Artificial Rabbits Optimizer with Deep Learning Model for Blockchain-Assisted Secure Smart Healthcare System

Mousa Mohammed Khubrani
College of Computer Science and IT, Jazan University, Jazan, Saudi Arabia

***Abstract*—Smart healthcare is based on the electronic health and medical histories of residents, combined with information technology (IT) which can be used to construct a variety of systems including humanised health management systems and convenient medical service systems. The transparency, traceability, decentralization and security of BC technology and machine learning (ML) will enable the medical sector to upgrade and optimise different forms of quality and service. Therefore, this study introduces an artificial rabbit optimizer with deep learning for Blockchain Assisted Secure Smart Healthcare System (ARODL-BSSHS) technique. The presented ARODL-BSSHS technique designs a new healthcare monitoring technique by using blockchain (BC) technology and classifies the presence of malicious activities in the healthcare system, and takes needed actions to predict the disease. For intrusion detection, the ARODL-BSSHS technique exploits the ARO algorithm with Hop field neural network (IHNN) model. On the other hand, the ARODL-BSSHS technique applies a deep extreme learning machine (DELM) model for disease detection purposes. Finally, the heap-based optimization (HBO) technique is exploited as a hyperparameter optimizer for the DELM model. The ARODL-BSSHS technique involves BC technology for the secure transmission of healthcare data. A series of simulations were carried out on benchmark datasets: heart disease and NSL-KDD database for examining the performance of the ARODL-BSSHS technique. The experimental values highlighted that the ARODL-BSSHS method obtains superior performance than other approaches.**

Keywords—Blockchain; smart healthcare; artificial rabbit's optimizer; deep learning; intrusion detection

I. INTRODUCTION

The connection of clinically related technologies will have a major impact on healthcare professionals and patients [1] . Along with the diversified nature and fast growth of the health care atmosphere, protection becomes a major problem as advanced security problems develop and earlier security problems become more acute. Data protection can be defined as the capability to transmit and store data without enabling unauthorized access to make sure confidentiality, data consistency, legality, and legitimacy [2]. Only authorized users have access to the protected data. Due to their unauthorized access and unauthenticated users, cybercrime develops and often affects healthcare sensors and systems [3]. A considerable amount of healthcare data is distributed, collected and gathered among various health care sectors. The data transmission must take place in a protected manner. The number of cyber-attacks is increasing drastically due to enormous data transformation. It denotes the demand for a reliable system for protecting health care datasets [4]. Potential mining methods are demanded to inspect clinical data to assist in enhancing patient care, disease discovery, and offering medical treatment [5]. ML can be a complex computational method that was employed in various fields like health care, image recognition, and language processing [6]. Still, ML methods obtain a higher level of accuracy with a large volume of the training set that can be vital in health care, where accuracy may, in some cases, denote the difference between losing and saving the life of the patient. In many cases, centralized training methods acquire a large quantity of data from robust cloud servers that result in major consumer privacy violations, particularly in the clinical domain [7]. As an accountable and open data protection system, the progression of the BC technology opens the way for novel ways to solve the main problems of ethics, privacy, and security in domains that require privacy, anonymity and security of records including health care system [8] [9] . But BC has attained remarkable achievement for different smart healthcare technologies like patient record access control, data distribution, etc. [10].

Today, BC and ML technology are preferred [11]. The security, traceability, transparency, and decentralization of these two technologies will assist the healthcare sector to upgrade and optimize in several aspects [12]. The implementation of and making the functioning of the health care sector more efficient [13]. Few studies have explored the implementation of ML and BC. For instance, a health management platform based on BC can allow users to track personal data securely, and smart contracts are utilized in clinical detection to automatically manage emergencies [14].

This research is driven by the urgent need to address the growing vulnerabilities in healthcare systems due to escalating cyber threats and the rapid advancements in healthcare technologies. This study introduces an Artificial Rabbit Optimizer with Deep Learning for Blockchain-Assisted Secure Smart Healthcare System (ARODL-BSSHS) technique. This novel technique focuses on creating a secure and intelligent healthcare system, specializing in intrusion detection and disease diagnosis. It strategically employs the Artificial Rabbit Optimizer (ARO) algorithm and the Hopfield Neural Network (HNN) model for intrusion detection, and a Deep Extreme Learning Machine (DELM) model for accurate disease detection, with Blockchain technology incorporated to secure data transmission. The efficacy and improved performance of the ARODL-BSSHS technique have been validated through extensive experiments on recognized datasets, showcasing its potential for real-world applications in enhancing healthcare security and efficiency.

II. Literature Review

In [15], the authors introduced a smart BC Manager (BM) depends on the DRL for optimizing the BC behavior of the network in real-time while concerning clinical data needs, like security levels and urgency. Utilizing 3 RL-related methods like Dueling Double Deep Q-Network (D3QN), Double Deep Q-Networks (DDQN), and DQN, the optimization approach can be developed as a Markov Decision Process (MDP). Lakhan et al. [16] present a DRLBTS abbreviated as DRL-aware BC-related task scheduling structure with various goals. The presented method offers security and makespan potential scheduling for medicinal purposes. Singh et al. [17] modelled a DL-related IoT-based structure for the secured smart city where BC offers a dispersed atmosphere at the transmission stage of CPS, and SDN established the protocol for transporting data. A DL–related cloud was applied at the application layer of the presented structure to solve scalability, centralization, and communication latency.

Mantey et al. [18] presented a BC privacy system (BPS) as DL for diet recommendation mechanisms for patients. This study applied DL and ML approaches like MLP, RNN, LR etc., to the Internet of Medical Things (IoMT) data obtained. The product section contains a collection of eightattributes. The IoMT dataset features are examined with BPS and encoded in advance to the implementation of DL and ML-related structures. In [19], presented a BC-orchestrated DL method (BDSDT) for Secured Data transmission in IoT-based healthcare systems. First, a new scalable BC structure is devised to ensure secure data transmission and data integrity using Zero Knowledge Proof (ZKP) system. Afterwards, BDSDT integrated with the off-chain storage IPFS abbreviated as InterPlanetary File mechanism, to solve problems with data storing costs to solve data security problems. Sammeta and Parthiban [20] developed a new method HBESDM-DLD abbreviated as hyperledger BC-based secure clinical data management with DL-related diagnosis method. This method includes different stages of operations such as hyperledger BC-based secure data management, encryption, diagnosis and optimal key generation. For encryption, SIMON block cipher method can be implemented. For optimal key generation, a group teaching optimization algorithm (GTOA) was adopted.

In [21], the authors proposed a Decentralized Interoperable Trust framework (DIT) based on BC for the Internet of Things (IoT) platform. The DIT IoHT employs a private BC ripple chain to establish secure and reliable data transmission by authenticating nodes in relation to their interoperable structures. Purbey, Khandelwal, and Choudhary in [22] introduced a method for secure and efficient ontology generation using BC, named BOGMAS. This approach employs a semi-supervised technique to generate ontologies from structured or unstructured datasets. It combines techniques such as extra trees (ET) stratification and linear support vector machine (LSVM) for predicting variances. Almaiah et al. [23] proposed a Deep Learning (DL) architecture integrated with BC to ensure dual levels of privacy and security. Firstly, they establish a BC model where participating entities undergo registration, validation, and verification through smart contracts using Proof of Work. Subsequently, they model BiLSTM for intrusion detection and apply a DL method incorporating a Variational Autoencoder (VAE) technique for privacy preservation.

The reviewed studies, despite their innovative contributions to blockchain and deep learning in healthcare, exhibit several overarching limitations. Many face issues related to scalability, adaptability, and specificity, which can restrict their applicability across diverse healthcare environments and requirements. Several solutions also struggle with the balance between complexity and user-friendly implementation, posing challenges in deployment and interpretation. Additionally, the methods proposed often focus narrowly on specific aspects of healthcare or technology, neglecting a holistic approach that addresses the multifaceted nature of healthcare systems, thus necessitating further holistic and integrative research endeavors.

III. Proposed Model

In this study, the ARODL-BSSHS technique has been developed to accomplish security in the healthcare system. The presented ARODL-BSSHS technique involves the design of secured and smart healthcare system using two major processes, namely intrusion detection and disease diagnosis. To accomplish this, the ARODL-BSSHS technique follows a series of processes: HNN based intrusion detection, ARO based parameter tuning, DELM-based disease detection, and HBO based parameter optimization. Fig. 1 illustrates the workflow of ARODL-BSSHS algorithm.

A. BC Technology

In this work, the ARODL-BSSHS technique involves BC technology for secure transmission of healthcare data. Electronic Health Records (EHR) are well functioning on smart contracts [24]. It developed the framework for a decentralized medical service stage and aids as an interface to the patient records that can be shared by suppliers and patients. BC is separated into research-centric and patient-centric BC network classes, as stated by “BC Technology in Healthcare”. The security concern regarding EHR is tackled by the patient-centric BC network, which gives the authority over sharing medicinal data with multiple users. BC technology can be able to modernize healthcare management by permitting unambiguous and transparent data access through every stakeholder involved, comprising hospitals, therapists, medical experts, and general practitioners [25]. In such cases, several medicinal stakeholders do not necessarily use resource- and time-consuming information and verification progressions.

Furthermore, this approach could contribute to the early detection of health-related issues, thereby reducing instances of medical malpractice arising from coordination issues [26]. It instills trust in individuals regarding their comprehensive care, as the integrity of healthcare records from previous visits to different medical practitioners remains intact within the network. Additionally, BC serves as a valuable tool for constructing patient-centric networks through various means, such as augmenting data availability, thereby enhancing data liquidity, establishing unique patient identifiers, and implementing digital access control. The Hyperledger Fabric system can be leveraged to establish a permissioned BC network. Within this system, two distinct types of peers exist: validating peers, responsible for ledger management, consensus procedures, and transaction validation. The data is stored within a distributed system, facilitating the upload of patient medical histories, verification of healthcare records, and the facilitation of data access requests and permissions.

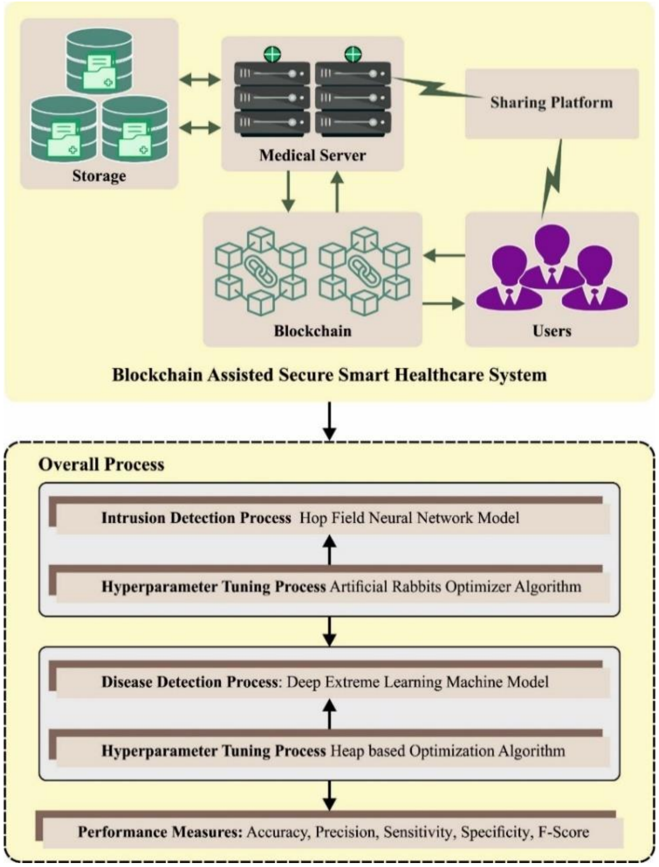
Storage
Medical Server
Sharing Platform
Blockchain
Users
Blockchain Assisted Secure Smart Healthcare System
Overall Process
Intrusion Detection Process Hop Field Neural Network Model
Hyperparameter Tuning Process Artificial Rabbits Optimizer Algorithm
Disease Detection Process: Deep Extreme Learning Machine Model
Hyperparameter Tuning Process Heap based Optimization Algorithm
Performance Measures: Accuracy, Precision, Sensitivity, Specificity, F-Score

Fig. 1. Workflow of ARODL-BSSHS approach.

B. Intrusion Detection using Optimal HNN Model

For intrusion detection process, the HNN classifier is used. The HNN exhibits abundant dynamical behavior owing to its hyperbolic tangent function and special network structure [27]. The HNN with n neurons is defined by the series of dimensionless non-linear ordinary differential equations as in the following:

$$\dot{x} = -x + Y tanh(x) + I \tag{1}$$

Where

$$x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_i \\ \vdots \\ x_n \end{bmatrix}, I = \begin{bmatrix} I_1 \\ I_2 \\ \vdots \\ I_i \\ \vdots \\ I_n \end{bmatrix}$$

$$\text{Y}= \begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1j} & \cdots & y_{1n} \\ y_{21} & y_{22} & \cdots & y_{2j} & \cdots & y_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ y_{i1} & y_{i2} & \cdots & y_{ij} & \cdots & y_{in} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ y_{n1} & y_{n2} & \cdots & y_{nj} & \cdots & y_{nn} \end{bmatrix} \tag{2}$$

In Eq. (2), $\tanh(x)$ shows the neuron activation function, x_i embodies the $i\text{-}th$ neuron membrane voltage, Y characterizes the synaptic weight matrix, and y_{ij} denotes the synaptic weight between $j\text{-}th$ and $i\text{-}th$ neurons. Moreover, I_i characterizes $i\text{-}th$ neuron external stimulate current. In recent times, improved model has been created on the basis of original HNN models, namely HNN with time delay, fractional HNN, discrete HNN, HNN with dissimilar active functions, etc.

The ARO algorithm can be applied to improve the detection rate of the HNN model. The ARO can be stimulated by the survival skills of the rabbit [28]. Rabbits are herbivores which mainly consume leafy weeds and grass. Rabbits wouldn't eat the grass nearby the holes; rather, they find food far away from their nests to avoid predators identifying the nest. These foraging strategies are determined as exploration. Furthermore, to lessen the possibility of being captured by hunters or predators, they are skilled at digging a lot of holes for the nest and randomly choose one as a shelter. This random hiding approach can be assumed as exploitation in ARO. Rabbits must run faster to avoid dangers from the predator owing to their low level in the food chain, resulting in a decline in their energy, so they should shift between random hiding and detour foraging based on their energy status. The mathematical model of ARO is constructed with previous knowledge about the natural behaviors of rabbits, such as exploitation, exploration, and transition from exploration to exploitation.

Consider that every individual in the population has an individual area with burrows and few grass. In foraging activity, the rabbit has a tendency to move towards the faraway area of other rabbits in finding food and overlook what lies nearby, same as an old Chinese proverb says: "A rabbit doesn't eat grass close to their nests". These behaviors are named detour foraging, and they can be mathematically formulated as:

$$X_i(t+1) = X_j(t) + A \times \left(X_i(t) - X_j(t)\right) + round\big(0.5 \times (0.05 + R_1)\big) \times n_1, \tag{3}$$

$$i, j = 1, \dots, N \; and \; i \neq j$$

$$A = L \times c \tag{4}$$

$$L = \left(e - e^{\left(\frac{t-1}{T}\right)^2}\right) \times \sin\left(2\pi R_2\right) \tag{5}$$

$$c(k) = \begin{cases} 1, if \; k == g(l) \\ 0, otherwise \end{cases} k = 1, \dots, D \; and \; l = 1, \dots, [R_3 \times D] \tag{6}$$

$$g = randperm(D) \tag{7}$$

$$n_1 \sim N(0,1) \tag{8}$$

Where $X_i(t)$ and $X_j(t)$ signify the location of $i\text{-}th$ and $j\text{-}th$ rabbits at the t existing iteration, $X_i(t+1)$ indicates the candidate location of $i\text{-}th$ rabbit at $t+1$ the next iteration correspondingly. T denotes the higher iteration counts. N shows the size of population. t represents the existing iteration. $\lceil\cdot\rceil$ refers to the ceiling function. D symbolizes the dimensional of specific problem. $randperm(\cdot)$ shows the arbitrary value within 1 and D. R_1, R_2, and R_3 indicates the random integer within [0,1]. round $(\cdot)$ indicates rounding to the nearby integer. L stands for the length of movement stage while implementing the detour foraging. n_1 follows the uniform distribution.

Here, rabbits tend to conduct continuous detour foraging at the beginning of iteration; then, they often implement random hiding. The idea of rabbit energy E was introduced to retain a better balance between exploitation and exploration that is gradually reduced over time:

$$E(t) = 4\left(1-\frac{t}{T}\right)\ln\frac{1}{R_4} \tag{9}$$

In Eq. (9), R_4 indicates the random integer having range of [0, 1]. The value of E energy co-efficient differs from zero to two. If $E \leq 1$, it shows that rabbit has lesser energy for physical activities. Hence it is necessary to carry out random hiding to escape from the predators, and the ARO method enters the exploitation stage. If $E > 1$, it shows that rabbit has sufficient energy to discover the foraging region of other individuals such that the detour foraging takes place, and this stage can be determined by the exploration. Rabbits are generally met with attack and chase from the hunters. To survive, they should dig several holes nearby their nests for shelter.

In Eq. (9), the variable R_4 represents a randomly generated integer within the range [0, 1]. The energy coefficient E assumes values from zero to two. When $E \leq 1$, it indicates that the rabbit possesses limited energy for engaging in physical activities. As a result, the rabbit adopts a strategy of random hiding to evade predators, marking the onset of the exploitation stage in the ARO method. Conversely, when $E > 1$, the rabbit possesses sufficient energy to explore the foraging regions of other individuals. This condition triggers detour foraging and signifies the exploration stage. In their natural environment, rabbits often encounter threats from predators, leading to pursuits and attacks. To ensure survival, they create several burrows in close proximity to their nests, offering shelter from potential threats.

$$X_i(t+1) = X_i(t) + A \times \left(R_5 \times b_{i,r}(t) - X_i(t)\right) \tag{10}$$

$$b_{i,r}(t) = X_i(t) + H \times g_r(k) \times X_i(t) \tag{11}$$

$$g_r(k) = \begin{cases} 1, if\ k == \lceil R_6 \times D \rceil \\ 0, otherwise \end{cases} \tag{12}$$

$$H = \frac{T-t+1}{T} \times n_2 \tag{13}$$

$$n_2 \sim N(0,1) \tag{14}$$

Where the parameter A is evaluated by Eqs. (4)-(7), R_5 and R_6 shows two random integers within [0,1], $b_{i,r}(t)$ signify the arbitrarily chosen burrow of $i\text{-}th$ rabbits in D burrows applied to hide at t existing iteration, and n_2 follows the uniform distribution.

Fitness selection is a crucial component of the ARO technique. Encoded outcomes are utilized to assess the quality of solution candidates. In this context, the accuracy value serves as the primary criterion for designing a fitness function (FF).

$$Fitness = \max(P) \tag{15}$$

$$P = \frac{TP}{TP+FP} \tag{16}$$

Where TP denote the true positive and FP specifies the false positive value.

C. Disease Detection using DELM Model

At this stage, the DELM model is used to detect the presence of the disease. ELM is the first presented by Huang et al. that is utilized for SLFNs [29]. An input weighted and hidden layer (HL) biases can be arbitrarily allocated at first, so the trained databases for determining the resultant weighted of SLFNs are integrated. For N random various instances (x_i, t_i), $i = 1,2,\ldots,N$, whereas $x_i = [x_{i1}, x_{i2}, \ldots, x_{in}]^T$, $t_i = [t_{i1}, t_{i2}, \ldots, t_{im}]^T$. Thus, the ELM technique is expressed as:

$$\sum_{j=1}^{L} \beta_j\, g_j(x_i) = \sum_{j=1}^{L} \beta_j\, g(w_j \cdot x_i + b_j) = 0_i (i = 1,2,\ldots,N), \quad (17)$$

Whereas $\beta_j = [\beta_{j1}, \beta_{j2}, \ldots, \beta_{jm}]^T$ states the j^{th} hidden node weighted vector, but the weighted vector among the j^{th} hidden node and the resultant layer is defined as $w_j = [w_{1j}, w_{2j}, \ldots, w_{nj}]^T$. The threshold of j^{th} hidden node is expressed as b_j, and $0_i = [0_{11}, 0_{12}, \ldots, 0_{im}]^T$ refers to the i^{th} resultant vector of ELM.

It is estimated the resultant of DELM when the activation function $g(x)$ with 0 error that implies as Eq. (18):

$$\textstyle\sum_{i=1}^{N} ||0_i - t_i|| = 0. \tag{18}$$

Thus, Eq. (17) is termed as Eq. (19):

$$\textstyle\sum_{j=1}^{L} \beta_j\, g_j(x_i) = \sum_{j=1}^{L} \beta_j\, g(w_j \cdot x_i + b_j) = t_i (i = 1,2,\ldots,N). \tag{19}$$

Eventually, Eq. (19) is easily defined as Eq. (20):

$$H\beta = T, \tag{20}$$

whereas, H defines the HL resultant matrix, and $H = H(w_1, w_2, w_L, b_1, b_2, b_L, x_1, x_2, x_N)$. So, h_{ij}, β, and T are demonstrated as:

$$[h_{ij}] = \begin{bmatrix} g(w_L \cdot x_1 + b_L) & \ldots & g(vv_L . x_1 + b_L) \\ \vdots & \ddots & \ldots \\ g(w_L \cdot x_N + b_L) & \ldots & g(vv_L \cdot x_N + b_L) \end{bmatrix}, \tag{21}$$

$$\beta = \begin{bmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{L1} & \beta_{L2} & \cdots & \beta_{Lm} \end{bmatrix} \tag{22}$$

and

$$T = \begin{bmatrix} t_{11} & t_{12} & \cdots & t_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ t_{N1} & t_{N2} & \cdots & t_{Nm} \end{bmatrix}. \tag{23}$$

Afterwards, the minimal norm least-squares solution of Eq. (20) as:

$$\hat{\beta} = H^{\dagger}T, \tag{24}$$

Whereas $H^{\dagger}$ implies the Moore Penrose generalization of the inverse of matrix H. The resultant of DELM is defined as Eq. (25):

$$f(x) = h(x)\beta = h(x)H^{\dagger}T. \tag{25}$$

From the above mentioned, the procedure of ELM is defined as follows. Initially, DELM is arbitrarily allocated the input weighted and HL biased (w_i, b_i). Next, it can compute the HL resultant matrix H based on Eq. (21). Afterward, by employing Eq. (24), it attains the resultant weighted vector β. Lastly, it classifies the novel database based on the above-trained procedure. Fig. 2 represents the framework of ELM.

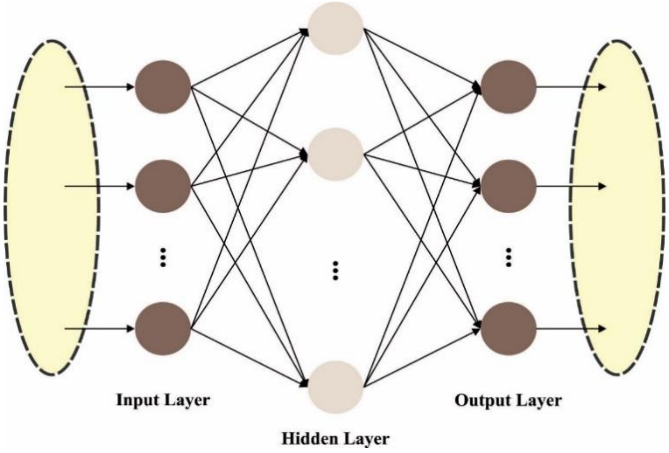

Fig. 2. Architecture of ELM.

D. Parameter Tuning using HBO Algorithm

At the final stage, the HBO algorithm was utilized for the optimal parameter tuning of the DELM Model. HBO algorithm was inspired by the social behaviours of human beings according to the hierarchy of organization [30]. This approach stimulates the corporate rank hierarchy (CRH), which implies that the member of the teamwork in the specific organization should be organized in a hierarchical form for completing the specific task. The presented method exploits the CRH model for hierarchically arranging the search candidate according to the fitness of this candidate. For the hierarchy construction, the heap-based data organization can be exploited. Besides the modeling of CRH, the whole concept involves three stages: (i) modeling of the collaborations between their direct manager and the subordinators; (ii) modeling of interactivity amongst the workers; and (iii) lastly, the modeling of self-contribution of the subordinators to accomplish the required task.

E. Modelling of the CRH Concept

The presented approach can be conceptualized as a population. In this context, each searching agent within the search space can be likened to a heap node, with the fitness function (FF) of optimizer problems serving as the master key to access these heap nodes.

In a large organization that operates under a centralized infrastructure, laws and regulations are enforced unilaterally, flowing from senior leadership down to employees. In such a setup, employees are expected to adhere to the instructions of their superiors. With upgrading the place of searching candidate, this stage is mathematically defined:

$$x_i^k(t+1) = B^k + \gamma(2r-1)\left|B^k - x_i^k(t)\right| \tag{26}$$

In Eq. (26), x indicates the position of search agent; t and k show the existing iteration and the vector element, correspondingly; and B shows the parental node. The term $(2r-1)$ symbolizes the k-th components of the vector γ and is produced randomly and defined as follows:

$$\lambda^k = 2r - 1 \tag{27}$$

In Eq. (27), r indicates the arbitrary parameter within [0,1] in a uniform distribution:

$$\gamma = \left| 2 - \frac{\left(t mod \frac{T}{C}\right)}{\frac{T}{4C}} \right| \tag{28}$$

In Eq. (28), T shows the maximal amount of iterations, and C indicates an adjustable parameter and relies on the iteration based on Eq. (29):

$$C = \frac{T}{25} \tag{29}$$

Colleagues (Subordinators) in a specific organization co-operate to accomplish official tasks. In the presented method, the nodes at a similar location from the heap are considered colleagues:

$$x_i^k(t+1) = \begin{cases} S_r^k + \gamma\lambda^k\left|S_r^k + x_i^k(t)\right|, & f(S_r) < f(x_i(t)) \\ x_i^k + \gamma\lambda^k\left|S_r^k - x_i^k(t)\right|, & f(S_r) \geq f(x_i(t)) \end{cases} \tag{30}$$

The self-contribution of every sub-ordinator from the organization was defined as follows:

$$x_i^k(t+1) = x_i^k(t) \tag{31}$$

In this section, the three position updating equation defined in the prior subsection is combined as one formula. A roulette wheel was exploited for making a balance among exploitation as well as exploration stages. The P_1, P_2, and P_3 probabilities are used for achieving the balance between this phase. An initial probability p1 can be exploited to update the location of the searching agent from the population and is formulated as follows:

$$P_1 = 1 - \frac{t}{T} \tag{32}$$

The second proportion, p_2 can be evaluated by Eq. (33):

$$P_2 = P_1 + \frac{1-P_1}{2} \tag{33}$$

Lastly, the probability p_3 was evaluated by Eq. (33):

$$P_3 = P_2 + \frac{1-P_1}{2} = 1 \tag{34}$$

$$x_i^k(t+1) = \begin{cases} x_i^k(t), & P < P_1 \\ B^k + \gamma\lambda^k\left|B^k - x_i^k(t)\right|, & P_1 < P < P_2 \\ S_r^k + \gamma\lambda^k\left|S_r^k - x_i^k(t)\right|, & P_2 < P < P_3 \text{ and } f(S_r) < f\big(x_i(t)\big) \\ x_i^k + \gamma\lambda^k\left|S_r^k - x_i^k(t)\right|, & P_2 < P < P_3 \text{ and } f(S_r) \geq f\big(x_i(t)\big) \end{cases} \quad (35)$$

Where p shows a random value within [0,1].

The HBO technique not only grows a FF to attain higher accuracy of classifier and determines a positive integer to represent the greater efficacy of candidate solutions. The decline of classifier error rate is assumed as FF.

$$fitness(x_i) = ClassifierErrorRate(x_i) = \frac{no.of\ misclassified\ instances}{Total\ no.of\ instances} * 100 \quad (36)$$

IV. Results

A. Results Analysis on Intrusion Detection Dataset

In this section, the intrusion detection results of the ARODL-BSSHS approach were tested on the NSL database [31], including 2100 instances and five classes, as shown in TableI.

TABLE I. DETAILS OF NSL DATASET

Class	No. of Instances
Normal_Class	500
DoS_Class	500
Probe_Class	500
R2-L_Class	500
U2-R_Class	100
Total Number of Instances	**2100**

Fig. 3 illustrates the classifier outcomes generated by the ARODL-BSSHS technique when applied to the NSL dataset. Figs. 3(a) and 3(b) depict the confusion matrix derived from the ARODL-BSSHS method using a 70:30 split of Training and Testing Data Split (TRP/TSP). The outcomes indicate that the ARODL-BSSHS approach effectively identified and correctly categorized all five classes. Similarly, Fig. 3(c) showcases the Precision-Recall (PR) curve yielded by the ARODL-BSSHS approach. The findings suggest that the ARODL-BSSHS system achieved favorable PR performance across all five classes. Lastly, Fig. 3(d) displays the Receiver Operating Characteristic (ROC) curve resulting from the ARODL-BSSHS technique. This graph highlights that the ARODL-BSSHS approach yielded commendable results, exhibiting superior ROC values for all five classes.

The intrusion detection outcomes of the ARODL-BSSHS technique under 70:30 of TRP/TSS are demonstrated in Table II. The results reported that the ARODL-BSSHS technique recognizes five class labels effectually. For instance, with 70% of TRP, the ARODL-BSSHS technique obtains average $accu_y$ of 99.73%, $prec_n$ of 99.19%, $sens_y$ of 99.18%, $spec_y$ of 99.83%, and F_{score} of 99.19%. Additionally, with 30% of TSP, the ARODL-BSSHS method attains average $accu_y$ of 99.75%, $prec_n$ of 99.45%, $sens_y$ of 99.46%, $spec_y$ of 99.83%, and F_{score} of 99.45%.

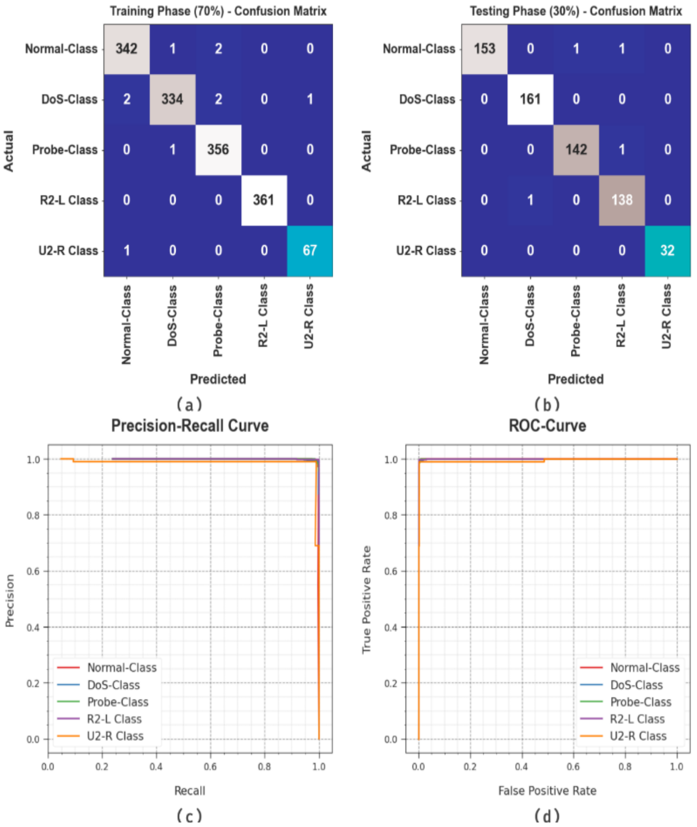

Fig. 3. Classifier outcome on NSL dataset (a-b) Confusion matrices, (c) PR curve, and (d) ROC curve.

TABLE II. INTRUSION DETECTION OUTCOME OF ARODL-BSSHS SYSTEM ON NSL DATASET

Class	$Accu_y$	$Prec_n$	$Sens_y$	$Spec_y$	F_{Score}
		Training Phase (70%)			
Normal-Class	99.59	99.13	99.13	99.73	99.13
DoS-Class	99.52	99.40	98.53	99.82	98.96
Probe-Class	99.66	98.89	99.72	99.64	99.30
R2-L Class	100.00	100.00	100.00	100.00	100.00
U2-R Class	99.86	98.53	98.53	99.93	98.53
Average	**99.73**	**99.19**	**99.18**	**99.83**	**99.19**
		Testing Phase (30%)			
Normal-Class	99.68	100.00	98.71	100.00	99.35
DoS-Class	99.84	99.38	100.00	99.79	99.69
Probe-Class	99.68	99.30	99.30	99.79	99.30
R2-L Class	99.52	98.57	99.28	99.59	98.92
U2-R Class	100.00	100.00	100.00	100.00	100.00
Average	**99.75**	**99.45**	**99.46**	**99.83**	**99.45**

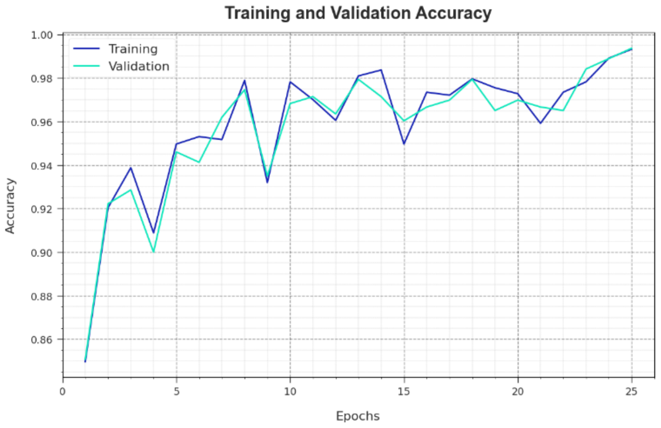

Fig. 4. Accuracy curve of ARODL-BSSHS system on NSL dataset.

Fig. 4 examines the accuracy performance of the ARODL-BSSHS algorithm through the training and validation phases on the NSL dataset. The findings indicate that the ARODL-BSSHS system achieves peak accuracy values as the epochs progress. Notably, the higher validation accuracy in comparison to the training accuracy signifies the proficient learning capability of the ARODL-BSSHS system on the NSL dataset.

The evaluation of loss during both training and validation stages of the ARODL-BSSHS algorithm on the NSL dataset is presented in Fig. 5. The results suggest that the ARODL-BSSHS algorithm maintains similar values of training and validation loss. This observation underscores the effective learning of the ARODL-BSSHS approach on the NSL dataset.

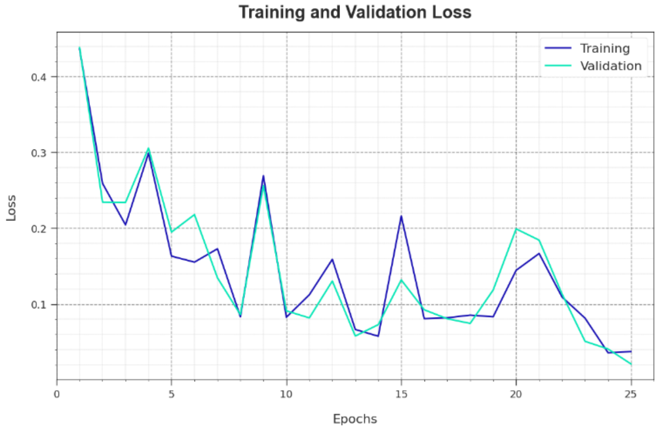

Fig. 5. Loss curve of ARODL-BSSHS system on NSL dataset.

Table III and Fig. 6 reports the comparative intrusion detection results of the ARODL-BSSHS technique. The outcomes implied that the SVM model and LDA model achieves worse outcomes. Although the RF, NB, CART, and HNIDS models offer slightly improved results, the ARODL-BSSHS technique outperforms the other existing models with maximum $accu_y$ of 99.75%, $prec_n$ of 99.45%, $sens_y$ of 99.46%, and F_{score} of 99.45%.

TABLE III. COMPARISION OF ARODL-BSSHS ALGORITHM WITH DIFFERENT METHODOLOGIES ON THE NSL DATASET

Classification Method	Accuracy	Precision	Sensitivity	F-Score
SVM Model	87.80	97.85	91.41	96.67
LDA Model	91.57	96.78	90.57	96.32
RF Model	97.50	97.85	94.67	97.48
Naïve Bayes	94.66	95.62	93.55	95.08
CART	94.59	96.55	92.78	95.62
LR Model	92.31	91.26	90.11	91.26
HNIDS	98.97	98.85	96.12	99.04
ARODL-BSSHS	99.75	99.45	99.46	99.45

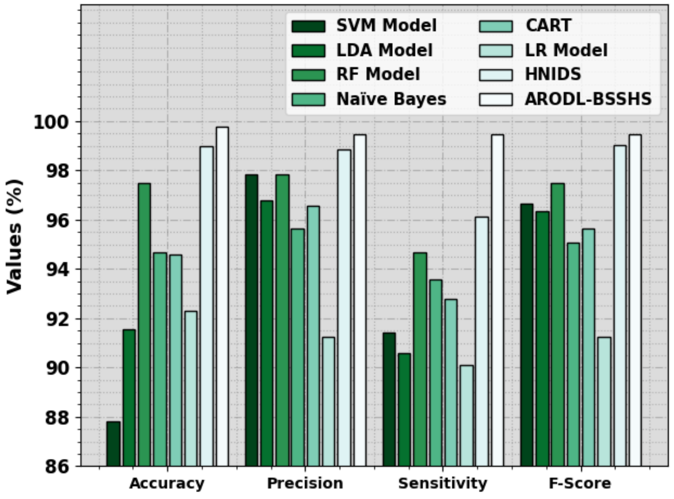

Fig. 6. Comparative outcome of ARODL-BSSHS approach with other methods on NSL dataset.

The computation time (CT) examination of the ARODL-BSSHS technique with recent models on the intrusion detection process is reported in Table IV and Fig. 7. The outcomes reported that the ARODL-BSSHS approach gains least CT of 9.50s. On the other hand, the existing SVM, LDA, RF, NB, CART, LR, and HNIDS models obtain increased CT of 20.54s, 18.89s, 12.37s, 19.77s, 16.09s, 12.97s, and 11.21s respectively.

TABLE IV. COMPARISON OF CT OUTCOME OF ARODL-BSSHS APPROACH WITH OTHERS ON NSL DATASET

Classifier	Computational Time (sec)
SVM	20.54
LDA	18.89
RF	12.37
Naïve Bayes	19.77
CART	16.09
LR	12.97
HNIDS	11.21
ARODL-BSSHS	09.50

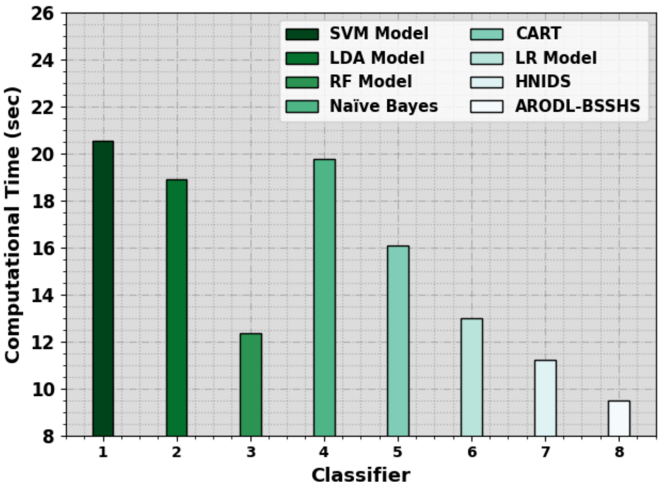

Fig. 7. CT outcome of ARODL-BSSHS approach with other methods on NSL dataset.

B. Results Analysis on Disease Diagnosis Dataset

The Cleveland heart dataset (CHD) [32] contains of 303 samples with 76 features, but only 14 features can be assumed that more appropriate for study experimental purposes. Table V illustrates the details on CHD.

TABLE V. DETAILS ON CHD

Class	No. of Samples
Absence	138
Presence	165
Total Number of Samples	303

Fig. 8 presents the classifier outcomes achieved by the ARODL-BSSHS algorithm when applied to the CHD dataset. Sub-figures 8a and 8b display the confusion matrix generated by the ARODL-BSSHS system using a 70:30 split of Training and Testing Data Split (TRP/TSP). The outcomes indicate that the ARODL-BSSHS system effectively recognized and accurately classified both of the available classes.

Similarly, Fig. 8(c) illustrates the Precision-Recall (PR) analysis performed by the ARODL-BSSHS model. The results reported demonstrate that the ARODL-BSSHS system achieved superior PR performance across the two classes. Lastly, Fig. 8(d) showcases the Receiver Operating Characteristic (ROC) analysis conducted by the ARODL-BSSHS approach. This graph demonstrates that the ARODL-BSSHS algorithm has delivered capable results, achieving maximum ROC values for the two classes.

The classification outcome of the ARODL-BSSHS method under 70:30 of TRP/TSS is established in Table VI. The outcomes stated that the ARODL-BSSHS system recognizes five class labels effectively. For example, with 70% of TRP, the ARODL-BSSHS method attains average $accu_y$ of 95.07%, $prec_n$ of 95.32%, $sens_y$ of 95.07%, $spec_y$ of 95.07%, and F_{score} of 95.19%. Furthermore, with 30% of TSP, the ARODL-BSSHS method acquires average $accu_y$ of 97.83%, $prec_n$ of 97.87%, $sens_y$ of 97.83%, $spec_y$ of 97.83%, and F_{score} of 97.80%.

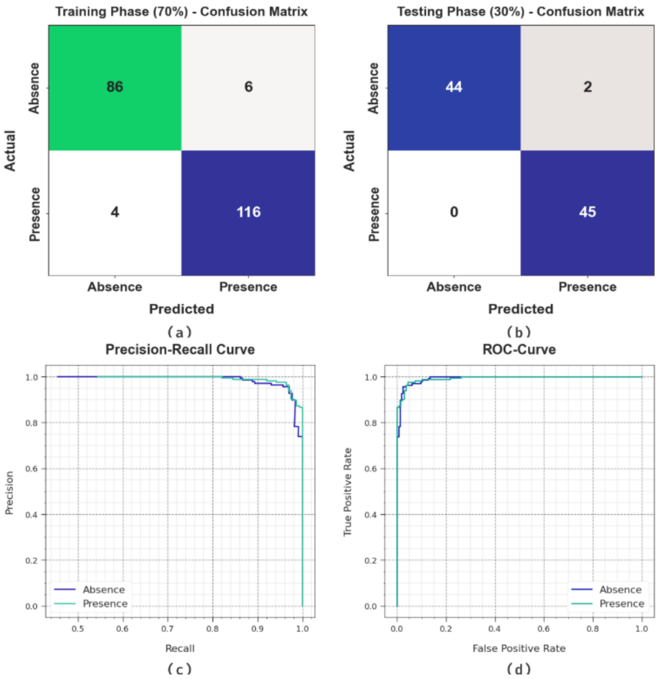

Fig. 8. Classifier outcome on CHD (a-b) Confusion matrices, (c) PR curve, and (d) ROC curve.

TABLE VI. CLASSIFIER OUTCOME OF ARODL-BSSHS SYSTEM ON CHD

Class	$Accu_y$	$Prec_n$	$Sens_y$	$Spec_y$	F_{Score}
Training Phase (70%)					
Absence	93.48	95.56	93.48	96.67	94.51
Presence	96.67	95.08	96.67	93.48	95.87
Average	**95.07**	**95.32**	**95.07**	**95.07**	**95.19**
Testing Phase (30%)					
Absence	95.65	100.00	95.65	100.00	97.78
Presence	100.00	95.74	100.00	95.65	97.83
Average	**97.83**	**97.87**	**97.83**	**97.83**	**97.80**

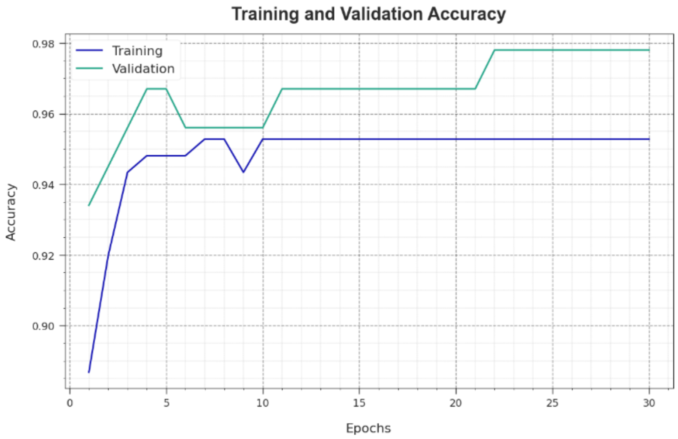

Fig. 9. Accuracy curve of ARODL-BSSHS system on CHD.

Fig. 9 examines the accuracy performance of the ARODL-BSSHS approach within the training and validation phases using the CHD dataset. The results highlight that the ARODL-BSSHS system achieves its highest accuracy values as the epochs progress. Furthermore, the notably superior validation accuracy compared to the training accuracy underscores the efficient learning capacity of the ARODL-BSSHS algorithm on the CHD dataset.

The analysis of loss during both the training and validation stages of the ARODL-BSSHS approach using the CHD dataset is depicted in Fig. 10. The findings suggest that the ARODL-BSSHS algorithm maintains closely aligned values for both training and validation loss. This observation emphasizes the capable learning behavior of the ARODL-BSSHS algorithm on the CHD dataset.

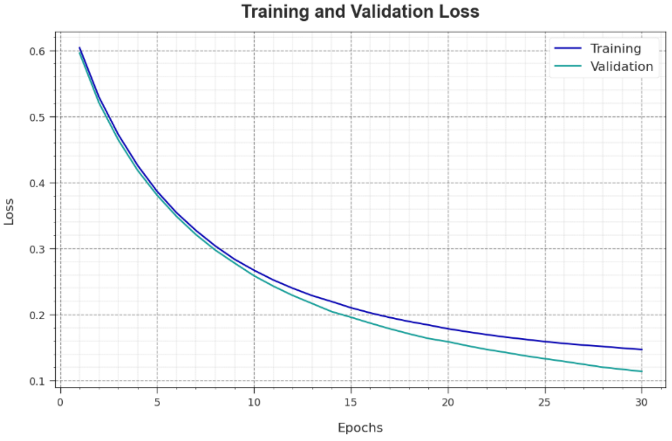

Fig. 10. Loss curve of ARODL-BSSHS system on CHD.

V. Discussion

In Table VII and Fig. 11, the comparative outcome of the ARODL-BSSHS approach is reported in [33][34]. The results implied that the RF algorithm gains worse performance. But, the NB, LR, SMO, AdaBoostM1 + DS, and Bagging + REPTree approaches offer somewhat higher outcomes; the ARODL-BSSHS system demonstrates the other existing models with maximal $accu_y$ of 97.83%, $prec_n$ of 97.87%, $sens_y$ of 97.83%, and F_{score} of 97.80%.

TABLE VII. Comparative Outcome of ARODL-BSSHS Approach With Other Methods on CHD

Classifier	Accuracy	Precision	Sensitivity	Specificity	F-Measure
NB Model	84.49	84.50	84.50	87.00	84.50
LR Model	84.49	84.50	84.50	87.00	84.50
SMO Model	86.14	86.20	86.10	90.00	86.10
AdaBoostM1 + DS	83.83	83.90	83.80	88.00	83.80
Bagging + REPTree	83.83	83.90	83.80	88.00	83.80
RF Model	81.19	81.20	81.20	85.00	81.10
ARODL-BSSHS	97.83	97.87	97.83	97.83	97.80

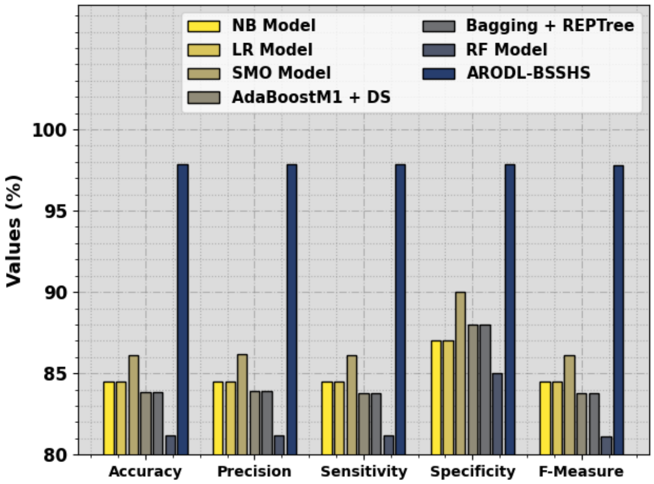

Fig. 11. Comparative outcome of ARODL-BSSHS approach with other methods on CHD.

The CT inspection of the ARODL-BSSHS approach with recent algorithms is reported in Table VII and Fig. 12. The outcomes inferred that the ARODL-BSSHS algorithm reaches a minimal CT of 8.17s. Also, the existing NB, LR, SMO, AdaBoostM1 + DS, Bagging + REPTree, and RF approaches reach maximum CT of 23.20s, 25.10s, 15.90s, 25s, 23.40s, and 20.30s correspondingly. These results analysis assured the better performance of the ARODL-BSSHS technique on the smart healthcare system.

TABLE VIII. CT Outcome of ARODL-BSSHS Approach with Other Methods on CHD

Classifier	Computational Time (sec)
NB	23.20
LR	25.10
SMO	15.90
AdaBoostM1 + DS	25.00
Bagging + REPTree	23.40
RF	20.30
ARODL-BSSHS	08.17

The results of the comparative analysis illustrate the superior efficacy of the ARODL-BSSHS approach in securing healthcare systems over the studied alternative models. It was found that ARODL-BSSHS significantly outperforms other classifiers in terms of accuracy, precision, sensitivity, specificity, and F-measure, achieving a maximum accuracy of 97.83% and a minimal Computational Time (CT) of 8.17s. This implies that the ARODL-BSSHS not only is more accurate in predictions and classifications but also is more efficient, making it a preferable choice for real-time applications in smart healthcare systems. This superior performance of ARODL-BSSHS emphasizes the critical role of sophisticated techniques in addressing the complexity and diversity of healthcare requirements and environments. The increased accuracy and reduced computational time are indicative of its capability to deal with the multifaceted and dynamic nature of healthcare data more effectively and efficiently. The discussed results reinforce the viability and superiority of the ARODL-BSSHS approach in enhancing security and optimizing performance in smart healthcare systems, presenting it as a promising solution for future integrations and developments in healthcare technology.

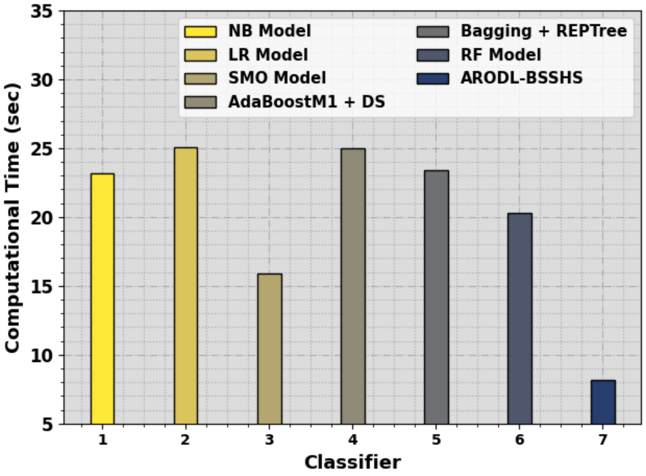

Fig. 12. CT outcome of ARODL-BSSHS approach with other methods on CHD.

VI. Recommendations & Future Works

It is recommended that future research on the ARODL-BSSHS approach should explore its adaptability across diverse sectors like finance, education, and supply chain management. Integration with emerging technologies such as Edge and Quantum Computing and 5G can be crucial to enhance the method's capabilities and to cater to the evolving needs of modern applications. Developing scalable and user-friendly implementations is imperative to ensure broader applicability and user acceptance.

The integration with Edge and Quantum Computing is being explored to optimize computational processes and solve complex problems efficiently [35]. There is also a heightened emphasis on developing robust security and privacy-preserving protocols due to the escalating concerns related to data breaches and cyber-attacks in healthcare systems. The application of Federated Learning and Decentralized AI is gaining traction, addressing the need for decentralized model training and decision-making processes that adhere to data privacy standards. Moreover, the utilization of AI for personalized and predictive healthcare is becoming pivotal, allowing for the development of individualized treatment plans and early detection of diseases.

VII. Conclusion

The ARODL-BSSHS technique has been developed for accomplishing security in the healthcare system in this study. The presented ARODL-BSSHS technique involves the design of secured and smart healthcare system using two major processes, namely intrusion detection and disease diagnosis. To accomplish this, the ARODL-BSSHS technique follows a series of processes: HNN based intrusion detection, ARO based parameter tuning, DELM based disease detection, and HBO based parameter optimization. In addition, the ARODL-BSSHS technique involves BC technology for secure transmission of healthcare data. A widespread experimental analysis is made on benchmark datasets: heart disease and NSL-KDD dataset to ensure the improved results of the ARODL-BSSHS technique. The experimental values highlighted that the ARODL-BSSHS technique obtains better performance than other approaches. In the upcoming years, the performance of the ARODL-BSSHS algorithm can be improved by multimodal DL techniques.

References

[1] Ali et al., "Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography," Sensors, vol. 22, no. 2, p. 528, 2022.

[2] H. Bi, J. Liu, and N. Kato, "Deep learning-based privacy preservation and data analytics for IoT enabled healthcare," IEEE Trans. Ind. Informatics, vol. 18, no. 7, pp. 4798–4807, 2021.

[3] 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. (Ny)., vol. 629, pp. 703–718, 2023.

[4] S. Alam et al., "An Overview of Blockchain and IoT Integration for Secure and Reliable Health Records Monitoring," Sustainability, vol. 15, no. 7, p. 5660, 2023.

[5] R. Nishanthini, B. Srimathi, R. S. Kumaran, and I. Yamuna, "Deep Learning on Healthcare Ecosystem using Blockchain Based Security System," in 2021 IEEE Mysore Sub Section International Conference (MysuruCon), 2021, pp. 352–357.

[6] 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. Informatics, vol. 18, no. 11, pp. 8065–8073, 2022.

[7] M. Z. U. Rahman, S. Surekha, K. P. Satamraju, S. S. Mirza, and A. Lay-Ekuakille, "A collateral sensor data sharing framework for decentralized healthcare systems," IEEE Sens. J., vol. 21, no. 24, pp. 27848–27857, 2021.

[8] M. M. Khubrani and S. Alam, "Blockchain-Based Microgrid for Safe and Reliable Power Generation and Distribution: A Case Study of Saudi Arabia," Energies, vol. 16, no. 16, p. 5963, 2023.

[9] M. M. Khubrani and S. Alam, "A detailed review of blockchain-based applications for protection against pandemic like COVID-19," TELKOMNIKA (Telecommunication Comput. Electron. Control., vol. 19, no. 4, pp. 1185–1196, 2021.

[10] S. Namasudra, P. Sharma, R. G. Crespo, and V. Shanmuganathan, "Blockchain-based medical certificate generation and verification for IoT-based healthcare systems," IEEE Consum. Electron. Mag., vol. 12, no. 2, pp. 83–93, 2022.

[11] S. Alam, "The Current State of Blockchain Consensus Mechanism: Issues and Future Works," Int. J. Adv. Comput. Sci. Appl., vol. 14, no. 8, 2023, doi: 10.14569/IJACSA.2023.0140810.

[12] G. A. Rakib et al., "DeepHealth: A secure framework to manage health certificates through medical IoT, blockchain and deep learning," in 2021 IEEE International Symposium on Medical Measurements and Applications (MeMeA), 2021, pp. 1–6.

[13] H. S. K. Sheth, A. K. Ilavarasi, and A. K. Tyagi, "Deep Learning, blockchain based multi-layered Authentication and Security Architectures," in 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2022, pp. 476–485.

[14] P. W. Khan, Y.-C. Byun, and N. Park, "IoT-blockchain enabled optimized provenance system for food industry 4.0 using advanced deep learning," Sensors, vol. 20, no. 10, p. 2990, 2020.

[15] G. Zhang, X. Zhang, M. Bilal, W. Dou, X. Xu, and J. J. P. C. Rodrigues, "Identifying fraud in medical insurance based on blockchain and deep learning," Futur. Gener. Comput. Syst., vol. 130, pp. 140–154, 2022.

[16] A. Lakhan, M. A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, and N. Kumar, "DRLBTS: deep reinforcement learning-aware blockchain-based healthcare system," Sci. Rep., vol. 13, no. 1, p. 4124, 2023.

[17] S. K. Singh, Y.-S. Jeong, and J. H. Park, “A deep learning-based IoT-oriented infrastructure for secure smart city,” Sustain. Cities Soc., vol. 60, p. 102252, 2020.

[18] E. A. Mantey, C. Zhou, J. H. Anajemba, I. M. Okpalaoguchi, and O. D.-M. Chiadika, “Blockchain-secured recommender system for special need patients using deep learning,” Front. Public Heal., vol. 9, p. 737269, 2021.

[19] 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, 2023.

[20] N. Sammeta and L. Parthiban, “Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model,” Complex Intell. Syst., vol. 8, no. 1, pp. 625–640, 2022.

[21] E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O.-Y. Song, A. K. Bashir, and A. A. Abd El-Latif, “DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems,” IEEE access, vol. 8, pp. 111223–111238, 2020.

[22] S. Purbey, B. Khandelwal, and A. K. Choudhary, “Design of a blockchain-based secure and efficient ontology generation model for multiple data genres using augmented stratification in the healthcare industry,” Signal, Image Video Process., pp. 1–9, 2023.

[23] M. A. Almaiah, A. Ali, F. Hajjej, M. F. Pasha, and M. A. Alohali, “A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things,” Sensors, vol. 22, no. 6, p. 2112, 2022.

[24] S. P. Dash, “An Introduction to Blockchain Technology: Recent Trends,” Recent Adv. Blockchain Technol. Real-World Appl., pp. 1–24, 2023.

[25] S. Alam et al., “Blockchain-Based Solutions Supporting Reliable Healthcare for Fog Computing and Internet of Medical Things (IoMT) Integration,” Sustainability, vol. 14, no. 22, p. 15312, 2022.

[26] S. Alam et al., “Blockchain-based Initiatives: Current state and challenges,” Comput. Networks, vol. 198, p. 108395, 2021.

[27] H. Lin et al., “A review of chaotic systems based on memristive Hopfield neural networks,” Mathematics, vol. 11, no. 6, p. 1369, 2023.

[28] Y. Wang, Y. Xiao, Y. Guo, and J. Li, “Dynamic chaotic opposition-based learning-driven hybrid Aquila Optimizer and artificial rabbits optimization algorithm: framework and applications,” Processes, vol. 10, no. 12, p. 2703, 2022.

[29] S. S. Sammen, M. Ehteram, Z. Sheikh Khozani, and L. M. Sidek, “Binary Coati Optimization Algorithm-Multi-Kernel Least Square Support Vector Machine-Extreme Learning Machine Model (BCOA-MKLSSVM-ELM): A New Hybrid Machine Learning Model for Predicting Reservoir Water Level,” Water, vol. 15, no. 8, p. 1593, 2023.

[30] A. S. Menesy, H. M. Sultan, I. O. Habiballah, H. Masrur, K. R. Khan, and M. Khalid, “Optimal Configuration of a Hybrid Photovoltaic/Wind Turbine/Biomass/Hydro-Pumped Storage-Based Energy System Using a Heap-Based Optimization Algorithm,” Energies, vol. 16, no. 9, p. 3648, 2023.

[31] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the KDD CUP 99 data set,” in 2009 IEEE symposium on computational intelligence for security and defense applications, 2009, pp. 1–6.

[32] J. Andras, S. William, P. Matthias, and D. Robert, “Heart disease. UCI Machine Learning Repository.” 1988.

[33] K. V. V. Reddy, I. Elamvazuthi, A. A. Aziz, S. Paramasivam, H. N. Chua, and S. Pranavanand, “Heart disease risk prediction using machine learning classifiers with attribute evaluators,” Appl. Sci., vol. 11, no. 18, p. 8352, 2021.

[34] A. K. Balyan et al., “A hybrid intrusion detection model using ega-pso and improved random forest method,” Sensors, vol. 22, no. 16, p. 5986, 2022.

[35] M. Shuaib et al., “An Optimized, Dynamic, and Efficient Load-Balancing Framework for Resource Management in the Internet of Things (IoT) Environment,” Electronics, vol. 12, no. 5, p. 1104, 2023