IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 17 June 2023, accepted 8 August 2023, date of publication 10 August 2023, date of current version 22 August 2023.

*Digital Object Identifier 10.1109/ACCESS.2023.3304269*

RESEARCH ARTICLE

# Blockchain Enabled Smart Healthcare System Using Jellyfish Search Optimization With Dual-Pathway Deep Convolutional Neural Network

**FAHAD F. ALRUWAILI[1], BAYAN ALABDUALLAH[2], HAMED ALQAHTANI[3], AHMED S. SALAMA[4], GOUSE PASHA MOHAMMED[5], AND AMANI A. ALNEIL[5]**

[1]Department of Computer Science, College of Computing and Information Technology, Shaqra University, Shaqra, Saudi Arabia
[2]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia
[3]Department of Information Systems, College of Computer Science, Center of Artificial Intelligence, Unit of Cybersecurity, King Khalid University, Abha, Saudi Arabia
[4]Department of Electrical Engineering, Faculty of Engineering and Technology, Future University in Egypt, New Cairo 11845, Egypt
[5]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia

Corresponding author: Gouse Pasha Mohammed (g.mohammed@psau.edu.sa)

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number (RGP2/ 159 /44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R440), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444). This study is partially funded by the Future University in Egypt (FUE).

**ABSTRACT** Blockchain (BC) and Artificial intelligence (AI) based technologies have earned a better reputation amongst the research community, especially in the medical field. BC technology has emerged as a promising solution to revolutionize the medical field by addressing challenges related to efficiency, data security, and interoperability. A BC-aided smart healthcare system leverages the immutable and decentralized nature of BC to construct a secured and transparent ecosystem to manage processes and healthcare data. It leverages the secure and decentralized nature of BC to optimize the processes, security, interoperability, and efficiency of medical data. The existing system is exposed to security attacks on healthcare data. It can be necessary to construct a real-time detection device utilizing a cyber-physical system (CPS) with BC technology in a significant way. This article designs a novel Blockchain-Enabled Smart Healthcare System using Jellyfish Search Optimization with Dual-Pathway Deep Convolutional Neural Network (JSO-DPCNN) technique. The presented JSO-DPDCNN technique exploits the concept of BC-enabled secure data transmission and DL-based diagnosis model for moneypox disease on smart healthcare monitoring. To accomplish this, the JSO-DPCNN technique uses Ethereum-based public BC to secure the privacy of healthcare images. In addition, the JSO-DPCNN technique applies a feature extraction module using DPCNN, which extracts the suitable set of features in the input images. Moreover, the multiplicative long short-term memory (MLSTM) approach was used for the disease detection process. Lastly, the JSO system can be employed for the parameter tuning of the MLSTM model. The simulation result of the JSO-DPCNN system was executed on a benchmark medical dataset. The comprehensive outcomes highlighted the significant outcome of the JSO-DPCNN approach in terms of different measures.

**INDEX TERMS** Blockchain, sustainability, smart healthcare, deep learning, jellyfish search optimizer.

## I. INTRODUCTION

Nowadays, the smart healthcare system has paid more attention to the revolution of medical infrastructures. Smart healthcare can be referred to as a new concept that denotes a set

The associate editor coordinating the review of this manuscript and approving it for publication was Thanh Ngoc Dinh.

of rules that combine treatment, prevention, management, and diagnosis [1]. Unlike conventional healthcare systems, smart medical systems can connect and exchange data at any place and time. Compared with conventional healthcare treatment, smart healthcare has fearers of the interconnection of immediacy, information, and preventability [2]. Medical staff can constantly examine, perceive, and process major medical events (preventability) via wireless networks, utilizing portable mobile devices [3]. Currently, many doctors do not maintain records of a patient's data, treatments, and diagnostic details rather they maintain health records electronically. Such reports have the complete data of the patient like his treatment taken, history, allergies, etc [4]. It is viewed by healthcare providers, clinicians, and hospitals for any cause. Such records need security and safety to avoid misuse by cyber attackers or third parties. It has confidential data regarding scan reports, medication, biometrics, and symptoms [5]. This study makes use of Blockchain (BC) related storage for Electronic Health Records (EHR) to present security and privacy for the dataset [6]. It is decisive that EHR be kept as it has delicate data. The EHR comprises very delicate data, and in the centralized storage setting, the likelihoods of cyber attackers misusing the records are maximum. Further, the patients track their records for diagnosis appointments, regular consultations, treatment, etc [7].

Privacy and Security in medical data are challenging. Privacy can be described as protecting delicate data. The attack on medical data is because the increased amount of clinical data is a vital part of patient care [8]. Encryption and authentication methods commonly prevent outsider adversaries, but the big concern comes from the malicious actions that cause attacks namely denial of service attacks, eavesdropping, and replay attacks. The aim of this study is to analyze the patient's EHR with a DL system saved in the BC and to make an alert method for the patient. BC follows absolute privacy rules for finding users relevant to transactions [9]. It is utilized for the management of information systems to process automation, and aid achieve secure storage, transactions, and other applications [10]. ML is the leading technology to perform complicated analysis, creative problem-solving, and intelligent judgment in healthcare.

This article designs a novel Blockchain-Enabled Smart Healthcare System using Jellyfish Search Optimization with Dual-Pathway Deep Convolutional Neural Network (JSO-DPCNN) technique. The presented JSO-DPDCNN technique exploits the concept of BC-enabled secure data transmission and DL-based diagnosis model for moneypox disease on smart healthcare monitoring. To accomplish this, the JSO-DPCNN technique uses Ethereum-based public BC to secure the privacy of healthcare images. In addition, the JSO-DPCNN technique applies a feature extraction module using DPCNN, which extracts the suitable set of features in the input images. Moreover, the multiplicative long short-term memory (MLSTM) model can be employed for the disease detection process. Finally, the JSO system was used for the parameter tuning of the MLSTM approach. The simulation result of the JSO-DPCNN system was executed on a benchmark medical dataset

## II. RELATED WORKS

Kalapaaking et al. [11] developed BC-based FL with SMPC verification against poisoning attacks in the healthcare system. Firstly, verify the ML algorithm in the FL participant via the encryption inference method and eliminate the compromised method. When the participants' local model has been tested, the model was transmitted to BC nodes that aggregated securely. Mantey et al. [12] introduced an integrated environment of BC-DL used to analyze the EHR. The EHR is the health record of the patient that is shared amongst public health organizations and other hospitals. The presented method allows the DL method acts as an agent for analyzing the EHR that is kept in the BC.

The authors [13] introduced a new group theory (GT)-based binary spring search (BSS) technique that includes a hybrid DNN method. The presented method efficiently identifies the intrusion in the IoT platform. The security of patient health records (PHR) is a significant aspect of cryptography on the Internet owing to its importance and value, rather in the IoMT. In [14], the Bayesian grey filter-based CNN (BGF-CNN) method was utilized for enhancing accuracy and reducing overhead and time complexity. In addition, GWO and PSO methods are used for enhancing the efficiency of the model. Consequently, the privacy preservation of healthcare information was optimized with maximum accuracy using a BC-based cyber-physical system with DNN (BGF BC).

In [15], the authors devised a FIDChain IDS with lightweight ANN in an FL method for ensuring the privacy preservation of medical data with the advancements of BC technology that gives a distributed ledger to aggregate the local weight and later transmit the upgrade global weight that provides immutability and full transparency and avoids poisoning attacks over the distributed method with small overhead. In [16], we incorporate permission BC and smart contract with the DL method to develop a new protected and effective information distribution architecture called PBDL. Especially, the authenticated information was used for presenting a new DL system that integrates stacked sparse VAE (SSVAE) with self-attention-based BiLSTM (SA-BiLSTM).

Bhattacharya et al. [17] present an architecture named as BC-Based DL as-a-Service (BinDaaS). Initially, an authentication and signature system is introduced by using lattice-based cryptography for resisting collusion attacks amongst N-1 medical experts in N. Next, the DaaS was exploited on kept EHR databases to forecast future diseases dependent upon present indicators and features of patients. The authors [18] introduce an infrastructure which gathers a limited amount of information from dissimilar sources and trains a global DL algorithm using the BC-based FL method. Firstly, the authors present a data-normalized method which handles the data heterogeneity as the information is gathered in various hospitals having dissimilar types of CT scanners.

Next, Capsule Network-based segmentation and classification are exploited for detecting COVID19 patients.

## III. THE PROPOSED MODEL

In this manuscript, we have presented the JSO-DPDCNN system for smart healthcare systems. The presented JSO-DPDCNN technique attains security using BC technology. In addition, the JSO-DPDCNN technique performs DL based diagnosis model for moneypox disease on smart healthcare monitoring using three different processes namely DPCNN-based feature extraction, MLSTM-based classification, and JSO-based hyperparameter tuning. Fig. 1 displays the workflow of the JSO-DPDCNN approach.

### A. BLOCKCHAIN TECHNOLOGY

BC-based secure cyberspace has been employed to preserve medical information utilizing Ethereum-based public BC, TEST RPC, Meta-mask Wallet for ETH (cryptocurrency), and DAPP which challenge another mobile application. Ethereum has been utilized rather than the common BC in the presented method as Ethereum could not contain 3rd parties for performing transactions and downtime was significantly small. The next procedure demonstrates that transactions utilizing BC technology work: 1) DAPP was utilized for sending medical information as BC, 2) Design the TEST RPC that performs as a BC emulator, 3) Arrange the meta-mask wallet as a chrome extension for accessing the Ethereum-based BC-allowed DAPP, 4) Create smart contracts on TESTRPC to carry out the functions above BC, 5) All the medicinal data comprises transactions carried out utilizing BC. Later the procedure on Meta-mask was started. ETH balance in the meta-mask is diminished to function on the block from the BC, and 6) A unique ID was assigned for every effective transaction.

Scripting language and solidity programming can be utilized for designing a decentralized application on TEST RPC, the BC emulator. By confirming the ETH balance reduction from the Meta-mask wallet, the medicinal information smart contract is 1st registered, afterward it could be compiled, and next it could be utilized on Ethereum-based BC. An ETH balance was needed for utilizing and compiling the system functions which are retained as smart contracts utilizing solidity programming. All the patient information was kept in BC as a transaction in a certain block. Each block was interrelated with the crypto hash value which is dependent upon the previous block hash value and the present block data transaction. The patient information Is tamper-proof due to BC technologies' advanced features like distributive, immutability, security, transparency, and reliability.

### B. FEATURE EXTRACTION USING DPCNN MODEL

To generate a set of features from the input medical images, the DPCNN model is used. The suggested DPCNN model was planned with the dual pathway architecture [19]. This model added 2 parallel convolution pathways, each having 2 max-pooling layers and convolution layers. Both pathways

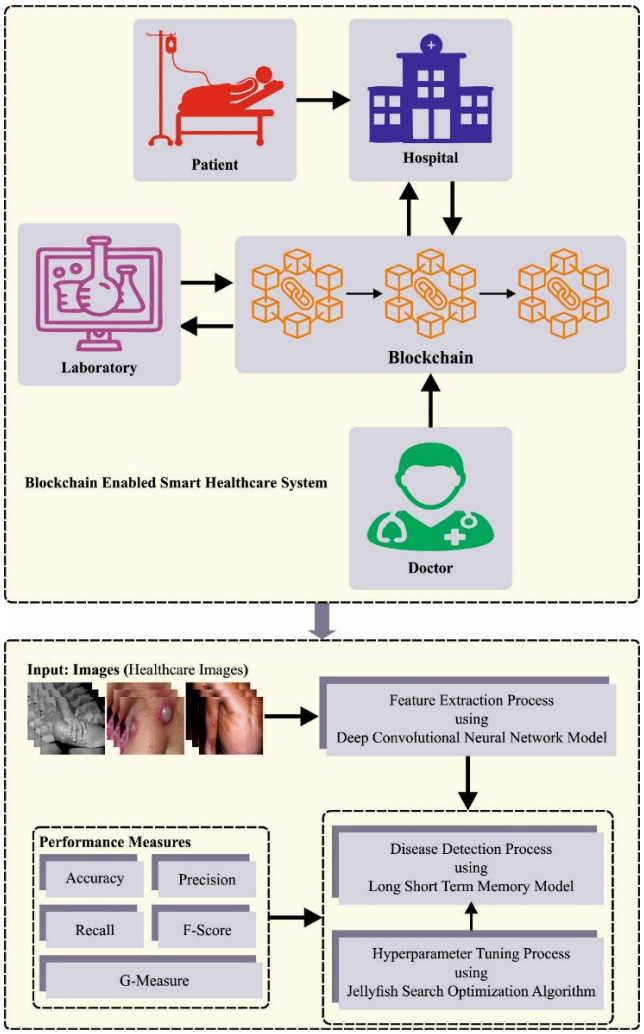


**FIGURE 1.** Workflow of JSO-DPDCNN approach.

are combined as a single resultant layer. Also, the architecture integrated 2 FC layers with the dropout layer to avoid over-fitting.

The dual pathway DPCNN determines the structural design that takes the shape of input images and the amount of resultant classes as input argument. An input shape is (224, 224, 3) which characterizes the RGB images of 224 × 224 size. The *num_classes* parameter can be fixed to 2 which implies the model was developed to categorize the input image as each probable class. All the pathways are based on two pooling and two convolutional layers.

The input for these two pathways was a 224 × 224 × 3 matrix. The proposed DPCNN architecture comprises two max pooling layers and two convolutional layers in the primary and secondary routes. Two FC layers were employed to the concatenated pathways after adding a dropout layer to avoid over-fitting. Lastly, the class probability was predicted by means of the softmax activation function from the resultant layer. The softmax function can be defined as *softmax*, and the ReLU function is represented by *ReLU*.

Convolution layer: The convolution layer exploits a series of filters to input images and generates a mapping feature. The convolutional process among a filter, $w$, and the input image, $\chi$, can be mathematically defined as follows:

$$y(i,j) = sum(sum(x(m,n) * w(i-m, j-n+b \quad (1)$$

In Eq. (1),$x(m,n)$ shows the input image pixel at $(m,n)$ location, $y(i,j)$ indicates the outcome of the mapping feature at location $(i,j)$,$b$ stands for a bias term and $w(i-m, j-n)$ refers to the filter coefficient at location $(i-m, j-n)$.

ReLU activation function: ReLU function set each negative value from the input to 0 and leaves the positive value the same. This can be determined as follows:

$$f(x) = \max(0,x) \quad (2)$$

In Eq. (2), $f(x)$ indicates the results of the activation function with input $x$.

Max-pooling layer: This decreases the spatial size of mapping features via a max function on non-overlapping rectangular regions of mapping features. This can be mathematically modelled as follows:

$$y(i,j) = \max(x(i*stride{:}i*stride + pool_{size}, j*stride{:}j*stride + pool_{size})) \quad (3)$$

here $x$ indicates the input feature map, $y(i,j)$ signifies the outcome of the mapping feature at location $(i,j)$, $stride$ shows the stride length and $pool_{size}$ represents the size of the pooling window.

Concatenation layer: It integrates mapping features in various routes by concatenating them along the channel axis. The concatenation process is mathematically expressed as follows:

$$y = \text{concat}[x_1, x_2, \ldots, x_n] \quad (4)$$

In Eq. (4),$x_1, x_2, \ldots, x_n$ shows the input feature maps, and $y$ represents the output feature map.

Fully connected layer: FC layer interconnects each neuron in the input layer to every neuron in the output layer. The outcome of the FC layer is mathematically defined as follows:

$$y = f(Wx + b) \quad (5)$$

In Eq. (9),$x$ indicates the input, $y$ denotes the output, $W$ refers to the weight matrix, $f$ shows the activation function, and $b$ stands for the bias vector.

### C. IMAGE CLASSIFICATION

For image classification purposes, the MLSTM model is applied. The fundamental concept of the LSTM network was comparatively easy. The hidden layer (HL) in the original RNN has a single state $h$ that is sensitive to short-term input [20]. Here, the state $c$ named a cell state was more to store the long-term state. $x(t)$ denotes the trained input of NN at $t$ time.

LSTM developed a gated infrastructure for controlling the discarding and retention of data. The LSTM contains 3 gates.

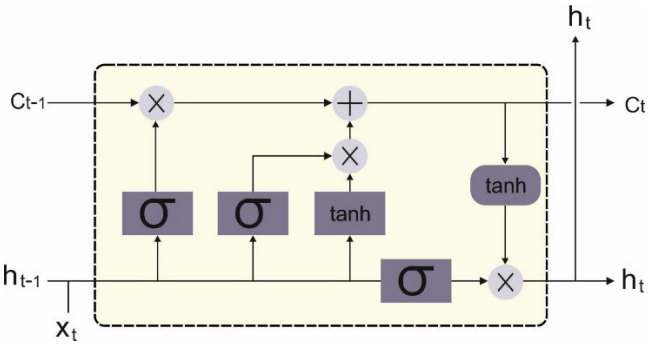


**FIGURE 2.** Framework of LSTM.

The architecture of LSTM includes: forget, input, and output gates. Fig. 2 illustrates the infrastructure of LSTM.

LSTM cyclic networks don't easily execute component-wise non-linearity to the affine transformation of input and cyclic components. $LU_t$ indicates the forget gate, where the data outcome of the node at the last time could be restricted. $i_t$ denotes the input gate where the newest input data is chosen attained, and $o_t$ shows the output gate, where the outcome at the present time is transferred based on the new input data and the prior time.

Where $f_t$ demonstrates the outcome of the forgetting gate, and then adopts the Sigmoid activation function for mapping the outcome to the interval of zero and one. Once the cell state $c_{t-1}$ passed over the oblivion gate at the prior time, then the outcome would be multiplied to $f_t$. This defines that a lot of prior cell state $c_{t-1}$ is enter the existing state $c_t$.

The equation of forgot gate is as:

$$f_t = \sigma\left(h_{t-1} \cdot W_f + x(t-1) \cdot 1 U_f + b_f\right) \quad (6)$$

In Eq. (6)$W_f$ and $U_f$ signify the parameter matrix, and $b_f$ signifies the parameter vector. $\sigma$ denotes the sigmoid activation function, and $h_{t-1}$ shows the HL at the final moment. $x(t-1)$ indicates the input at the existing time.

An input gate exploits the Sigmoid activation function for mapping the outcome to an interval of zero and one. The input gate $i_t$ defines that input data is reserved. $\tilde{c_t}$ filter data over the input gate.

The equation of the input gate is as:

$$i_t = \sigma(h_{t-1} \cdot W_i + x(t) \cdot U_i + b_i) \quad (7)$$

The equation of the instant cell state is as:

$$\tilde{c_t} = \tanh(h_{t-1} \cdot W_c + x(t) \cdot U_c + b_c) \quad (8)$$

The data taken at the prior time, plus the data taken by the existing recipient, form the cell state $c_t$ at the current time.

The equation of the present cell state is as:

$$c_t = f_t \circ c_{t-1} + i_t \circ \tilde{c_t} \quad (9)$$

The output gate defines that data is in $h_{t-1}$, and $x_t$ would be output.

The equation of output gate is as:

$$h_t = o_t \circ \tanh(c) \tag{10}$$

In Eq. (10), $\cdot$ and $\circ$ represents matrix and the element products.

The MLSTM, a hybrid method which integrates the hidden-to-hidden alteration of RNN utilizing the LSTM gate infrastructure was suggested to manage the overfitting problem. By interrelating all the gate elements from the LSTM to the intermediate state $m_t$ of RNN, the typical RNN and LSTM approaches are integrated. This infrastructure's purpose is for integrating the extended time lag and entire working of LSTM with the adaptable input-dependent transition of RNN. An Input-dependent transition design than typical LSTM is offered by supplementary sigmoid input and $f$ which is present in multiplicative LSTM.

### D. HYPERPARAMETER TUNING USING JSO ALGORITHM

At this stage, the JSO system was exploited for the optimal hyperparameter tuning of the MSTLM model. Jellyfish (JF) are found mainly in the water of different depths and temperatures around the world [21]. JF could swarm once the condition is favorable, and a large set of them is called a JF bloom. The direction of JF with regard to current plays a major role in supporting JF blooms and avoiding them from being stranded due to their poor swimming capabilities. The swarm formation can be impacted by different variables including temperature, ocean currents, predation, and nutrient and oxygen availability. Ocean current is the most vital of this factor since they could collect JF into the swarm. Moreover, the swarm is highly possible to follow once the ocean temperature was enhanced because JF could be survived in this environment superior to other marine creatures. In summary, the JF swarm is significantly impacted by the surrounding ecosystems, and the capability of swimming towards the current is crucial to their survival.

The 3 fundamental principles that procedure the basis of the proposed method are given below:

A ''time control system'' controls the switching behaviors of JF among tracking the ocean current movement and in the swarm.

In the migration, JF can be attracted to the region but the food is longer and actively find the region.

The quantity of food existing at a provided position, along with the main function dictates the degree of attractiveness.

The presence of nutrient concentration from the ocean current is that draws JF to it. The ocean current's direction ($\overrightarrow{flow}$) can be determined by averaging each vector from all the JF in the ocean to JF in the optimum place.

$$\begin{aligned}\overrightarrow{flow} &= \frac{1}{n_{jel}}\sum\overrightarrow{flow}_j = \frac{1}{n_{jel}}\sum(X_c - a_f X_j)\\ &= X_c - a_f\frac{\Sigma X_j}{n_{jel}} = X_c - a_f m\end{aligned} \tag{11}$$

In Eq. (11),*njel* denotes the population of JF; *Xc* shows the present optimum location of JF in the swarm; *af* shows the attraction feature; *m* indicates the average location of JF. The difference among the interest JF's present optimum position and the swarm mean place was represented by *df*. The distance of $\pm\beta\sigma$ about the mean location has the provided probability of JF, where $\beta$ denotes the distribution co-efficient and $\sigma$ indicates the SD which JF have a standard spatial distribution in each dimension,

$$d_f = \sigma \times rand^w(0,1) \times \beta, \sigma = rand^y(0,1) \times m \tag{12}$$

In Eq. (12), $rand(0,1)^w \times rand(0,1)^y = rand(0,1)$:

$$\vec{flow} = X_c - m \times rand(0,1) \times \beta \tag{13}$$

A new location of JF can be formulated as follows:

$$X_j(t+1) = X_j(t) + rand(0,1) \times \overrightarrow{flow} \tag{14}$$

In Eq. (14), $X_j(t)$ represents the location of the $j^{th}$ JFes at $t$ time.

Once the JF is in a swarm, it is moved actively (Type $B''$) or passively (Type' $A''$). At first, JF in the swarm show Type $''A''$ motion, but it is slowly changing to display more of Type ''B'' motion. In the Type ''$A''$ movement, JF moves within the existing position, and the location of all the JFs can be upgraded as follows:

$$X_j(t+1) = X_j(t) + \gamma \times (B_u - B_l) \times rand(0,1) \tag{15}$$

In Eq. (15), $\gamma$ denotes the motion co-efficient was related to the extent of movement nearby the JF location. The lower as well as upper boundaries are represented as $B_l$ and $B_u$, correspondingly. The JF of interest ($j$) was selected arbitrarily to simulate the second motion, and the vector in the selected JF ($r$) to JF of interest ($j$) was used for calculating the direction of motions. When the food counts available to the selected JF ($r$) are lesser than that accessible to JF of interest ($j$), then it instantly moves close to it. Every JF in the swarm directs toward the optimum direction for finding food. The new location of the JF is given as follows:

$$\overrightarrow{step} = X_j(t+1) - X_j(t) \tag{16}$$

$$\overrightarrow{step} = dir \times rand(0,1)$$

$$\overrightarrow{dir} = \left\{\begin{matrix} X_r(t) - X_j(t) \\ X_j(t) - X_r(t) \end{matrix}\right\} if \left\{\begin{matrix} o(X_r) \le O(X_j) \\ O(X_r) > O(X_j) \end{matrix}\right\} \tag{17}$$

where $''O(\cdot)''$ denotes the objective function of location $X$.

$$X_j(t+1) = \overrightarrow{step} + X_j(t) \tag{18}$$

This model manages the behaviors of JF by navigating them nearby the ocean current, along with *Type*''$A''$ and *Type*''$B''$ motions in the swarm. The time control process was made up of a time control function, $f_t(t)$ and constant value, $C_t$, which controls the JF's capability to shift among moving within the swarm and with the ocean current. On the other hand, once the value is lesser than $C_t$, the JF moves in the swarm and it can be formulated as follows:

$$f_t(t) = \left|\left(1 - \frac{t}{iter_{\max}}\right) \times (2 \times rand(0,1) - 1)\right| \tag{19}$$

**TABLE 1. Details of database.**

| Class | No. of Samples |
|---|---|
| Monkeypox | 500 |
| Others | 500 |
| Total Number of Samples | 1000 |

In Eq. (19), $iter_{\max}$ denotes the maximal amount of iteration.

Typically, the JF population was randomly initialized. Many chaotic maps were established to improve population initialization. Because of the spherical shape of Earth, the world has oceans distributed over its entire surface, if the JF move beyond a certain search region, it *re*-enters the opposite boundary as follows:

$$X'_{j,d} = \left(X_{j,d} - B_{u,d}\right) + B_l\,(d)\; if\; X_{j,d} > B_{u,d}$$
$$X'_{j,d}, = (X_{j,d} - B_{l,d}) + B_u(d) if\; X_{j,d} < B_{l,d} \quad (20)$$

In Eq. (20), $X'_{jd}$ denotes the $j^{th}$JF's location in the $d^{th}$ dimension. Afterwards executing boundary constraint, the new location is represented as $X_{jd}, \cdot$ The upper as well as lower boundaries of searching space in the $d^{th}$ dimension are characterized by $B_{u,d}$ and $B_{l,d}$, correspondingly.

The fitness choice is a fundamental aspect of the JSO system. An encoding result was employed to develop the goodness of candidate performances. At present, the accuracy value is a major state employed to design a FF.

$$Fitness = \max\,(P) \quad (21)$$
$$P = \frac{TP}{TP + FP} \quad (22)$$

whereas $TP$ and $FP$ exemplify the true and false positive values.

## IV. RESULTS AND DISCUSSION

The experimental results of the JSO-DPDCNN technique are validated on the monkeypox dataset [22], comprising 1000 samples and two classes as defined in Table 1. It can be generated by assembling images gathered in newspapers, websites, and online portals and presently comprises about 1905 images then data augmentation. The database was generated by gathering images in multiple open-source and online portals which could not execute some limitations on employ, even for commercial drives, offering a safer path to utilize and disseminate such data if creating and employing some ML approaches. Fig. 3 depicts the sample images.

Fig. 4 validates the classifier outcome of the JSO-DPDCNN approach on the test dataset. Fig. 4a represents the confusion matrix provided by the JSO-DPDCNN approach on 70% of TRP. The result implied that the JSO-DPDCNN system has recognized 344 instances of Monkeypox and 342 instances of others. In addition, Fig. 4b illustrates the confusion matrix offered by the JSO-DPDCNN system on 30% of TSP. The outcome inferred that the JSO-DPDCNN algorithm has recognized 150 instances under Monkeypox and 149 instances

**FIGURE 3. Sample images.**

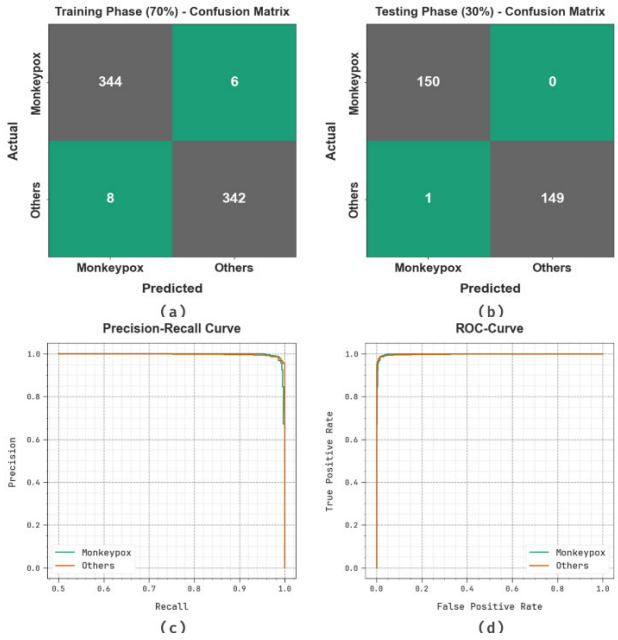


**FIGURE 4. Classifier outcome of (a-b) Confusion matrices, (c) PR-curve, and (d) ROC-curve.**

under others. Also, Fig. 4c determines the PR curve of the JSO-DPDCNN approach. The outcomes stated that the JSO-DPDCNN method has achieved higher PR outcomes under 2 classes. Eventually, Fig. 4d explains the ROC curve of the JSO-DPDCNN algorithm. The result outperformed that the JSO-DPDCNN approach has led to capable outcomes with superior ROC values under 2 classes.

In Table 2, the overall outcomes of the JSO-DPDCNN methodology are investigated under 70% of TRP. Fig. 5 examines the monkeypox detection results of the JSO-DPDCNN technique with 70% of TRP. The experimental values highlighted that the JSO-DPDCNN technique has gained effectual results under two classes. In monkeypox

**TABLE 2.** Classifier outcome of JSO-DPDCNN approach on 70:30 of TRP/TSP.

| Class | $Accu_y$ | $Prec_n$ | $Reca_l$ | $F_{Score}$ | $G_{Measure}$ |
|---|---|---|---|---|---|
| Training Phase (70%) | | | | | |
| Monkeypox | 98.29 | 97.73 | 98.29 | 98.01 | 98.01 |
| Others | 97.71 | 98.28 | 97.71 | 97.99 | 97.99 |
| Average | 98.00 | 98.00 | 98.00 | 98.00 | 98.00 |
| Testing Phase (30%) | | | | | |
| Monkeypox | 100.00 | 99.34 | 100.00 | 99.67 | 99.67 |
| Others | 99.33 | 100.00 | 99.33 | 99.67 | 99.67 |
| Average | 99.67 | 99.67 | 99.67 | 99.67 | 99.67 |

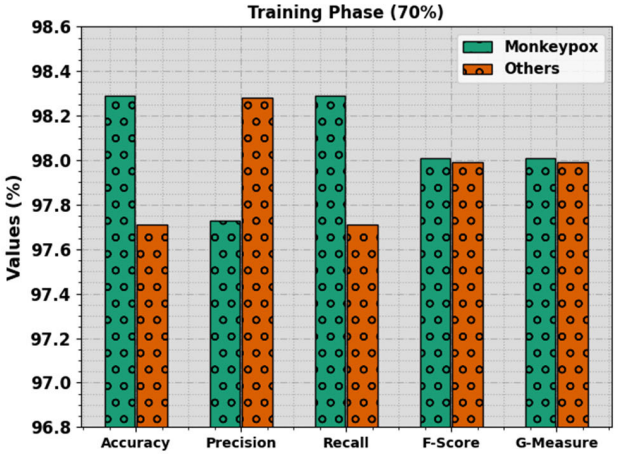


**FIGURE 5.** Classifier outcome of JSO-DPDCNN approach on 70% of TRP.

class, the JSO-DPDCNN technique attained $accu_y$, $prec_n$, $reca_l$, $F_{score}$, and $G_{measure}$ of 98.29%, 97.73%, 98.29%, 98.01%, and 98.01% respectively. Also, in other classes, the JSO-DPDCNN approach gained $accu_y$, $prec_n$, $reca_l$, $F_{score}$, and $G_{measure}$ of 97.71%, 98.28%, 97.71%, 97.99%, and 97.99% correspondingly.

Fig. 6 scrutinizes the monkeypox detection outcome of the JSO-DPDCNN system with 30% of TSP. The result values inferred that the JSO-DPDCNN method has obtained effective outcomes under 2 classes. In monkeypox class, the JSO-DPDCNN approach achieved $accu_y$, $prec_n$, $reca_l$, $F_{score}$, and $G_{measure}$ of 100%, 99.34%, 100%, 99.67%, and 99.67% correspondingly. Also, in other classes, the JSO-DPDCNN method reached $accu_y$, $prec_n$, $reca_l$, $F_{score}$, and $G_{measure}$ of 99.33%, 100%, 99.33%, 99.67%, and 99.67% correspondingly.

Fig. 7 inspects the accuracy of the JSO-DPDCNN approach in the training and validation procedure on the test database. The result inferred that the JSO-DPDCNN system gains higher $accu_y$ values over maximum epochs. Next, the enhanced validation $accu_y$ over training $accu_y$ displays that the JSO-DPDCNN approach acquires capably on the test database.

The loss curve of the JSO-DPDCNN system at the time of training and validation is revealed on the test database in Fig. 8. The outcome implied that the JSO-DPDCNN approach gains nearby values of training and validation loss.

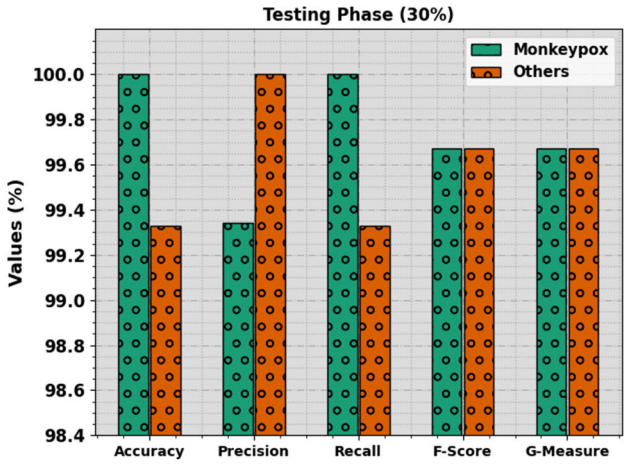


**FIGURE 6.** Classifier outcome of JSO-DPDCNN approach on 30% of TSP.

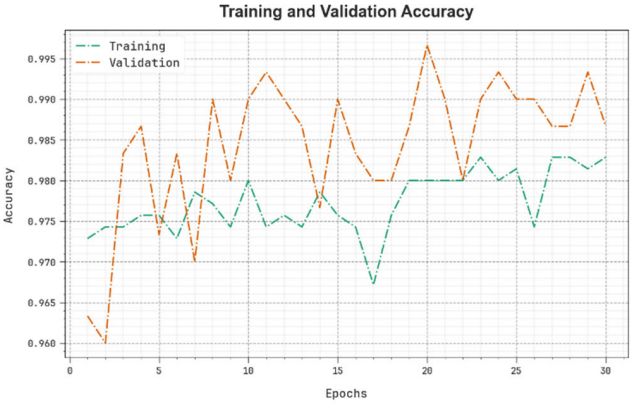


**FIGURE 7.** $Accu_y$ curve of the JSO-DPDCNN system.


**FIGURE 8.** Loss curve of the JSO-DPDCNN approach.

It could be obvious that the JSO-DPDCNN system learns capably on the test database.

A brief comparative study of the JSO-DPDCNN technique with recent approaches is made in Table 3 and Fig. 9 [23]. The outcome stated that the JSO-DPDCNN technique gains improved performance over other models. Based on $accu_y$, the JSO-DPDCNN technique attains increased $accu_y$ of 99.67% while the Xception, VGG16, VGG19, and Blockchain-EHMSEMD techniques offer decreased $accu_y$ values of 76.19%, 89.28%, 94.04%, and 98.80% respectively.

**TABLE 3.** Comparative outcome of JSO-DPDCNN approach with other recent systems.

| Model | $Accu_y$ | $Prec_n$ | $Reca_l$ | $F1_{Score}$ |
|---|---|---|---|---|
| Xception Algorithm | 76.19 | 76.53 | 76.19 | 75.61 |
| VGG16 Algorithm | 89.28 | 89.34 | 89.28 | 89.30 |
| VGG19 Algorithm | 94.04 | 94.77 | 94.04 | 94.07 |
| Blockchain-EHMSEMD | 98.80 | 98.84 | 98.80 | 98.81 |
| JSO-DPDCNN | 99.67 | 99.67 | 99.67 | 99.67 |

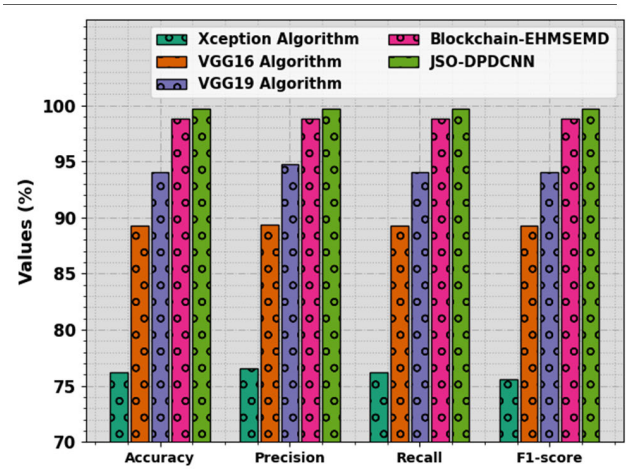


**FIGURE 9.** Comparative outcome of JSO-DPDCNN approach with other recent systems.

Eventually, with respect to $prec_n$, the JSO-DPDCNN method accomplishes a higher $prec_n$ of 99.67% while the Xception, VGG16, VGG19, and Blockchain-EHMSEMD approaches provide lesser $prec_n$ values of 76.53%, 89.34%, 94.77%, and 98.84% correspondingly.

Concurrently, interms of $reca_l$, the JSO-DPDCNN technique attains increased $reca_l$ of 99.67% while the Xception, VGG16, VGG19, and Blockchain-EHMSEMD techniques offer reduced $reca_l$ values of 76.19%, 89.28%, 94.04%, and 98.80% correspondingly. At last, based on $F1_{score}$, the JSO-DPDCNN system obtained a maximum $F1_{score}$ of 99.67% while the Xception, VGG16, VGG19, and Blockchain-EHMSEMD systems offer minimal $F1_{score}$ values of 75.19%, 89.30%, 94.07%, and 98.81% correspondingly.

In Table 4 and Fig. 10, the transaction cost (TC) and execution cost (EC) analysis of the JSO-DPDCNN technique is investigated under different functions. The results imply that the JSO-DPDCNN technique attains effectual outcomes with the least cost values under all functions.

For instance, for patient registration function, the JSO-DPDCNN technique attains TC and EC of 44303.65 and 21582.79 respectively. Besides, for the doctor registration function, the JSO-DPDCNN method achieves TC and EC of 53354.00 and 26382.90 correspondingly. Meanwhile, for the data retrieve function, the JSO-DPDCNN system accomplishes TC and EC of 60087.88 and 33698.58

**TABLE 4.** TC and EC analysis of JSO-DPDCNN approach with distinct functions.

| Functions | Transaction Cost (in gas) | Execution Cost (in gas) |
|---|---|---|
| Patient Registration | 44303.65 | 21582.79 |
| Doctor Registration | 53354.00 | 26382.90 |
| Authentication | 40620.63 | 20102.26 |
| Data Publish | 71316.95 | 46355.20 |
| Data Retrieve | 60087.88 | 33698.58 |

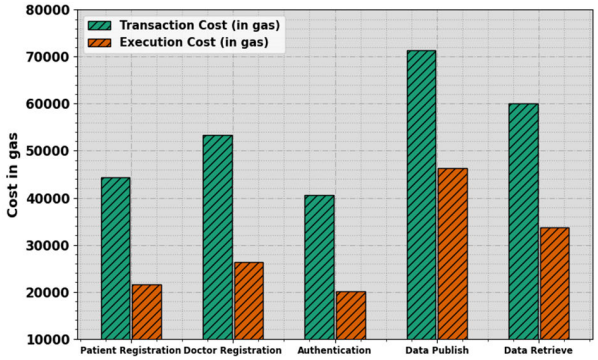


**FIGURE 10.** TC and EC analysis of JSO-DPDCNN approach with distinct functions.

correspondingly. These outcomes stated the greater efficiency of the JSO-DPDCNN approach than other approaches.

## V. CONCLUSION

In this manuscript, we have presented the JSO-DPDCNN system for smart healthcare systems. The presented JSO-DPDCNN technique attains security using BC technology. In addition, the JSO-DPDCNN technique performs DL based diagnosis model for moneypox disease on smart healthcare monitoring using three different processes namely DPCNN-based feature extraction, MLSTM-based classification, and JSO-based hyperparameter tuning. Besides, the JSO-DPCNN technique uses Ethereum-based public BC to secure the privacy of healthcare images. At last, the JSO system was used for the parameter tuning of the MLSTM approach. The simulation outcome of the JSO-DPCNN system was applied to benchmark medical datasets. The widespread outcome highlighted the significant performance of the JSO-DPCNN system in terms of different measures.

## ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number (RGP2/ 159 /44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R440), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444). This study is partially funded by the Future University in Egypt (FUE).

## REFERENCES


[1] P. Sharma, S. Namasudra, R. G. Crespo, J. Parra-Fuente, and M. C. Trivedi, "EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain," *Inf. Sci.*, vol. 629, pp. 703–718, Jun. 2023.

[2] O. Cheikhrouhou, K. Mershad, F. Jamil, R. Mahmud, A. Koubaa, and S. R. Moosavi, "A lightweight blockchain and fog-enabled secure remote patient monitoring system," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100691.

[3] P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, A. Jolfaei, and A. K. M. N. Islam, "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system," *J. Parallel Distrib. Comput.*, vol. 172, pp. 69–83, Feb. 2023.

[4] A. P. Singh, N. R. Pradhan, A. K. Luhach, S. Agnihotri, N. Z. Jhanjhi, S. Verma, U. Ghosh, and D. S. Roy, "A novel patient-centric architectural framework for blockchain-enabled healthcare applications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5779–5789, Aug. 2021.

[5] S. Jain, A. Anand, A. Gupta, K. Awasthi, S. Gujrati, and J. Channegowda, "Blockchain and machine learning in health care and management," in *Proc. Int. Conf. Mainstreaming Block Chain Implement. (ICOMBI)*, Feb. 2020, pp. 1–5.

[6] S. Vyas, M. Gupta, and R. Yadav, "Converging blockchain and machine learning for healthcare," in *Proc. Amity Int. Conf. Artif. Intell. (AICAI)*, Feb. 2019, pp. 709–711.

[7] M. S. Arza and S. K. Panda, "An integration of blockchain and machine learning into the health care system," in *Machine Learning Adoption in Blockchain-Based Intelligent Manufacturing*. Boca Raton, FL, USA: CRC Press, 2022, pp. 33–58.

[8] A. Maseleno, W. Hashim, E. Perumal, M. Ilayaraja, and K. Shankar, "Access control and classifier-based blockchain technology in e-healthcare applications," in *Intelligent Data Security Solutions for e-Health Applications*. New York, NY, USA: Academic Press, 2020, pp. 151–167.

[9] M. Chen, T. Malook, A. U. Rehman, Y. Muhammad, M. D. Alshehri, A. Akbar, M. Bilal, and M. A. Khan, "Blockchain-enabled healthcare system for detection of diabetes," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102771.

[10] N. V. Pardakhe and V. M. Deshmukh, "Machine learning and blockchain techniques used in healthcare system," in *Proc. IEEE Pune Sect. Int. Conf. (PuneCon)*, Dec. 2019, pp. 1–5.

[11] A. P. Kalapaaking, I. Khalil, and X. Yi, "Blockchain-based federated learning with SMPC model verification against poisoning attack for healthcare systems," *IEEE Trans. Emerg. Topics Comput.*, early access, Apr. 21, 2023, doi: 10.1109/TETC.2023.3268186.

[12] E. A. Mantey, C. Zhou, S. R. Srividhya, S. K. Jain, and B. Sundaravadivazhagan, "Integrated blockchain-deep learning approach for analyzing the electronic health records recommender system," *Frontiers Public Health*, vol. 10, May 2022, Art. no. 905265.

[13] A. Ali, M. A. Almaiah, F. Hajjej, M. F. Pasha, O. H. Fang, R. Khan, J. Teo, and M. Zakarya, "An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network," *Sensors*, vol. 22, no. 2, p. 572, Jan. 2022.

[14] R. Ch, G. Srivastava, Y. L. V. Nagasree, A. Ponugumati, and S. Ramachandran, "Robust cyber-physical system enabled smart healthcare unit using blockchain technology," *Electronics*, vol. 11, no. 19, p. 3070, Sep. 2022.

[15] E. Ashraf, N. F. Areed, H. Salem, E. H. Abdelhay, and A. Farouk, "FID-Chain: Federated intrusion detection system for blockchain-enabled IoT healthcare applications," *Healthcare*, vol. 10, no. 6, p. 1110, Jun. 2022.

[16] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, A. K. M. N. Islam, and M. Shorfuzzaman, "Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems," *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 8065–8073, Nov. 2022.

[17] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi, and N. Kumar, "BinDaaS: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1242–1255, Apr. 2021.

[18] R. Kumar, A. A. Khan, J. Kumar, N. A. Golilarz, S. Zhang, Y. Ting, C. Zheng, and W. Wang, "Blockchain-federated-learning and deep learning models for COVID-19 detection using CT imaging," *IEEE Sensors J.*, vol. 21, no. 14, pp. 16301–16314, Jul. 2021.

[19] A. Shahzad, A. Mushtaq, A. Q. Sabeeh, Y. Y. Ghadi, Z. Mushtaq, S. Arif, M. Z. U. Rehman, M. F. Qureshi, and F. Jamil, "Automated uterine fibroids detection in ultrasound images using deep convolutional neural networks," *Healthcare*, vol. 11, no. 10, p. 1493, May 2023.

[20] R. Wang, Y. Rui, J. Zhao, Z. Xiong, and J. Liu, "An adaptive multi-mode navigation method with intelligent virtual sensor based on long short-term memory in GNSS restricted environment," *Sensors*, vol. 23, no. 8, p. 4076, Apr. 2023.

[21] Y. L. Karnavas and E. Nivolianiti, "Optimal load frequency control of a hybrid electric shipboard microgrid using jellyfish search optimization algorithm," *Appl. Sci.*, vol. 13, no. 10, p. 6128, May 2023.

[22] *Monkeypox-Dataset*. Accessed: Feb. 13, 2023. [Online]. Available: https://github.com/mahsan2/Monkeypox-dataset-2022

[23] A. Gupta, M. Bhagat, and V. Jain, "Blockchain-enabled healthcare monitoring system for early monkeypox detection," *J. Supercomput.*, pp. 1–25, Apr. 2023.