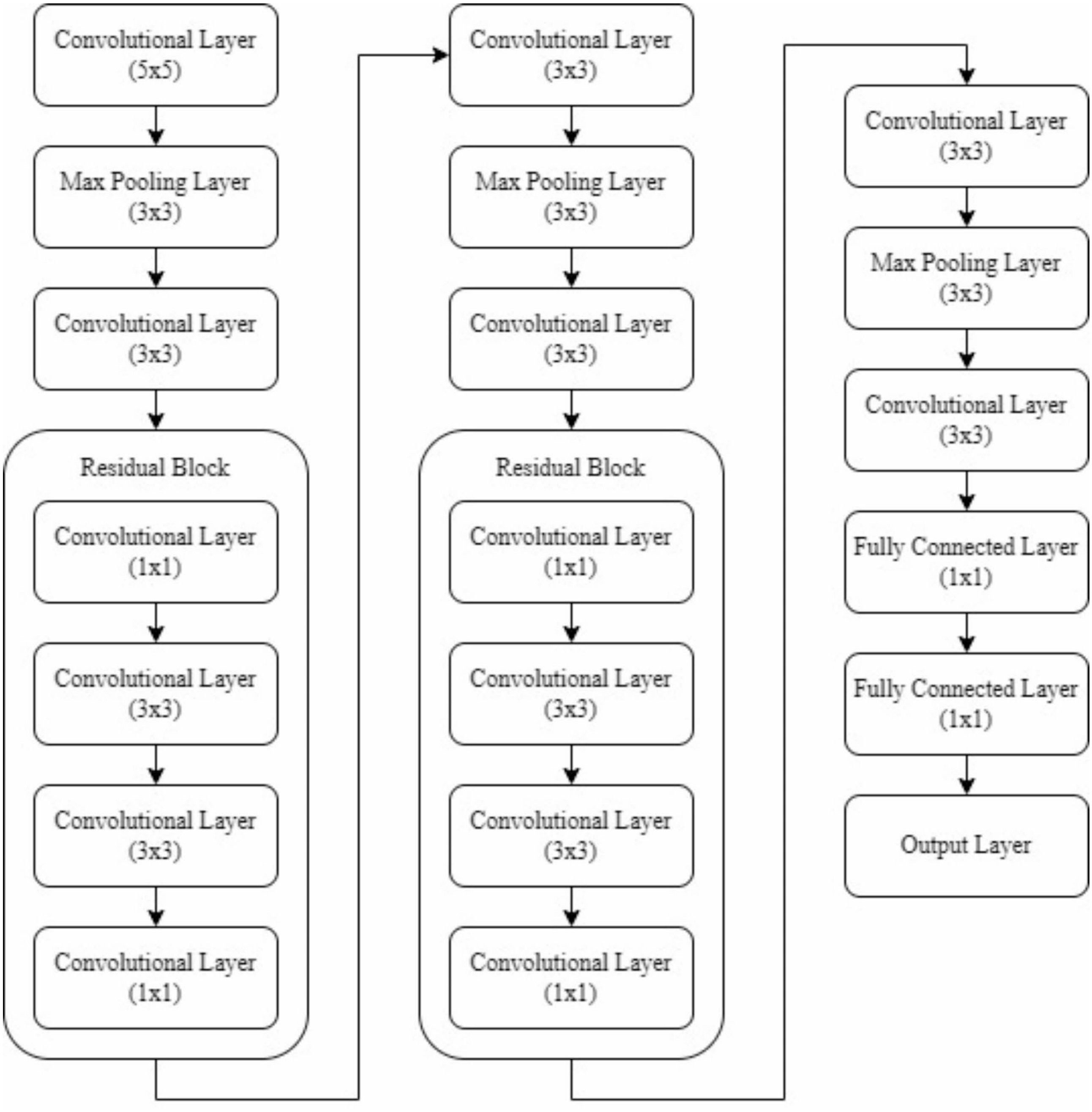

Convolutional Layer (5x5)
Max Pooling Layer (3x3)
Convolutional Layer (3x3)
Residual Block
Convolutional Layer (1x1)
Convolutional Layer (3x3)
Convolutional Layer (3x3)
Convolutional Layer (1x1)
Convolutional Layer (3x3)
Max Pooling Layer (3x3)
Convolutional Layer (3x3)
Residual Block
Convolutional Layer (1x1)
Convolutional Layer (3x3)
Convolutional Layer (3x3)
Convolutional Layer (1x1)
Convolutional Layer (3x3)
Max Pooling Layer (3x3)
Convolutional Layer (3x3)
Fully Connected Layer (1x1)
Fully Connected Layer (1x1)
Output Layer

Fig. 6. Architecture of the EDCNN methodology.

Measure	Evaluation formula
Precision	$\frac{\mathrm{TP}}{\mathrm{TP+FP}}$
Recall	$\frac{\mathrm{TP}}{\mathrm{TP+FN}}$
F-Measure	$2 \times \frac{\mathrm{Precision} \times \mathrm{Recall}}{\mathrm{Precision+Recall}}$
Accuracy	$\frac{\mathrm{TP+TN}}{\mathrm{TP+TN+FP+FN}}$

Table 3. Classification performance measures.

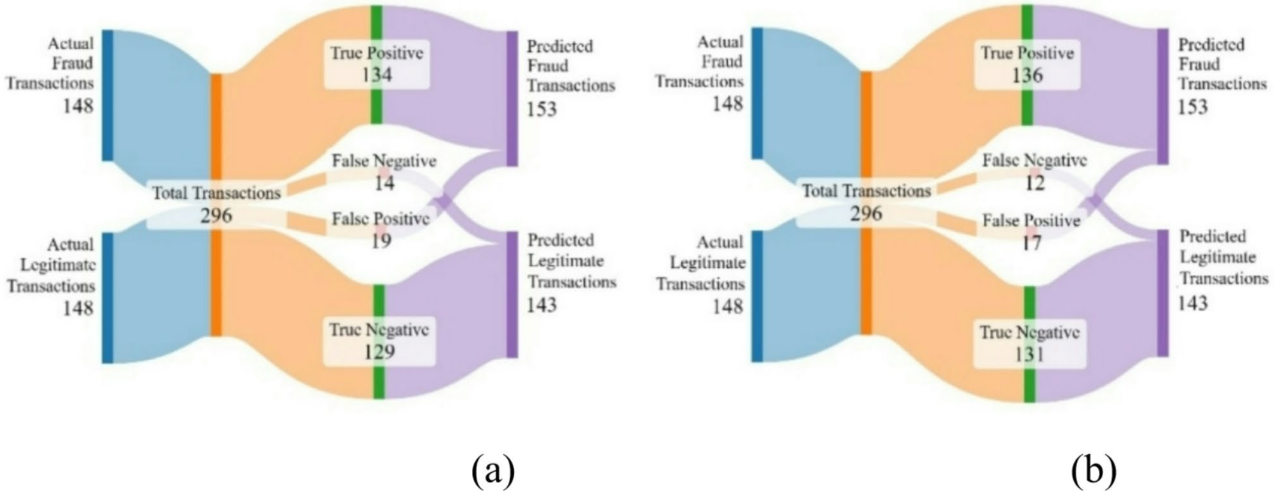


Fig. 7. Sankey Diagram illustrating the Confusion Matrix results for (**a**) Without feature selection method with the DCNN classifier, and (**b**) Without feature selection method with the EDCNN classifier.

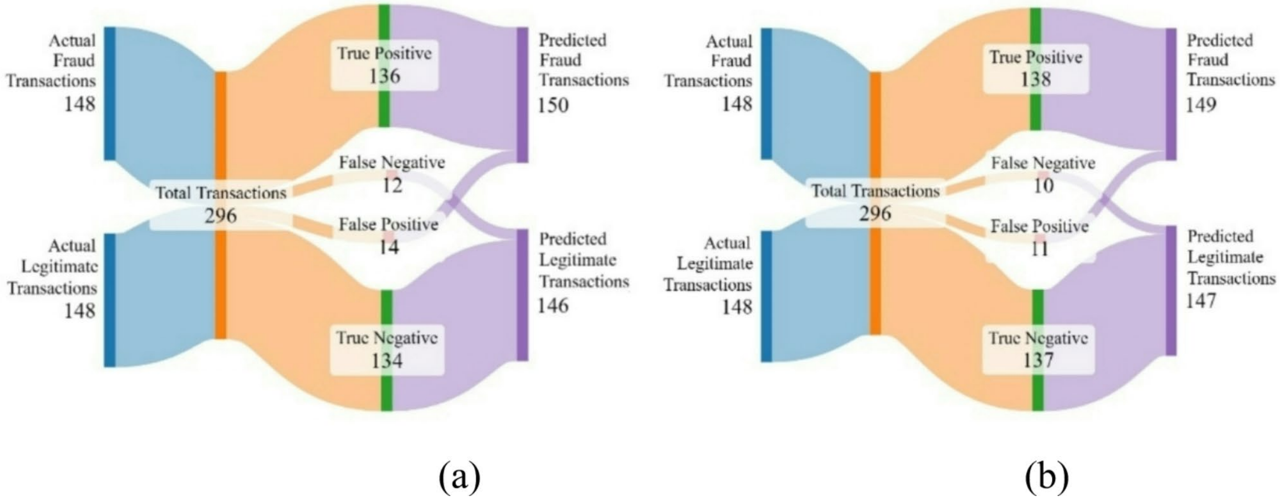


Fig. 8. Sankey Diagram illustrating the Confusion Matrix results for (**a**) BB-BC feature selection method with the DCNN classifier, and (**b**) BB-BC feature selection with the EDCNN classifier.

model in fraud detection. These measures are mainly vital for evaluating the trade-off between false positives and false negatives, ensuring a balanced assessment of fraud detection performance. The formulations of these parameters are described in Table 3.

In Table 3, TP (True Positive) refers to the count of accurately identified instances of fraudulent credit card transactions; FP (False Positive) represents the count of legitimate credit card transactions that are classified as fraudulent; FN (False Negative) represents the count of fraudulent credit card transactions that are classified as legitimate; and TN is the count of accurately identified instances of legitimate credit card transactions.

Results and analysis

The results depict the efficacy of our proposed framework in detecting credit card fraud. The result evaluation is conducted on the ECC dataset, with 70% of the data allocated for training and 30% for testing, employing a random selection approach.

To assess the significance of feature selection, results are calculated in four categories: the first category did not use any feature selection method, the second category utilized the BB-BC method, the third category incorporated the CS method, and the fourth category employed the proposed HB^{3}C^{2}S method.

Since fraud detection is a binary classification problem, the evaluation metrics from the confusion matrix are used. The confusion matrix results are depicted in Figs. 7, 8 and 9, and 10 using Sankey diagrams. In these diagrams, positive instances represent fraudulent transactions, while negative instances represent legitimate transactions.

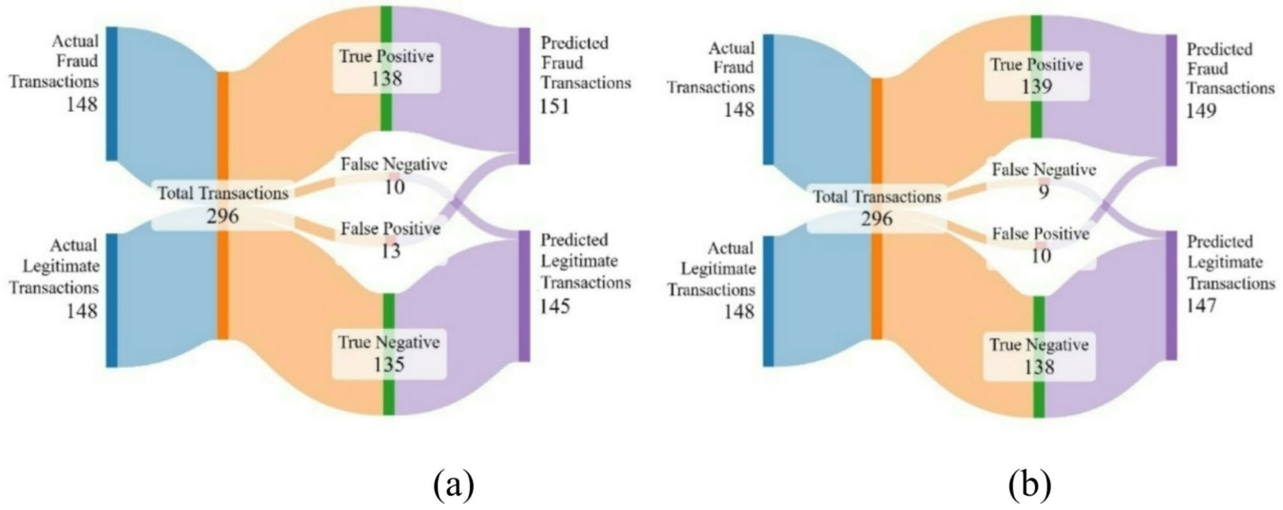

Actual Fraud Transactions 148
True Positive 138
Predicted Fraud Transactions 151
False Negative 10
Total Transactions 296
False Positive 13
Actual Legitimate Transactions 148
Predicted Legitimate Transactions 145
True Negative 135
(a)
Actual Fraud Transactions 148
True Positive 139
Predicted Fraud Transactions 149
False Negative 9
Total Transactions 296
False Positive 10
Actual Legitimate Transactions 148
Predicted Legitimate Transactions 147
True Negative 138
(b)

Fig. 9. Sankey Diagram illustrating the Confusion Matrix results for (**a**) CS feature selection method with the DCNN classifier, and (**b**) CS feature selection with the EDCNN classifier.

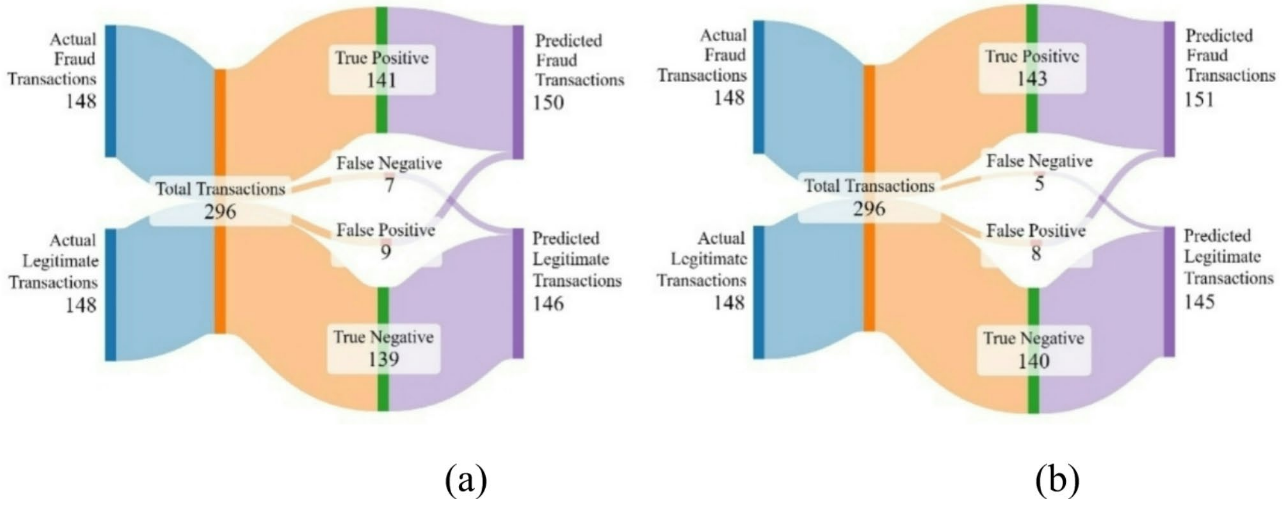

Actual Fraud Transactions 148
True Positive 141
Predicted Fraud Transactions 150
False Negative 7
Total Transactions 296
False Positive 9
Actual Legitimate Transactions 148
Predicted Legitimate Transactions 146
True Negative 139
(a)
Actual Fraud Transactions 148
True Positive 143
Predicted Fraud Transactions 151
False Negative 5
Total Transactions 296
False Positive 8
Actual Legitimate Transactions 148
Predicted Legitimate Transactions 145
True Negative 140
(b)

Fig. 10. Sankey Diagram illustrating the Confusion Matrix results for (**a**) HB^3C^2S feature selection method with the DCNN classifier, and (**b**) HB^3C^2S feature selection with the EDCNN classifier.

Measure	DCNN	EDCNN
Precision (%)	87.58	88.89
Recall (%)	90.54	91.89
F-measure (%)	89.04	90.37
Accuracy (%)	88.85	90.20

Table 4. Classification results without the feature selection method.

The classification performance measures, including precision, recall, f-measure, and accuracy, are computed based on the confusion matrix results. Tables 4, 5, 6 and 7 present the classification results obtained without feature selection, and with feature selection using the BB-BC, CS, and HB^3C^2S methods, respectively.

Table 4 displays the classification results obtained using the DCNN and EDCNN classifiers without employing any feature selection. The results indicate that DCNN achieved an accuracy of 88.85%, while EDCNN achieved 90.20% accuracy.

Table 5 shows the classification results obtained using the BB-BC method for feature selection with DCNN and EDCNN classifiers. It resulted in an accuracy of 91.22% for DCNN and 92.91% for EDCNN.

Measure	DCNN	EDCNN
Precision (%)	90.67	92.62
Recall (%)	91.89	93.24
F-measure (%)	91.28	92.93
Accuracy (%)	91.22	92.91

Table 5. Classification results using the BB-BC feature selection method.

Measure	DCNN	EDCNN
Precision (%)	91.39	93.29
Recall (%)	93.24	93.92
F-measure (%)	92.31	93.60
Accuracy (%)	92.23	93.58

Table 6. Classification results using the CS feature selection method.

Measure	DCNN	EDCNN
Precision (%)	94	94.70
Recall (%)	95.27	96.62
F-measure (%)	94.63	95.65
Accuracy (%)	94.59	95.61

Table 7. Classification results using the HB^{3}C^{2}S feature selection method.

Method	Feature selection time (s)	Training time (s)	Total execution time (s)
HB^{3}C^{2}S	2.3	121	123.3
BB-BC	3.2	149	152.2
CS	2.9	137	139.9

Table 8. Computational time analysis of the proposed HB^{3}C^{2}S method and individual methods with DCNN.

Method	Feature selection time (s)	Training time (s)	Total execution time (s)
HB^{3}C^{2}S	2.3	128	130.3
BB-BC	3.2	161	164.2
CS	2.9	146	148.9

Table 9. Computational time analysis of the proposed HB^{3}C^{2}S method and individual methods with EDCNN.

Table 6 depicts the classification results obtained using the CS method for feature selection with DCNN and EDCNN classifiers. It yielded an accuracy of 92.23% for DCNN and 93.58% for EDCNN.

Furthermore, Table 7 illustrates the performance of the proposed HB^{3}C^{2}S method for feature selection. The HB^{3}C^{2}S method achieved 94.59% accuracy with DCNN and 95.61% accuracy with EDCNN.

The results described in Tables 4, 5, 6 and 7 indicate that the proposed HB^{3}C^{2}S method effectively improves the system's performance in detecting fraudulent transactions. Specifically, the HB^{3}C^{2}S method led to an improvement of more than 5.4% in accuracy compared to fraud detection without any feature selection method for both classifiers. Additionally, EDCNN consistently outperformed DCNN across all cases to classify the transactions.

Computational efficiency analysis

In addition to evaluating the classification performance in terms of precision, recall, f-measure, and accuracy, the results are also evaluated for computational time for each phase of the process. These results are compared for the proposed HB^{3}C^{2}S method and the individual BB-BC and CS methods. Tables 8 and 9 show the computational efficiency results for DCNN and EDCNN, respectively, in terms of the average execution times for feature selection, model training, and total execution.

Method	F-measure (%)	Accuracy (%)
HB^{3}C^{2}S + DCNN	94.63	94.59
HB^{3}C^{2}S + EDCNN	95.65	95.61
CS + DCNN	92.31	92.23
CS + EDCNN	93.60	93.58
BB-BC + DCNN	91.28	91.22
BB-BC + EDCNN	92.93	92.91
DCNN	89.04	88.85
EDCNN	90.37	90.20
SVDD [6]	91	90
Filter feature selection + SVDD[6]	92	91
Wrapper feature selection + SVDD[6]	92	92
Embedded feature selection + SVDD[6]	93	93
ABC + TAS[40]	83.01	85.15
ABC + LGBP[40]	90.58	90.60
ABC + LGBP-ENN[40]	92.54	93.10

Table 10. Performance comparison of the proposed HB^{3}C^{2}S method with state-of-the-art methods.

The results evaluated in Tables 8 and 9 indicate that the proposed HB^{3}C^{2}S method not only selects a more optimal subset of features but also significantly reduces computational cost compared to the standalone BB-BC and CS methods. The lower execution times observed in both the feature selection and deep learning training phases highlight its computational efficiency. This efficiency gain is primarily attributed to the balanced integration of local exploitation (via BB-BC) and global exploration (via CS), which enables faster convergence and lower overall execution time.

Performance comparison

The efficacy of the proposed HB^{3}C^{2}S method is analyzed by comparing it with established methods from the literature. For this purpose, the techniques presented by Mniai et al.[6], and Geetha and Dheepa[40], are incorporated.

Mniai et al.[6] employed three feature selection methods of filter, wrapper, and embedded feature selection, along with various machine learning classifiers. Among these classifiers, SVDD demonstrated superior performance. Therefore, for comparison, the SVDD classifier is selected along with the incorporated feature selection methods, aligning with the research focus on evaluating the significance of feature selection.

Additionally, Geetha and Dheepa[40] utilized the ABC feature selection method in conjunction with TAS, LGBP, and LGBP-ENN classifiers. Table 10 summarizes the performance comparison.

The performance comparison results presented in Table 10 demonstrate the effectiveness of the proposed HB^{3}C^{2}S method in credit card fraud detection compared to state-of-the-art methods. The HB^{3}C^{2}S method enhances feature selection efficiency, reduces computational cost, and achieves a better exploration-exploitation balance which leads to faster convergence. Furthermore, the integration of the HB^{3}C^{2}S method with deep neural networks as classifiers yields remarkable classification performance, further validating its superiority over existing approaches.

Conclusion and future scope

Credit card fraud is a growing menace to the financial institutions. Despite advances in technology and security measures, fraudsters devise novel techniques for committing fraud and avoid being detected. Addressing this challenge requires the implementation of an advanced and effective system. This research paper introduces a novel framework for credit card fraud detection, with a particular focus on the proposed HB^{3}C^{2}S method. This proposed method is utilized for feature selection, recognizing the need of robust features for effective performance of the classifiers. The HB^{3}C^{2}S method combines the strengths of the BB-BC and CS algorithms to balance exploration and exploitation. BB-BC focuses on analyzing detailed patterns locally, while CS explores broader patterns globally. The features selected using the HB^{3}C^{2}S method are utilized for the classification of transactions. The classification is conducted using the DCNN and EDCNN methods. To analyze the effectiveness of the proposed HB^{3}C^{2}S method, feature selection is also performed using the individual BB-BC and CS algorithms. The proposed system with the HB^{3}C^{2}S method as a feature selector has achieved 94.59% accuracy with DCNN and 95.61% accuracy with EDCNN. Through rigorous evaluation and comparison with existing approaches, the proposed framework demonstrates its superiority in detecting credit card frauds.

While the proposed system enhances the credit card fraud detection performance, further research can focus on enhancing optimization, including the improvements of the feature selection techniques and model generalization. Additionally, integrating adaptive learning mechanisms and expanding the experiments to multi-source and real-time data with diverse transaction patterns can further enhance the system's ability to address evolving fraud strategies more effectively.

Data availability

The data will be available on request to the corresponding author.

Received: 17 November 2024; Accepted: 2 April 2025
Published online: 04 July 2025

References

1. Khando, K., Islam, M. S. & Gao, S. The emerging technologies of digital payments and associated challenges: A systematic literature review. *Future Internet* **15** (1), 21. (2022).
2. Ansarinasab, S., Ghassemi, F., Nazarimehr, F., Ghosh, D. & Jafari, S. Phase synchronization in cryptocurrency network and its features. *Int. J. Mod. Phys. C (IJMPC)*. **35** (02), 1–21 (2024).
3. Mittal, S. & Tyagi, S. Computational techniques for real-time credit card fraud detection. In *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 653–681 (2020).
4. de Best, R. Annual number of credit card transactions in India 2012–2021, per capita (2024). https://www.statista.com/statistics/1309045/total-number-of-credit-card-payments-in-india/
5. de Best, R. Visa, MasterCard, UnionPay transaction volume worldwide 2014–2022. https://www.statista.com/statistics/261327/number-of-per-card-credit-card-transactions-worldwide-by-brand-as-of-2011/
6. Mniai, A., Tarik, M. & Jebari, K. A novel framework for credit card fraud detection. *IEEE Access*. **11**, 112776–112786. (2023).
7. Dyvik, E. H. Card fraud in U.S. versus rest of the world 2014–2021 (2023). https://www.statista.com/statistics/1264329/value-fraudulent-card-transactions-worldwide/
8. Wang, Y. et al. August. Privacy preserving distributed deep learning and its application in credit card fraud detection. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 1070–1078. (IEEE, 2018).
9. Alarfaj, F. K. et al. Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. *IEEE Access*. **10**, 39700–39715 (2022).
10. Natarajan, R. et al. Hybrid big bang–big crunch with ant colony optimization for email spam detection. *International Journal of Modern Physics C*, *33*(04), p.2250051. (2022).
11. Xiong, Y., Zou, Z. & Cheng, J. Cuckoo search algorithm based on cloud model and its application. *Sci. Rep.*, **13** (1), 10098. (2023).
12. Erol, O. K. & Eksin, I. A new optimization method: big bang–big crunch. *Adv. Eng. Softw.* **37** (2), 106–111 (2006).
13. Yang, X. S. & Deb, S. Engineering optimisation by cuckoo search. *Int. J. Math. Modelling Numer. Optimisation*. **1** (4), 330–343 (2010).
14. Houssein, E. H. et al. Hybrid Harris hawks optimization with cuckoo search for drug design and discovery in chemoinformatics. *Sci. Rep.*, **10** (1), 14439. (2020).
15. Hill, M. Q. et al. Deep convolutional neural networks in the face of caricature. *Nat. Mach. Intell.* **1** (11), 522–529 (2019).
16. Asha. Deep neural networks-based classification optimization by reducing the feature dimensionality with the variants of gravitational search algorithm. *Int. J. Mod. Phys. C*, **32** (10), 2150137. (2021).
17. Jindal, S., Sachdeva, M. & Kushwaha, A. K. S. A novel quantum-behaved binary firefly algorithm with gravitational search algorithm to optimize the features for human activity recognition. *Int. J. Mod. Phys. C*, **33** (11), 2250146. (2022).
18. Bhatt, A. et al. Quantum-inspired meta-heuristic algorithms with deep learning for facial expression recognition under varying yaw angles. *Int. J. Mod. Phys. C*, **33** (04), 2250045. (2022).
19. Saheed, Y. K., Hambali, M. A., Arowolo, M. O. & Olasupo, Y. A. November. Application of GA feature selection on Naive Bayes, random forest and SVM for credit card fraud detection. In *2020 International Conference on Decision Aid Sciences and Application (DASA)*, 1091–1097. (IEEE, 2020).
20. Saheed, Y. K., Baba, U. A. & Raji, M. A. Big data analytics for credit card fraud detection using supervised machine learning models. In *Big Data Analytics in the Insurance Market*, 31–56. (Emerald Publishing Limited, 2022).
21. Sailusha, R., Gnaneswar, V., Ramesh, R. & Rao, G. R. May. Credit card fraud detection using machine learning. In *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 1264–1270. (IEEE, 2020).
22. Rajora, S. et al. A comparative study of machine learning techniques for credit card fraud detection based on time variance. In *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, 1958–1963. (IEEE, 2018).
23. Randhawa, K., Loo, C. K., Seera, M., Lim, C. P. & Nandi, A. K. Credit card fraud detection using AdaBoost and majority voting. *IEEE Access*, **6**, 14277–14284 (2018).
24. Sulaiman, R. B., Schetinin, V. & Sant, P. Review of machine learning approach on credit card fraud detection. *Human-Centric Intell. Syst.* **2** (1), 55–68 (2022).
25. Kumar, S., Gunjan, V. K., Ansari, M. D. & Pathak, R. Credit card fraud detection using support vector machine. In *Proceedings of the 2nd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications: ICMISC 2021*, 27–37. (Springer, 2022).
26. Khan, M. Z. et al. The performance analysis of machine learning algorithms for credit card fraud detection. *Int. J. Online Biomed. Eng.* **19** (3), 82–98 (2023).
27. Alfaiz, N. S. & Fati, S. M. Enhanced credit card fraud detection model using machine learning. *Electronics* **11** (4), 662 (2022).
28. Jurgovsky, J. et al. Sequence classification for credit-card fraud detection. *Expert Syst. Appl.* **100**, 234–245 (2018).
29. Fiore, U., De Santis, A., Perla, F., Zanetti, P. & Palmieri, F. Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. *Inf. Sci.* **479**, 448–455 (2019).
30. Zioviris, G., Kolomvatsos, K. & Stamoulis, G. Credit card fraud detection using a deep learning multistage model. *J. Supercomputing*. **78** (12), 14571–14596 (2022).
31. Forough, J. & Momtazi, S. Sequential credit card fraud detection: A joint deep neural network and probabilistic graphical model approach. *Expert Syst.* **39** (1), e12795 (2022).
32. Kasasbeh, B., Aldabaybah, B. & Ahmad, H. Multilayer perceptron artificial neural networks-based model for credit card fraud detection. *Indonesian J. Electr. Eng. Comput. Sci.* **26** (1), 362–373 (2022).
33. Karthika, J. & Senthilselvi, A. Smart credit card fraud detection system based on dilated convolutional neural network with sampling technique. *Multimedia Tools Appl.* **82** (20), 31691–31708 (2023).
34. Ileberi, E., Sun, Y. & Wang, Z. Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and adaboost. *IEEE Access*. **9**, 165286–165294 (2021).
35. Khalid, A. R. et al. Enhancing credit card fraud detection: an ensemble machine learning approach. *Big Data Cogn. Comput.* **8** (1), 6 (2024).
36. Singh, P., Singla, K., Piyush, P. & Chugh, B. 145632 anomaly detection classifiers for detecting credit card fraudulent transactions. In *2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, 1–6. (IEEE, 2024).
37. Mim, M. A., Majadi, N. & Mazumder, P. A soft voting ensemble learning approach for credit card fraud detection. *Heliyon* **10** (3), e25466. (2024).

38. Mienye, I. D. & Sun, Y. A deep learning ensemble with data resampling for credit card fraud detection. *IEEE Access.* **11**, 30628–30638 (2023).
39. Ileberi, E., Sun, Y. & Wang, Z. A machine learning based credit card fraud detection using the GA algorithm for feature selection. *J. Big Data*, **9** (1), 24. (2022).
40. Geetha, N. & Dheepa, G. Transaction fraud detection using artificial bee colony (ABC) based feature selection and enhanced neural network (ENN) classifier. *Int. J. Mech. Eng.*, **7** (3) (2022).
41. Geetha, N. & Dheepa, G. A hybrid deep learning and modified butterfly optimization based feature selection for transaction credit card fraud detection. *J. Posit. School Psychol.* **6** (7), 5328–5345 (2022).
42. Arun, G. K. & Rajesh, P. Design of metaheuristic feature selection with deep learning based credit card fraud detection model. In *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, 191–197. (IEEE, 2022).
43. Karthika, J. & Senthilselvi, A. August. Detection of Credit Card Fraud Detection Using HPO with Inception Based Deep Learning Model. In *2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA)*, 70–77. (IEEE, 2023).
44. Rawashdeh, E., Al-Ramahi, N., Ahmad, H. & Zaghloul, R. Efficient credit card fraud detection using evolutionary hybrid feature selection and random weight networks. *Int. J. Data Netw. Sci.* **8** (1), 463–472 (2024).
45. Yang, X. S. & Deb, S. Cuckoo search via Lévy flights. In *2009 World Congress on Nature & Biologically Inspired Computing (NaBIC)*, 210–214. (IEEE, 2009).
46. Andrea and Machine Learning Group – ULB, Credit Card Fraud Detection Dataset, Kaggle, San Francisco, CA, USA. (2018). https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud
47. Udeze, C. L., Eteng, I. E. & Ibor, A. E. Application of machine learning and resampling techniques to credit card fraud detection. *J. Nigerian Soc. Phys. Sci.*, 769–769 (2022).

Author contributions

Mohd Shukri Ab Yajid: Conceptualization, writingNilesh Bhosle: Data analysis, softwareGadug Sudhamsu: Figure preparation, AnalysisAli Khatibi: Supervision, Table preparationSahil Sharma: Methodology, conceptualizationRubal Jeet: Writing, Technical analysisR Sivaranjani: Figure preparation, softwareA Bhowmik: Technical Analysis, MethodologyA. Johnson Santhosh: Funding, Supervision.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to A.J.S.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.