A Novel Blockchain-Assisted Deep Learning Model for Enhancing Healthcare Data Security with Advanced Metaheuristic Optimization Techniques in Internet of Things

R. Sugantha Lakshmi[1,*], N. Suguna[2]

[1]Research Scholar, Department of Computer Science and Engineering , FEAT, Annamalai University, Chidambaram, India

[2]Associate Professor ,Department of Computer Science and Engineering , FEAT, Annamalai University, Chidambaram, India

Emails: uganthi83@gmail.com; rajusuguna81@gmail.com

Abstract

The Internet of Things (IoT) devices and technologies are more effective in the medical sector. It includes the combination of numerous interrelated sensor, systems, and devices for gathering, examining, and conveying health-related information for medicinal uses. In the healthcare field, Blockchain (BC) technology embraces huge latent for increasing the security and confidentiality of data. BC-aided intrusion detection on IoT healthcare methods is a new technique for increasing the privacy and security of complex health data. Patients have superior control throughout their information's growth, granting or revoking access as needed, but healthcare employees will modernize data sharing and certify the reliability of significant data. On the other hand, deep learning (DL) is excellent for transforming healthcare analytics, presenting rapid and tremendously precise estimations of medicinal circumstances. This paper presents a Blockchain-Assisted Deep Learning Model for Enhancing Healthcare Data Security with Metaheuristic Optimization Techniques (BCDL-HDSMOT) model. The main intention of the BCDL-HDSMOT technique is to develop an effective method for enhancing data security in the medical sector. At first, the blockchain technique is applied in healthcare to enhance data security, interoperability, and transparency while ensuring patient privacy and efficient record management. Next, the data pre-processing stage employs min-max normalization to clean, transform, and organize input data into a suitable quality for analysis. Besides, the black widow optimization algorithm (BWOA) has been deployed for the feature selection process to select the relevant features from input data. For the classification process, the proposed BCDL-HDSMOT technique designs a versatile long-short-term memory (VLSTM) method. At last, the improved seagull optimization algorithm (ISOA)--based hyperparameter selection process is performed to optimize the classification results of the VLSTM method. The experimental evaluation of the BCDL-HDSMOT algorithm can be tested on a benchmark dataset. The wide-ranging outcomes highlight the significant solution of the BCDL-HDSMOT approach to the cyberattack detection process.

Keywords: Blockchain; Deep Learning; Healthcare Data Security; Improved Seagull Optimization Algorithm; Feature Selection; IoT

1. Introduction

Healthcare is identified as a large-scale method that involves diverse components such as warehouses, health insurance, medicine, sensors, and more [1]. Modern technologies had a significant consequence on medical care practices and changed from traditional to technological practices such as monitoring medical care conditions utilizing wearable devices and sensors namely smart watches and wristbands [2]. It is vital for a huge amount of patients, those with abnormal blood pressure or diabetes, who need faster interference and periodical observation by specialists to solve possible and prompt solutions. The Internet of Things (IoT) connects laptops, tablets, and phones to a CPU for handling programs or applications [3]. The target of IoT is increasing the Internet function

DOI: https://doi.org/10.54216/FPA.190229
Received: December 29, 2024 Revised: February 13, 2025 Accepted: March 15, 2025

for linking things, which is unequipped with CPU, such as daily live devices, clinical equipment, and other sensors. Therefore, they occur multiple applications of IoT from diverse fields of life, like security, military, transportation, and economy [4]. Nevertheless, smart medical care methods are prone to various threats and security risks, namely system-level attacks, network attacks, and hardware and software-based attacks by the existence of patients at risk [5].

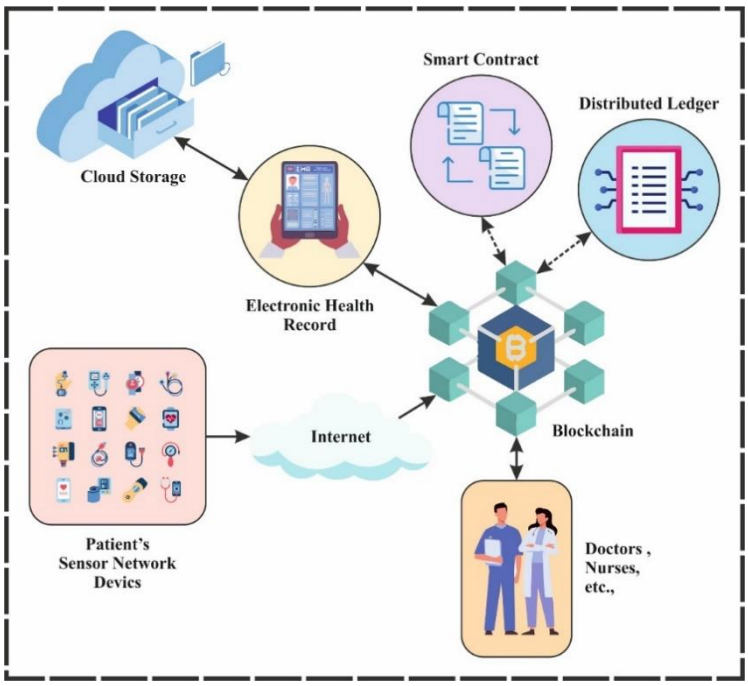

Figure 1. Structure of Blockchain in IoT healthcare system

Currently, emerging technologies, such as blockchain (BC), are employed for offering advanced solutions in various environments, one amongst them being the medical care region [6]. The technology of BC is utilized in the clinical area to ensure the safety of patient reports and the sharing of data among medical care providers, labs, and pharmaceutical companies. Clinical institutions are assisted by BC technology to attain vision and improve clinical report inspection. Fig. 1 represents the general structure of BC in the IoT healthcare system. Subsequently, the medical care supportive method demands a novel processing approach with delay-sensitive monitoring [7]. Moreover, BC comforts electronic medical records sharing among applications of end-user and medical care frameworks without disrupting the method of communication. Such capabilities are offered over the line-of-trust and authentication with inter-operability utilizing the distributed electronic ledger technology. The latest medical care applications focus on the safety of consumers and data shared to avoid unauthorized access and anonymity to illegal consumers [8]. Recently, managing the BC model as a decentralized ledger for observing shared data is becoming a well-known practice [9]. BC-aided trust-based security and authentication are incorporated with the clinical methods for enhancing the data-sharing qualities and precluding unauthorized interruptions.

Despite BC, technology offers a significant source for a guaranteed medical care model, increasing its capability by integrating it with Deep learning (DL) methodologies. In recent times, DL models have developed in data mining, artificial intelligence (AI), data classification, and more [10]. In general, the DL model is a deep neural network (DNN) involved in a process layer that can learn data representation and features with multiple abstraction layers. In the past decade, DL had a significant effect through different applications like Computer Vision (CV), speech recognition, reinforcement learning, and NLP.

This paper presents a Blockchain-Assisted DL Model for Enhancing Healthcare Data Security with Metaheuristic Optimization Techniques (BCDL-HDSMOT) model. At first, the blockchain technique is applied in the healthcare system. Next, the data pre-processing stage employs min-max normalization. Besides, the black widow optimization algorithm (BWOA) has been deployed for the feature selection process to select the relevant features. For the classification process, the proposed BCDL-HDSMOT technique designs a versatile long-short-term memory (VLSTM) method. At last, the improved seagull optimization algorithm (ISOA)--based hyperparameter selection process is performed to optimize the classification results of the VLSTM method. The experimental evaluation of the BCDL-HDSMOT algorithm can be tested on a benchmark dataset.

DOI: https://doi.org/10.54216/FPA.190229
Received: December 29, 2024 Revised: February 13, 2025 Accepted: March 15, 2025

2. Literature Survey

Khan et al. [11] developed a new Binary Spring Search (BSS) model based on group theory and combined it with a hybrid DNN method. The presented model integrates dynamic policy updates and secure key revocation. The projected structure employs BC technology for decentralized and immutable data management, AI for dynamic threat detection and data analysis, and progressive searchable encryption models to enable safeguard and effective data queries. The developed patient-centered data access technique, which integrates BC technology with trust chains, creates the model safer and more effective and determines a return on investment. Alanazi et al. [12] project an innovative BCODL-SDSC model in an upcoming medical care method. Initially, the projected model allows the technology of BC to maintain and store the patient's data. Likewise, the Fractional Order Lorenz system (FOLS)-based encryption model is implemented with tuna swarm optimizer (TSO) model-based optimum key generation. Eventually, a multistage procedure accomplishes the medical image classification: MobileNet-v1 feature extractor, artificial rabbit optimizer (ARO)-based hyper-parameter tuning, and stacked recurrent neural network (SRNN)-based classification. In [13], a holistic method that combines numerous cutting-edge models is projected to assist in patient monitoring and higher disease prediction, with privacy protection and data security. It applies the Hybrid ML methodologies; RF combined with a k-means clustering model for forecasting disease.

In [14], a BC-based data broadcast approach with a classification method in the medical care industry is projected. Data from various IoT data providers, namely BC is employed for creating protected training models. The oppositional-based harmony search (OHS) model is employed to create the finest strategy for the HE model. Furthermore, the technology of BC is employed to send data securely to the cloud server. In [15], an innovative approach named BC Consensus Decision-Making Random-coupled GroNet (BCDMRCGN) model is formed by secure data exchange in medical care methods. To ensure data integrity and safety, the initial phase in this plan is to accept BC Consensus Decision-Making with Proof of Authority (BCDPA). A Random-coupled GroNet (RCGN) is built for anomaly recognition inside the medical care system utilizing the validated data. Kiruthikadevi et al. [16] project a BC with DL Assisted Data Transmission and Classification (BDC-DTC) model in the medical care sector. Primarily, the Elgamal encryption method is employed to encode the clinical images that are stored safely employing BC technology. Afterward, the disease recognition method is implemented by utilizing a multi-faceted model such as backpropagation neural network (BPNN)-based classification, ResNet-18 feature extractor, and weIghted meaNoFvectOrs (INFO)-based hyper-parameter selection.

Swanthana and Aravinth [17] present a novel method called Buffalo Recurrent Diffie Hellman (BRDH), intended for increasing the security of data by proactively recognizing and reducing possible risks. The projected model integrates the ability of RNN and African Buffalo optimizer to constantly observe data in the cloud. Data encryption is utilized for determining strong security measures leveraging the Diffie-Hellman model. Authorized consumers accept a private key to decrypt cypher Text and access the unique data securely. In [18], a BC-aided secure data management framework (BSDMF) is presented. The projected methodology offers secure data management amongst personal servers and implantable clinical gadgets with personal and cloud servers. The IoMT-based security structure employs BC for ensuring data management and data transmission amongst connected nodes.

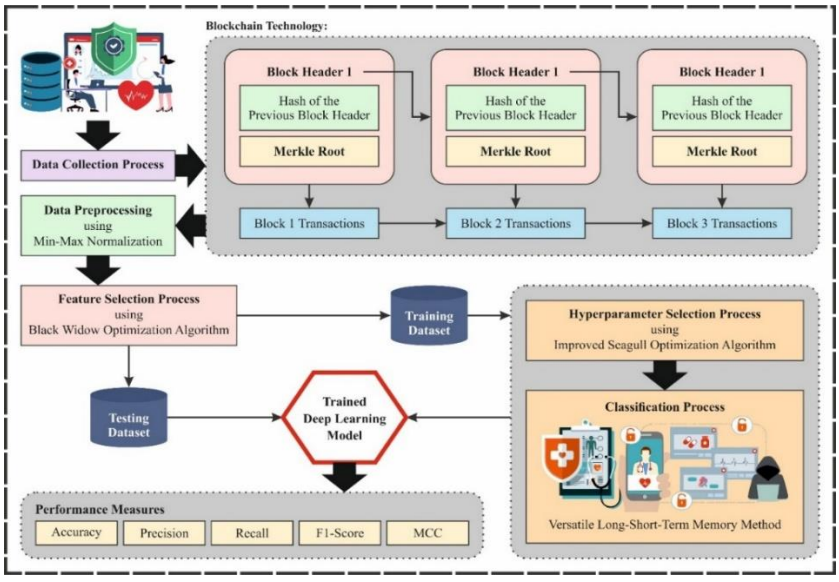

Figure 2. Workflow of BCDL-HDSMOT model

DOI: https://doi.org/10.54216/FPA.190229
Received: December 29, 2024 Revised: February 13, 2025 Accepted: March 15, 2025

3. Materials and Methods

In this paper, we have projected an innovative BCDL-HDSMOT model. The major aim of the BCDL-HDSMOT methodology is to develop an effective method for enhancing data security in the medical sector. Fig. 2 depicts the workflow of the BCDL-HDSMOT model.

A. BC Technology in Healthcare System

At first, the BC technique is applied in healthcare to enhance data security. The medical care industry is actively investigating innovative methods like combining Health Monitoring Systems with BC, to tackle numerous challenges comprising traceability, data integrity, interoperability, privacy, and security [19]. Initially presented in a manuscript aiming at Bitcoin, BC has transcended beyond its economic roots for finding applications through different segments, with medical care being a prominent region of focus. These technologies have huge promise in revolutionizing the industries by offering strong solutions to vital concerns namely interoperability and data security. Recently, there has been a growth in studies focused on employing the possibility of BC in the medical care industry. This contains recommendations to combine BC with the present framework, intending to make standardized and unified methods for the continuous exchange of clinical data and records through diverse institutions and platforms. Thus, BC can effectually reduce the interoperability challenges, longer plagued the segment of medical care, pave the method for additional secure and efficient sharing of data.

The major advantage of combining BC with the medical care industry is its capability to allow patients to handle their medical data. Over the decentralized stages assisted by BC, patients can securely control, share, and access their clinical reports with researchers or medical care providers are required. Additionally, the latest investigations have projected novel protocols that employ BC alongside protected cloud storage for modernizing knowledge provider transactions inside a content-centric system.

Moreover, there is an emerging interest in incorporating BC with the Internet of Things (IoT) to improve medical care management and delivery. This method can considerably decrease medical care costs while concurrently enhancing patient care by employing IoT gadgets for data collection and real-world monitoring, complementing the security of BC's and transparency aspects. By improving patient empowerment, data security, efficiency, and interoperability in medical care management and delivery, BC can change the healthcare is experienced and delivered, eventually enhancing results for providers and patients similarly.

B. Data Pre-processing

Next, the data preprocessing stage employs min-max normalization to clean, transform, and organize input data into a suitable quality for analysis. Min-Max normalizes numeric data to a pre-determined range, such as features namely test results, length of therapy, and patient age in comparison with a reliable scale [20]. This improves the performance and convergence of the model. The model Eq. (1) is,

$$X_{normalized} = \frac{x - x_{\min}}{x_{\max} - x_{min}} \tag{1}$$

The novel value can be signified by x, the maximal and minimal values for the attribute during the database are signified by $x_{\min}$ and $x_{\max}$, and the standardized value within the range [0,1] was signified by $X_{normalized}$.

C. Feature Selection using BWOA

Besides, the BWOA has been deployed for the FS process to select the relevant features from input data. The black widow is a kind of poisonous spider that weaves its webs in trees, occupies swamps and forests, and feeds on insects like butterflies, crickets, and beetles [21]. The succeeding stages exemplify the mathematical modeling of the model

Stage (1): Movement

The succeeding equation demonstrates the movement of the spider

$$x_k(\tau+1) = \begin{Bmatrix} x^*(\tau) - & mx_{r_1}(\tau) & if rand & \leq 0.3 \\ x^*(\tau) - & \cos(2\pi r)\, x_k(T) & ino Therwise & in\ otherwise \end{Bmatrix} \tag{2}$$

Whereas $x_k(t+1)$ refers to the novel position and specifies the spider's movement, $x^*(t)$ signifies the optimal position discovered thus far, m denotes a randomly generated number, r_1 signifies randomly generated number between 1 and the maximal size of the population, $x_{r_1}(t)$ denote initial position as $k \neq$, denote randomly generated number described within the range $[-1,1]$, $x_k(t)$ represents present position.

Stage (2): Pheromones

DOI: https://doi.org/10.54216/FPA.190229
Received: December 29, 2024 Revised: February 13, 2025 Accepted: March 15, 2025

For well-fed females create more silk than starving females and for male spiders are more responsive to the pheromones of well-fed females, pheromones are important in mating the spider. The rate of pheromone is computed utilizing the following Eq. (3).

$$pheromone(k) = \frac{fitness_{\max} - fitness_{(k)}}{fitness_{\max} - fitness_{\min}} \quad (3)$$

Whereas $fitness_{\max}$ and $fitness_{\text{in}}$ represent the worst and best fitness values in the present generation correspondingly, $fitness_{(k)}$ The pheromone vector in Eq. (3) has the proper fitness within the range [0,1], when the pheromone rates are lower in female spiders lower than or equivalent to 0.3, it is substituted by other ones with the succeeding Eq. (4).

$$x_k(t) = x_*(t) + \frac{1}{2}[x_{r1}(t) - 1\sigma * x_{r2}(t)] \quad (4)$$

Black Widow Algorithm Steps

The algorithm steps were outlined as shown:

Step (1): Set the primary community.

Step (2): The step counts are lower than the maximal iteration counts.

Step (3): Initialization of the random parameter m and α like $0.4 \le m \le 0.9 - 1.0 \le \alpha \le 1.0$

Step (4): Upgrade the motion of the spider utilizing Eq. (2)

Step (5): Compute the pheromone for every position utilizing Eq. (3)

Step (6): Upgrade sites with lower pheromone values utilizing Eq. (4)

Step (7): Establish the value of x_{new} for the novel location

Step (11): If $x_{new} < x_*$ then

Step (12): $x_* = x_{new}$

Step (13): End the steps once the end condition is encountered, and the best solution is located.

The fitness function (FF) reflects the precision of the classifier and the amount of elected features. It exploits the precision of the classifier and reduces the fixed size of the preferred features. Hence, the below-mentioned fitness function (FF) is employed for evaluating an individual solution, as exposed in Eq. (5).

$$Fitness = \alpha * ErrorRate + (1 - \alpha) * \frac{\#SF}{\#All\_F} \quad (5)$$

Here, $ErrorRate$ means a classifier rate of error by leveraging the desired feature. $ErrorRate$ is intended as the ratio of improper that classified to the amount of classification made among 0 and 1. $\#SF$ denotes an amount of chosen attributes and $\#All\_F$ refers to a total quantity of features in the original dataset. α is applied to influence the prominence of classifier superiority and sub-set length. The value of α is assigned as 0.9.

D. VLSTM-based Classification Process

For the classification process, the proposed BCDL-HDSMOT algorithm designs the VLSTM method. The VLSTM system excels at processing the temporal nature of medical data, permitting it to record time dependencies like treatment progress, outcome progress, and symptom development [22]. It assesses the sequence to utilize the $patient\ 's$ medical background and genetic features to forecast upcoming responses.

The RNN is the improved model of it. It can be distinct from RNN, it presents the theory of cell states. It should be selected by the LSTM state of the cell that states should be recollected and that must be escaped from. The hidden layer of LSTM system architecture comprises 3 gates: output, forget, and input gates. The output gate controls the data flow to another cell, while the input gates control the data flow into the cell memory. The forget gate task is to successfully eradicate the cell's present information state. Due to its complex architecture, the traditional LSTM system needs additional time to learn. It decreases the complexity of the network by incorporating forget and input gates into particular novel gates.

$$net\tau_{vs} = X_v \cdot \begin{bmatrix} g_{s-1} \\ W_s \end{bmatrix} + a_v = X_{vg} \cdot g_{s-1} + X_{vw} \cdot w_s + a_v \quad (6)$$

$$v_s = \sigma(net_{vs}) \quad (7)$$

DOI: https://doi.org/10.54216/FPA.190229
Received: December 29, 2024 Revised: February 13, 2025 Accepted: March 15, 2025

Define the present state of the information in Eq. (8),

$$net_{\widetilde{ds}} = X_{c\tilde{\imath}} \cdot \begin{bmatrix} g_{s-1} \\ W_s \end{bmatrix} + a_D = X_{\widetilde{dg}} \cdot g_{s-1} + X_{\widetilde{dw}} . w_s + a_v \quad (8)$$

$$\tilde{d}_s = \tanh(net_{\widetilde{ds}}) \quad (9)$$

Improve the memory cell in Eq. (10),

$$D_s = (1 - v_{s-1}) \times D_{s-1} + \tilde{d}_s \times v_s \quad (10)$$

Establish the output gates in Eqs. (11) and (12),

$$\text{ne } t_{ps} = X_p \cdot \begin{bmatrix} g_{s-1} \\ W_s \end{bmatrix} + a_p = X_{pg} \cdot g_{s-1} + X_{pw} \cdot w_s + a_p \quad (11)$$

$$p_s = \sigma(neT_{ps}) \quad (12)$$

Estimate the output of the hidden 1ayer in Eq. (13),

$$g_s = p_s \times \tanh(d_s) \quad (13)$$

Calculate the outcome of anticipated value in Eqs. (14) and (15),

$$y_s = X_Z \cdot g_s + a_Z \quad (14)$$

$$z_s = \sigma(ys) \quad (15)$$

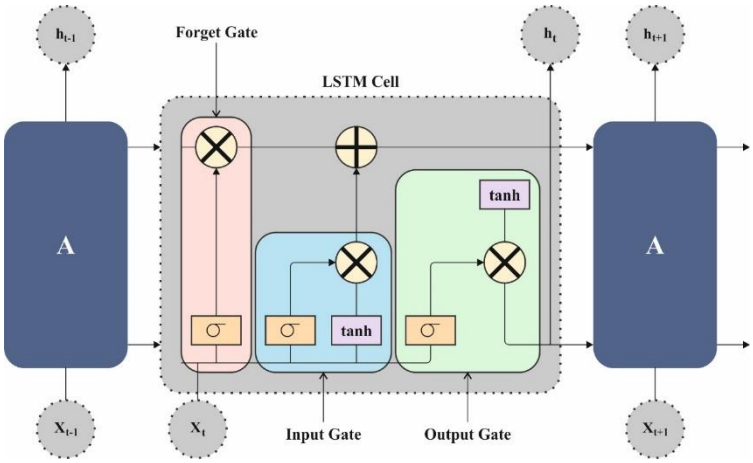

Figure 3. VLSTM Structure

The steps of the present phase are described by net_{vsv} ne $\widetilde{eds}$, net_{ps}, and y_s. The weighting of the arrays denotes X_v, X_d, and X_p. The bias vectors are signified by a_v, a , and a_p. In this specific duration, v_s, w_s, p_s, and $\widetilde{ds}$, represent sharing gates, inputs layer, outputs gates, and informational state, in sequence. The cell's status in the previous and the present periods are characterized by D_s and D_{s-1}. The symbol · used to multiply the matrix, whereas the $matrix$ components are multipy by each other utilizing the (.) symbol. The activation function of Sigmoid is $\sigma(w)$, and the $tanh()$ activation function is $\tanh(w)$.

$$\begin{cases} \sigma(w) = z = \dfrac{1}{A + f^{-w}} \\ \tanh(w) = z = \dfrac{f^{w} - f^{-w}}{f^{w} + f^{-w}} \end{cases} \quad (16)$$

VLSTM decreases the gate counts in comparison with LSTM which reduces the variable counts, which should be assessed in the weighted matrix. It utilizes the activation function $Tanh()$ to first stimulate the present knowledge condition before upgrading the cell of the memory. Then, it utilizes an improved gate v_s like the weighting of the present data condition d_s and 1- v_s like the weighting of the preceding cell memory D_{s-1} to make the linear mixture of the 2. The dual weighting calculated equals 1. Fig. 3 signifies the structure of VLSTM.

DOI: https://doi.org/10.54216/FPA.190229
Received: December 29, 2024 Revised: February 13, 2025 Accepted: March 15, 2025

E. Parameter Optimizer using ISOA

At last, the ISOA-based hyperparameter selection process is performed to optimize the classification results of the VLSTM method. The SOA is a new meta-heuristic model stimulated by the attacking and migratory behaviours of seagulls naturally [23]. Local searching has been performed by mimicking the seagull's spiral motion throughout their attacks. These features are taken advantage of it perform a detailed exploration of the local region. In the meantime, the model coordinates global and individual information throughout the search procedure. This coordination creates the method of flexible switching amongst numerous local bests and constant searches. During this power distribution system enhanced through the SOA method, N section switches or circuit breakers are involved, along with M. An array M $= [M_1, M_2, \cdots M_m]$ is organized by these m. According to array M, the switching function array $D^* = [D_1^*, D_2^*, \cdots D_N^*]$ related to the section switches or circuit breakers are created. Arrays D and $D^\star$ are created from the overcurrent information transmitted.

Elite reverse learning approach

The primary population quality is important to the model's performance. Therefore, the model is simply stuck in local bests. The Elite opposition-based learning (EOBL) approach is presented to create the original population of the seagull. The EOBL approach estimates the opposition solution by computing the opposite condition of the solution of the problems. This development guarantees that the population shields different regions within the solution area, provided that the model with complete searching abilities. Diversity was improved in the primary arbitrary seagull population. This results in a uniform choice in the complete iteration computation procedure. The early convergence of the model is prevented.

$M = \{MX,$ MY $\}$

$MX = [Mxl, Mx2, ..., MxN]$

$$MY = [Myl, My2, \dots, MyN]$$

$$MYi = (\max(Mx) + \min(Mx)) - Mxi$$

Here, M is related to the seagull group. The maximal and minimal function is represented as max and min. MX denotes an array arbitrarily produced. MY refers to the array gained based on this approach. Afterward, the primary population of the seagull is established, and the array inside group M of the consistent feeding sector state was replaced into Eq. (3) switching function to discover $Di(Mnew)^*$. $Mnew$ stands for an array of feeding sector states for the iteration rotation computation. $Di(Mnew)^*$ and D_i subsequently replaced into Eq. (4) goal function communicate into compute the objective function value.

Levy flight (LF) and random walk tactics

The location upgrade of the seagull's searching procedure is very significant. The upgrade of seagulls was influenced by the step-size selection. Once the step size is larger, it might stop traversing the complete space, and possibly lose the best solution inside the interval. On the other hand, a smaller step size might lead to a slower seagull upgrade, resulting in lower algorithmic efficacy. To deal with the problem, the study presents LF and random walk tactics to update seagull locations. LF, a searching tactic, that follows the Levy distribution, has been applied for controlling the step size. This guarantees that often spending on shorter-distance searches, with random longer-distance searches. The presentation of the LF approach precludes the model from converging early.

$Le\eta \sim u = t^{-\lambda} \quad 1 < \lambda \leq 3$

$$s = \frac{\mu}{|v|^{1/\beta}}$$

$$\sigma\mu = \left\{ \frac{\Gamma(1+\beta)\sin\left(\frac{\pi\beta}{2}\right)}{\Gamma\left[\frac{(1+\beta)}{2}\right]\beta^{2^{\frac{(\beta-1)}{2}}}} \right\} \tag{17}$$

During which the parameter was normally considered as 1.5, the function of Gamma was signified as Γ, and the standard distribution that complies with it is signified as μ, v.

The search route was made by the incorporation of LF and random walk tactics. The controlling of lengths of the step by LF guarantees that shorter-distance search is performed at particular times and longer-distance searches for others.

The location-updated equation for seagulls is reconsidered over the overview of the LF approach. Global optimizer is preserved whereas solution efficacy is highlighted. Good global searching abilities are presented with the seagull population afterward the LF is presented. The location-updated equation for seagulls is offered below:

DOI: https://doi.org/10.54216/FPA.190229
Received: December 29, 2024 Revised: February 13, 2025 Accepted: March 15, 2025

$$Ps^t = x \cdot y \cdot z \cdot Ds \cdot Levy + Pbs^t \tag{18}$$

The movement of the seagull group is separated from the xyz coordinated method. The movement procedure is spiral in condition.

$$\begin{aligned} x &= u * e^{\theta v} * \cos(2\pi\theta) \\ y &= u * e^{\theta v} * \sin(2\pi\theta) \\ z &= u * e^{\theta v} * \theta \end{aligned} \tag{19}$$

The constants u and v describe the spiral condition. θ denotes a randomly generated number. To guarantee a fast search is most closely related in the globally best way, a variable Ds is presented in the moving location of the seagull group. A similar equation for Ds is shown:

$$\begin{cases} Ds = |Cs + Ms| \\ Cs = Lold * A \\ Ms = B * (Lnew - Lold) \\ A = fc - \dfrac{t * fc}{Mox\_iter} \\ B = 2 * A^2 * rd \end{cases} \tag{20}$$

Cs refers to movement behavior by which seagulls prevent collisions. A denotes parameters that are linearly lowered using the iteration. rd stands for randomly generated number range between (0-1). fc is fixed to 2. t represents iteration rounds. Ms signifies movement behavior as the seagull approaches the nest location.

The ISOA originates an FF to accomplish the boosted performance of the classifier. It regulates a positive number to express the better efficiency of the candidate solution. The classification rate of error minimization is measured as FF, as specified in Eq. (21).

$$\begin{aligned} fitness(x_i) &= ClassifierErrorRate(x_i) \\ &= \frac{no.of\ misclassified\ samples}{Total\ no.of\ samples} * 100 \end{aligned} \tag{21}$$

4. Performance Validation

The performance study of the BCDL-HDSMOT technique is inspected below in the IoT healthcare security database [24]. This dataset contains 188694 instances under dual classes such as normal traffic and attack traffic as depicted in Table 1. There are 50 features accessible but only selected features are 38.

Table 1: Details of database

Class Label	No. of Samples
Normal Traffic (Patient Monitoring, Environment Monitoring)	108568
Attack Traffic	80126
Total Number of Instances	188694

DOI: https://doi.org/10.54216/FPA.190229
Received: December 29, 2024 Revised: February 13, 2025 Accepted: March 15, 2025

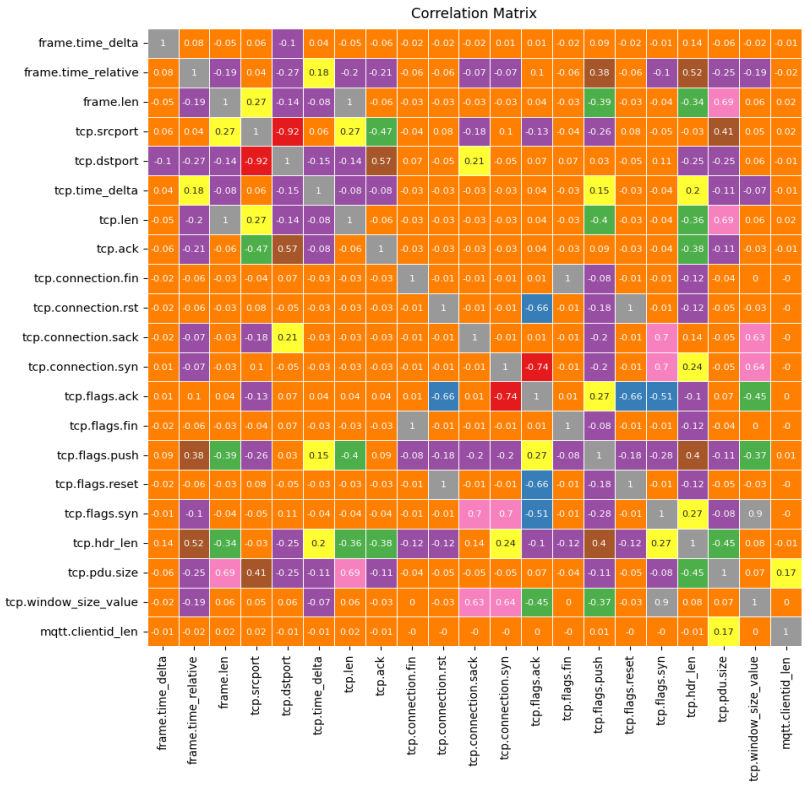

Figure 4. Correlation Matrix of BCDL-HDSMOT model

Fig. 4 establishes the correlation matrix created by the BCDL-HDSMOT approach. The outcomes identify that the BCDL-HDSMOT methodology has an effective prediction of each classes precisely.

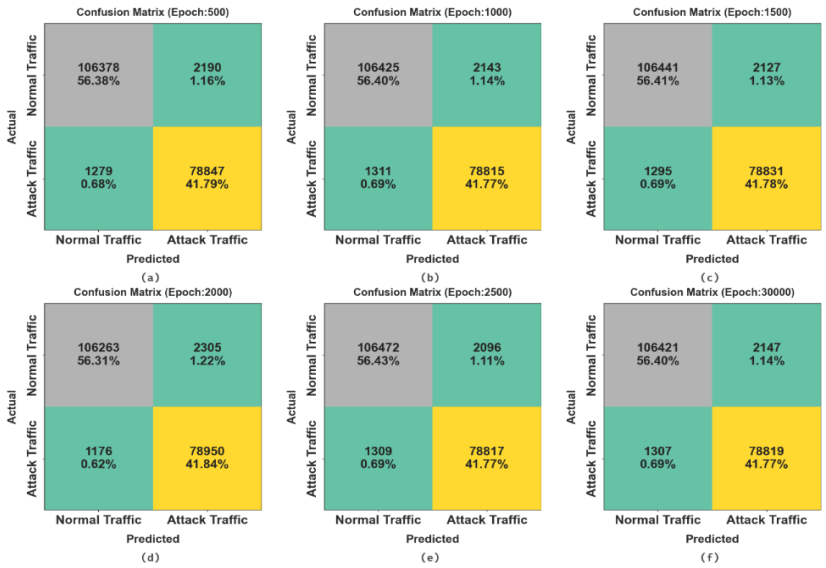

Figure 5. Confusion matrices of BCDL-HDSMOT model (a-f) Epochs 500-3000

Fig. 5 presents the confusion matrices produced by the BCDL-HDSMOT algorithm below several epochs. On 500 epochs, the BCDL-HDSMOT methodology has identified 106378 samples in normal traffic, and 78847 samples in attack traffic. Similarly, on 1500 epochs, the BCDL-HDSMOT method has known 106441 samples into normal traffic and 78831 samples in attack traffic. Followed by, on 2500 epochs, the BCDL-HDSMOT system has identified 106472 samples in normal traffic and 78817 samples in attack traffic. Finally, on 3000 epochs, the BCDL-HDSMOT approach has identified 106421 samples in normal traffic and 78819 samples in attack traffic.

DOI: https://doi.org/10.54216/FPA.190229
Received: December 29, 2024 Revised: February 13, 2025 Accepted: March 15, 2025

The classifier result of the BCDL-HDSMOT approach is determined below different epoch counts in Table 2 and Fig. 6. The table values state that the BCDL-HDSMOT approach correctly recognized every instance. On 500 epochs, the BCDL-HDSMOT methodology provides an average $accu_y$ of 98.19%, $prec_n$ of 98.05%, $reca_l$ of 98.19%, $F1_{score}$ of 98.12%, and MCC of 96.25%. Besides, on 1000 epochs, the BCDL-HDSMOT approach offers an average $accu_y$ of 98.19%, $prec_n$ of 98.07%, $reca_l$ of 98.19%, $F1_{score}$ of 98.13%, and MCC of 96.26%. Moreover, on 1500 epochs, the BCDL-HDSMOT algorithm delivers an average $accu_y$ of 98.21%, $prec_n$ of 98.09%, $reca_l$ of 98.21%, $F1_{score}$ of 98.15%, and MCC of 96.30%. Also, on 2500 epochs, the BCDL-HDSMOT system delivers an average $accu_y$ of 98.22%, $prec_n$ of 98.10%, $reca_l$ of 98.22%, $F1_{score}$ of 98.16%, and MCC of 96.32%. At last, on 3000 epochs, the BCDL-HDSMOT technique provides an average $accu_y$ of 98.20%, $prec_n$ of 98.07%, $reca_l$ of 98.20%, $F1_{score}$ of 98.13%, and MCC of 96.26%.

Table 2: Classifier result of BCDL-HDSMOT method below diverse epochs

Class Labels	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{score}$	MCC
Epoch - 500					
Normal Traffic	97.98	98.81	97.98	98.40	96.25
Attack Traffic	98.40	97.30	98.40	97.85	96.25
Average	98.19	98.05	98.19	98.12	96.25
Epoch - 1000					
Normal Traffic	98.03	98.78	98.03	98.40	96.26
Attack Traffic	98.36	97.35	98.36	97.86	96.26
Average	98.19	98.07	98.19	98.13	96.26
Epoch - 1500					
Normal Traffic	98.04	98.80	98.04	98.42	96.30
Attack Traffic	98.38	97.37	98.38	97.88	96.30
Average	98.21	98.09	98.21	98.15	96.30
Epoch - 2000					
Normal Traffic	97.88	98.91	97.88	98.39	96.24
Attack Traffic	98.53	97.16	98.53	97.84	96.24
Average	98.20	98.03	98.20	98.12	96.24
Epoch - 2500					
Normal Traffic	98.07	98.79	98.07	98.43	96.32
Attack Traffic	98.37	97.41	98.37	97.89	96.32
Average	98.22	98.10	98.22	98.16	96.32
Epoch - 3000					
Normal Traffic	98.02	98.79	98.02	98.40	96.26
Attack Traffic	98.37	97.35	98.37	97.86	96.26
Average	98.20	98.07	98.20	98.13	96.26

DOI: https://doi.org/10.54216/FPA.190229
Received: December 29, 2024 Revised: February 13, 2025 Accepted: March 15, 2025

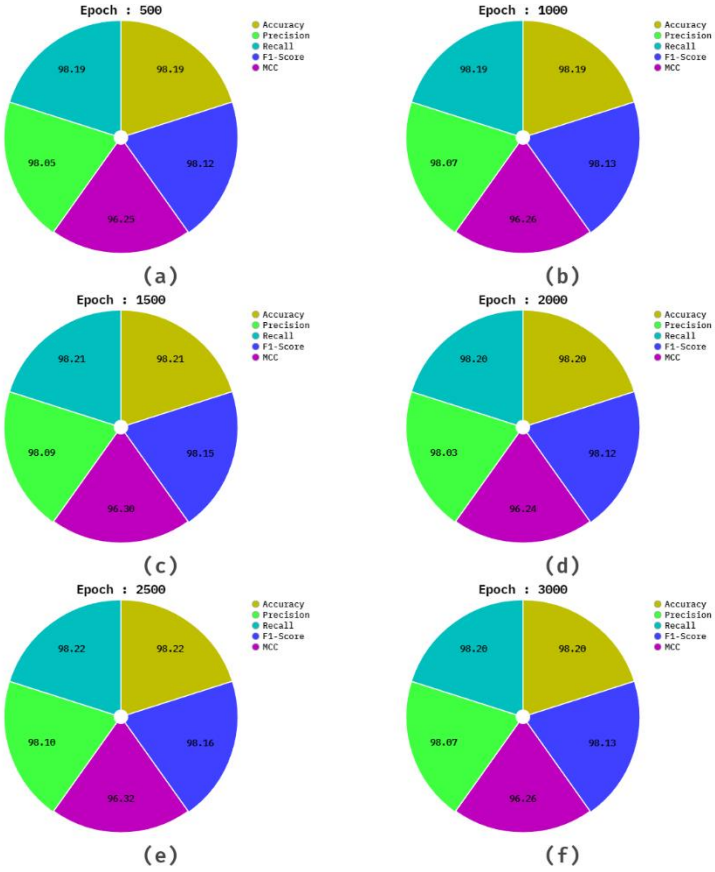

Figure 6. Average result of BCDL-HDSMOT method (a-f) Epochs 500-3000

In Fig. 7, the training (TRAN) $accu_y$ and validation (VALN) $accu_y$ performance of the BCDL-HDSMOT methodology below epoch 2500 is illustrated. The values of $accu_y$ are computed through an interval of 0-2500 epochs. The figure highlights that both $accu_y$ analyses exhibit a rising trend, which reported the capability of the BCDL-HDSMOT approach with maximal performance across several iteration counts. Besides, both $accu_y$ leftovers closer across the epoch counts, which indicates lesser overfitting and exhibitions superior outcomes of BCDL-HDSMOT methodology, ensuring dependable prediction on unseen instances.

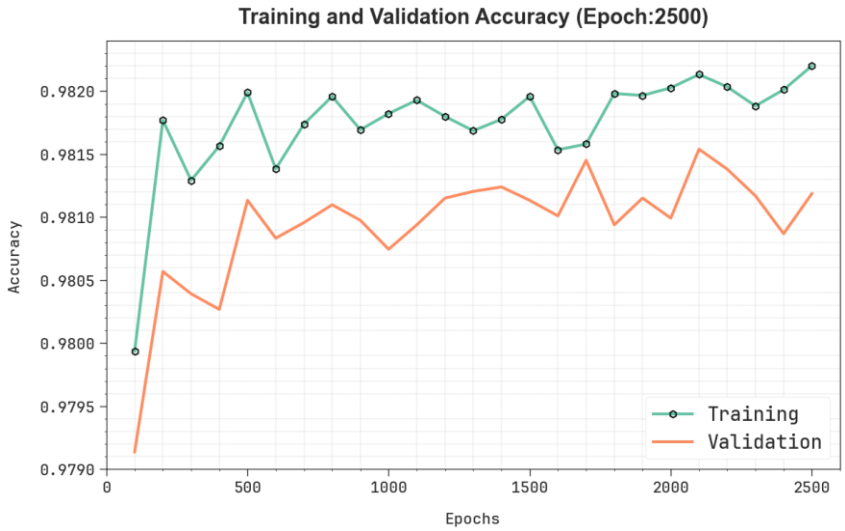

Figure 7. $Accu_y$ Curve of BCDL-HDSMOT model under Epoch 2500

DOI: https://doi.org/10.54216/FPA.190229
Received: December 29, 2024 Revised: February 13, 2025 Accepted: March 15, 2025

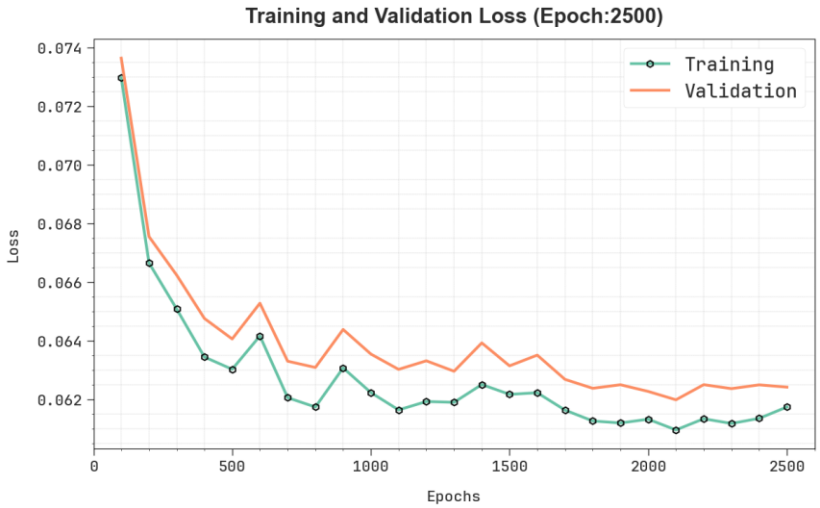

Figure 8. Loss graphs of the BCDL-HDSMOT method under Epoch 2500

In Fig. 8, the TRA loss (TRANLOS) and VAL loss (VALNLOS) graph of the BCDL-HDSMOT algorithm below epoch 2500 is displayed. The loss values are measured within the interval of 0-2500 epochs. It is signified that both values exemplify a reducing tendency, informing the ability of the BCDL-HDSMOT algorithm in balancing a trade-off amongst generalization and data fitting. The continual decreasing in values of loss likewise guarantees the optimal solution of the BCDL-HDSMOT system and tune the prediction outcomes.

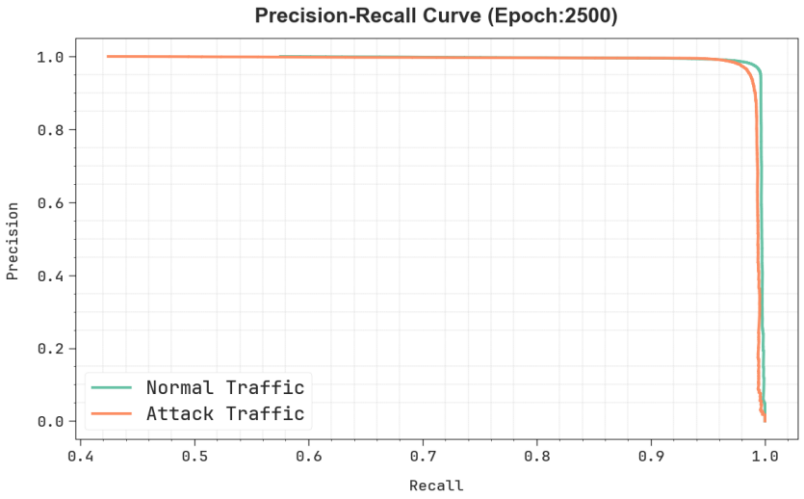

Figure 9. PR graph of BCDL-HDSMOT approach under Epoch 2500

In Fig. 9, the precision-recall (PR) graph outcomes of the BCDL-HDSMOT system below epoch 2500 provide clarification into its performance by plotting Precision besides Recall for each of the classes. The figure shows that the BCDL-HDSMOT methodology continually accomplishes high PR analysis over various classes, signifying its ability to sustain an important section of true positive predictions between all positive predictions (precision) whereas besides takes a huge proportion of actual positives (recall). The steady increase in PR outcomes between every class label describes the efficacy of the BCDL-HDSMOT methodology in the classification procedure.

In Fig. 10, the ROC graph of the BCDL-HDSMOT system is examined. The results imply that the BCDL-HDSMOT technique below epoch 2500 accomplishes better ROC results across each class, representing the important ability to discern these class labels. This reliable trend of maximum ROC analysis over numerous classes means the proficient outcomes of the BCDL-HDSMOT algorithm on predicting classes; highlight the strong nature below the classification procedure.

DOI: https://doi.org/10.54216/FPA.190229
Received: December 29, 2024 Revised: February 13, 2025 Accepted: March 15, 2025

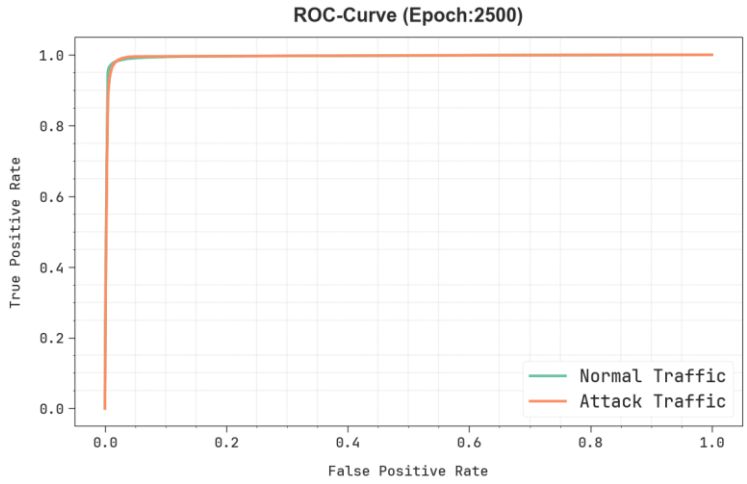

Figure 10. ROC curve of BCDL-HDSMOT approach under Epoch 2500

Table 3 and Fig. 11 inspect the comparative examination of BCDL-HDSMOT approach with the existing techniques [25-27]. The results emphasized that the SWPAH, FCTTP, One Class SVM, Xgboost, NB, GA-RFNN and Bi-LSTM techniques have reported minimal performance. Furthermore, the proposed BCDL-HDSMOT system reported greater performance with superior $accu_y, prec_n, reca_l$, and $F1_{score}$ of 98.22%, 98.10%, 98.22%, and 98.16%, respectively.

Table 3: Comparative outcomes of BCDL-HDSMOT technique with existing techniques

Technique	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{score}$
SWPAH	94.15	87.26	91.21	94.40
FCTTP	91.57	95.95	94.95	95.06
One Class SVM	89.46	91.27	96.86	94.69
Xgboost	90.99	93.28	88.61	95.37
Naïve Bayes	96.06	89.98	87.66	87.91
GA-RFNN	90.53	87.70	87.83	88.75
Bi-LSTM Model	89.46	96.14	96.83	93.74
BCDL-HDSMOT	98.22	98.10	98.22	98.16

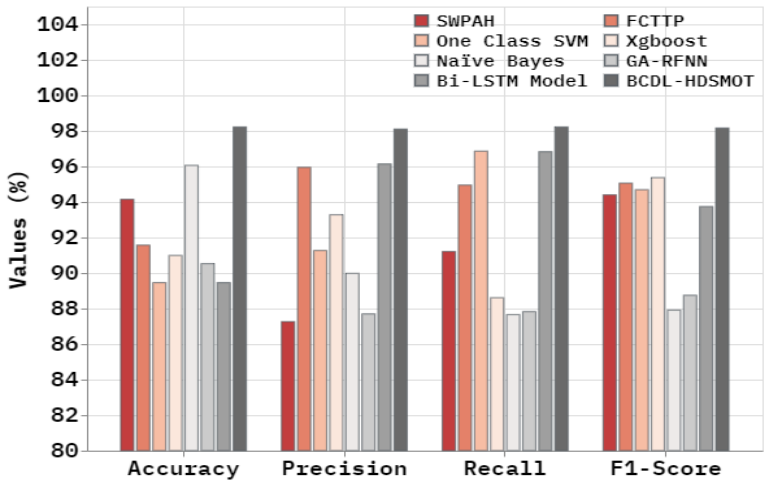

Figure 11. Comparative performance of BCDL-HDSMOT model with present algorithms

DOI: https://doi.org/10.54216/FPA.190229
Received: December 29, 2024 Revised: February 13, 2025 Accepted: March 15, 2025

In Table 4 and Fig. 12, the execution time (ET) of BCDL-HDSMOT techniques with existing systems are displayed. Based on ET, the BCDL-HDSMOT approach gained worse ET of 12.35sec while the existing algorithm such as SWPAH, FCTTP, One Class SVM, Xgboost, NB, GA-RFNN and Bi-LSTM have achieve maximum ET values of 15.36sec, 27.15sec, 20.81sec, 26.44sec, 27.35sec, 23.41sec, and15.52sec, respectively.

Table 4: ET outcome of BCDL-HDSMOT method with existing techniques

Technique	Execution Time (sec)
SWPAH	15.36
FCTTP	27.15
One Class SVM	20.81
Xgboost	26.44
Naïve Bayes	27.35
GA-RFNN	23.41
Bi-LSTM Model	15.52
BCDL-HDSMOT	12.35

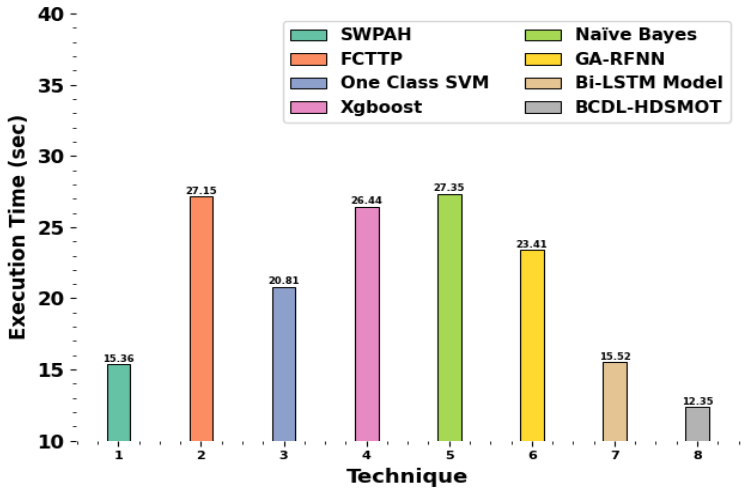

Figure 12. ET outcome of BCDL-HDSMOT method with existing models

5. Conclusion

In this paper, we have projected an innovative BCDL-HDSMOT model. The major aim of BCDL-HDSMOT technique is to develop an effective method for enhancing data security in medical sector. At first, the BC technique is applied in healthcare to enhance data security, interoperability, and transparency while ensuring patient privacy and efficient record management. Next, the data pre-processing stage employs min-max normalization to clean, transform, and organize input data into a suitable quality for analysis. Besides, the BWOA has been deployed for the FS process to select the relevant features from an input data. For the classification process, the proposed BCDL-HDSMOT technique designs VLSTM method. At last, the ISOA-based hyperparameter selection process is performed to optimize the classification results of VLSTM method. The experimental evaluation of the BCDL-HDSMOT algorithm can be tested on a benchmark dataset. The wide-ranging outcomes highlight the significant solution of the BCDL-HDSMOT approach to the cyberattack detection process.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

DOI: https://doi.org/10.54216/FPA.190229
Received: December 29, 2024 Revised: February 13, 2025 Accepted: March 15, 2025

References

[1] S. Neelakandan et al., "Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model," *Int. J. Model. Simul. Sci. Comput.*, vol. 13, no. 04, p. 2241006, 2022.

[2] K. Raju et al., "Blockchain assisted cloud security and privacy preservation using hybridized encryption and deep learning mechanism in IoT-healthcare application," *J. Grid Comput.*, vol. 21, no. 3, p. 45, 2023.

[3] T. Veeramakali et al., "An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model," *J. Supercomput.*, vol. 77, no. 9, pp. 9576–9596, 2021.

[4] M. Shafay et al., "Blockchain for deep learning: review and open challenges," *Cluster Comput.*, vol. 26, no. 1, pp. 197–221, 2023.

[5] Z. A. Khan et al., "A blockchain-based deep-learning-driven architecture for quality routing in wireless sensor networks," *IEEE Access*, vol. 11, pp. 31036–31051, 2023.

[6] A. Albakri and Y. M. Alqahtani, "Internet of medical things with a blockchain-assisted smart healthcare system using metaheuristics with a deep learning model," *Appl. Sci.*, vol. 13, no. 10, p. 6108, 2023.

[7] K. Kulandaivelu, S. Rajappan, and V. Murugasamy, "Blockchain enabled secure medical data transmission and diagnosis using golden jackal optimization algorithm with deep learning," *Braz. Arch. Biol. Technol.*, vol. 67, p. e24240214, 2024.

[8] P. Kumar et al., "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system," *J. Parallel Distrib. Comput.*, vol. 172, pp. 69–83, 2023.

[9] B. R. Bezanjani, S. H. Ghafouri, and R. Gholamrezaei, "Fusion of machine learning and blockchain-based privacy-preserving approach for healthcare data in the Internet of Things," *J. Supercomput.*, vol. 80, no. 17, pp. 24975–25003, 2024.

[10] S. Neelakandan et al., "Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model," *Int. J. Model. Simul. Sci. Comput.*, vol. 13, no. 04, p. 2241006, 2022.

[11] S. Khan et al., "A blockchain-enabled AI-driven secure searchable encryption framework for medical IoT systems," *IEEE J. Biomed. Health Inform*, 2025.

[12] A. A. Alanazi et al., "Blockchain with optimal deep learning assisted secure data sharing and classification on future healthcare systems," *Alex. Eng. J.*, vol. 99, pp. 168–179, 2024.

[13] K. K. Chanumolu and G. M. Nagamani, "An enhanced model for smart healthcare by integrating hybrid ML, LSTM, and blockchain," *Ingénierie des Systèmes d'Information*, vol. 30, no. 1, p. 43, 2025.

[14] R. Vatambeti et al., "Securing the medical data using enhanced privacy preserving based blockchain technology in Internet of Things," *Cluster Comput.*, vol. 27, no. 2, pp. 1625–1637, 2024.

[15] M. S. Ramkumar et al., "A consensus random-coupled growth network with secure blockchain storage in healthcare applications," in *Proc. Int. Conf. Multi-Agent Syst. Collaborative Intell. (ICMSCI)*, 2025, pp. 216–222.

[16] K. Kiruthikadevi, R. Sivaraj, and M. Vijayakumar, "A blockchain and hybrid deep learning for secure and efficient healthcare data transmission and management," *Tehnički vjesnik*, vol. 31, no. 6, pp. 2140–2145, 2024.

[17] K. Swanthana and S. S. Aravinth, "A malicious feature detection and prevention mechanism with BRDH approach for improved security in homomorphic blockchain," *Knowl.-Based Syst.*, vol. 310, p. 112872, 2025.

[18] A. Abbas et al., "Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things," *Pers. Ubiquitous Comput.*, vol. 28, no. 1, pp. 59–72, 2024.

[19] S. Krishnan and L. P. Ganesan, "NFTs and smart contracts," *Syst.*, vol. 13, no. 1, p. 65, 2025.

[20] P. Kumar et al., "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system," *J. Parallel Distrib. Comput*, vol. 172, pp. 69–83, 2023.

[21] A. H. Khalaf, "A novel modified swarm intelligence algorithm combining black widow optimization algorithm and pelican optimization algorithm to solve global optimization problems," *J. Pendidik. Mat.*, vol. 2, no. 2, p. 11, 2025.

DOI: https://doi.org/10.54216/FPA.190229
Received: December 29, 2024 Revised: February 13, 2025 Accepted: March 15, 2025

[22] Y. Li et al., "A novel fault location method for distribution networks with distributed generators based on improved seagull optimization algorithm," *Energy Rep.*, vol. 13, pp. 3237–3245, 2025.

[23] R. R. Irshad et al., "Towards enhancing security of IoT-enabled healthcare system," *Heliyon*, vol. 9, no. 11, 2023.

[24] G. Singh, "Wearable IoT (w-IoT) artificial intelligence (AI) solution for sustainable smart-healthcare," *Int. J. Inf. Manag. Data Insights*, vol. 5, no. 1, p. 100291, 2025.

[25] S. A. Alzakari et al., "Enhanced heart disease prediction in remote healthcare monitoring using IoT-enabled cloud-based XGBoost and Bi-LSTM," *Alex. Eng. J.*, vol. 105, pp. 280–291, 2024.

[26] M. A. Ganaie et al., "A hybrid deep learning framework for healthcare data prediction using IoT-enabled devices," *Future Gener. Comput. Syst.*, vol. 127, pp. 159–168, 2023.

[27] A. Elhoseny et al., "Blockchain-based healthcare data management with deep learning for predictive diagnosis," *Comput. Networks*, vol. 192, p. 108081, 2021.

DOI: https://doi.org/10.54216/FPA.190229
Received: December 29, 2024 Revised: February 13, 2025 Accepted: March 15, 2025