



Optimizing Financial Fraud Detection: Understandings from Variable Selection with Neutrosophic Vague Soft Set

Z.A. Latipov¹, K.A. Naminova², I.S. Abdullayev³, A.E. Ilyin⁴, R.A. Shichiyakh⁵, E. Laxmi Lydia^{6*}

¹Department of Mathematics and Natural Sciences of Elabuga Institute, Kazan Federal University, Kazan, 420008, Russia

²Department of Management, Kalmyk State University, Elista, 358000, Russia

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

⁴Kursk Branch, Financial University under the Government of the Russian Federation, Moscow, 125167, Russia

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

⁶Department of Information Technology, VR Siddhartha Engineering College (A), Siddhartha Academy of Higher Education (Deemed to be University), Vijayawada, India

Emails: latipov.z.a@inbox.ru; naminova.k@yahoo.com; is.abdullayev@yahoo.com; Ilyin.aleksey.e@yandex.ru; rushichiyakh@yahoo.com; elaxmi2002@yahoo.com

Abstract

Neutrosophy is the neutralities study and prolongs the discussion of the truth of opinions. Neutrosophic logic might be used in all sectors, to provide the solution for the indeterminate challenges. Some real-time data experience issues like inconsistency, incompleteness, and indeterminacy. A fuzzy set (FS) offers an uncertain solution, and an intuitionistic fuzzy set (IFS) processes partial data, but both fail to handle uncertain data. Financial fraud, believed as a deceptive strategy to gain financial assistance, has recently become a common threat in organizations and companies. Traditional methods namely manual inspections and verifications are costly, time-consuming, and imprecise to identify such fraudulent actions. With the development of artificial intelligence (AI), machine learning (ML)-based algorithms are applied logically to identify fraud transactions by investigating a larger amount of financial data. Therefore, the study offers an Optimizing Financial Fraud Detection using Bayesian Optimization and Variable Selection with Neutrosophic Vague Soft Set (OFFDBO-VSNVS) Algorithm. The OFFDBO-VSNVS model presents an optimized framework for fraud detection by integrating advanced variable selection techniques and classification models. Initially, the OFFDBO-VSNVS technique applies the Z-score data normalization technique to transform input data into a compatible layout. Next, the grey wolf optimizer (GWO)--based feature selection to effectively reduce dimensionality and highlight the most relevant features. For the classification and detection of financial fraud, the neutrosophic vague soft set (NVS) model can be employed. Eventually, the Bayesian optimization (BO) model adjusts the hyperparameter values of the NVS algorithm optimally and outcomes in greater classification performance. The stimulated outcome study of the OFFDBO-VSNVS model occurs and the outcomes are examined in terms of changing features. The experimental study represented the superiority of the OFFDBO-VSNVS method across the existing state-of-the-art methods

Keywords: Neutrosophic Logic; Fuzzy Set; Soft Set; Financial Fraud Detection; Bayesian Optimization; Neutrosophic Vague Soft Set

1. Introduction

One of the most effective devices to model uncertainties in decision-making difficulties is the neutrosophic set (NS) and its extensions, namely interval NS (INS), complex NS (CNS), and interval complex NS (ICNS) [1]. A well-organized device for establishing vagueness and uncertainty in decision-making is the NS which is the more commonly traditional set, intuitionistic fuzzy set (IFS), and fuzzy set by including 3 ratings of falsehood, indeterminacy, and truth, of an established report [2]. It is used in different decision-making methods. However,

to modify NS with more actual composite examples, INS and CNS were presented for that reason. As the economy develops quickly, the amount of registered companies in the universe is improving yearly. Simultaneously, more corporations have financial difficulties than earlier [3]. It's not only very disruptive to the status of companies and their organization but also has a bad influence on shareholders and investors. Financial fraud talks about the usage of illegal and fraudulent models or misleading strategies to get financial advantages [4]. Fraud is performed in several fields of finance, like insurance, banking, corporates, taxation, and so on. Fiscal evasion and fraud, namely tax evasion, credit card fraud, money laundry, financial statement fraud, and other kinds of financial scams, becoming increasingly difficult [5]. Regardless of efforts to remove financial scams, their incidence undesirably affects society and businesses as several hundred billion dollars are lost to fraudulent attacks every year. This important financial loss has considerably changed merchants, banks, and individuals [6].

Fraudulent financial activity is very complicated and sophisticated to recognize. Frauds are improving considerably with the growth of modern technology, mainly in the financial area [7]. There are numerous methods of fraud in financial methods including fraudulent loans, scamming, online banking fraud, falsification of documents, Phishing, fraudulent accounts among others, and credit card fraud. Fraudulent crimes cost financial formations millions of dollars every year, which influences the establishment's financial condition and the assurance of customers [8]. Worldwide financial companies and institutions are undergoing huge losses because of numerous financial frauds. Numerous fraud detection methods have been presented in earlier times. Most of the conventional models are manual, and it is not only costly, time-consuming, and inaccurate but also unrealistic [9]. Using the development of the AI model, data mining and machine learning (ML) were used for detecting fraud actions in the financial area. Either supervised or unsupervised models have been applied to predict fraudulent actions [10]. Classification models are the most common technique to detect financial fraud transactions.

The study offers an Optimizing Financial Fraud Detection using Bayesian Optimization and Variable Selection with Neutrosophic Vague Soft Set (OFFDBO-VSNVS) Algorithm. Initially, the OFFDBO-VSNVS technique applies the Z-score data normalization technique to transform input data into a compatible layout. Next, the grey wolf optimizer (GWO)--based feature selection to effectively reduce dimensionality and highlight the most relevant features. For the classification and detection of financial fraud, the neutrosophic vague soft set (NVS) model can be employed. Eventually, the Bayesian optimization (BO) model adjusts the hyperparameter values of the NVS algorithm optimally and outcomes in greater classification performance. The experimental study represented the superiority of the OFFDBO-VSNVS method across the existing state-of-the-art methods.

2. Related Works

Islam et al. [11] introduced rules for detecting fraudulent transactions that may not include some resampling model. The efficiency of the rule-based model (RBM) can be considered by a metrics variety. The presented rule-based method in comparison with some recent ML algorithms namely KNN, NB, DT, RF, MLP, and LR. Zhang et al. [12] presented the usage of ML models to improve the recognition of fraudulent transactions. The dataset was pre-processed for processing missing values and balancing the fraud samples. Huang et al. [13] implemented an ML-based K-means clustering model to improve the efficiency and accuracy of financial fraud detection. By gathering huge quantities of transaction of financial data, this paper properly recognizes abnormal behaviours and patterns, thus identifying possible fraud. In Comparison with conventional rule-based detection models, ML-based techniques well adjust to ever-changing fraudulence methods and patterns while increasing precision and flexibility in recognition. Additionally, K-means clustering helps in enhancing resource allocation inside fiscal organizations by allowing concentrated prevention and monitoring tries in higher-risk regions, therefore successfully modifying the influence of fraud on the complete financial method.

In [14], a fraud detection framework can be proposed by applying an ML model combined with a newly presented metaheuristic model Egret Swarm Optimization Algorithm (ESOA). A cost-sensitive loss and objective function were then built, and a nonlinear approach was carried out for mapping the forecast values into the labels. Njoku et al. [15] use web-based model for developing fraud detection process with ML algorithm and rule-based technique. By using ML techniques and a collection of rules, the method should precisely classify transactions as fraudulent or legitimate and additionally enable describing of fraudulent cases for the valuation of risks. These active models search to bolster the stability and security of the financial (banking) industries by successfully countering fraudulent patterns and fostering more protected financial conditions. Mohsen et al. [16] implemented a method for credit card fraud detection with ML methods. A new approach to credit card fraud detection deals with ML has been presented in this work. ML is an AI subdivision in comparison with learning methods from knowledge and implementation tasks without being designed. Three ML models were applied: RF, LR, Artificial Neural network, and SVM. Initially, the most important features that disturb the kind of transactions were designated. Next, the ML algorithm has been utilized.

3. The Proposed Method

In the article, we offer an OFFDBO-VSNVS Algorithm. The OFFDBO-VSNVS model presents an optimized framework for fraud detection by integrating advanced variable selection techniques and classification models. It contains four various processes, as demonstrated in Fig. 1.

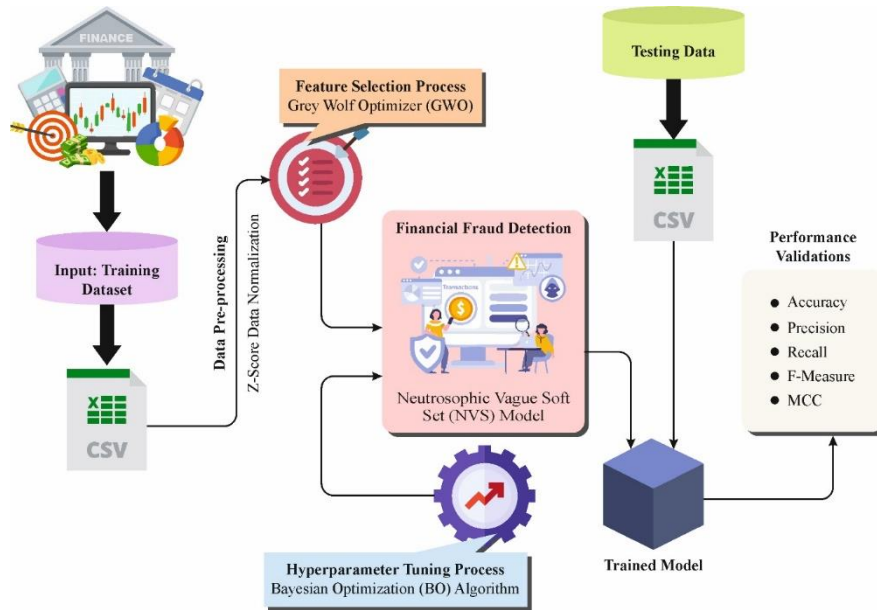


Figure 1. Overall process of OFFDBO-VSNVS Algorithm

A. Z-score Normalization

Initially, the OFFDBO-VSNVS technique applies the Z-score data normalization technique to transform an input data into a compatible layout. Z-score normalization is a crucial pre-processing stage in financial fraudulent detection, converting raw data into a normalized form by scaling features depending on their standard deviation and mean [17]. This model guarantees that each feature has a standard deviation of 1 and a mean of 0, permitting models to treat every variable on a related scale. In fraudulent detection, whereas variables can differ generally in magnitude, Z-score normalization aids in increasing model performance by removing biases due to different ranges or units. It improves accuracy by allowing more reliable and consistent detection of abnormal patterns in financial data.

B. GWO-based Feature Selection

Next, the GWO-based FS effectively reduces dimensionality and highlights the most relevant features. GWO is an accomplished development-established swarm intelligence (SI) technique presented by Mirjalili [18]. These types of methods depend on the simulation of the social order and seeking actions of Grey Wolf Herd. GW has purely hierarchic social types including $\alpha, \beta, \delta,$ and ω . Because of its easy infrastructure, irrelevant parameter variation essential, and maximum accuracy, the GWO technique is continuously employed for functional optimization. The place of i^{th} wolf is represented as $X_j = X_1^i, X_2^i, \dots, X_d^i$. X_d^i implies the location of the i^{th} wolf is d -dimension space, for a population comprising N grey wolves ($X = X_1, X_2, \dots, X_N$). The particular hunting role is as follows:

$$D = |C * X_i(t) - X(t)| \tag{1}$$

$$X_i(t + 1) = X(t) - A * D \tag{2}$$

whereas A and C denote the co-efficient vectors, t signifies the iteration counts, $X(t)$ refers to the position vector of GW , $X_i(t)$ indicates the target position vector of GW , D appears to the distance among the prey as well as grey wolf.

Determining the coefficient vector as:

$$A = 2 * a * r_1 - a \tag{3}$$

$$C = 2 * r_2 \tag{4}$$

$$a = 2 - i * \left(\frac{2}{\text{Maximum iteration}} \right) \tag{5}$$

In which, r_1 and r_2 appears to the random vectors with a range of zero and one, and a implies the iteration feature. During this case, the population, iteration counts, and run counts for every method are 25, 100, and 7, respectively. Besides, a reduced in 2 to 0. GW has a strong food search capability. α signifies the boss who will serve in every activity and sometimes β and δ can join. β and δ is also offering α with effective goal data in the GWO as an optimum solution. So, α , β , and δ are the 3 ideal replacements really and their altered positions:

$$D_\alpha = |C_1 * X_\alpha(t) - X(t)| \tag{6}$$

$$D_\beta = |C_2 * X_\beta(t) - X(t)| \tag{7}$$

$$D_\delta = |C_3 * X_\delta(t) - X(t)| \tag{8}$$

$$X_1 = X_\alpha - A_1 * D_\alpha \tag{9}$$

$$X_2 = X_\beta - A_2 * D_\beta \tag{10}$$

$$X_3 = X_\delta - A_3 * D_\delta \tag{11}$$

$$X(t + 1) = \frac{X_1 + X_2 + X_3}{3} \tag{12}$$

whereas X_α , X_β , and X_δ Implies the existing positions of the 3 better performances α , β , and δ , correspondingly; $X(t)$ denotes the target position; D_α , D_β , and D_δ demonstrates the distances from the prey to 3 performances, correspondingly; $X(t + 1)$ refers to the location vector with upgraded seeking factor; C and A define the arbitrary vectors. Fig. 2 illustrates the flowchart of GWO.

The fitness function (FF) applied in the GWO technique is considered to have a balance between the number of nominated features in every solution (minimum) and the classification precision (maximum) gained by utilizing these chosen features, Eq. (13) characterizes the FF to assess solutions.

$$Fitness = \alpha \gamma_R(D) + \beta \frac{|R|}{|C|} \tag{13}$$

Here $\gamma_R(D)$ epitomizes the classifier rate of error of an assumed classifier. $|R|$ represents the cardinalities of the designated sub-set and $|C|$ denotes the total feature counts in the dataset, α and β are dual parameters equal to the significance of classifier qualities and sub-set length. $\alpha \in [1,0]$ and $\beta = 1 - \alpha$.

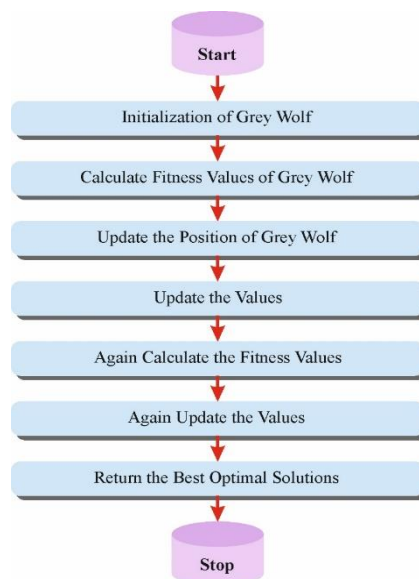


Figure 2. Flowchart of GWO

C. Financial Fraud Detection using NVS

For the classification and detection of financial fraud, the NVS model can be employed. Definition2.1. In U , assume L as a PIVFS is the method $\tilde{L} = \{\vartheta, \langle \gamma_L^T(\vartheta), \gamma_L^F(\vartheta) \rangle | \vartheta \in U\}$, $\gamma_L^T(\vartheta) = [\gamma_L^{Tl}(\vartheta), \gamma_L^{Tu}(\vartheta)]$ and $\gamma_L^F(\vartheta) = [\gamma_L^{Fl}(\vartheta), \gamma_L^{Fu}(\vartheta)]$ means the non- and membership degree of L correspondingly [19]. Here γ_L^T and γ_L^F denotes the function from \mathbb{U} into $\mathbb{D}[0,1]$ and $0 \leq (\gamma_L^T(\vartheta))^2 + (\gamma_L^F(\vartheta))^2 \leq 1$ it has been detected that $0 \leq (\gamma_L^{Tu}(\vartheta))^2 + (\gamma_L^{Fu}(\vartheta))^2 \leq 1$.

Definition2.2. The neutrosophic set (NS) $L = \{\vartheta, \langle \gamma_L^T(\vartheta), \gamma_L^I(\vartheta), \gamma_L^F(\vartheta) \rangle | \vartheta \in \mathbb{U}\}$, whereas $\gamma_L^T(\vartheta)$, $\gamma_L^I(\vartheta)$ and $\gamma_L^F(\vartheta)$ were termed TG, IG, and FG of L correspondingly.

Definition 2.3. The valued interval of NS $\tilde{L} = \{\vartheta, \langle x_L^T(\vartheta), x_L^I(\vartheta), x_L^F(\vartheta) \rangle | \vartheta \in \mathbb{U}\}$, whereas $\tilde{x}_L^T(\vartheta) = [x_L^{Tl}(\vartheta), x_L^{Tu}(\vartheta)]$, $\tilde{x}_L^I(\vartheta) = [x_L^{Il}(\vartheta), x_L^{Iu}(\vartheta)]$; $\tilde{x}_L^F(\vartheta) = [x_L^{Fl}(\vartheta), x_L^{Fu}(\vartheta)]$ and $\tilde{x}_L^T(\vartheta) = [x_L^{Tl}(\vartheta), x_L^{Tu}(\vartheta)]$, signifies the grade of indeterminacy, falsity, and truth-membership of L correspondingly. Let the map $\tilde{x}_L^T: \mathbb{U} \rightarrow D[0,1]$, $\tilde{x}_L^I: \mathbb{U} \rightarrow D[0,1]$, $\tilde{x}_L^F: \mathbb{U} \rightarrow D[0,1]$ and $0 \leq (\tilde{x}_L^T(\vartheta))^2 + (\tilde{x}_L^I(\vartheta))^2 + (\tilde{x}_L^F(\vartheta))^2 \leq 2$. Now $\tilde{L} = ([\chi_L^{Tl}, \chi_L^{Tu}], [\chi_L^{Il}, \chi_L^{Iu}], [\chi_L^{Fl}, \chi_L^{Fu}])$ is named a Pythagorean neutrosophic interval-valued number (PyNIVN).

Definition2.4. Assume E and \mathbb{U} as a set and universe of parameters correspondingly. The set $(\tilde{\Gamma}, \tilde{L})$ or $\tilde{\Gamma}_L$ is named a PyNIVFS set on \mathbb{U} if $L \subseteq E$ and $\Gamma: L \rightarrow PyNIVF^{\mathbb{U}}$, $PyNIVF^{\mathbb{U}}$ is represents the collection of every Pythagorean neutrosophic interval-valued fuzzy sub-sets of \mathbb{U} . So

$$\tilde{\Gamma}_L = \left\{ e, \left\{ \frac{x}{([\chi_{F_L^Tl}^T(\vartheta), \chi_{F_L^Tu}^T(\vartheta)], [\chi_{F_L^Il}^I(\vartheta), \chi_{F_L^Iu}^I(\vartheta)], [\chi_{F_L^Fl}^F(\vartheta), \chi_{F_L^Fu}^F(\vartheta)])} \right\} : e \in L, \vartheta \in \mathbb{U} \right\}.$$

Remark 2.5. Utilizing vital processes of arithmetic leads as follows.

- (i) $[u, v] + [w, x] = [u + w, v + x]$
- (ii) $[u, v] - [w, x] = [u - \vartheta, v - w]$
- (iii) $[u, v] \cdot [w, x] = [uw, vx]$, when $u \geq 0$ and $v \geq 0$
- (iv) $\frac{1}{[u, v]} = \left[\frac{1}{v}, \frac{1}{u} \right]$, when $0 \notin [u, v]$, $u, v, w, \vartheta \in \mathbb{R}$.

Definition2.6. The VS L of \mathbb{U} , for each $\vartheta \in \mathbb{U}$. Then

1. $T_L(\vartheta) = 1$ and $F_L(\vartheta) = 0$ is signify unit VS of \mathbb{U} .
2. $T_L(\vartheta) = 0$ and $F_L(\vartheta) = 1$ is signify zero VS of \mathbb{U} .

Step1: Assume that $\Theta = \{\theta_i : i \in \mathbb{N}\}$ as the decision maker, $\mathcal{C} = \{\zeta_i : i \in \mathbb{N}\}$ as the substitutes and $D = \{e_i : i \in \mathbb{N}\}$ denotes a parameter.

Step2: Define the matrix of linguistic variables and weighted parameter

$$\mathcal{P} = [\zeta_{ij}^l, \zeta_{ij}^u] = \begin{bmatrix} [\zeta_{11}^l, \zeta_{11}^u] & [\zeta_{12}^l, \zeta_{12}^u] & \dots & [\zeta_{1m}^l, \zeta_{1m}^u] \\ [\zeta_{21}^l, \zeta_{21}^u] & [\zeta_{22}^l, \zeta_{22}^u] & \dots & [\zeta_{2m}^l, \zeta_{2m}^u] \\ \vdots & \vdots & \ddots & \vdots \\ [\zeta_{i1}^l, \zeta_{i1}^u] & [\zeta_{i2}^l, \zeta_{i2}^u] & \dots & [\zeta_{im}^l, \zeta_{im}^u] \\ \vdots & \vdots & \ddots & \vdots \\ [\zeta_{n1}^l, \zeta_{n1}^u] & [\zeta_{n2}^l, \zeta_{n2}^u] & \dots & [\zeta_{nm}^l, \zeta_{nm}^u] \end{bmatrix}$$

While, $[\zeta_{ij}^l, \zeta_{ij}^u]$ denotes weight and allocated to the expert θ_i to e_j .

Step3: Form the matrix of weighted normalized decision as

$$\hat{N} = [\hat{\eta}_{ij}^l, \hat{\eta}_{ij}^u]_{n \times m} = \begin{bmatrix} [\hat{\eta}_{11}^l, \hat{\eta}_{11}^u] & [\hat{\eta}_{12}^l, \hat{\eta}_{12}^u] & \dots & [\hat{\eta}_{1m}^l, \hat{\eta}_{1m}^u] \\ [\hat{\eta}_{21}^l, \hat{\eta}_{21}^u] & [\hat{\eta}_{22}^l, \hat{\eta}_{22}^u] & \dots & [\hat{\eta}_{2m}^l, \hat{\eta}_{2m}^u] \\ \vdots & \vdots & \ddots & \vdots \\ [\hat{\eta}_{i1}^l, \hat{\eta}_{i1}^u] & [\hat{\eta}_{i2}^l, \hat{\eta}_{i2}^u] & \dots & [\hat{\eta}_{im}^l, \hat{\eta}_{im}^u] \\ \vdots & \vdots & \ddots & \vdots \\ [\hat{\eta}_{n1}^l, \hat{\eta}_{n1}^u] & [\hat{\eta}_{n2}^l, \hat{\eta}_{n2}^u] & \dots & [\hat{\eta}_{nm}^l, \hat{\eta}_{nm}^u] \end{bmatrix}$$

Where, $[\hat{\eta}_{ij}^l, \hat{\eta}_{ij}^u] = \left[\frac{\zeta_{ij}^l}{\sqrt{\sum_{i=1}^n \zeta_i^{2u}}}, \frac{\zeta_{ij}^u}{\sqrt{\sum_{i=1}^n \zeta_i^{2l}}} \right]$ represents normalized condition and discover the weighted vector

$\mathcal{W} = ([m_1^l, m_1^u], [m_2^l, m_2^u], \dots, [m_m^l, m_m^u])$, while $[m_j^l, m_j^u] = \left[\frac{\zeta_{ij}^l}{\sqrt{\sum_{i=1}^n \zeta_{ij}^u}}, \frac{\zeta_{ij}^u}{\sqrt{\sum_{i=1}^n \zeta_{ij}^l}} \right]$ mean relative weight of the j th

parameter and $[\zeta_j^l, \zeta_j^u] = \left[\frac{\sum_{i=1}^n \hat{\eta}_{ij}^l}{n}, \frac{\sum_{i=1}^n \hat{\eta}_{ij}^u}{n} \right]$.

Step4: The NVS decision matrix is set by

$$\theta_i = [q_{jk}^{li}, q_{jk}^{ui}]_{l \times m}$$

$$= \begin{bmatrix} [(q_{11}^T, q_{11}^{1-F}), (q_{11}^l, q_{11}^l), (q_{11}^F, q_{11}^{1-T})]_i & [(q_{12}^T, q_{12}^{1-F}), (q_{12}^l, q_{12}^l), (q_{12}^F, q_{12}^{1-T})]_i & \dots & [(q_{1m}^T, q_{1m}^{1-F}), (q_{1m}^l, q_{1m}^l), (q_{1m}^F, q_{1m}^{1-T})]_i \\ [(q_{21}^T, q_{21}^{1-F}), (q_{21}^l, q_{21}^l), (q_{21}^F, q_{21}^{1-T})]_i & [(q_{22}^T, q_{22}^{1-F}), (q_{22}^l, q_{22}^l), (q_{22}^F, q_{22}^{1-T})]_i & \dots & [(q_{2m}^T, q_{2m}^{1-F}), (q_{2m}^l, q_{2m}^l), (q_{2m}^F, q_{2m}^{1-T})]_i \\ \vdots & \vdots & \ddots & \vdots \\ [(q_{j1}^T, q_{j1}^{1-F}), (q_{j1}^l, q_{j1}^l), (q_{j1}^F, q_{j1}^{1-T})]_i & [(q_{j2}^T, q_{j2}^{1-F}), (q_{j2}^l, q_{j2}^l), (q_{j2}^F, q_{j2}^{1-T})]_i & \dots & [(q_{jm}^T, q_{jm}^{1-F}), (q_{jm}^l, q_{jm}^l), (q_{jm}^F, q_{jm}^{1-T})]_i \\ \vdots & \vdots & \ddots & \vdots \\ [(q_{i1}^T, q_{i1}^{1-F}), (q_{i1}^l, q_{i1}^l), (q_{i1}^F, q_{i1}^{1-T})]_i & [(q_{i2}^T, q_{i2}^{1-F}), (q_{i2}^l, q_{i2}^l), (q_{i2}^F, q_{i2}^{1-T})]_i & \dots & [(q_{im}^T, q_{im}^{1-F}), (q_{im}^l, q_{im}^l), (q_{im}^F, q_{im}^{1-T})]_i \end{bmatrix}$$

Here, $[\rho_{jk}^l, \rho_{jk}^u]$ signifies i th decision maker $[\theta_i^l, \theta_i^u]$ for every i . The matrix of aggregating $[A^l, A^u] = \frac{[\theta_1^l, \theta_1^u] + [\theta_2^l, \theta_2^u] + \dots + [\theta_n^l, \theta_n^u]}{n} = [x_{jk}^l, x_{jk}^u]_{l \times m}$.

Step5: Discover the weighted NVS decision matrix

$$[\psi^l, \psi^u] = \begin{bmatrix} [\zeta_{jk}^l, \zeta_{jk}^u]_{l \times m} \\ [(z_{11}^T, z_{11}^{1-F}), (z_{11}^l, z_{11}^l), (z_{11}^F, z_{11}^{1-T})]_i & [(z_{12}^T, z_{12}^{1-F}), (z_{12}^l, z_{12}^l), (z_{12}^F, z_{12}^{1-T})]_i & \dots & [(z_{1m}^T, z_{1m}^{1-F}), (z_{1m}^l, z_{1m}^l), (z_{1m}^F, z_{1m}^{1-T})]_i \\ [(z_{21}^T, z_{21}^{1-F}), (z_{21}^l, z_{21}^l), (z_{21}^F, z_{21}^{1-T})]_i & [(z_{22}^T, z_{22}^{1-F}), (z_{22}^l, z_{22}^l), (z_{22}^F, z_{22}^{1-T})]_i & \dots & [(z_{2m}^T, z_{2m}^{1-F}), (z_{2m}^l, z_{2m}^l), (z_{2m}^F, z_{2m}^{1-T})]_i \\ \vdots & \vdots & \ddots & \vdots \\ [(z_{j1}^T, z_{j1}^{1-F}), (z_{j1}^l, z_{j1}^l), (z_{j1}^F, z_{j1}^{1-T})]_i & [(z_{j2}^T, z_{j2}^{1-F}), (z_{j2}^l, z_{j2}^l), (z_{j2}^F, z_{j2}^{1-T})]_i & \dots & [(z_{jm}^T, z_{jm}^{1-F}), (z_{jm}^l, z_{jm}^l), (z_{jm}^F, z_{jm}^{1-T})]_i \\ \vdots & \vdots & \ddots & \vdots \\ [(z_{i1}^T, z_{i1}^{1-F}), (z_{i1}^l, z_{i1}^l), (z_{i1}^F, z_{i1}^{1-T})]_i & [(z_{i2}^T, z_{i2}^{1-F}), (z_{i2}^l, z_{i2}^l), (z_{i2}^F, z_{i2}^{1-T})]_i & \dots & [(z_{im}^T, z_{im}^{1-F}), (z_{im}^l, z_{im}^l), (z_{im}^F, z_{im}^{1-T})]_i \end{bmatrix}$$

While $[\zeta_{jk}^l, \zeta_{jk}^u] = [m_k^l \times x_{jk}^l, m_k^u \times x_{jk}^u]$.

Step6: Calculate the NVS-PIS and NVS-NIS values. Next,

$$\begin{aligned} \text{NVS-PIS} &= ([z_1^{l+}, z_1^{u+}], [z_2^{l+}, z_2^{u+}], \dots, [z_l^{l+}, z_l^{u+}]) \\ &= \{(\vee_k [\zeta_{jk}^l, \zeta_{jk}^u], \wedge_k [\zeta_{jk}^l, \zeta_{jk}^u], \wedge_k [\zeta_{jk}^l, \zeta_{jk}^u]) : j = 1, 2, \dots, l\} \text{ and} \\ \text{NVS-NIS} &= ([z_1^{l-}, z_1^{u-}], [z_2^{l-}, z_2^{u-}], \dots, [z_l^{l-}, z_l^{u-}]) \\ &= \{(\wedge_k [\zeta_{jk}^l, \zeta_{jk}^u], \vee_k [\zeta_{jk}^l, \zeta_{jk}^u], \vee_k [\zeta_{jk}^l, \zeta_{jk}^u]) : j = 1, 2, \dots, l\}. \end{aligned}$$

Here NVS intersection \wedge and NVS union \vee .

Step7: Define the values of utility $[S_i^l, S_i^u]$, individual regret $[\mathbb{R}_i^l, \mathbb{R}_i^u]$ and cooperate \mathbb{Q}_i , whereas $[S_i^l, S_i^u] = \left[\max_{j=1}^m m_j^l \cdot \left(\sqrt{\frac{(\zeta_{ij}^l - \zeta_j^{u+})^2}{(\zeta_j^{u+} - \zeta_j^{l-})^2}} \right), \max_{j=1}^m m_j^u \cdot \left(\sqrt{\frac{(\zeta_{ij}^u - \zeta_j^{l+})^2}{(\zeta_j^{l+} - \zeta_j^{u-})^2}} \right) \right]$

$$\text{and } [\mathbb{R}_i^l, \mathbb{R}_i^u] = \left[\max_{j=1}^m m_j^l \cdot \left(\sqrt{\frac{(\zeta_{ij}^l - \zeta_j^{u+})^2}{(\zeta_j^{u+} - \zeta_j^{l-})^2}} \right), \max_{j=1}^m m_j^u \cdot \left(\sqrt{\frac{(\zeta_{ij}^u - \zeta_j^{l+})^2}{(\zeta_j^{l+} - \zeta_j^{u-})^2}} \right) \right]$$

$$\text{and } \mathbb{Q}_i = \frac{\kappa \left(\frac{s_i^l - s^{u-}}{s^{u+} - s^{l-}} \right) + \kappa \left(\frac{s_i^u - s^{l-}}{s^{l+} - s^{u-}} \right) + (1-\kappa) \left(\frac{\mathbb{R}_i^l - \mathbb{R}^{u-}}{\mathbb{R}^{u+} - \mathbb{R}^{l-}} \right) + (1-\kappa) \left(\frac{\mathbb{R}_i^u - \mathbb{R}^{l-}}{\mathbb{R}^{l+} - \mathbb{R}^{u-}} \right)}{2}$$

D. Hyperparameter Tuning Process

Eventually, the BO algorithm adjusts the hyperparameter values of the NVS algorithm optimally and outcomes in greater classification performance. BO is an estimated model that uses several probability-based surrogate methods like RF, Gaussian processes, and so on, for modelling the relationship between model performance and hyperparameters, finally recognizing the grouping of optimum hyperparameters [20]. In BO, the probability-based surrogate method represents replacing the objective function using a particular probabilities technique. The updated equation for the posterior probabilities is as demonstrated:

$$p(f|D) = \frac{p(D|f)p(f)}{p(D)} \tag{14}$$

Here, $D = \{(x_1, f_1), (x_2, f_2), (x_n, f_n)\}$ denotes the gathered sampled points; $p(f)$ means the previous distribution, which is calculated with the Bayesian equation to gain the posterior distribution of f .

BO surrogated methods are mostly classified into three categories: Gaussian Processes (GPs), Sequential Model-based Algorithm Configuration (SMAC) using regression of random forest, and Tree Parzen Estimator (TPE). This work uses TPE, a nonstandard BO model that depends on a tree structure density estimator of Parzen. Compared to another model, TPE establishes greater performance in higher-dimension spaces, with considerably increased speed.

The sample spaces for TPE parameters were tree-structured, mainly modeling $p(x)$ and $p(y)$. The previous parameter defines the parameters selected successively and the value ranges for this parameter.

TPE outlines the following dual probability distribution functions:

$$p(x|y) = \begin{cases} l(x), y < y^* \\ g(x), y > y^* \end{cases} \tag{15}$$

Now, $l(x)$ refers to the likelihood densities of $\{x_i\}$ equivalent to $f(x_i)$ become less than the threshold y^* , and $g(x)$ denotes the likelihood densities of $\{x_i\}$ equivalent to $f(x_i)$ be better than the threshold y^* .

By continually calculating the objective function at various positions, additional information is attained to estimate the objective function distribution. It allows the search for the optimum measurement position, targeting to gain the value of an optimum function. To measure whether a position is best, function assessments are gathered. During this optimum position, the function reaches its value of maximum. In TPE, the gaining functions for gathering function means Expected Improvement (EI), which denotes the probability of becoming less than the threshold. It executes well in the majority of the cases, and the equation is as demonstrated:

$$\begin{aligned} EI_{y^*}(x) &= \int_{-\infty}^{+\infty} \max(y^* - y, 0) p(y|x) dy \\ &= \int_{-\infty}^{y^*} \max(y^* - y, 0) \frac{p(x|y)p(y)}{p(x)} dy \end{aligned} \tag{16}$$

During this equation, the model p means posterior Gaussian distribution across the field of observation.

During this TPE structure, let $\gamma = p(y < y^*)$ and $p(x) = \int p(x|y)p(y)dy = \gamma l(x) + (1 - \gamma)g(x)$, formerly, the succeeding relationships hold:

$$EI_{y^*} = \frac{l(x)y^*\gamma - l(x) \int_{-\infty}^{y^*} p(y)dy}{\gamma l(x) + (1-\gamma)g(x)} \tag{17}$$

$$EI_{y^*} = \left(\gamma + \frac{g(x)}{l(x)}(1 - \gamma) \right)^{-1} \tag{18}$$

Eq. (9) indicates that $l(x)$ recognizes value with high probability, and $g(x)$ determines value with low probability, leading to a greater (EI). Either $l(x)$ or $g(x)$ are symbolized in a tree structure, enabling the sample gathering to gain additional extracted information. In every iteration, the model proceeds with the value x^* the maximum EI. The BO model obtains an FF to achieve increased classification performance. It defines a positive integer to symbolize the superior performance of the solutions of the candidate. In this work, the decrease of the classifier rate of error is careful as the FF.

$$\begin{aligned} \text{fitness}(x_i) &= \text{ClassifierErrorRate}(x_i) \\ &= \frac{\text{no of misclassified samples}}{\text{Total no of samples}} * 100 \end{aligned} \quad (19)$$

4. Result Analysis and Discussion

In this section, the performance validation analysis of the OFFDBO-VSNVS technique uses using financial fraud detection dataset [21], which contains 2000 samples under two classes as defined in Table 1. The total number of features is 9 (amount, nameOrig, step, type, nameDest, newbalanceDest, oldbalanceOrg, oldbalanceDest, and newbalanceOrig) and the selected features are 7 (oldbalanceOrg, type, step, newbalanceOrig, amount, newbalanceDest and oldbalanceDest).

Table 1: Details of dataset

Classes	No. of Samples
Is_Fraud_Yes	1000
Is_Fraud_No	1000
Total Samples	2000

In Table 2 and Fig. 3, the complete financial fraud detection outcomes of the OFFDBO-VSNVS method are on 500-3000 epochs. The table values stated that the OFFDBO-VSNVS model has properly classified as two classes. On 500 epochs, the OFFDBO-VSNVS algorithm attains average $accu_y$ of 95.20%, $prec_n$ of 95.27%, $reca_l$ of 95.20%, $F_{measure}$ of 95.20%, and MCC of 90.47%, respectively. Followed by, on 1000 epoch counts, the OFFDBO-VSNVS model achieves average $accu_y$ of 95.80%, $prec_n$ of 95.84%, $reca_l$ of 95.80%, $F_{measure}$ of 95.80%, and MCC of 91.64%, correspondingly. Likewise, on 1500 epoch counts, the OFFDBO-VSNVS technique reaches average $accu_y$ of 96.25%, $prec_n$ of 96.26%, $reca_l$ of 96.25%, $F_{measure}$ of 96.25%, and MCC of 92.51%, individually. In addition, on 2000 epoch counts, the OFFDBO-VSNVS method gains average $accu_y$ of 96.70%, $prec_n$ of 96.70%, $reca_l$ of 96.70%, $F_{measure}$ of 96.70%, and MCC of 93.40%, correspondingly. Eventually, on 3000 epoch counts, the OFFDBO-VSNVS system obtains average $accu_y$ of 96.50%, $prec_n$ of 96.52%, $reca_l$ of 96.50%, $F_{measure}$ of 96.50%, and MCC of 93.0%, appropriately.

Table 2: Financial fraud detection of OFFDBO-VSNVS method under 500-3000 epochs

Classes	$Accu_y$	$Prec_n$	$Reca_l$	$F_{Measure}$	MCC
Epoch - 500					
Is_Fraud_Yes	93.20	97.08	93.20	95.10	90.47
Is_Fraud_No	97.20	93.46	97.20	95.29	90.47
Average	95.20	95.27	95.20	95.20	90.47
Epoch - 1000					
Is_Fraud_Yes	94.30	97.22	94.30	95.74	91.64
Is_Fraud_No	97.30	94.47	97.30	95.86	91.64
Average	95.80	95.84	95.80	95.80	91.64
Epoch - 1500					
Is_Fraud_Yes	95.40	97.05	95.40	96.22	92.51
Is_Fraud_No	97.10	95.48	97.10	96.28	92.51
Average	96.25	96.26	96.25	96.25	92.51
Epoch - 2000					
Is_Fraud_Yes	97.00	96.42	97.00	96.71	93.40
Is_Fraud_No	96.40	96.98	96.40	96.69	93.40

Average	96.70	96.70	96.70	96.70	93.40
Epoch - 2500					
Is_Fraud_Yes	97.00	97.88	97.00	97.44	94.90
Is_Fraud_No	97.90	97.03	97.90	97.46	94.90
Average	97.45	97.45	97.45	97.45	94.90
Epoch - 3000					
Is_Fraud_Yes	95.50	97.45	95.50	96.46	93.02
Is_Fraud_No	97.50	95.59	97.50	96.53	93.02
Average	96.50	96.52	96.50	96.50	93.02

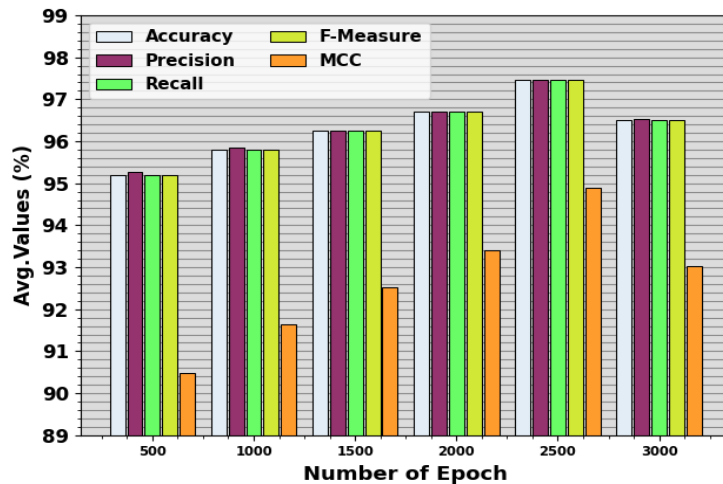


Figure 3. Average outcome of OFFDBO-VSNVS method under 500-3000 epochs

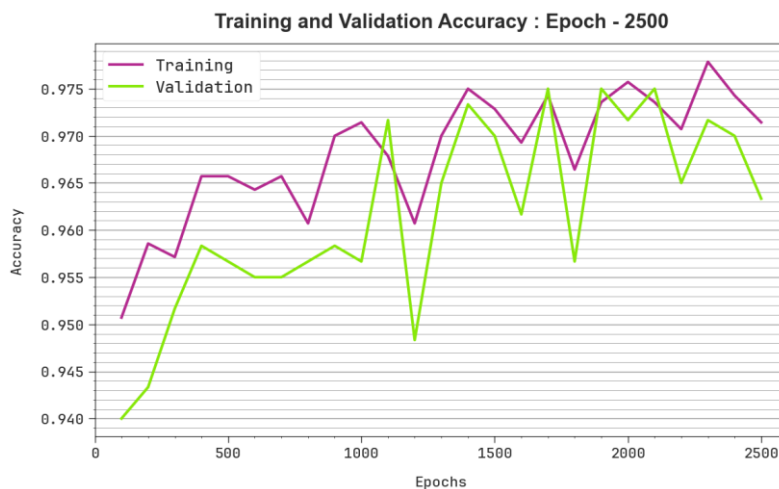


Figure 4. $Accu_y$ Curve of OFFDBO-VSNVS method under 2500 epochs

In Fig. 4, the TRA $accu_y$ (TRAAC) and validation $accu_y$ (VLAAC) outcomes of the OFFDBO-VSNVS approach are depicted. The $accu_y$ values are calculated throughout 0-2500 epochs. This figure discovered that the TRAAC and VLAAC values show a growing tendency that indicates the capabilities of the OFFDBO-VSNVS approach with better performance across distinct iterations. Additionally, the TRAAC and VLAAC stay adjacent across the epoch counts, which specifies least overfitting and presents the superior performance of the OFFDBO-VSNVS system, pledging continual prediction on unidentified instances.

In Fig. 5, the TRA loss (TRALO) and VLA loss (VLALO) graphs of the OFFDBO-VSNVS algorithm have been illustrated. The loss values are calculated for 0-2500 epochs. It is illustrated that the TRALO and VLALO values described a declining tendency that specified the capacities of the OFFDBO-VSNVS system to balance a trade-off between generality and data fitting. The incessant decrease in loss values also promises the heightened performance of the OFFDBO-VSNVS methodology and tuning the prediction results on time.

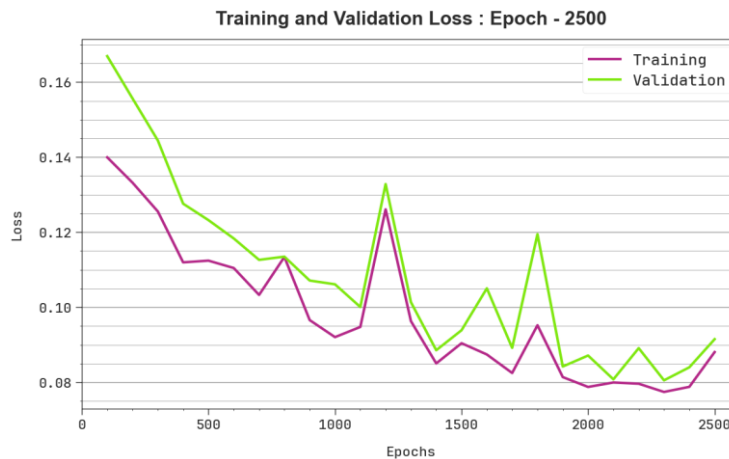


Figure 5. Loss curve of OFFDBO-VSNVS method under 2500 epochs

In Table 3 and Fig. 6, the stimulated results of the OFFDBO-VSNVS method with recent techniques are specified [22, 23]. The outcomes show that the ANN technique has exposed poor performance with $accu_y$, $prec_n$, $reca_l$, and $F_{measure}$ of 90.99%, 90.87%, 94.94%, and 92.49%, correspondingly. Simultaneously, the SVM algorithm has gained somewhat improved results with $accu_y$, $prec_n$, $reca_l$, and $F_{measure}$ of 91.80%, 93.97%, 90.56%, and 92.09%, individually. Moreover, the DT, HMM, FL, and LR methodologies have achieved relatively adjacent outcomes. In the meantime, the NB system has led to significant results with $accu_y$, $prec_n$, $reca_l$, and $F_{measure}$ of 95.27%, 93.56%, 96.12%, and 89.40%, correspondingly. Nevertheless, the OFFDBO-VSNVS algorithm outshines the other technique with higher $accu_y$, $prec_n$, $reca_l$, and $F_{measure}$ of 97.45%, 97.45%, 97.45%, and 97.45%, respectively.

Table 3 Comparative analysis of OFFDBO-VSNVS algorithm with other existing models

Methodology	$Accu_y$	$Prec_n$	$Reca_l$	$F_{Measure}$
Decision-Tree	93.23	92.29	94.42	91.11
Logistic Regression	95.05	91.95	91.15	97.18
ANN Algorithm	90.99	90.87	94.94	92.49
SVM Classifier	91.80	93.97	90.56	92.09
Fuzzy Logic Model	94.57	93.79	95.06	92.69
Naïve Bayes Method	95.27	93.56	96.12	89.40
HMM Technique	93.82	94.22	95.18	91.28
OFFDBO-VSNVS	97.45	97.45	97.45	97.45

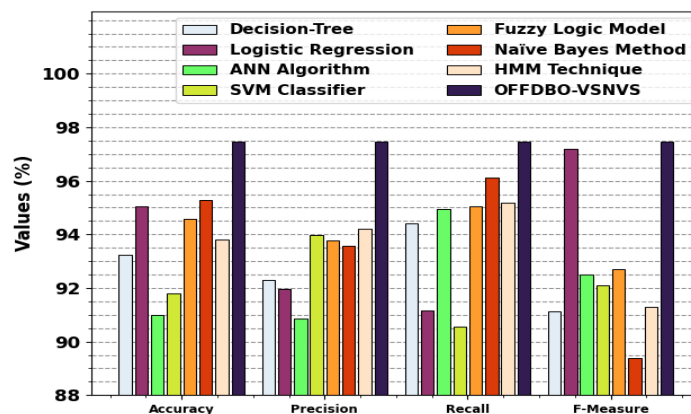


Figure 6. Comparative analysis of OFFDBO-VSNVS algorithm with other existing models

5. Conclusion

In the study, we offer an OFFDBO-VSNVS Algorithm. The OFFDBO-VSNVS model presents an optimized framework for fraud detection by integrating advanced variable selection techniques and classification models. Initially, the OFFDBO-VSNVS technique applies the Z-score data normalization technique to transform input data into a compatible layout. Next, the GWO-based FS effectively reduces dimensionality and highlights the most relevant features. For the classification and detection of financial fraud, the NVS model can be employed. Eventually, the BO algorithm adjusts the hyperparameter values of the NVS algorithm optimally and outcomes in greater classification performance. The stimulated outcome study of the OFFDBO-VSNVS model occurs and the outcomes are examined in terms of changing features. The experimental study represented the superiority of the OFFDBO-VSNVS method across the existing state-of-the-art methods.

Funding: “This research received no external funding”

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

References

- [1] Parimala, M., Karthika, M. and Smarandache, F., 2020. A review of fuzzy soft topological spaces, intuitionistic fuzzy soft topological spaces and neutrosophic soft topological spaces. *International Journal of Neutrosophic Science*, Vol. 10, No. 2, 2020 ,PP. 96-104.
- [2] Ashraf, S. and Abdullah, S., 2020. Decision support modeling for agriculture land selection based on sine trigonometric single valued neutrosophic information. *International Journal of Neutrosophic Science (IJNS)*, 9(2), pp.60-73.
- [3] Ashraf, S. and Abdullah, S., 2020. Decision support modeling for agriculture land selection based on sine trigonometric single valued neutrosophic information. *International Journal of Neutrosophic Science (IJNS)*, 9(2), pp.60-73.
- [4] Al-Hamido, R.K., Salha, L. and Gharibah, T., 2020. Pre Separation Axioms In Neutrosophic Crisp Topological Spaces. *International Journal of Neutrosophic Science*, 8(2), pp.72-79.
- [5] Salama, A.A., Henawy, M.B. and Alhabib, R., 2020. Online Analytical Processing Operations via Neutrosophic Systems. *International Journal of Neutrosophic Science*, 8(2), pp.87-109.
- [6] D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, “Credit card fraud detection-machine learning methods,” in *Proceeding of the 2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH)*, pp. 1–5, IEEE, East Sarajevo, Bosnia and Herzegovina, March 2019.
- [7] F. Carcillo, Y.-A. Le Borgne, O. Caelen, Y. Kessaci, F. Oble, ' and G. Bontempi, “Combining unsupervised and supervised learning in credit card fraud detection,” *Information Sciences*, vol. 557, pp. 317–331, 2021.
- [8] S. Sanober, I. Alam, S. Pande et al., “An enhanced secure deep learning algorithm for fraud detection in wireless communication,” *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6079582, 14 pages, 2021.
- [9] Randhawa, K.; Loo, C.K.; Seera, M.; Lim, C.P.; Nandi, A.K. Credit Card Fraud Detection Using AdaBoost and Majority Voting. *IEEE Access* 2018, 6, 14277–14284.
- [10] Craja, P.; Kim, A.; Lessmann, S. Deep learning for detecting financial statement fraud. *Decis. Support Syst.* 2020, 139, 113421.
- [11] Islam, S., Haque, M.M. and Karim, A.N.M.R., 2024. A rule-based machine learning model for financial fraud detection. *International Journal of Electrical & Computer Engineering (2088-8708)*, 14(1).
- [12] Zhang, R., Cheng, Y., Wang, L., Sang, N. and Xu, J., 2023. Efficient Bank Fraud Detection with Machine Learning. *Journal of Computational Methods in Engineering Applications*, pp.1-10.
- [13] Huang, Z., Zheng, H., Li, C. and Che, C., 2024. Application of machine learning-based k-means clustering for financial fraud detection. *Academic Journal of Science and Technology*, 10(1), pp.33-39.
- [14] Yi, Z., Cao, X., Pu, X., Wu, Y., Chen, Z., Khan, A.T., Francis, A. and Li, S., 2023. Fraud detection in capital markets: A novel machine learning approach. *Expert Systems with Applications*, 231, p.120760.
- [15] Njoku, D.O., Iwuchukwu, V.C., Jibiri, J.E., Ikwuazom, C.T., Ofoegbu, C.I. and Nwokoma, F.O., 2024. Machine learning approach for fraud detection system in financial institution: a web base application. *Machine Learning*, 20(4), pp.01-12.
- [16] Mohsen, O.R., Nassreddine, G. and Massoud, M., 2023. Credit Card Fraud Detector Based on Machine Learning Techniques. *Journal of Computer Science and Technology Studies*, 5(2), pp.16-30.
- [17] Prihanditya, H.A., 2020. The implementation of z-score normalization and boosting techniques to increase accuracy of c4. 5 algorithm in diagnosing chronic kidney disease. *Journal of Soft Computing Exploration*, 1(1), pp.63-69.

- [18] Adnan, R.M., Dai, H.L., Mostafa, R.R., Islam, A.R.M.T., Kisi, O., Elbeltagi, A. and Zounemat-Kermani, M., 2023. Application of novel binary optimized machine learning models for monthly streamflow prediction. *Applied Water Science*, 13(5), p.110.
- [19] Raja, K., Meenakshi, P.M., Al-Husban, A., Al-Qadri, M.O., Rajesh, N. and Palanikumar, M., 2024. Multi-criteria group decision making approach based on a new type of neutrosophic vague approach is used to select the shares of the companies for purchase. *Full Length Article*, 23(3), pp.296-96.
- [20] Fu, X., Chen, S. and Zhang, T., 2024. Prediction of Rock Bursts Based on Microseismic Energy Change: Application of Bayesian Optimization–Long Short-Term Memory Combined Model. *Applied Sciences*, 14(20), p.9277.
- [21] <https://www.kaggle.com/datasets/sriharshaedala/financial-fraud-detection-dataset>
- [22] Ali, A., Abd Razak, S., Othman, S.H., Eisa, T.A.E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H. and Saif, A., 2022. Financial fraud detection based on machine learning: a systematic literature review. *Applied Sciences*, 12(19), p.9637.
- [23] Shetty, V.R. and Malghan, R.L., 2023. Safeguarding against cyber threats: machine learning-based approaches for real-time fraud detection and prevention. *Engineering Proceedings*, 59(1), p.111.