SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

AI-Driven UCCGAN Framework for Detecting and Preventing Fake Check Scams

M. Srinivasa Varma[1], G.P.S.Varma[2], Indukuri Hemalatha[3]

[1] Research Scholar, Dept. of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, A.P, India.
E-mail: varma@srimaharshiconsultancy.com
[2] Professor, Dept. of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, A.P, India.
E-mail: gpsvarma@gmail.com
[3] Professor, Dept. of Information Technology, S.R.K.R Engineering College, A.P, India. E-mail: drindukurihemalatha@gmail.com

Abstract
Check fraud has become a major menace within current banking systems and has caused huge financial losses and mistrust of financial dealings. Conventional fraud detection techniques tend to be either rule-based or supervised learning techniques, are constrained by the presence of labelled data, and are not flexible to changing fraud patterns. To overcome these issues, this study introduces a smart architecture, AI-UCCGAN-DST-FCS, that combines the advantages of blockchain-based authentication with unsupervised deep learning to effectively detect fraud. First, to verify the integrity of the data and establish trust among the involved banks, cheque transactions are verified using a proof-of-green (POG) consensus mechanism inside a blockchain network. An adapted Unsupervised Cycle-Consistent Generative Adversarial Network (UCCGAN) is then used to learn complicated patterns in transactions and identify anomalies without any labelled data. In addition, the Secretary Bird Optimization Algorithm (SBOA) was applied to optimize the parameters of the model, improving the detection accuracy and computational efficiency. The experimental analysis of publicly available financial fraud dataset shows that the proposed approach has better performance, with an AUC of 0.984 and greatly reduced error rate and computation time in comparison with the existing methods. The findings affirm the suitability of the proposed system for detecting cheque fraud in real time and securely.

Keyword: Artificial Intelligence, Blockchain, Proof-of-Green, Secretary Bird Optimization Algorithm, Unsupervised Cycle-Consistent Generative Adversarial Networks

1. Introduction

Over the last few years, the rapid digitalization of financial systems has made banking transactions highly vulnerable to advanced fraudulent schemes, particularly cheque-based ones. Checks are one of the most widely used forms of payment in the modern world. A check is a formal request that a depositor sends to a bank instructing it to transfer a certain amount from the depositor's bank account to a designated recipient [1]. Regretfully, many dishonest fraud actors take advantage of certain holes in the banking system to perpetrate fraud. In fact, frauds using counterfeit checks are becoming increasingly common and cost billions of dollars. The Internet Fraud Complaint Center (IC3) and the Consumer Sentinel database (Sentinel) of the Federal Trade Commission (FTC) received more than twice as many complaints. Fake check scams are the main topic of this study [2]. To commit this fraud, victims are mostly targeted using email scams; a relationship is typically formed for business purposes, an overpaid counterfeit paycheck is sent to them, and finally, an overpayment request is made. More victims of fake check fraud suffer catastrophic effects than those of many other attacks [3]. Furthermore, incidents of check fraud are probably underreported. Only 29% of fraud victims are thought to have reported to any type of authority, such as the Federal Trade Commission, and less than one in ten victims have ever complained to law enforcement. Apart from financial and emotional distress, victims frequently face legal action because they are perceived by the authorities as having attempted to defraud the bank [4].

In this situation, identifying fraudulent checks long before they are cashed is the best way to safeguard users [5]. Undoubtedly, there are ways to determine whether physical checks are authentic. However, fraud actors are skilled at cheating and produce quite realistic checks, particularly in the modern day, when many con artists use magnetic ink and high-end printers. Furthermore, many banks now advise customers to print their own checks, which eliminates the checks' physical security. As a result, before cashing a submitted check, each bank must ensure that it is provided by a legitimate, trustworthy authority and that a more effective check authentication mechanism has been put in place. Conventional fraud detection systems are based on rule-based systems and manual verification, which are inefficient and cannot keep up with the changing trends of fraud. This has led to an increasing demand for smart, automated, and scalable solutions capable of identifying anomalies in real time with very high accuracy [6]. Artificial Intelligence (AI) and deep learning methods have become powerful instruments for detecting financial fraud because they can learn complicated data distributions and detect subtle anomalies. Specifically, unsupervised learning methods are becoming popular because they do not rely on any labelled datasets, which are typically limited or unavailable in real-world banking conditions [7]. GANs have proven to be effective in detecting anomalies based on the modelling of normal data distributions and deviations as possible fraud cases [8]. Moreover, blockchain technology has found greater acceptance in financial systems to improve transparency, security, and confidence among the involved parties. Blockchain offers a strong system for verifying transactions and deterring fraudulent manipulations by allowing decentralized and tamper-proof record-keeping [9]. Nonetheless, blockchain integration with smart detection models can be considered a daunting task because of the problems of scalability and computational overheads. To overcome these drawbacks, nature-inspired optimization algorithms, including metaheuristic algorithms, have been proposed to enhance the performance and speed of convergence of the models. The algorithms increase parameter tuning, thus resulting in improved accuracy and less complexity in the computation of fraud detection systems [10]. Hence, the combination of blockchain-based authentication, unsupervised deep learning, and optimization methods is a promising pathway for creating an efficient and reliable check fraud detection system. The proposed study will help fill the current gaps by suggesting a hybrid framework that combines these technologies to obtain high detection performance and real-time applicability.

In this study, blockchain-based authentication and AI were used to detect suspicious trends and prevent fake check scams that address the challenges of assisting banks in exchanging details about issued and cashed checks while protecting the privacy of the banks' clients.

(i) AI-UCCGAN-DST-FCS is proposed for domestic and international banks to publish valid check details on the blockchain, which are simultaneously analyzed by POG for authentication.

(ii) Unsupervised Cycle-Consistent Generative Adversarial Networks do not require labelled data, making them suitable for scenarios in which labelled fraudulent check data are scarce.

(iii) AI is used to analyses new check transactions and identify those that deviate significantly from the learned patterns as potentially fraudulent.

2. Literature Survey

Several research studies were suggested in literature related to deep learning depend on Several research studies were suggested in literature related to deep learning depend on Detecting Suspicious Trends also preventing fake check scams, a few recent works are reviewed here, In [11], the authors presented a Blockchain-based solution for detecting also preventing Fake check scams. One of the most popular methods used to defraud consumers is the forged check. This fraud is particularly costly for victims, who usually lose thousands of dollars and must deal with legal proceedings. Currently, there is no way to quickly identify mobile checks and authenticate real ones. Rather, banks are required to wait longer than 48 hours to identify a scam. In particular, a blockchain-based system for checking and detecting check fraud is proposed. It attains a higher accuracy and a higher error rate. In [12], the authors presented Eth-PSD: an ML-PSD. The recent rapid adoption of blockchain technology in the financial industry has drawn the attention of cybercriminals to undertake blockchain-based attacks, including phishing scams, scam wallets, and Ponzi schemes. The most popular blockchain platform is Ethereum, which was the first to enable smart contracts. However, it has been reported that over 50% of all Ethereum cybercrimes are phishing scams. In contrast, a unique machine learning-based detection mechanism known as Ethereum Phishing Scam Detection (Eth-PSD) attempts to identify transactions connected to phishing scams. It attains a lower error rate and lower accuracy. In [13], the authors presented a blockchain and machine learning for fraud detection: a privacy-preserving and adaptive incentive-based approach. Despite recent technical breakthroughs, financial fraud cases are increasing. Authentic financial transaction information is rarely available because of privacy issues and a lack of inter-organization synergy. However, for data-driven technologies, such as machine learning, to function accurately in real-world systems, they require genuine data. Blockchain technology is used in this strategy to protect the data privacy. A network-deployed smart contract completely automates this system. It attains a lower error rate and a higher computation time.

In [14], the authors have presented towards using blockchain technology to prevent diploma fraud. Blockchain technology has garnered considerable interest and is being utilized as a reliable black box in numerous applications. Many apps pay less attention to the needs unique to their particular use case and instead concentrate on taking advantage of the Blockchain's natural features, such as smart contracts and trust from consensus. Here, we start a methodical investigation into the ways in which blockchain can be used to contest certificate fraud in the training and education industry. It attains a lower computation time and a higher error rate. In [15], the authors presented a blockchain-based novel solution for online fraud prevention and detection. Here, the terms "online fraud" and "identity theft" are now widely used to describe those who utilize the internet for professional purposes. It frequently results in several issues, including harming consumers' credit standing, requiring time and money, and eroding their confidence when making purchases online. The goal of this study is to develop a system that uses a non-fungible token based on blockchain technology and stores user data on a decentralized blockchain system. It attains a higher accuracy and it attains higher computation time. Recent developmentsin financial fraud detection have been directed towards combining deep learning with secure data-sharing models. In [16], the authors suggested a deep Autoencoder-based credit card fraud detector and proved that unsupervised models can be effective in identifying concealed transaction patterns and do not require labelled data. Nevertheless, their model is limited in terms of generalisation in the case of heterogeneous financial systems. Similarly, in [17], the authors introduced a hybrid blockchain-enabled fraud-detection system that enhances transparency and data integrity. Although their approach guarantees safe data transfer, it has a high computational cost and is thus inapplicable in real time. In [18], the authors. investigated recurrent neural networks (RNNs) in the context of the sequential analysis of transactions in another study. They have been effective in modelling the temporal dependencies of financial data, but they require large labelled datasets, which are not usually available in check fraud cases.

In [19], the authors explored GAN-based oversampling to solve the problem of class imbalance in fraud detection (FD). These methods are effective in enhancing recall but can give rise to synthetic noise, which can impact the reliability of the model. Recently, the authors of [20] suggested a highly accurate transformer-based fraud detection system that discovers global relationships in transaction data. The model is computationally intensive and does not have the capability to integrate with secure validation mechanisms, such as blockchain, although it is effective. Based on the studies above, it can be seen that current methods are either deep learning-based fraud detection methods or blockchain-based transaction validation methods, and in a few instances, both methods are combined effectively. Moreover, most models require labelled data, which restricts their use in practical check fraud detection applications where labelled data are not easily available. Moreover, the current approaches have high computational costs, an inability to employ optimization techniques, and poor management of information asymmetry and evolving fraud trajectories. The proposed AI-UCCGAN-DST-FCS framework combines unsupervised deep learning (UCCGAN) with blockchain-based authentication (POG) and metaheuristic optimization (SBOA) to achieve a higher accuracy, lower error rate, and efficient computation time.

3. Materials and methods

In this section, the proposed AI-UCCGAN-DST-FCS is introduced. This process consists of four steps: Data Acquisition, Blockchain, Detection, and optimization. In the proposed section, real-time data are initially collected, such as cheque details, account number, and routing number. It is used to authenticate checks and undergoes blockchain to prepare them for further analysis. Next, an Unsupervised Cycle-Consistent Generative Adversarial Network (UCCGAN) is employed to detect suspicious trends and prevent fake check scams. Finally, Artificial Intelligence (AI) is used to verify the validity of transactions. The SBOA method was introduced to optimize the UCCGAN. The block diagram of the proposed AI-UCCGAN-DST-FCS approach is shown in Figure 1. The novel concept of Proof-of-Green (POG), originally associated with environmentally friendly consensus, is redefined in this study as a trust-aware blockchain consensus scheme that was used to certify checks in banking systems. The proposed POG aims to ensure the authenticity and integrity of cheque transactions by endorsing the distributed agreement of several financial institutions.

Let C_i is a cheque transaction that is sent to the network and is sent to N bank nodes in the network. The nodes individually check the transaction according to predetermined requirements, such as the credibility of the issuers, consistency of the transaction, and account history.

$$V(C_i) = \frac{1}{N}\sum_{j=1}^{N} \delta_j (C_i) \quad (1)$$

where $\delta_j(C_i) \in \{0,1\}$ represents the verification result from the j^{th} node. A consensus decision is then obtained using a threshold τ:

$$C_i = \begin{cases} \text{Valid}, & V(C_i) \geq \tau \\ \text{Suspicious}, & V(C_i) < \tau \end{cases} \quad (2)$$

To ensure trust propagation and transparency, a confidence score is further defined as:

$$T(C_i) = \frac{\sum_{j=1}^{N} w_j \cdot \delta_j(C_i)}{\sum_{j=1}^{N} w_j} \quad (3)$$

where w_j is the weight of trust of individual bank node. This equation is stronger because it focuses on reliable validators. Therefore, the POG mechanism guarantees decentralized, secure, and efficient cheque validation, decreases fraud risk, and increases system reliability as shown in Figure 2.

Authenticating Checks using Proof-of-Green (POG) Consensus Mechanism

In this section, the checks are authenticated using the POG a Consensus Mechanism [21] in consumers and banks. The POG consensus technique incorporates environmental factors into the transaction or action validation process. Before authorizing a transaction or action, it confirms that it complies with the specific environmental requirements.

Sending in the Check the bank's system would start the POG authentication procedure when a customer submitted a check for processing using Equation (4).

$$F_i = \frac{1}{\lambda} g_i \rho \tag{4}$$

where F_i denotes the input data from bank consumers, λ indicates the average time between block arrival occurrences or the mining rate, g_i represents the transaction of checks, and ρ indicates the total number of checks. The POG specifies particular environmental requirements that must be fulfilled for a check transaction to be accepted. The requirements can include checks written out to environmentally conscious businesses or checks utilized for environmentally beneficial endeavours. The bank's system would then use the specified criteria to evaluate the check's environmental credentials as part of the verification process.

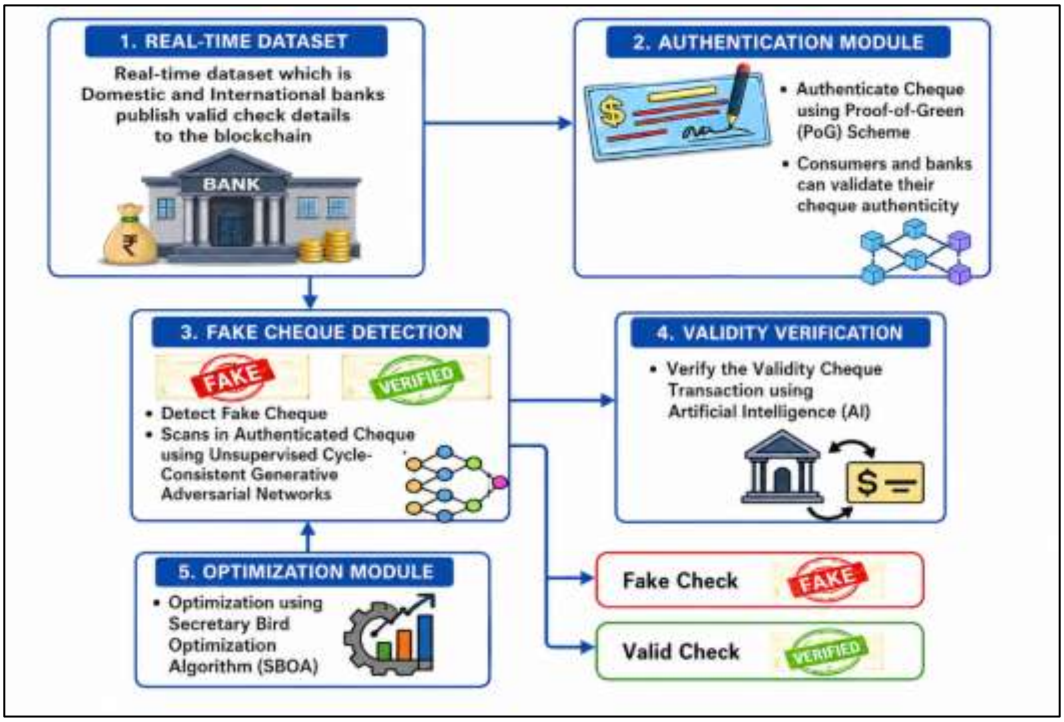

Figure 1: Block diagram for Proposed AI-UCCGAN-DST-FCS method

Verification could entail looking up the issuer's environmental certifications, the check's intended use, or other pertinent information using Equation (5).

$$F = \rho \frac{1}{\lambda} \sum_{i=1}^{n} g_i \tag{5}$$

where F indicates the verification process of each check, and n indicates the n^{th} number of authenticated checks.

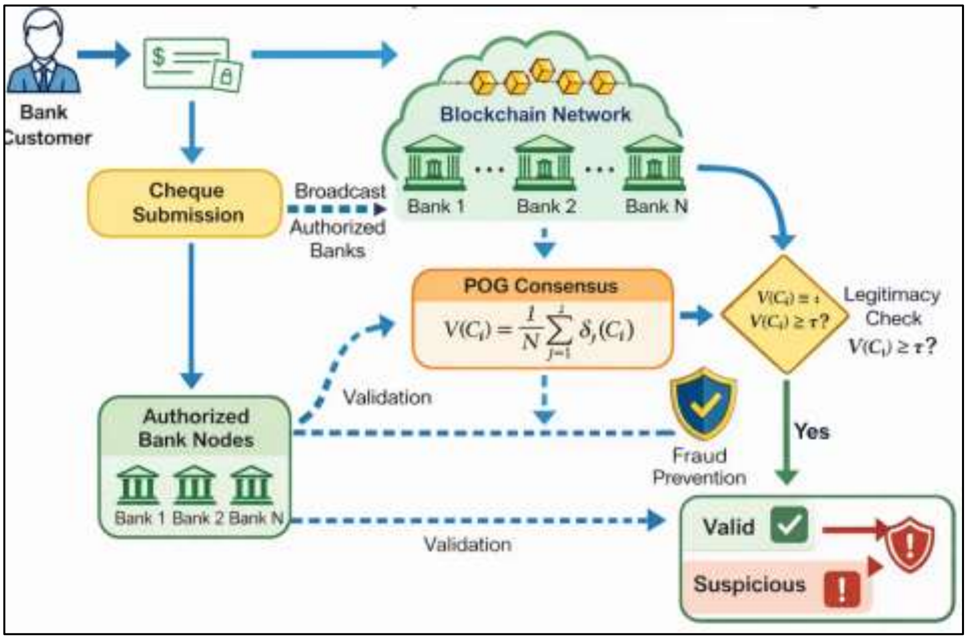

Figure 2: Proof-of-Green (POG) Consensus Mechanism

The POG consensus process decides whether to authenticate the check after verification is completed. If the check satisfies the established environmental requirements, a determination will be made. The check would be permitted for processing if it passed the POG verification and satisfied the environmental requirements.

If not, it would decline, and the customer would be informed of the rationale behind the decline using Equation (6).

$$F_{1^{st}} = \rho\left(\frac{1}{\lambda} + \sum_{i=p}^{l} T_i\left(1 - g_e + \sum_{j=i-1}^{l-1} g_j\right)\right) \qquad (6)$$

where, $F_{1^{st}}$ indicates the trust and transparency in financial transactions of consumers; $\sum_{i=p}^{l} T_i$ indicates the authentication process of verified checks; g_e indicates the customer a chequebook which transmits its data about the consumer and the supplied and $\sum_{j=i-1}^{l-1} g_j$ ensures that the check was really provided by a trusted authority. By processing POG method, the checks are authenticated. Then the authenticated checks are fed to detect fake checks scams in authenticated cheque phase.

Detect Fake Checks Scams in Authenticated Checks using UCCGAN

In this section, to detect fake checks scams in authenticated cheque using UCCGAN is discussed to identify suspicious trends in previous transactions as fake check and valid check, by selecting an unlabeled instance batch from the bank consumers. The amount of classification layers, input resolution, and bounding all data are all carefully scaled using UCCGAN method. Here, the victim is urged to deposit a check, usually for a sum greater than what they owe in fake check scam requests the victim to send back a portion of the money after that. GANs [22], especially Cycle-Consistent GANs (CycleGANs), have proven to be incredibly effective in image-to-image translation tasks. Nevertheless, they cannot be easily applied directly to financial transaction data, which are inherently non-spatial, heterogeneous, and tabular. To mitigate this shortcoming, the proposed study proposes a variant of the Unsupervised Cycle-Consistent Generative Adversarial Network (UCCGAN) framework that is specifically tailored to detect financial fraud in cheque transactions. This adaptation bridges the gap between conventional image-based GAN architectures and structured financial data. The raw cheque transaction data $X = \{x_1, x_2, \ldots, x_n\}$, which is composed of attributes such as transaction amount, account details, timestamp, and transaction history, is first converted into a latent feature representation in the proposed approach. This is accomplished via an embedding function $f_\theta(\cdot)$ that maps tabular data into a high-dimensional form in a structured latent space:

$$Z = f_\theta(X) \qquad (7)$$

This transformation helps the model reflect the intricate interdependencies and latent patterns of financial data. Financial data do not have explicit spatial relationships, such as image data, but instead necessitate learning feature correlations and temporal behavior, which can be well learned in this latent space. The modified UCCGAN model determines two mapping functions: $G: Z \rightarrow Z'$, which encodes the representations of the space of valid transactions into fraudulent patterns, and $F: Z' \rightarrow Z$, which recovers the original distribution. The cycle-consistency constraint is a condition in which the transformation maintains crucial information:

$$L_{cyc} = \mathbb{E}_z\left[\left\|F\big(G(z)\big) - z\right\|_1\right] + \mathbb{E}_{z'}\left[\left\|G\big(F(z')\big) - z'\right\|_1\right] \quad (8)$$

Additionally, adversarial learning is incorporated to distinguish between real and generated samples:

$$L_{GAN}(G, D) = \mathbb{E}_{z'}[logD(z')] + \mathbb{E}_z\left[log\left(1 - D\big(G(z)\big)\right)\right] \quad (9)$$

The total objective function is expressed as:

$$L_{total} = L_{GAN} + \lambda L_{cyc} \quad (10)$$

where λ balances reconstruction and adversarial losses.

The main benefit of this method is that it has the ability to perform unsupervised learning, which is very appropriate in fraud detection cases, whereby there is a lack of labelled data of fraudulent cheques. By learning the distribution of normal transactions and creating possible anomalies, UCCGAN successfully detects suspicious patterns without any explicit supervision. Moreover, bidirectional mapping increases the robustness of the model by providing consistency between domains, lowering the instances of false positives, and increasing generalisation. To modify the UCCGAN to suit financial data, other mechanisms, such as feature normalization, attention-based weighting, and noisy regularization, were added.These improvements enabled the model to emphasize important transaction characteristics and prevent the influence of noisy or irrelevant characteristics. Consequently, the proposed UCCGAN system is an effective and versatile solution for identifying fraudulent cheque transactions, and is more accurate and adaptable than traditional machine learning and deep learning architectures.

Optimization using Secretary Bird Optimization Algorithm

The proposed SBOA is utilized to enhance weight parameters g *and* h of proposed UCCGAN. The parameter g is implemented for increasing the accuracy and h reducing the computation time. The Secretary bird is an African raptor that stands out for both its unusual habits and looks. Secretary birds usually live in wide spaces, savannahs with few trees, and tropical grasslands [23]. With thick grass, as well as in environments that are forested with wide clearings or that are semi-desert. Secretary birds have unique plumage that includes deep black bellies, pure white chests, and grey-brown feathers on their wings and backs. Here, step by step procedure for obtaining appropriate UCCGAN values using SBOA is described. To generates a uniformly distributed population for optimizing the ideal UCCGAN parameters. The entire step method is then presented in below,

Step 1: Initialization

Initial population of SBOA is initially generated by randomness. Then the initialization is derived in equation (11).

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,j} & \cdots & a_{1,dim} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,j} & \cdots & a_{2,dim} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{i,1} & a_{i,2} & \cdots & a_{i,j} & \cdots & a_{i,dim} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,j} & \cdots & a_{n,dim} \end{bmatrix}_{n\times d} \quad (11)$$

where, A indicates the group of secretary bird; a_i indicates the i^{th} secretary bird; $a_{i,j}$ indicate the i^t secretary bird and j^{th} value of variable; n indicates the n^{th} members of the secretary's group bird also dim indicates the issue of variable dimension.

Step 2: Random generation

An input weight parameter g *and* h developed randomness via SBOA method.

Step 3: Fitness function

Through initialized values, a random solution is produced. It is calculated by optimizing parameter. Then the formula is derived in equation (12)

$$Fitness\ Function = optimizing\ \ [g\ and\ h] \quad (12)$$

where, g is implemented for increasing the accuracy and h is used to Lessing the computation time.

Step 4: Hunting strategy of secretary bird for Optimizing g

Secretary birds usually start their hunting season by looking for possible prey, particularly snakes. Because of their exceptionally keen vision, secretary birds can detect snakes concealed in the savannah's dense grass with ease. With their lengthy legs, they carefully scan the ground, keeping an eye on their surroundings and looking for any indications of snakes. They can stay quite secure away from snakes thanks to their lengthy necks and legs. This comes up during the early stages of optimization, when investigation is quite important using equation (13).

$$A_i = \begin{cases} A_i^{New\,S1}, \; if \; G_i^{New,S1} \\ \frac{A_i}{g}, \quad else \end{cases} \qquad (13)$$

Where, A_i ; $A_i^{New\,S1}$ symbolizes the initial stage of the new condition of i[th] secretary bird also $G_i^{New,S1}$ indicates objective function's fitness value.

Step 5: Escape strategy of secretary bird for Optimizing

Large predators like eagles, hawks, foxes, and jackals are the natural enemies of secretary birds because they can attack them or take their food. Secretary birds usually use a variety of evasion techniques to defend themselves or their food when faced with these hazards. These tactics can be divided roughly into two primary groups. The first tactic is either quick running or fighting. Because of their incredibly long legs, secretary birds are able to run at very high speeds using equation (14).

$$A_{i,j}^{New,S2} = \begin{cases} Z_1: a_{best} + (2 \times Rand\; Y - 1) \times \left(1 - \frac{T}{t}\right)^2 \times a_{i,j}, \\ \qquad if \; R \; and \; < R_i \\ Z_2: a_{i,j} + Rand_2 \times \left(a_{Ramdom} - L \times \frac{a_{i,j}}{h}\right), \; else \end{cases} \qquad (14)$$

where, $A_{i,j}^{New,S2}$ symbolizes the initial stage of new condition of the i[th] secretary bird; Z_1 and Z_2 indicates the camoufage by environment and fly or run away; a_{best}; $Rand_2$ indicates the array of dimension $1 \times dim$ is randomly generated via normal distribution; a_{Ramdom} symbolizes current iteration's random candidate solution; L denotes picking of an integer at random 1 or 2 and T and t indicate the total number of iteration.

Step 6: Termination

The generator's weight value for parameters g and h from UCCGAN is optimized by utilizing SBOA; and it will recurrence step 3 until it obtains its hesitant criteria A= A+1. Then AI-UCCGAN-DST-FCS accurately detecting suspicious trends and preventing fake check scams by higher accuracy, lessening computational time with error.

Algorithm 1: Pseudo Code of AI-UCCGAN-DST-FCS framework

Input: Transaction dataset D
Output: Classified transactions (Valid / Fake)
1: Preprocess dataset D (normalization, encoding, balancing)
2: Encode each transaction Ci into blockchain block Bi
3: Broadcast Bi to N bank nodes
4: For each node j do
5: Verify Ci → compute δj(Ci)
6: End For
7: Compute validation score V(Ci)
8: If V(Ci) ≥ τ then
9: Mark Ci as authenticated
10: Else mark Ci as suspicious
11: Transform Ci into latent space Z using embedding function
12: Apply UCCGAN (G, F) for anomaly detection
13: Optimize parameters using SBOA
14: Classify transaction as Valid or Fake
15: Return classification results

The proposed Algorithm 1 starts with preprocessing the input dataset to enhance the quality of the data and address imbalance. Every transaction is then transformed into a blockchain block and sent to several bank nodes for decentralized verification. The POG system calculates a consensus-based scoring system that secures the authenticity of transactions. Verified transactions only go through the next stage, eliminating noise and enhancing their detection accuracy. The validated information is converted into a latent feature space, in which the UCCGAN model captures the underlying trends of transactions via unsupervised learning. The generator and discriminator are used to detect anomalies by separating normal and fraudulent behaviors. The SBOA can be used to optimize important parameters like learning rate and weights to optimize model performance. Finally, the system divides transactions into valid and fake according to the learned patterns. This combined method enhances accuracy, minimizes errors, and facilitates effective fraud detection in real-time banking environments.

Verify the Validity of Cheque Transactions using AI

The proposed Algorithm 1 starts with preprocessing the input dataset to enhance the quality of the data and address imbalance. Every transaction is then transformed into a blockchain block and sent to several bank nodes for decentralized verification. The POG system calculates a consensus-based scoring system that secures the authenticity of transactions. Verified transactions only go through the next stage, eliminating noise and enhancing their detection accuracy. The validated information is converted into a latent feature space, in which the UCCGAN model captures the underlying trends of transactions via unsupervised learning. The generator and discriminator are used to detect anomalies by separating normal and fraudulent behaviors. The SBOA can be used to optimize important parameters like learning rate and weights to optimize model performance. Finally, the system divides transactions into valid and fake according to the learned patterns. This combined method enhances accuracy, minimizes errors, and facilitates effective fraud detection in real-time banking environments.

4. Results and Discussion

The proposed AI-UCCGAN-DST-FCS model was developed in Python with TensorFlow on a computer with an Intel i7 processor, 16 GB RAM, and optional GPU acceleration. The ULB Credit Card Fraud dataset was used in the experiments with a stratified division of 70-10-20 training, validation, and testing data. The preprocessing of the data involved normalization, one-hot encoding, and balancing of the classes using SMOTE. The SBOA was used to carefully tune the hyperparameters. The learning rate was 0.001, the batch size was 64, and the number of training epochs was 100. In the UCCGAN model, two layers of hidden neurons with 128 and 64 neurons were utilized. The cycle-consistency loss coefficient (λ) fixed to 10 to trade-off between reconstruction and adversarial loss. The optimizer used was Adam with $\beta 1 = 0.5$ and $\beta 2 = 0.999$. Attained result of AI-UCCGAN-DST-FCS method is analyzed with existing techniques likes BC-DP-FCS, ML-PSD and BC-ML-FD systems. The ULB Credit Card Fraud dataset is a publicly available benchmark dataset [24] that is commonly used to test financial fraud detection models. It was created by Universite libre de Bruxelles and includes real-life anonymized credit card transactions of European cardholders. There are 284,807 transactions in the dataset, including only 492 fraudulent transactions, which makes the dataset very skewed with a fraud rate of approximately 0.172. All transactions are represented by 30 features, 28 of which are anonymized variables derived using Principal Component Analysis (PCA), and two non-transformed variables: Time and Amount. The anonymization process guarantees the privacy of sensitive information about customers and maintains relevant statistical patterns needed to analyses the information. The given dataset is especially appropriate for conducting research on fraud detection because of its realistic features, such as the imbalance of classes and concealed fraud patterns. It offers a good framework for testing unsupervised learning models, such as UCCGAN, that can identify anomalies without using labelled data. As such, it is suitable as a proxy for cheque fraud detection case scenarios in this study.

Figure 3 shows the accuracy (%) of the four baseline models and the proposed AI-UCCGAN-DST-FCS in the two classes of fake and valid checks. In the case of fake checks, the proposed model has the highest accuracy (~99), which is much higher than that of ML-PSD (~ 86), BC-ML-FD (~78), and BC-DP-FCS (~69). Similarly, in the validity checks, the proposed model outperformed the others with a higher accuracy of ~99% as opposed to the accuracy of ML-PSD (~79%), BC-DP-FCS (~74%), and BC-ML-FD (~69%). This steady high performance indicates that the suggested method is effective in capturing both fraudulent and legitimate patterns of transactions. The enhancement is largely attributed to the fact that it has been integrated with blockchain-based authentication (POG) which guarantees data reliability, and UCCGAN, which learns complex hidden patterns. Moreover, SBOA optimization improves parameter tuning and minimizes misclassification. Comparatively, current models have poorer performance because they have few features to learn and are not optimized, making them more prone to errors in identifying subtle fraud patterns.

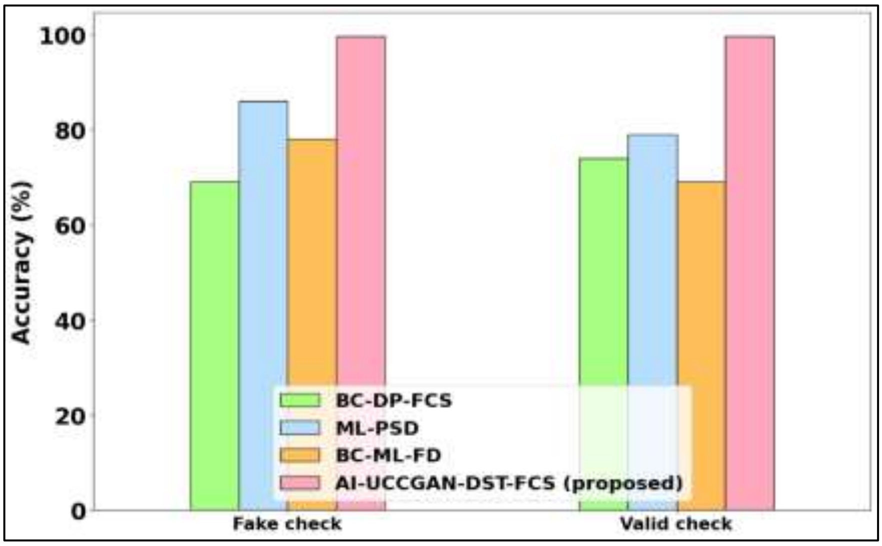

Figure 3 : Performance analysis of Accuracy

Figure 4 shows a comparison of the error rate (percentage) of the baseline models and the proposed AI-UCCGAN-DST-FCS for both fake and valid check classifications. In the case of fake checks, BC-DP-FCS is the largest with an error of ~31, followed by BC-ML-FD (~22) and ML-PSD (~14), and the proposed model has an error of approximately 1. Likewise, valid checks revealed that BC-ML-FD had the maximum error (~31%), followed by BC-DP-FCS (~26%) and ML-PSD (~21%), and the proposed method had a small error (~1%). This significant decrease in the error rate demonstrates the strength of the proposed AI-UCCGAN-DST-FCS model. This is because of effective feature learning using UCCGAN, which helps detect the hidden patterns of fraud, and blockchain-based POG authentication, which guarantees data integrity. In addition, SBOA optimization was used to optimize the model parameters and reduce misclassification. Conversely, current practices do not have deep representation learning and optimization which leads to increased error rates.

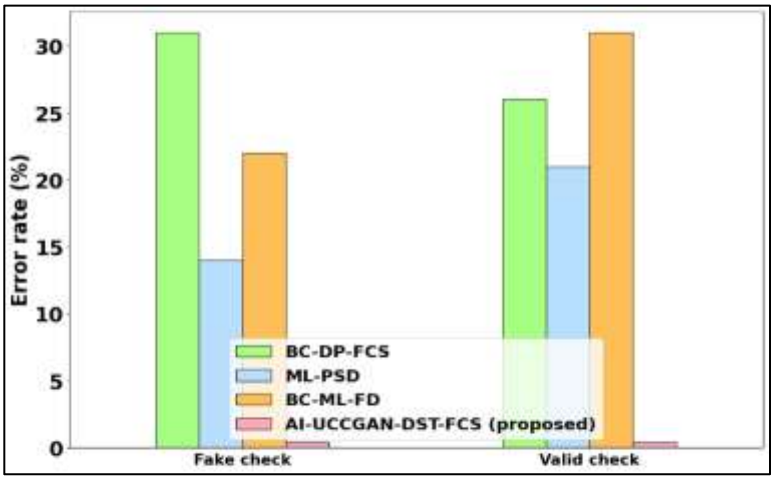

Figure 4: Performance analysis of Error Rate

Figure 5 shows the computation time (in seconds) of the four baseline models and the proposed AI-UCCGAN-DST-FCS. The best computation time of the proposed model is ~90 s, which is much better than those of BC-DP-FCS (~350 s), ML-PSD (~290 s), and BC-ML-FD (~460 s). BC-ML-FD has the largest processing cost among the current techniques because of the complicated blockchain-ML integration with no effective optimization, whereas BC-DP-FCS and ML-PSD have longer processing times for transaction validation and feature extraction. The high efficiency of the AI-UCCGAN-DST-FCS can be explained by an optimized learning process caused by the SBOA, which optimizes the parameters and speeds up convergence. Moreover, the unsupervised UCCGAN architecture avoids reliance on labelled training data and minimizes the training loads. Lightweight POG-based blockchain validation is also integrated to further reduce verification steps. Therefore, the proposed model is faster in execution and highly accurate; hence, it is applicable in real-time fraud detection in banking systems, where low latency is a major consideration.

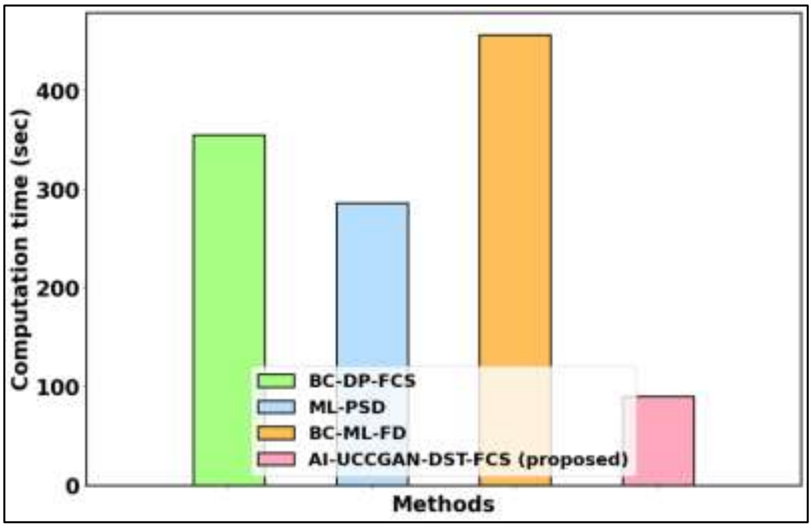

Figure 5: Performance analysis of Computation Time

Figure 6 illustrates the trade-off between the TPR and FPR in the ROC curve based on the classification threshold. The proposed AI-UCCGAN-DST-FCS model has an AUC of 0.984, which is much higher than the current methods, including BC-DP-FCS (0.921), ML-PSD (0.903), and BC-ML-FD (0.887). This shows that it has a better ability to differentiate between fraudulent and legitimate cheque transactions. The curve of the proposed model always tends to be closer to the top-left corner, which indicates high sensitivity and low false alarm. This is explained by the inclusion of blockchain-based validation and optimization of UCCGAN feature learning, which improves anomaly detection. In addition, SBOA optimization helps improve parameter tuning, which minimizes misclassification. In general, the ROC analysis proves that the proposed model can offer sound and stable performance in fraud detection, and it can be significantly used in the context of real-life financial security applications.

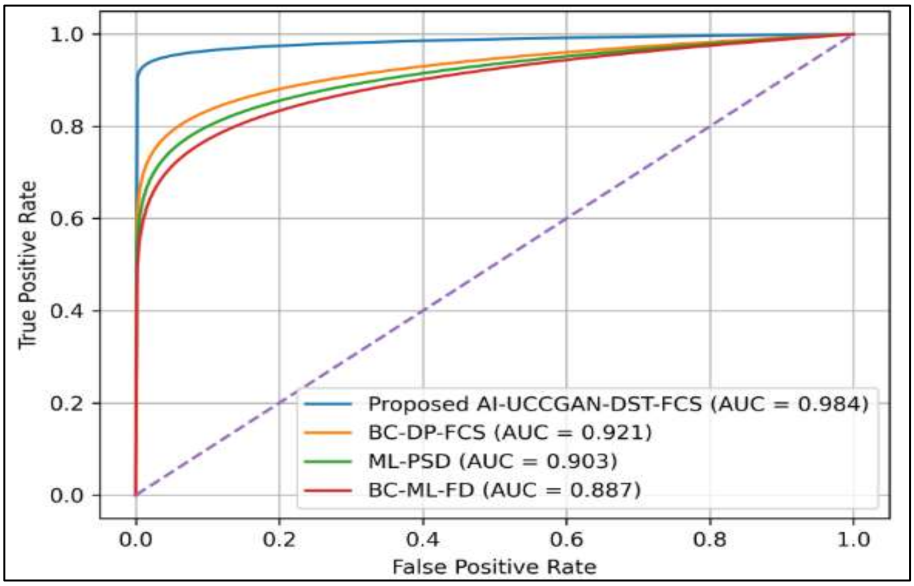

Figure 6: ROC of the proposed AI-UCCGAN-DST-FCS model with existing methods

Figure 7 presents the PR curve that measures the effectiveness of the model in processing imbalanced datasets, an important aspect of fraud detection, where fraudulent cases are not common. The proposed AI-UCCGAN-DST-FCS has an average accuracy of 0.962, which is better than BC-DP-FCS (0.889), ML-PSD (0.861), and BC-ML-FD (0.842). Its increased accuracy implies that the model has fewer false positives, whereas the high recall ensures that most fraud cases are accurately detected. The PR curve indicates that the proposed method is robust, as its performance increases even at high recall rates. This was made possible mainly because of the unsupervised capacity of feature extraction in UCCGAN in combination with SBOA optimization, which improves minority class learning. Moreover, the validation of the blockchain minimizes noise in the data. Therefore, the suggested model is very practical for fraud detection systems where the issue of class imbalance is a major problem.

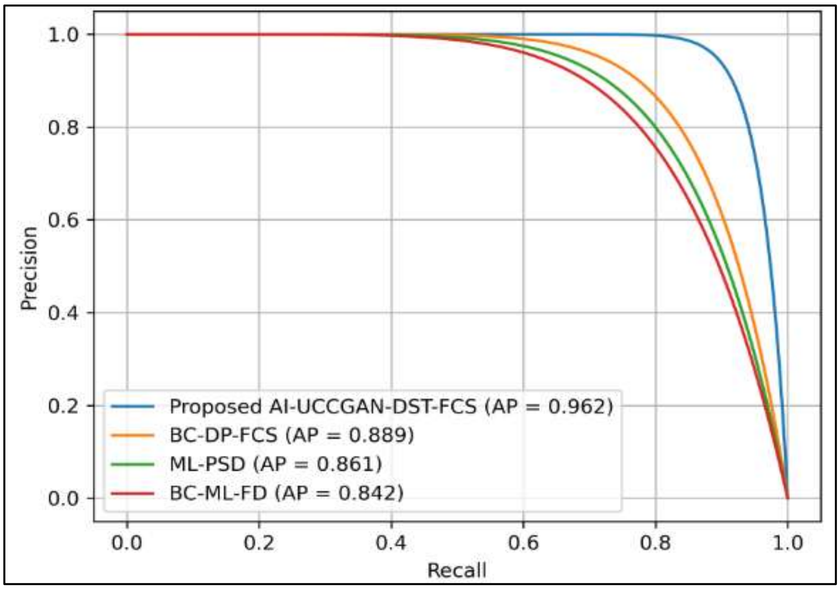

Figure 7: PR comparison of the proposed AI-UCCGAN-DST-FCS model with existing methods

5. Conclusion

This study introduces a new AI-based model, AI-UCCGAN-DST-FCS, to detect suspicious trends and prevent fake cheque scams in banking systems. Combining blockchain-based Proof-of-Green (POG) authentication and an adapted Unsupervised Cycle-Consistent Generative Adversarial Network (UCCGAN), the suggested approach helps secure transaction validation and effective fraud identification. The addition of the Secretary Bird Optimization Algorithm (SBOA) also contributes to higher model performance by maximizing some important parameters, leading to higher accuracy and shorter computational time. The experimental evidence shows that the suggested solution is better than current solutions in terms of detection accuracy, error rate, and efficiency, and can be used in a financial setting in real time. In addition, unsupervised learning allows the model to address data sparsity and changing fraud trends. The model can be extended in future work with real-time streaming data, explainable AI methods to enable interpretability, and multi-bank collaborative models to further scale up the model and robustness of large-scale financial systems.

References

1. Thakral, M. and Singh, S.P., 2022. A Secure Bank Transaction Using Blockchain Computing and Forest Oddity. In Security and Privacy in Cyberspace (pp. 101-113). Singapore: Springer Nature Singapore.
2. Madhuri, T.S., Babu, E.R., Uma, B. and Lakshmi, B.M., 2023. Big-data driven approaches in materials science for real-time detection and prevention of fraud. Materials Today: Proceedings, 81, pp.969-976.
3. Hasan, I. and Rizvi, S.A.M., 2022. AI-driven fraud detection and mitigation in e-commerce transactions. In Proceedings of Data Analytics and Management: ICDAM 2021, Volume 1 (pp. 403-414). Springer Singapore.
4. Rutskiy, V., Aljarbouh, A., Thommandru, A., Elkin, S., Amrani, Y.E., Semina, E., Mishchenko, A., Sorokina, N. and Tsarev, R., 2022. Prospects for the Use of Artificial Intelligence to Combat Fraud in Bank Payments. In Proceedings of the Computational Methods in Systems and Software (pp. 959-971). Cham: Springer International Publishing.
5. Piquero, N.L., Piquero, A.R., Gies, S., Green, B., Bobnis, A. and Velasquez, E., 2022. Preventing identity theft: perspectives on technological solutions from industry insiders. In The New Technology of Financial Crime (pp. 163-182). Routledge.
6. A. Ngai, Y. Hu, Y. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," Decision Support Systems, vol. 50, no. 3, pp. 559–569, 2011.
7. V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Computing Surveys, vol. 41, no. 3, pp. 1–58, 2009.
8. I. Goodfellow et al., "Generative adversarial nets," in Proc. Advances in Neural Information Processing Systems (NeurIPS), 2014, pp. 2672–2680.
9. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
10. X.-S. Yang, "Nature-inspired optimization algorithms," Elsevier, 2014.
11. Hammi, B., Zeadally, S., Adja, Y.C.E., Del Giudice, M. and Nebhen, J., 2021. Blockchain-based solution

for detecting and preventing fake check scams. IEEE Transactions on Engineering Management, 69(6), pp.3710-3725.

12. Kabla, A.H.H., Anbar, M., Manickam, S. and Karupayah, S., 2022. Eth-psd: A machine learning-based phishing scam detection approach in ethereum. IEEE Access, 10, pp.118043-118057.
13. Pranto, T.H., Hasib, K.T.A.M., Rahman, T., Haque, A.B., Islam, A.N. and Rahman, R.M., 2022. Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach. IEEE Access, 10, pp.87115-87134.
14. Tang, Q., 2021. Towards using blockchain technology to prevent diploma fraud. IEEE access, 9, pp.168678-168688.
15. Mundra, A., Mishra, J., Jha, H. and Sharma, C., 2023. Blockchain-Based Novel Solution for Online Fraud Prevention and Detection. In Blockchain for Cybersecurity in Cyber-Physical Systems (pp. 241-257). Cham: Springer International Publishing.
16. U. Fiore, F. De Santis, F. Perla, P. Zanetti, and F. Palmieri, "Using generative adversarial networks for improving classification effectiveness in credit card fraud detection," Information Sciences, vol. 479, pp. 448–455, 2019.
17. A. Roy, J. Das, and S. Ghosh, "Blockchain-based secure fraud detection framework for financial transactions," IEEE Access, vol. 11, pp. 34567–34580, 2023.
18. J. Jurgovsky, M. Granitzer, K. Ziegler, S. Calabretto, P.-E. Portier, L. He-Guelton, and O. Caelen, "Sequence classification for credit-card fraud detection," Expert Systems with Applications, vol. 100, pp. 234–245, Jan. 2018.
19. G. Douzas and F. Bacao, "Effective data generation for imbalanced learning using conditional generative adversarial networks," Expert Systems with Applications, vol. 91, pp. 464–471, 2018.
20. H. Wang, J. Zheng, I. E. Carvajal-Roca, L. Chen, and M. Bai, "Financial Fraud Detection based on Deep Learning: Towards Large-Scale Pre-training Transformer Models," in Communications in computer and information science, 2023, pp. 163–177.
21. Bae, C.H., Kim, S.B., Park, C.H. and Choo, S.Y., 2016. Studies on effectiveness proof of green building certification through the quantitative analysis of environmental performance of multi-residential buildings. Journal of the Architectural Institute of Korea Planning & Design, 32(1), pp.145-154.
22. Zhou, H., Liu, Q., Weng, D. and Wang, Y., 2022. Unsupervised cycle-consistent generative adversarial networks for pan sharpening. IEEE Transactions on Geoscience and Remote Sensing, 60, pp.1-14.
23. Fu, Y., Liu, D., Chen, J. and He, L., 2024. Secretary bird optimization algorithm: a new metaheuristic for solving global optimization problems. Artificial Intelligence Review, 57(5), pp.1-102.
24. A. Dal Pozzolo, O. Caelen, Y.-A. Le Borgne, S. Waterschoot, and G. Bontempi, "Calibrating probability with undersampling for unbalanced classification," in Proc. IEEE Symposium Series on Computational Intelligence (SSCI), Cape Town, South Africa, 2015, pp. 159–166, doi: 10.1109/SSCI.2015.33.