International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V71I2P202

Volume 71 Issue 2, 9-20, February 2023

Original Article

Blockchain Assisted Intrusion Detection and Data Classification on Smart Healthcare Management System

K. Rajeshkumar[1], C. Ananth[2], N. Mohananthini[3]

[1,2]*Department of Computer and Information Science, Annamalai University, Annamalainagar, India.*
[3]*Department of Electrical and Electronics Engineering, Muthayammal Engineering College, Rasipuram, India*

[2]*Corresponding Author : ananth.prog@gmail.com*

Received: 26 July 2022 Revised: 10 January 2023 Accepted: 21 January 2023 Published: 25 February 2023

Abstract *- Blockchain (BC) is a newer technology being applied for making creative solutions in different fields involving healthcare. A Blockchain network is used in the medical field for preserving and exchanging patient datasets through diagnostic laboratories, hospitals, physicians, and pharmaceutical firms. BC application could precisely classify severe and dangerous mistakes in the healthcare sector. Accordingly, it could enhance the transparency, performance, and security of sharing healthcare datasets in the medical system. This technique is useful to healthcare institutions to gain insight and improve the analysis of healthcare records. Therefore, this study focuses on the design of healthcare solutions with BC technology to accomplish security. This study presents a Blockchain Assisted Intrusion Detection and Data Classification on Smart Healthcare Management System (BAIDDC-SHMS). The presented BAIDDC-SHMS technique initially performs intrusion detection using spiral search optimization (SPO) with a deep stacked sparse autoencoder (DSSAE) model. Besides, the BAIDDC-SHMS model involves EfficientNet feature extraction with a softmax (SM) classifier for the medical image classification process. The SPO algorithm was utilized for optimal modification of the hyperparameters of the DSSAE method and thereby raised the intrusion detection efficacy of the DSSAE algorithm. To demonstrate the betterment of the BAIDDC-SHMS model, a wide range of experimental analyses can be conducted, and the outcomes are inspected under different measures. The comprehensive comparison study emphasized the superior performance of the BAIDDC-SHMS algorithm over other approaches.*

Keywords *- Blockchain, Security, Healthcare management, Deep learning, Intrusion detection, Privacy.*

1. Introduction

As far as healthcare is concerned, the emergency of development rises to more incredible speeds. Nowadays, new and advanced technology reinforces the demand for quality health facilities [1]. In this study, Blockchain (BC) plays a crucial part in transforming the healthcare field. Moreover, the landscape of the health mechanism moves towards a patient-centred method concentrating on 2 main aspects: suitable healthcare sources and accessible services at all times [2]. The BC improves healthcare organizations by providing high-quality health facilities and adequate patient care [3,4]. Health Information Exchange was time taking and repetitive process which caused high health industry costs but was rapidly solved by utilizing this technology [5]. Utilizing BC technology, people might participate in health study programs. Also, better studying and sharing data on public welfare would improve treatment for various groups [6]. A centralized database can be utilized for managing the complete healthcare mechanism and organization. Still, many important issues confronted were interoperability, data protection, and sharing in population health management. This specific issue was dependable by utilizing BC [7]. This technology improves integrity, security, interoperability, and data exchange and is realistically updated and accessible when properly applied. Patients and medical staffs need safe and direct means of consulting, recording, and sending data on networks with no safety concerns; therefore, BC technology can be applied to resolve such problems.

The main challenge with these medical data was ensuring its security from several cyber-attacks like unauthorized access and tampering. Thus, to ensure cyber-safety in the healthcare system, there comes a demand for updated and developed Hybrid ID Systems [8]. The common objective of any ID mechanism was to detect, flag, and log or block intrusions assaults by detecting any malicious network acts. Many prevailing realistic software for IDS rule-related methods include signature-based detection, statistical packet analysis, and stateful protocol analysis [9]. Mainly the IDS classification of a request into malicious and benign, benign is a regular request, and malicious is intrusion requests or anomalous. The IDS were also particularly devised for

identifying a particular set of assaults such as DDoS. Since the threats to these data have risen, preventive initiatives and studies for enhancing medical data security were very critical. One viable solution to improve healthcare data security was to utilize BC technology that assures the data's traceability, integrity, and immutability [10]. BC technology was initially introduced in 2008 with the introduction of Bitcoin as a substitute for the prevailing centralized banking and payment structure.

In this study, the researchers provided BC as a decentralized ledger with the ability to save transaction reports in blocks that were sequentially and serially connected. BC functions as a decentralized peer-to-peer network in which the participants (or nodes in the network) perform transactions, mining, and transaction verification, and willing participants contain a copy of the BC saved with them, offering redundancy [11]. In healthcare, applications of BC technology were in the domain of secure medical data storage and log management, data sharing and management, and pharmaceutical supply chain management.

This study presents a Blockchain Assisted Intrusion Detection and Data Classification on Smart Healthcare Management System (BAIDDC-SHMS). The presented BAIDDC-SHMS technique initially performs intrusion detection using spiral search optimization (SPO) with a deep stacked sparse autoencoder (DSSAE) model. Besides, the BAIDDC-SHMS model involves EfficientNet feature extraction with a softmax (SM) classifier for the medical image classification process. The SPO algorithm can be utilized for optimum modification of the hyperparameter of the DSSAE technique and thus raises the intrusion detection efficacy of the DSSAE technique. To demonstrate the betterment of the BAIDDC-SHMS model, a wide range of experimental analyses can take place, and the outcomes are scrutinized under several measures.

2. Literature Review

Nguyen et al. [12] devise a secured IDS with BC-related transmission of information with a classifier algorithm for CPS in the medicinal domain. The proposed technique executes data acquisition processes utilizing sensor array and ID carried out utilizing the deep belief network (DBN) method. Moreover, the formulated algorithm creates multiple shares of the image, which is gathered and accomplishes integrity and reliability. In addition, the BC technology can be implemented to secure data transmission to the cloud server that performs the ResNet-related classifier method for identifying the disease. Alkadi et al. [13] present a Deep BC Framework (DBF) modelled for offering security-related distributed ID and privacy-related BC smart contracts in the cloud. The ID algorithm can use a Bidirectional LSTM (BiLSTM) DL method for dealing with sequential network data.

The author in [14] introduced a BC technology-based Chaotic Deep Generative Adversarial Network (GAN) Encrypting technique. The BCDGE uses BC technology to defend private information and validates the authenticity of the information. The Deep-GAN constitute image specific secret key for enhancing resilience towards hacker; the formed key uses an input for diffusion and confusion stages. The sender transmits the encoded healthcare images to the server, signs the ciphertext ID, and stores them on BC.

Wang et al. [15] modelled a deep multi-scale CNN (DMCNN) for network ID. Various feature levels in a huge volume of high-dimension unlabelled original data were derived by distinct scale convolution kernels. Next, the network structure learning rates can be maximized by batch normalizing approach for optimally acquiring the raw data's feature representations.

In [16], a structure and prototype for secure medical application processing through BC were presented. The devised method employs an optimized Crow search method for ID and meddling data extraction in IoT networks. The method can be processed below deep CNN for detailed analysis and coordination of data security components.

Firdaus et al. [17] suggest leveraging the bio-inspired technique of PSO that automatically chooses the exclusive features which have the new android debug bridges (ADBs). This work even adopts boosting (multiboost, adaboost, logitboost, and realadaboost) for enhancing the ML estimation, which identifies unidentified root exploit, and analyzed 3 categories of features incorporating code-based, a system command, and directory path.

Udayakumar and Rajagopalan [18] introduce a BC-enabled secure image transmission and diagnosis (BESITD) for the MCPS atmosphere. The BESITD method includes an image acquisition process allowing wearable gadgets to capture healthcare images. After that, the proposed algorithm performs an ID system utilizing RNN to determine the existence of intruders in MCPS. Also, the block-wise encrypting procedure occurs where the healthcare image can be divided into n blocks, each individually encoded using the sign encryption method.

Using various DL and ML algorithms for the classification of diseases available in this literature, it is still necessary to increase the accuracy of the classification. The hyperparameters encompassing epoch count, batch size and learning rate selection are critical to obtaining effective outcomes. In the meantime, the trial and error approach for hyperparameter tuning is erroneous and tedious work, metaheuristic approaches can be employed. Thus, the study used employed the SPO technique for the variable selection of the DSSAE algorithm.

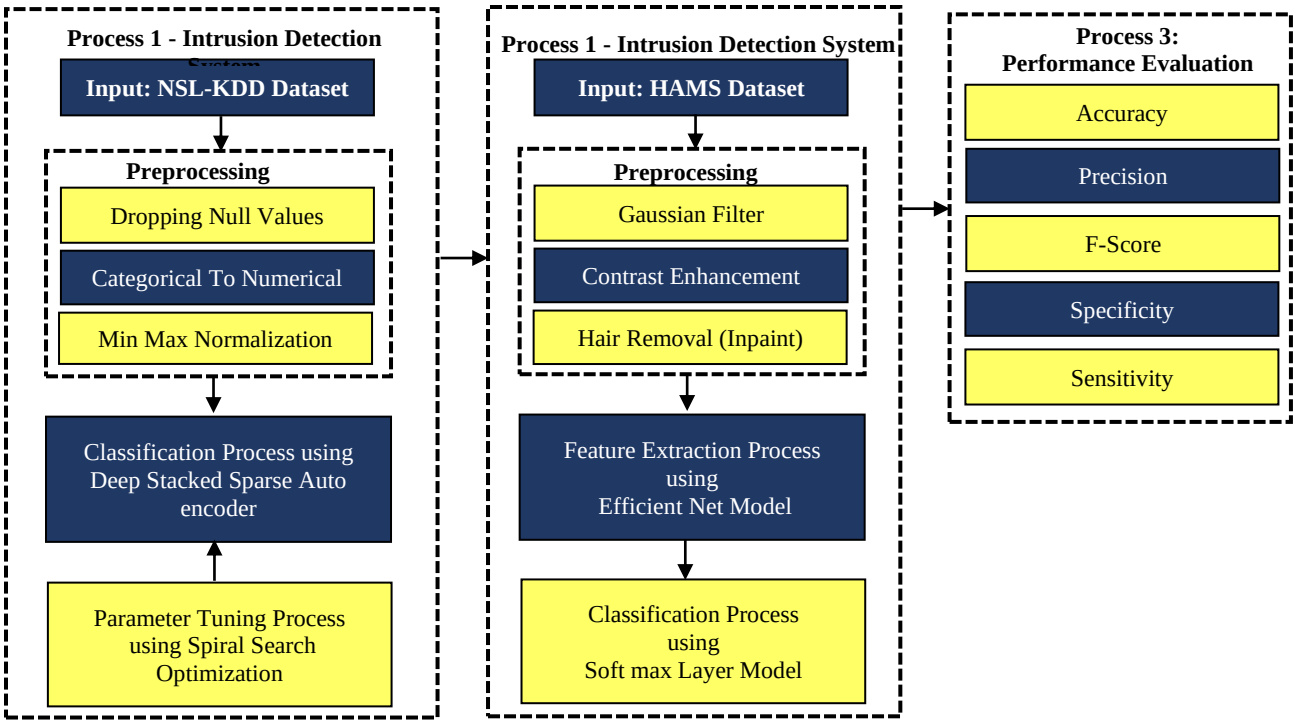

Fig. 1 The Working process of the BAIDDC-SHMS algorithm

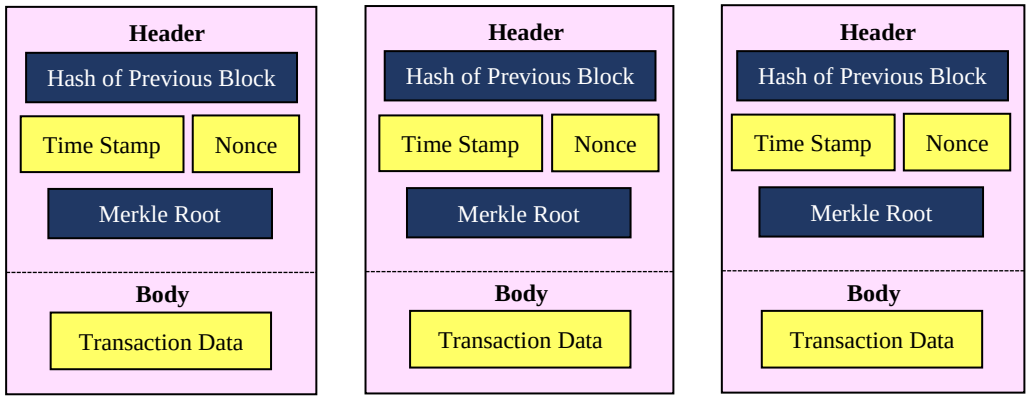

Fig. 2 Structure of Blockchain

3. The Proposed Healthcare Management System

An effective BAIDDC-SHMS algorithm is projected for intrusion detection and data classification in the medical sector. The BAIDDC-SHMS technique follows two major processes, namely intrusion detection and data classification. In the first stage, the BAIDDC-SHMS technique employed SPO with a DSSAE-based intrusion detection process where the hyperparameter of the DSSAE technique is tuned with the help of the SPO technique. Next, in the second stage, the image classification process is carried out via the EfficientNet feature extractor and SM classifier. Fig. 1 depicts the working process of the BAIDDC-SHMS algorithm.

3.1. Stage I: Blockchain Technology

This study uses BC technology to enable secure medical data transmission. The BC is a group of blocks, where each block is encompassed 4 portions such as transaction information (Ethereum and bitcoin), timestamp, existing block, and the hash value of the current block [19]. BC technology is a shared digital ledger exploited to store transactions in dissimilar methods. Therefore, the intruder records could not adapt as every block comprised cryptographical values of the existing block. Fig. 2 demonstrates the architecture of the BC technique. In the BC technique, every transaction was signed cryptographically via hash values and authenticated through a miner. It comprises a repetitive parameter of blocks and the whole ledger of each transaction. BC allows the distribution of the

dataset's ledger in a safe, decentralized, trusted, and collective method. Decentralized storage was a kind of BC that saves the maximal dataset interconnected to former and current blocks with smart contract code. For the decentralized data, SiacoinDB, LitecoinDB, Swarm, BigchainDB, IPFS, MoneroDB, etc., are exploited. The Interplanetary File System (IPFS) is described by the shared, Point to Point, and decentralized databases that have been connected and forward typical files. IPFS can be significantly saved that was applied by a BC technique for IoT function to obtain the highest throughput.

3.2. Stage II: Intrusion Detection

For intrusion detection, the BAIDDC-SHMS technique employed SPO with the DSSAE model. The AE attempt to attain the approximate value of the input in the hidden layer for ideally reproducing the input in the output layers [20]. The neurons in the first two layers complete the encoding process, and the last two complete the decoding process. Using the backpropagation mode, many key features of the input dataset are learned unsupervised by minimalizing the reconstructed error. The process of encoding and decoding is given in the following:

$$H = f_1(W_1 X + b_1) \tag{1}$$

$$X' = f_2(W_2 H + b_2) \tag{2}$$

Here, f_1 and f_2 denote the activation function of every layer, X and X' indicates the input and output components, H represents the hidden component, W_1 and W_2 show the weight matrixes among the neurons of all the layers, and b_1, b_2 indicates the bias of every layer.

Even though AE could ideally regenerate the input dataset in the output, the AE does not efficiently extract significant features by only copying the input to the hidden layers. The SAE, as an extension of AE, cause the AE to learn reasonably sparse feature by presenting a sparsity restriction. Sparsity is a property in that most neurons in the AE's hidden state are suppressed. In this work, the activation function $f(x) = (1 + e^{-x})^{-1}$, such as a sigmoid function, maps the output from the range of $(0,1)$. Consequently, if the output of the hidden layer is closer to zero, then it is considered in an inhibitory state, and the SAE can be constructed. At the same time, sparsity limitation is imposed on AE, and mostly hidden layers are in an inhibitory state. These conditions might enhance the conventional AE's efficiency and improve it.

While the output regenerates the input, the mean square error is employed for constructing the loss function. The unsupervised training on the SAE is performed by minimalizing the loss function.

$$J(w, b) = \frac{1}{2} ||X' - X||^2 \tag{3}$$

To accomplish the sparsity constraints, the average activation degree of $i\text{-}th$ neurons in the hidden layer is determined by

$$\hat{p}_i = \frac{1}{n} \sum_{j=1}^{n} h_i (\chi_j) \tag{4}$$

Here, n characterizes the neuron count in the input state. For making the activation degree of most neurons in the hidden layer tends to zero, sparse variables ρ closer to zero are presented, with $\widehat{p_i} = \mathrm{p}$. In the meantime, a penalty factor is presented based on relative entropy to the discount case with huge variations among $\widehat{p_i}$ and ρ.

$$KL(\widehat{p_i} || \rho) = \rho \log \frac{\rho}{\widehat{\rho_i}} + (1 - \rho) \log \frac{1 - \rho}{1 - \widehat{\rho_i}} \tag{5}$$

The penalty factor rises with the variance among $\widehat{\rho_i}$ and p, and the value is zero if $\widehat{\rho_i} = \rho$. The overall loss function for the SAE can be attained by

$$J_s(W, b) = J(W, b) + \beta \sum_{i=1}^{m} KL\,(\widehat{\rho_i} || \rho) \tag{6}$$

In Eq. (6), m denotes the neuron count in the hidden layer, and the network weight coefficients W and b are attained by minimalizing the loss function to acquire the optimum formula for the input dataset. The SAE could decrease the dimension of complicated signals without losing features. In this work, the DSSAE method is designed by stacking together to create a strong deep mechanism. Every DSSAE took its input from the activation of the preceding layer and pre-trained individually. The objective of pre-training is to enhance similar objectives to put the parameter of each layer in a region.

The SPO technique was leveraged to set the optimal hyperparameter values of the DSSAE method. The SPO algorithm is a new metaheuristic optimization method stimulated by spiral phenomena [21]. The presented model uses a multifold spiral model where the searching technique follows the logarithmic spiral path towards the focal point. The succeeded focal point is related to the locally optimal solution and is updated continuously if the best solution is obtained. The SPO technique is intended for a complicated n-dimension problem that involves a hybrid mechanism from a step rate and a rotation matrix. The objective is to construct a multiobjective SPO with the optimal setting for the rotation matrix, and the step rate converges to a stationary location as an optimum candidate solution. The SPO algorithm $x(k) \in \mathbb{R}^n$ is from a primary location, which converges to x^* as a center using a logarithmic spiral trajectory.

$$x(i + 1) = \chi^* + r\varphi(\alpha)(x(i) - x^*)(i = 0,1,2, \dots) \tag{7}$$

In Eq. (7), $\alpha \in [-\pi, \pi]$ and step level among $x^*$and$x(i)$ was indicated as r, and $\varphi(\alpha)$ is the rotation matrix.

$$\varphi(\alpha) = (-1)^{\beta}\varphi_{i_1 j_1}(\alpha) \times \cdots \times \phi\varphi_{i_\tau j_\tau}(\alpha), \beta \in \{0,1\} \quad (8)$$

$$\varphi_{i_{ljl}}(\alpha) = \begin{matrix} \\ i_l \\ j_l \\ \\ \end{matrix}\begin{bmatrix} l & 0 & 0 & 0 \\ 0 & cos(\alpha) & -sin(\alpha) & 0 \\ 0 & sin(\alpha) & cos(\alpha) & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (9)$$

Where $l = \{1, \cdots, \tau\}$.

The two entities highlighted in the SPO model that is diversification and intensification. Intensification refers to performing and exploring deeper exploration, whereas the factor that conducts the global searching process is named diversification.

The presented technique is demonstrated in Algorithm 1; a critical factor is developed that the hybrid rotation matrix is fixed as $\varphi(\alpha)$, and the step rate is used as $r(k)$ where k represents maximal iteration in the SPO model.

The search performance of Algorithm 1 depends on setting the initial positions $x_i(0)$, the composite rotation matrix (θ), and the step rate $r(k)$. Accurately, the SPO approach described is unassured for convergence towards a static point. The SPO method is derivative from the direct searching technique that converges towards the fixed location.

Then, add a finite search vector to the present optimal location to obtain a good result. At a minimum, one vector direction is reduced, and the size of the target search vector goes down with the search fail condition.

The SPO method derives a fitness function from attaining better classification accuracy and also determines a positive value to represent the candidate solution. The decline of the classification error rate is regarded as the fitness function.

Algorithm 1: Pseudocode of SPO Algorithm

1. Set the initial parameters: The rotation matrix$\varphi(\alpha)$, The step rate (k), the location of the search point with objective function value, The condition satisfied, $k_c = \min\{\text{argmin}(f(x(k)))\}$
2. Define the center of the position x^*
3. Define step rate based on setting rule
4. Upgrade search location with $\mathrm{x(i+1)} = \mathrm{x^*} + \mathrm{r\varphi(\alpha)(x(i) - x^*)}$
5. Upgrade centre location

$$x^*(i+1) =, \begin{cases} x_{i_b}(i+1) f\left(\mathrm{x}_{k_c}(i+1)\right) < f(x^*(i)) \\ x^*(i) \qquad\qquad o, w \end{cases}$$

6. Return to step 3, if the end criteria are not met

$$fitness(x_i) = ClassifierErrorRate(x_i) = \frac{No.of\ misclassified\ samples}{Total\ No.of\ samples} * 100 \quad (10)$$

3.3. Stage III: Medical Data Classification

The BAIDDC-SHMS technique uses the EfficientNet feature extractor and SM classifier for medical image classification in this study. DL comprises various interconnected layers with weights and different activation functions. The convolution, connected, and pooling layers are the fundamental DL models. Different activation functions are used to alter the weight. The activation function generates feature maps that are input into the subsequent layer. Pooling and Convolutional layers are used for the feature extracting. This layer is utilized for the visual extraction feature and to understand the complicated nature of an image. The neuron weight of the CNN layer is updated after every epoch in the training stage. For tuning and training, a deep network requires massive data. However, finding the local minima for the cost function becomes a challenge for smaller datasets, resulting in over-fitting.

Consequently, the pre-trained module established the weight. The pre-trained model applied in this work is discussed in the following. By scaling down the model equally in each 3D, such as resolution, depth, and width, EfficientNet accomplishes good outcomes [22]. There exist 7 modules between B0 and B6; the parameter count does not increase, but the model accuracy increase. EfficientNet B0 is the model where each succeeding EfficientNet model is formed. The scaling dimension of a CNN is resolution, depth, and breadth. The multiple layers within a network define the depth corresponding to the breadth. The image resolution transported to the CNN is represented as resolution. EfficientNet uses an effective and simple scaling model as a compound coefficient for equally scaling resolution, depth, and breadth of the network, as follows.

$$Depth, d = \alpha\ \phi\ , \alpha \geq 1,$$
$$Width, w = \beta\ \phi\ , \beta \geq 1;$$
$$Resolution, r = \gamma\ \phi\ , \gamma \geq 1;$$

Here, $\alpha, \beta, and\ \gamma$: denotes constant and are defined by the abovementioned model.

At the final layer of the EfficientNet model, the SM classifier is exploited to allocate proper class labels. In the previous method, what was eventually attained was the feature value of $x^{(i)}$. But in the prediction of input variables, there is a need to classify output and add a $softmax$ classifier to the output layer for organizing the learned features. The graphical illustration of the SM classifier [23]. The marked training sets $\{(\mathrm{x}^{(1)}, \mathrm{y}^{(1)}), (\mathrm{x}^{(2)}, \mathrm{y}^{(2)}), (\mathrm{x}^{(\mathrm{m})}, \mathrm{y}^{(\mathrm{m})})\}$, amongst $y^{(j)} \in \{1,2,\ldots,k\}$ demonstrative training samples $x^{(i)}$ is k. The given test input $x^{(i)}$, is the classifier method that estimates the probability that belongs to every class.

Therefore, to a sample subset with k types, output k-dimension vectors to characterize the probability vector. The

$j\text{-}th$ component in the likelihood vector symbolizes the possibility of belonging to the $j\text{-}th$ class, and the sum of the value of the element is 1. Especially the hypothesis function $h_\theta(x)$ is illustrated by

$$h_\theta\left(x^{(i)}\right)\begin{bmatrix} p\left(y^{(i)}=1\middle|x^{(i)};\theta\right) \\ p\left(y^{(i)}=2\middle|x^{(i)};\theta\right) \\ \vdots \\ p\left(y^{(i)}=k\middle|x^{(i)};\theta\right) \end{bmatrix} \quad (11)$$

$$= \frac{1}{\sum_{j=1}^{k} e^{\theta_j^T x(i)}} \begin{bmatrix} e^{\theta_1^T x^{(i)}} \\ e^{\theta_2^T x^{(i)}} \\ \vdots \\ e^{\theta_k^T x^{(i)}} \end{bmatrix} = \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_k \end{bmatrix}.$$

Amongst $\theta_1, \theta_2, \theta_3, \ldots, \theta_k$ are network model parameters as follows

$$\theta = \begin{bmatrix} -\theta_1^T - \\ -\theta_2^T - \\ \vdots \\ -\theta_k^T - \end{bmatrix}, \frac{1}{\sum_{j=1}^{k} e^{\theta_j^T x^{(i)}}} \quad (12)$$

This item primarily limits the likelihood value from zero to one, where the sum of the probability value is 1.

In Eq. (11), the probability of sample $x^{(i)}$ output by the classifier belonging to a $j\text{-}th$ category is $(1\{true\} = 1, 1\{false\} = 0)$:

$$p\left(y^{(i)}=j\middle|x^{(i)};\theta\right) = \frac{e^{\theta_j^T x^{(i)}}}{\sum_{j=1}^{k} e^{\theta_j^T x^{(i)}}} = p_1 = \prod_{j=1}^{k} p_j^{1\{y^{(i)}=j\}}. \quad (13)$$

The probability function respective to the training sample is

$$L(\theta) = \prod_{i=1}^{m} p\left(y^{(i)}=j\middle|x^{(i)};\theta\right) = \prod_{i=1}^{m}\prod_{j=1}^{k} p_j^{1\{y^{(i)}=j\}},$$

$$l(\theta) = \log L(\theta) = \sum_{i=1}^{m}\sum_{=1}^{k} 1\{y^{(i)}=j\} \log\left(p_j\right)$$

$$= \sum_{i=1}^{m}\sum_{=1}^{k} 1\{y^{(i)}=j\} \log\left(\frac{e^{\theta_j^T x^{(i)}}}{\sum_{l=1}^{k} e^{\theta_l^T x^{(i)}}}\right). \quad (14)$$

The variable θ maximizes the probability function as the optimum parameter of the $softmax$ classification. The cost function of $the\ softmax$ regression method is represented as follows

$$J(\theta) = -\frac{1}{m}\left[\sum_{i=1}^{m}\sum_{=1}^{k} 1\{y^{(i)}=j\} \log\left(\frac{e^{\theta_j^T x^{(i)}}}{\sum_{l=1}^{k} e^{\theta_l^T x^{(i)}}}\right)\right]. \quad (15)$$

By using the gradient descent model, the cost function is minimalized, as expressed by Eq. (16):

$$\nabla_{\theta_j} J(\theta) = -\frac{1}{m}\left[\sum_{i=1}^{m} x^{(i)}\left(1\{y^{(i)}=j\} - p\left(y^{(i)}=j\middle|x^{(i)};\theta\right)\right)\right] \quad (16)$$

The softmax classifiers have unusual features: it has a "redundant" set of variables. To demonstrate the feature, when the vector μ was subtracted from the variable vector θ_j, every θ_j become $\theta_j - \mu(j = 1,2,,k)$ as follows

$$p(y^{(i)}=j|x^{(i)};\theta) = \frac{e^{(\theta_j-\iota u)^T x^{(i)}}}{\sum_{l=1}^{k} e^{(\theta_l-\iota u)^\tau x^{(i)}}}$$

$$= \frac{e^{\theta_j^\tau x^{(i)}} e^{-\mu^T x^{(i)}}}{\sum_{l=1}^{k} e^{(\theta_l-\iota u)^\tau x^{(i)}} e^{-\mu^T x^{(i)}}} \quad (17)$$

Now, $\theta_j - \mu$ and θ_j parameters gain a similar outcome. In other words, if θ_j is the optimum variable, $\theta_j - \mu$ might have a similar effect. It is the drawback of having redundant variables in the $softmax$ classification. The loss function of $softmax$ classification is specifically non-convex. Even though there exists a minimal point, the minimum value is in a "flat" space and not at a single point. Specifically, each point in the region could obtain a minimal value. To make the cost function a strictly convex function, it is necessary to add a weight attenuation term in the following:

$$J(\theta) = J(\theta) + \frac{\lambda}{2}\sum_{i=1}^{m}\sum_{=1}^{k} \theta_{ij}^2, \quad (18)$$

$$\nabla_{\theta_j} J(\theta) = \nabla_{\theta_j} J(\theta) + \lambda\theta_j.$$

4. Results and Discussion

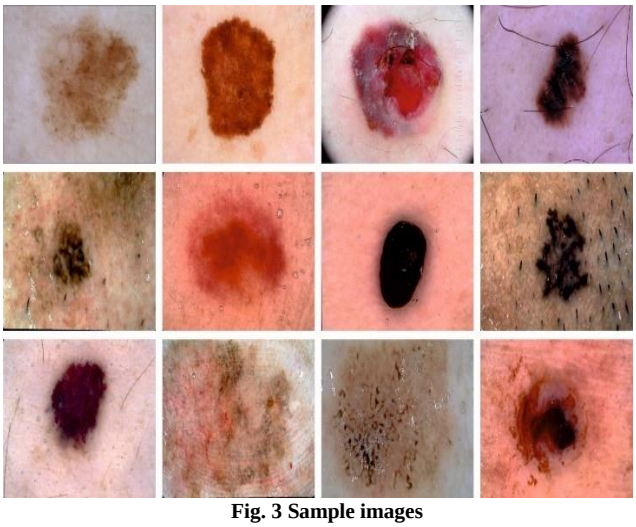

Fig. 3 Sample images

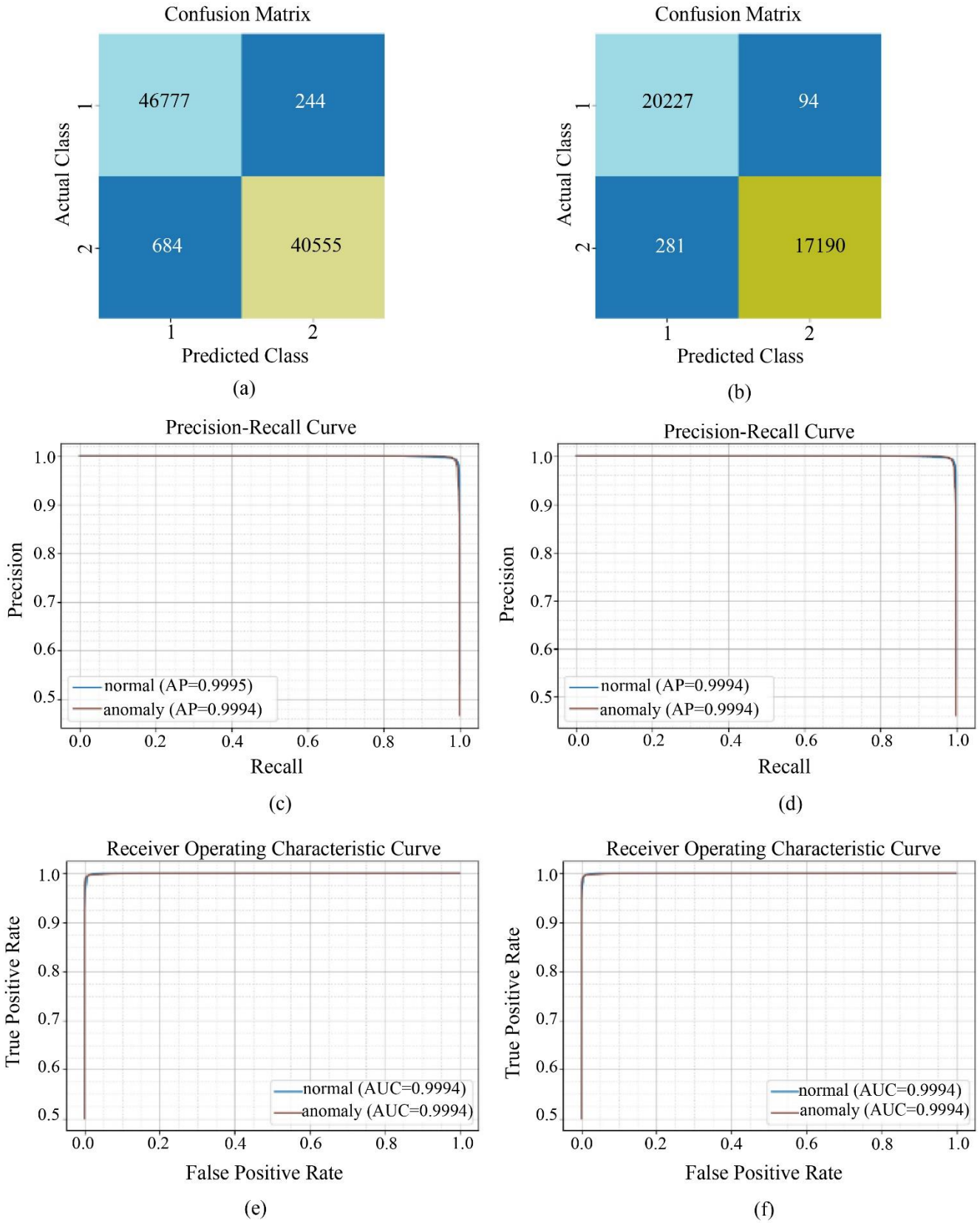

Fig. 4 Classification analysis of BAIDDC-SHMS method under NSL-KDD dataset (a-b) Confusion matrices, (c-d) Precision-recall curve, (e-f) ROC curve

The experimentation study of the BAIDDC-SHMS method takes place using two aspects, namely intrusion detection and image classification. Initially, the intrusion detection outcomes of the BAIDDC-SHMS model are tested using the NSL-KDD datasets [24]. Test images used for simulation are illustrated in Fig. 3.

Fig. 4 provides the overall results offered by the BAIDDC-SHMS approach on the NSL-KDD dataset. Fig. 4a indicates the confusion matrix of the BAIDDC-SHMS model on the TR data. Similarly, Fig. 4b implies the confusion matrix given by the BAIDDC-SHMS system on the TS data. Figs. 4c-4d demonstrates the precision-recall curve analysis of the BAIDDC-SHMS approach under test data.

The figure shows that the BAIDDC-SHMS model has established maximum precision-recall performance under all datasets. Figs. 4e-4f demonstrates the ROC curve analysis of the BAIDDC-SHMS approach under test data. The results indicated that the BAIDDC-SHMS method displayed its capability to classify all classes on the testing dataset.

Table 1 and Fig. 5 report the medical image classification results of the BAIDDC-SHMS approach. The experimental values denoted by the BAIDDC-SHMS algorithm have gained enhanced performance on training (TR) and testing (TS) datasets. For example, on the TR dataset, the BAIDDC-SHMS approach has presented $accu_y$, $pren_c$, $sens_y$ andF_{score} of 99.04%, 99.06%, 99.01, and 99.03%, correspondingly. Additionally, on TS data, the BAIDDC-SHMS approach has granted $accu_y$, $pren_c$, $sens_y$, and F_{score} of 99.01%, 99.04%,98.96 and 99% correspondingly.

The TAC and VAC attained through the BAIDDC-SHMS method on the NSL-KDD dataset are demonstrated in Fig. 6. The stimulation outcomes denoted by the BAIDDC-SHMS methodology have gained the greatest values of TAC and VAC. Predominantly the VAC is higher than TAC.

The TLOS and VLOSreached using the BAIDDC-SHMS technique in the NSL-KDD dataset are demonstrated in Fig. 7. The stimulation analysis outcomes demonstrated that the BAIDDC-SHMS approach had obtained the least values of TLOS and VLOS. Especially, the VLOS is lower than TLOS.

Table 1. Result analysis of BAIDDC-SHMS methodology with various measures under the NSL-KDD dataset

Metrics	Training Set	Testing Set
Accuracy	99.04	99.01
Precision	99.06	99.04
Sensitivity	99.01	98.96
F-Score	99.03	99.00

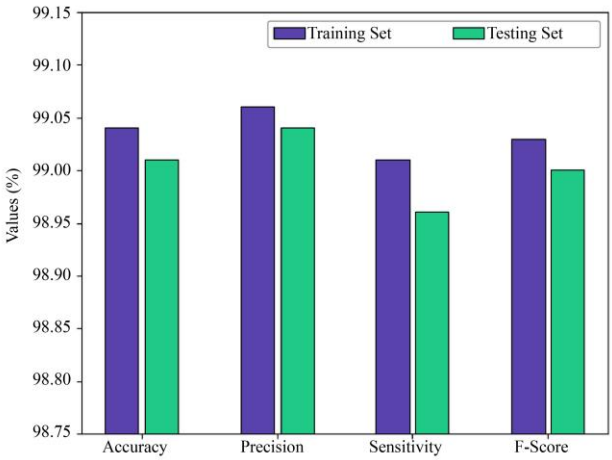

Fig. 5 Result in the analysis of the BAIDDC-SHMS method under the NSL-KDD dataset

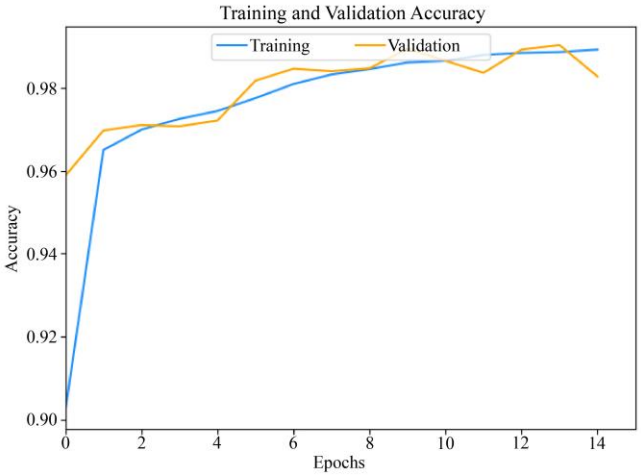

Fig. 6 TAC and VAOutcomes of BAIDDC-SHMS approach on the NSL-KDD database

Table 2. Comparative analysis of the BAIDDC-SHMS method with existing methodologies under the NSL-KDD dataset

Methods	Accuracy
BAIDDC-SHMS	0.994
DBN Model	0.990
DNN-SVM Model	0.920
Genetic-Fuzzy	0.965
FCM Clustering	0.953
GB Model	0.843

Table 2 and Fig. 8 offer comprehensive intrusion detection outcomes of the BAIDDC-SHMS with existing approaches. The results implied that the GB method had reported a lower $accu_y$ of 0.843. Following, the DNN-SVM method has shown a slightly enhanced$accu_y$of 0.920. Next, the genetic-fuzzy and FCM techniques have depicted reasonable $accu_y$ of 0.965 and 0.953 correspondingly. Though the DBN model has resulted in a near-optimal $accu_y$ of 0.990, the BAIDDC-SHMS model has exhibited a maximum $accu_y$ of 0.990.

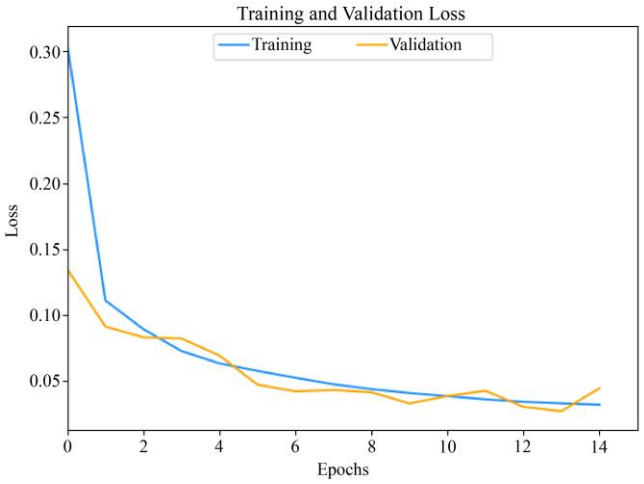

Fig. 7 TLOS and VLOS outcomes of the BAIDDC-SHMS method in the NSL-KDD dataset

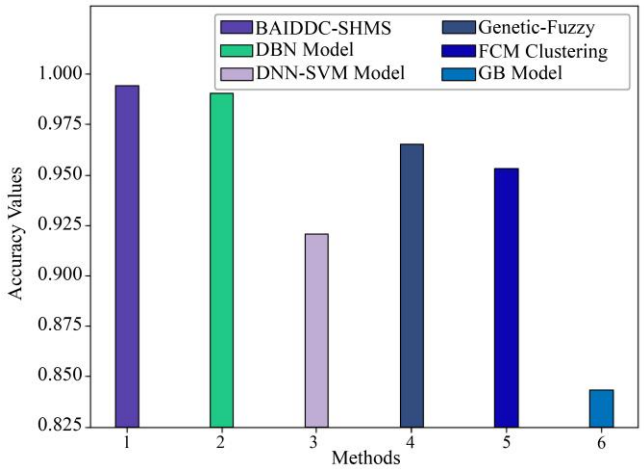

Fig. 8 Comparative analysis of BAIDDC-SHMS approach under the NSL-KDD dataset

Next, the medical image classification outcomes of the BAIDDC-SHMS model are tested using the ISIC dataset [25].

Fig. 9 provides the overall results rendered by the BAIDDC-SHMS method on the ISIC dataset. Fig. 9a indicates the confusion matrix of the BAIDDC-SHMS model on the TR data. Similarly, Fig. 9b implies the confusion matrix provided by the BAIDDC-SHMS technique on the TS dataset. Figs. 9c-9d demonstrates the precision-recall curve analysis of the BAIDDC-SHMS approach under test data. By observation, it is noted that the BAIDDC-SHMS method has established maximum precision-recall performance under all datasets. Figs. 9e-9f demonstrates the ROC curve analysis of the BAIDDC-SHMS approach under test data. The results indicated that the BAIDDC-SHMS model had demonstrated its capacity to categorize all classes on the test dataset.

Table 3 and Fig. 10 report the medical image classification outcomes of the BAIDDC-SHMS method under the ISIC dataset. The experimental values denoted by the BAIDDC-SHMS model have attained enhanced performance on both TR data and TS data. For example, on TR data, the BAIDDC-SHMS method has presented u_y, $sens_y$, and $spec_y$ of 98.58%, 95.05%, and 99.20% correspondingly. Besides, on TS data, the BAIDDC-SHMS model has provided $accu_y$, $sens_y$, and $spec_y$ of 98.51%, 95.87%, and 99.15% correspondingly.

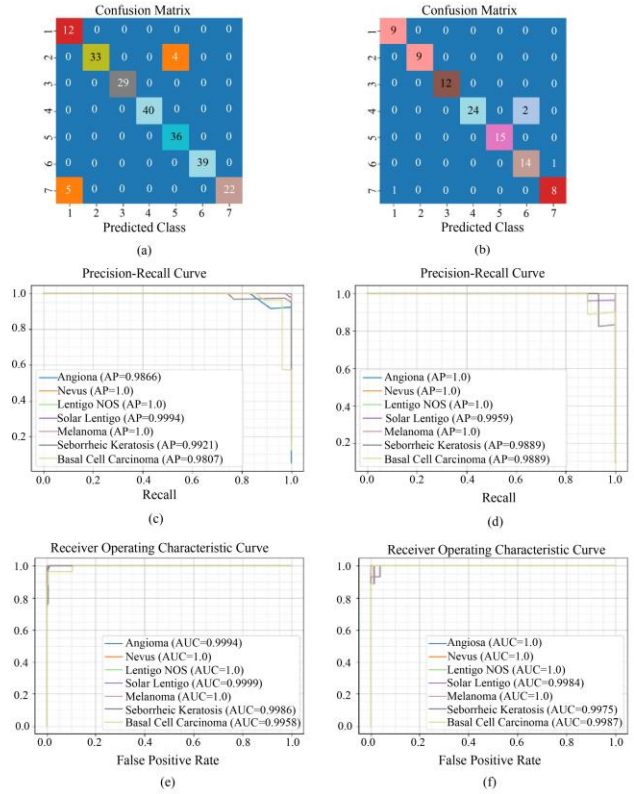

Fig. 9 Classification analysis of BAIDDC-SHMS approach under ISIC dataset (a and b) Confusion matrices, (c and d) Precision-recall curve, (e and f) ROC curve

Table 3. Medical image classifier outcome of BAIDDC-SHMS method with various measures on ISIC dataset

Metrics	Training Set	Testing Set
Accuracy	98.58	98.51
Sensitivity	95.05	95.87
Specificity	99.20	99.15

The TAC and VAC obtained by the BAIDDC-SHMS method in the ISIC dataset are demonstrated in Fig. 11. The stimulation outcomes represented by the BAIDDC-SHMS methodattainedthe greatest values of TAC and VAC. Especially, the VAC is higher than TAC.

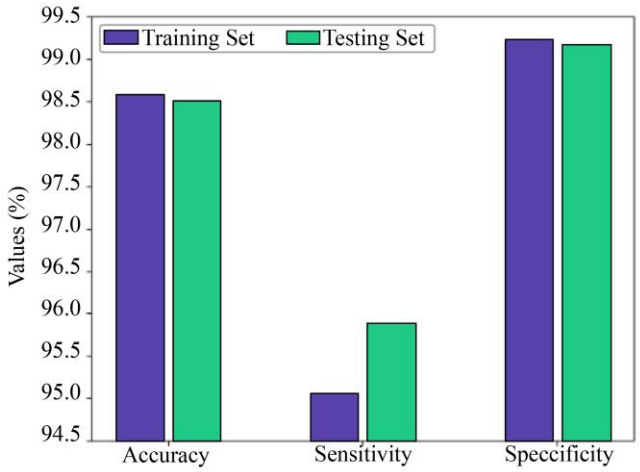

Fig. 10 Result in the analysis of the BAIDDC-SHMS method under the ISIC dataset

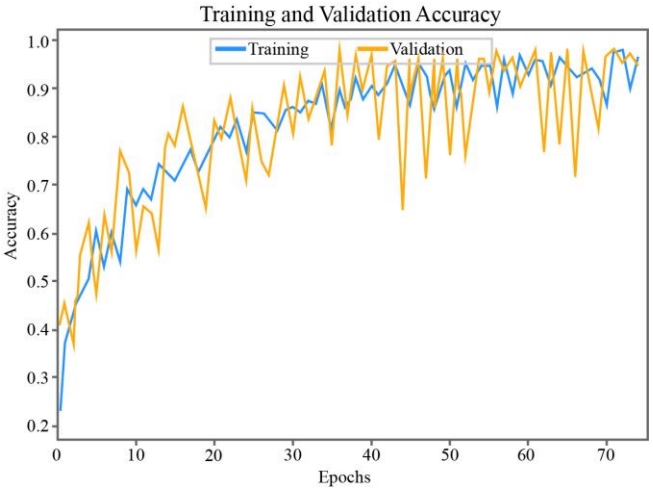

Fig. 11 TAC and VAC outcome of BAIDDC-SHMS method on ISIC dataset

The TLOS and VLOS achieved by the BAIDDC-SHMS approach on the ISIC dataset are portrayed in Fig. 12. The stimulation outcomes represented by the BAIDDC-SHMS method have established minimum values of TLOS and VLOS. Especially, the VLOS is lower than TLOS.

Table 4 and Fig. 13 exhibits the comparative image classification outcomes of the BAIDDC-SHMS method with other DL methods [12]. The stimulation outcomes reported that the BAIDDC-SHMS method had shown improved performance over other DL techniques. For example, concerning $accu_y$, the BAIDDC-SHMS method has provided a maximum$accu_y$ of 0.9851 whereas the CNN-ResNet 101, VGG-19, and ResNet-50 methods have obtained lower $accu_y$ of 0.9490, 0.8120, and 0.7550 correspondingly. Also, concerning $sens_y$, the BAIDDC-SHMS technique has attained a maximum$sens_y$ of 0.9587 while the CNN-ResNet 101, VGG-19, and ResNet-50 techniques have gained lower $sens_y$ of 0.9610, 0.9500, and 0.9000 correspondingly. Additionally, concerning $spec_y$, the BAIDDC-SHMS approach has rendered a higher $spec_y$ of 0.9915 whereas the CNN-ResNet 101, VGG-19, and ResNet-50 techniques have gained lower $spec_y$ of 0.9800, 0.6800, and 0.6100 correspondingly.

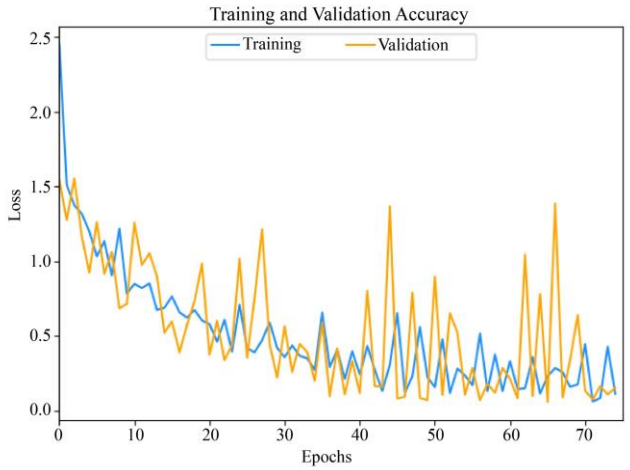

Fig. 12 TLOS and VLOS outcomes of BAIDDC-SHMS method on ISIC database

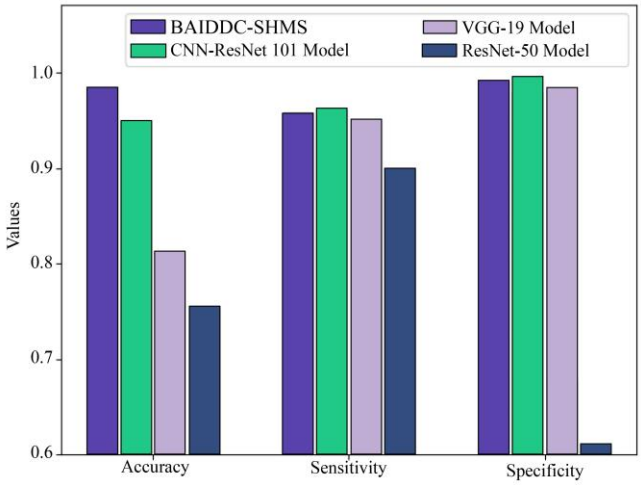

Fig. 13 Comparative analysis of BAIDDC-SHMS method with existing approaches

The comprehensive results and discussion show that the BAIDDC-SHMS model has ensured effectual and secure medical data management.

Table 4. Comparative analysis of BAIDDC-SHMS method with existing approaches

Methods	$Accu_y$	$Sens_y$	$Spec_y$
BAIDDC-SHMS	0.9851	0.9587	0.9915
CNN-ResNet 101 Model	0.9490	0.9610	0.9800
VGG19 Model	0.8120	0.9500	0.6800
ResNet50 Model	0.7550	0.9000	0.6100

5. Conclusion

A new intrusion detection using the BAIDDC-SHMS algorithm has been developed for the medical domain. The proposed BAIDDC-SHMS technique follows two major processes, namely intrusion detection and data classification. In the first stage, the BAIDDC-SHMS technique employed SPO with a DSSAE-based intrusion detection process where the hyperparameter of the DSSAE method is tuned with the help of the SPO technique. Next, the image classification process can occur via the EfficientNet feature extractor and SM classifier in the second stage. The SPO technique was utilized for the optimal modification of the hyperparameters of the DSSAE model and thereby raises the intrusion detection efficacy of the DSSAE approach. A wide range of experimental analyses was executed to demonstrate the betterment of the BAIDDC-SHMS model, and the outcomes are inspected under various measures. The comprehensive comparison study demonstrated the superior performance of the BAIDDC-SHMS algorithm over other approaches. In the future, the presented model can be extended into the IoT-enabled cloud computing environment to enable remote healthcare monitoring systems.

References

[1] Mohan Krishna, and Amit Kumar Tyagi, "Intrusion Detection in Intelligent Transportation System and Its Applications Using Blockchain Technology," *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), IEEE*, pp. 18, 2020. *Crossref*, https://doi.org/10.1109/ic-ETITE47903.2020.332

[2] Ananth, C., Karthikeyan, M., and Mohananthini. N, "A Secured Healthcare System Using Private Blockchain Technology," *Journal of Engineering Technology*, vol. 6, no. 2, pp. 42-54.

[3] Sujith Samuel Mathew et al., "Integration of Blockchain and Collaborative Intrusion Detection for Secure Data Transactions in Industrial IoT: A Survey," *Cluster Computing*, vol. 25, pp. 4129-4149, 2022. *Crossref*, https://doi.org/10.1007/s10586-022-03645-9

[4] Mohammad Dawood Momand, Dr Vikas Thada, and Mr. Utpal Shrivastava, "Intrusion Detection System in IoT Network," *SSRG International Journal of Computer Science and Engineering* , vol. 7, no. 4, pp. 11-15, 2020. *Crossref*, https://doi.org/10.14445/23488387/IJCSE-V7I4P104

[5] Mohananthini, N, Ananth, C, and Parvees, M.Y. Mohamed, "Secured Different Disciplinaries in Electronic Medical Record Based on Watermarking and Consortium Blockchain Technology," *KSII Transactions on Internet and Information Systems (TIIS),* vol. 16, no. 3, pp. 947-971, 2022. *Crossref*, https://doi.org/10.3837/tiis.2022.03.011

[6] Osama Alkadi, Nour Moustafa, and Benjamin Turnbull, "A Review of Intrusion Detection and Blockchain Applications in the Cloud: Approaches, Challenges and Solutions," *IEEE Access*, vol. 8, pp.104893-104917, 2020. *Crossref*, https://doi.org/10.1109/ACCESS.2020.2999715

[7] Wenjuan Li et al., "Toward a Blockchain-Based Framework for Challenge-Based Collaborative Intrusion Detection," *International Journal of Information Security*, vol. 20, pp. 127-139, 2021. *Crossref*, https://doi.org/10.1007/s10207-020-00488-6

[8] Javaria Amin et al., "A Secure Two-Qubit Quantum Model for Segmentation and Classification of Brain Tumor Using MRI Images Based on Blockchain," *Neural Computing and Applications*, vol. 34, pp. 17315–17328, 2022.

[9] Shuangquan Li et al., "Health Checkup Could Reveal Chronic Disorders with Support from Artificial Intelligence," *International Journal of Engineering Trends and Technology*, vol. 67, no. 11, pp. 8-15, 2019. *Crossref*, https://doi.org/10.14445/22315381/IJETT-V67I11P202

[10] Dilmurod Nabiev, and Khayit Turaev, "Study of Synthesis and Pigment Characteristics of the Composition of Copper Phthalocyanine with Terephthalic Acid," *International Journal of Engineering Trends and Technology*, vol. 70, no. 8, pp. 1-9, 2022. *Crossref*, https://doi.org/10.14445/22315381/IJETT-V70I8P201

[11] Shwetambari Borade et al., "Deep Scattering Convolutional Network for Cosmetic Skin Classification," *International Journal of Engineering Trends and Technology*, vol. 70, no. 7, pp. 10-23, 2022. *Crossref*, https://doi.org/10.14445/22315381/IJETT-V70I7P202

[12] Gia Nhu Nguyen, "Secure Blockchain Enabled Cyber–Physical Systems in Healthcare Using Deep Belief Network with Resnet Model," *Journal of Parallel and Distributed Computing*, vol. 153, pp.150-160, 2021. *Crossref*, https://doi.org/10.1016/j.jpdc.2021.03.011

[13] Osama Alkadi, Nour Moustafa, and Benjamin Turnbull, "A Collaborative Intrusion Detection System Using Deep Blockchain Framework for Securing Cloud Networks," *Proceedings of SAI Intelligent Systems Conference*, vol. 1250, pp. 553-565, 2020. *Crossref*, https://doi.org/10.1007/978-3-030-55180-3_41

[14] K. L. Neela, and V. Kavitha, "Blockchain Based Chaotic Deep GAN Encryption Scheme for Securing Medical Images in a Cloud Environment," *Applied Intelligence*, vol. 53, pp. 4733–4747, 2023. *Crossref*, https://doi.org/10.1007/s10489-022-03730-x

[15] Xiaowei Wang et al., "A Network Intrusion Detection Method Based on Deep Multi-Scale Convolutional Neural Network," *International Journal of Wireless Information Networks*, vol. 27, no. 4, pp.503-517, 2020. *Crossref*, https://doi.org/10.1007/s10776-020-00495-3

[16] N.K. Al-Shammari, T. H. Syed, and M.B. Syed, "An Edge–IoT Framework and Prototype Based on Blockchain for Smart Healthcare Applications," *Engineering, Technology & Applied Science Research*, vol. 11, no. 4, pp.7326-7331, 2021. *Crossref*, https://doi.org/10.48084/etasr.4245

[17] Ahmad Firdaus, "Root Exploit Detection and Features Optimization: Mobile Device and Blockchain Based Medical Data Management," *Journal of Medical Systems*, vol. 42, no. 6, pp.1-23, 2018. *Crossref*, https://doi.org/10.1007/s10916-018-0966-x

[18] Padmavathi Udayakumar, and Narendran Rajagopalan, "Blockchain Enabled Secure Image Transmission and Diagnosis Scheme in Medical Cyber-Physical Systems," *Journal of Electronic Imaging*, vol. 31, no. 6, p. 062002. *Crossref*, https://doi.org/10.1117/1.JEI.31.6.062002

[19] Funlade T. Sunmola, "Context-Aware Blockchain-Based Sustainable Supply Chain Visibility Management," *Procedia Computer Science*, vol. 180, pp.887-892, 2021. *Crossref*, https://doi.org/10.1016/j.procs.2021.01.339

[20] Yu-Dong Zhang et al., "Pseudo Zernike Moment and Deep Stacked Sparse Autoencoder for COVID-19 Diagnosis," *CMC-Computers Materials & Continua*, vol. 69, no. 3, pp. 3145-3162, 2021. *Crossref*, https://doi.org/10.32604/cmc.2021.018040

[21] A. Kaveh, and S. Mahjoubi, "Hypotrochoid Spiral Optimization Approach for Sizing and Layout Optimization of Truss Structures with Multiple Frequency Constraints," *Engineering with Computers*, vol. 35, pp.1443-1462, 2019. *Crossref*, https://doi.org/10.1007/s00366-018-0675-6

[22] Ümit Atila, "Plant Leaf Disease Classification Using Efficientnet Deep Learning Model," *Ecological Informatics*, vol. 61, p.101182, 2021. *Crossref*, https://doi.org/10.1016/j.ecoinf.2020.101182

[23] Jinping Liu et al., "Toward Robust Fault Identification of Complex Industrial Processes Using Stacked Sparse-Denoising Autoencoder with Softmax Classifier," *IEEE Transactions on Cybernetic*, vol. 53, no. 1, pp. 428-442, 2023. *Crossref*, https://doi.org/10.1109/TCYB.2021.3109618

[24] [Online]. Available: https://www.kaggle.com/hassan06/nslkdd

[25] [Online]. Available: https://challenge.isic-archive.com/data/