International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

# Dingo Energy Valley Optimization Based Deep Learning for Classification of Privacy Preserved Medical Data in Cloud

**Suruchi Deshmukh**[1], **Hiren Dand** [2]

**Submitted**: 27/01/2024 **Revised**: 05/03/2024 **Accepted**: 13/03/2024

**Abstract:** In cloud, data security is a major concern while storing and retrieving data. Lately, the growing challenges include handling sensitive data and the model's privacy. Data classification techniques are employed for providing data security and it categorizes the data depending on their sensitivity. In this paper, data classification for privacy-preserved medical data is performed via employing a novel secure technique Dingo-Energy Valley Optimization- Deep Neuro Fuzzy Network (DEVO- DNFN). Here DEVO is developed by integrating Energy Valley Optimizer (EVO) as well as Dingo Optimizer (DOX). Initially, the cloud simulation is carried out and from the dataset the input medical data is attained. Subsequently, the cloud data privacy is preserved with generation of a privacy utility coefficient matrix using DEVO based on deep learning. The privacy-preserved data is then stored up in the cloud, thus the same key is required by the third party for the data retrieval. Here, DNFN is employed for the classification, which is then tuned with DEVO. The DEVO- DNFN for classification of medical data is investigated using diverse evaluation measures, such as, True Negative Rate (TNR), True Positive Rate (TPR) and accuracy is observed to attain values of 0.912, 0.907, and 0.915 correspondingly.

***Keywords:*** *Dingo Energy Valley Optimization, Deep Neuro Fuzzy Network, privacy preserved data, cloud computing, deep learning.*

## 1. Introduction

Cloud computing has grown as a very popular topic recently. It has been an attractive area for the past 20–30 years on the Internet. The resources in cloud computing are supplied based on a ‘‘pay-per-use’’ service. It is a computing structure based on the internet [1]. In digital technology cloud computing is a widely employed in the healthcare field [23]. Cloud computing is capable of providing an ample number of computation, data storage, sharing services, analysis and without revealing its platform details and implementation to organizations [11]. Owing to these unlimited services, several organizations outsource their model and data from local devices to the cloud environment [9] [2]. The finest instances of cloud computing comprise Microsoft Windows Azure, Google App Engine, Google Docs, Amazon Elastic Compute Cloud (EC2), and Gmail. The cloud computing platform is segmented into three key parts, consisting operating system, software, and hardware that are offered over the Internet to provide effectual assessment to clients [1]. Cloud computing permits the internet-connected user to utilize virtual computing possessions, like network, storage, and computation. Therefore, a cloud service provider is able to manage flexibly and rapidly. The owner of data can reduce efforts to install, expand, and purchase computing structures, and alleviate the physical space constraints [6]. From the viewpoint of storage manner, the main cloud areas typically offer three wide classes of storage: object storage, file storage, and block storage [24]. Cloud computing possesses diverse benefits, like high scalability, maximum efficiency, and minimum cost. The cloud presents outsourced data for diverse objectives to additional entities [4].

Sensitive sample data are shared with the other parties or cloud for several services [16]. yet, the users are uncertain to share data with the cloud for storage and computation due to the privacy concerns [19], also the owners might lose the access of their data [17] [4]. The cloud offers outsourced data for different purposes to other entities [4]. In cloud, for the storage and retrieval process data security is the main issue. Because of this technological problem, when the safety of the client's data is not guaranteed they suffer from insecurity for their data, and did not provide the case studies in relation to the services [1]. Afterward, the emergent clash includes handling sensitive data and the privacy of the model [2]. Privacy preservation guarantees safety to the information and data irrespective of the kind of data. One of the crucial security guaranteeing systems is data encryption, and regardless of the data sensitivity the encryption should be guaranteed at no cost. Privacy protection of the cloud data is very necessary because the service provider itself may disclose the user information to the hackers and, thus there is an important need for the privacy method to guarantee security [1]. Homomorphic encryption forms the basis of most of the prevailing privacy-preserving methods for the convolutional neural network [18] [21].

[1] *Research Scholar, Shri Jagdishprasad Jhabarmal Tibrewala University, Rajasthan, INDIA*
*ORCID ID : 0009-0008-3069-8653*
[2] *Guide, Shri Jagdishprasad Jhabarmal Tibrewala University, Rajasthan, INDIA*
*ORCID ID : 0000-0001-5305-6735*
** Corresponding Author Email: suruchi.nannaware@gmail.com*

Homomorphic encryption methods are inadequate for estimating low-order polynomials from encrypted data. This method adds random noises to the data, which may cause a decline in the accessibility of the data [21].

Data classification techniques are employed for the security of the data which categorizes the data considering their sensitivity [1]. In many practical applications, classifier testing and training is one of the most common tasks. For instance, a well-trained classifier can provide online diagnosis services for patients based on their symptoms [11] [15]. In addition, the highly intelligent system distinguishes and groups the data as non-sensitive and sensitive and provides safety to sensitive data and it lessens the trouble inherent in the cloud information encryption methods. Also, classification techniques reduce the computational time, memory, and burden [1]. The classification process depended on the data divulgence threat, and thus, the data is distinguished as, confidential, restricted, regulatory, internal, public, etc. Using Neural Network (NN) intended for distinguishing medical relevant data has increased competent attention amid researchers as NN utilizes an easy process for training purpose. NN can be effectually employed by specifying the appropriate classification regulations for data classification [10]. Traditional cryptographic methods [20][22] contributes in resolving the troubles, but it possessed high memory and computation costs, and was not simple to implement these techniques directly like the Deep Neural Network (DNNs). In federated learning, the users are permitted to guide a global structure with no centralization of the training data, but it cannot protect privacy during the inference of test data when a model is installed in an untrustable cloud server [22].

The foremost target of this work is generating and implementing a capable solution for classification of privacy preserved medical data in the cloud environment by utilizing the linear polarized data. To begin with, the medical data is obtained from the dataset as input. After that, the privacy utility coefficient matrix is produced for the cloud data privacy using DEVO. Thereafter, the linear polarized data is generated to create the coefficients of the key matrix. Then the key matrix is then built to determine the data privacy. From the constructed key matrix, the cumulative key matrix is generated to determine the second key coefficient. The data is accumulated in the cloud platform such that the third party requests the same key for the data retrieval from cloud. Finally, the privacy preserved medical data classification is executed using the DNFN, which is trained by the DEVO.

The key influence of this paper is detailed below:

- **Proposed DEVO for classification of privacy preserved data in cloud:** A novel framework for privacy preserved data classification in cloud to provide a highly secured data classification is crucial. Therefore, DEVO is established here by combining the Energy Valley Optimizer (EVO).and Dingo Optimizer (DOX) to generate the privacy utility coefficient matrix to safeguard the medical data privacy in the cloud.

The residual portion of this work is positioned as follows: The review of literature on the related prevailing works is portrayed in Section 2. The system model of cloud is defined in Section 3, and Section 4 expounds the DEVO-DNFN for medical data classification in cloud. Section 5 interprets the practical findings and assessments. Section 6 provides the conclusion with the future development.

## 2. Motivation

Here, the prevailing frameworks for the privacy-preserved medical data classification are estimated along with the disputes faced by them. Since the data classification relied on threat of data disclosure, it is difficult for the current technology to classify privacy-preserved data effectually. Moreover, these existing models are greatly complex and the cost was high. Overcoming these concerns faced by prevailing systems is the key motivation of DEVO.

### 2.1 Literature Review

Subramaniyam, A., et al [1] devised an effective method for performing the medical data classification in cloud computing using a technique called Taylor Gradient Descent based Actor-Critic Neural Network (TGD based ACNN). This method was easy to maintain and had less processing time. However, it did not consider hybrid optimization methods to improve the classification. Gupta, R. and Singh, A.K., [2] devised a Differential Approach for data and classification service-based Privacy-preserving Machine Learning Model (DA-PMLM) in the cloud environment for multiple owners to share their data for utilization. This approach was more optimal, secure, and efficient but was not suitable for real-time applications. Liang, J., et al [3] devised a Privacy-Preserving Outsourcing Medical Image Classification (POMIC) scheme for adaptive classification of medical images based on a convolutional neural network to the cloud. The POMIC acted as storage, communication, and computationally proficient system for privacy-preserving health monitoring but with the raised in several biomedical features it suffered from high time complexity. Singh, A.K. and Gupta, R., et al. [4] devised Privacy Preserving Model based on Differential approach (PPMD) for sensitive data in the cloud environment. This model reduced the influence of inserted noise by sorting out data into non-sensitive and sensitive segments. However, it did not permit to sharing of collected data among requesting users.

Li, J., et al. [5] devised a privacy-preserving method utilizing block wise scrambled images and a modified ConvMixer that permited to lessen the manipulation of image encryption. This method accommodated well to private deep learning background with ciphertexts's deep iteration but it did not succeed in enhancing the encryption efficiency. Kim, Y.K., et al. [6] devised a privacy-preserving parallel K-nearest neighbors (Knn) classification algorithm to contribute a sufficient level of effectiveness for a huge number of encrypted data. This algorithm reduced query processing time and was safe but required high computational cost. Du, J. and Bian, F., [7] devised a Partially Homomorphic Encryption (PHE) scheme which allowed processing of private data with no contact of the underlying data. This technique required a lower run time and had a minimal computational overhead. However, the security of this technique was not improved. Park, J. and Lee, D.H., [8] devised a privacy-preserving k-nearest neighbor classification (PkNC) to resolve the data revelation troubles. This method handled large amount of data efficiently also it had more efficient running time but it required high memory and was computationally expensive.

### 2.2 Challenges

- ➢ TGD based ACNN developed in [1] did not employ other hybrid optimization to train the classifier and failed to improve the classification performance. Furthermore, the performance of this model was not examined with more datasets.
- ➢ The DA-PMLM in [2] protected the classification model as well as the data from illegal parties. However, a more capable privacy-preserving method to reduce the performance degradation was not considered.
- ➢ The PPDT devised in [3] had a cost and storage effective classification with minimum processing time but it was ineffectual in handling the applications encountering malicious attackers.
- ➢ Though the PPMD method in [4] prevented data against leakage or stealing and sustained high degree of accuracy, it did not devise an efficient privacy-preserving system to preserve the data for various owners.

## 3. System Model of Cloud

The cloud computing handles a large compilation of the data which belongs to a huge amount of patients and this is fetched at any destined time. The cloud system stores the medical records with a guaranteed retrieval at the required period. The user data are afforded with the key for the data security and accumulated in the cloud system. Using the key, the third party with the right to access can access the data in cloud at anytime. Figure 1 illustrates the system model of cloud for privacy preservation of medical data.

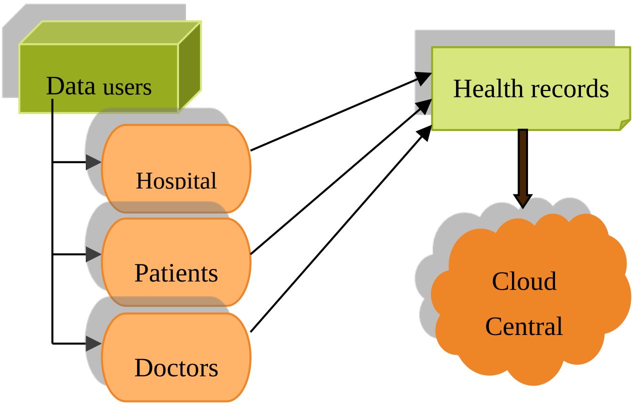

**Fig 1.** The system model of cloud for privacy preservation of medical data.

## 4. Proposed DEVO-DNFN Architecture for Privacy Preserved Medical Data Classification

This segment presents the DEVO-DNFN architecture in cloud environment for medical data classification. The developed DEVO-DNFN is realized using the following phases. Initially, the simulation of cloud network is done, and then the input medical data is attained from the dataset. After that, the privacy utility coefficient matrix is generated to preserve the privacy of the cloud medical data using the proposed DEVO which is obtained by combining the EVO [12] and (DOX)[13]. Thereafter, the linear polarized data is generated to create the coefficients of the key matrix. Then the key matrix is built and from the constructed key matrix, the cumulative key matrix is generated to establish the second key coefficient. The privacy-preserved data is then stored up in cloud network, thus the same key is required by the third party for the data retrieval. Finally, by using the DNFN the privacy preserved medical data classification is performed, which is tuned by the proposed DEVO. The structural design of DEVO-DNFN is displayed in figure 2.

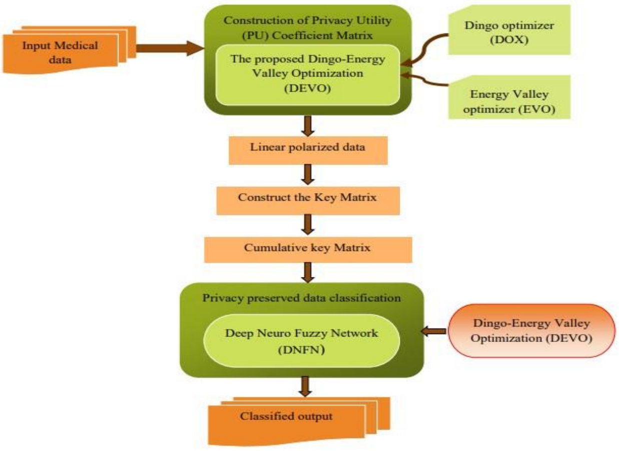
Input Medical data
Construction of Privacy Utility (PU) Coefficient Matrix
The proposed Dingo-Energy Valley Optimization (DEVO)
Dingo optimizer (DOX)
Energy Valley optimizer (EVO)
Linear polarized data
Construct the Key Matrix
Cumulative key Matrix
Privacy preserved data classification
Deep Neuro Fuzzy Network (DNFN)
Dingo-Energy Valley Optimization (DEVO)
Classified output

**Fig 2.** The structural design of the devised DEVO-DNFN

### 4.1 Data acquisition

In this work, the classification of numerous medical data in the cloud environment that are acquired from a dataset S, which can be represented as matrix using the following expression,

Let us consider the input data as,

$$S = [\, S_{tu}\,];\ \ 1 \leq t\ \leq v; 1 \leq u \leq w; \qquad (1)$$

Here, $t$ indicates the row of the data matrix, $v$ indicates the overall number of data records,$u$ indicates the column of the data matrix, and $w$ is overall feature.

### 4.2 Linear polarized data matrix

The input data S is fed to the linear polarized data and the PU coefficient matrix is produced to create the coefficients of key matrix and the linear polarized matrix is represented as follows;

$$L = S \otimes P \qquad (2)$$

Here, $\otimes$ is the linear interpolation operator, and $P$ represents the PU coefficient, which is produced by the proposed DEVO. The structure of the PU coefficient is given in figure 3.

| | | | |
|---|---|---|---|
| P1 | P2 | …………………………. | Pn |

**Fig 3.** The structure of PU coefficient

where, P1, P2…… Pn are the indexes of PU coefficient.

### 4.2.1 Proposed DEVO for privacy preserved medical data classification

DEVO was created to safeguard the medical data in the cloud by the generation of privacy utility coefficient matrix. DEVO is devised by incorporating EVO [12] and DOX [13]. EVO is a metaheuristic algorithm on the basis of the physics principles considering different modes and stability of particle decay and is divided into two classes: exploration and exploitation. The use of EVO helps in attempting and improving the precision of the optimization process for a host of issues. However, it did not consider difficult optimization problems in diverse fields, as well as real-size engineering design problems. DOX is a nature-based algorithm based on the hunting characteristics of dingo and it copes with diverse kind of constraints and provides sturdy options. However, the multiobjective problems were not solved. The novel DEVO handles a variety of optimization problems and generates more optimal solutions by overcoming the above mentioned limitations. The phases of the DEVO are detailed below:

***Step i) Initialization***

The initialization of the search space is performed on the basis of EVO. In this phase, the $Y_c$ solution candidates are implicated to be particles with diverse levels of stability, which is assumed as a specific part of the search space. The solution candidates are expressed as follows;

$$Y = \begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \\ \vdots \\ Y_c \\ \vdots \\ \vdots \\ Y_q \end{bmatrix} = \begin{bmatrix} y_1^1 & y_1^2 \cdots & y^d \cdots & y_1^r \\ y_2^1 & y_2^2 \cdots & y_2^d \cdots & y_2^r \\ \cdots\cdot & \cdots\cdot\cdot & \cdots\cdot\cdot & \cdots\cdot \\ \cdots\cdot & \cdots\cdot\cdot & \cdots\cdot\cdot & \cdots\cdot \\ y_c^1 & y_c^2 \cdots & y_c^d \cdots & y_c^r \\ \cdots\cdot & \cdots\cdot\cdot & \cdots\cdot\cdot & \cdots\cdot \\ \cdots\cdot & \cdots\cdot\cdot & \cdots\cdot\cdot & \cdots\cdot \\ y_q^1 & y_q^d \cdots & y_q^d \cdots & y_q^r \end{bmatrix}, \begin{cases} c = 1,2,..., q. \\ d = 1,2,..., r. \end{cases} \qquad (3)$$

where, $Y_c^d$ indicates the $d^{th}$ decision variable for the first position of the $c^{th}$ particle, $r$ is the dimension of the measured problem, and $q$ is the total particles in the search space.

$$y_c^d = y_{c,\min}^d + rand.\left(y_{c,\max}^d - y_{c,\min}^d\right), \begin{cases} c = 1,2,..., q. \\ d = 1,2,..., r. \end{cases} \qquad (4)$$

here, $Y_c^d$ and $y_{c,min}^a$ represents the lower and upper bounds of the $d^{th}$variable in the $c^{th}$ particle, *rand* denotes a random number of range [0, 1].

***Step ii) Fitness measure***

Here, the fitness of the particles in the search space is mathematically expressed as formulated beneath;

$$L^* = \frac{P^* + S^*}{2} \qquad (5)$$

Where $P^*$ denotes the Jaccard distance , and $S^*$ indicates the accuracy of the utility.

***Step iii) Enrichment Bounding (EB)***

In the next step, the divergence between the neutron-poor and neutron-rich particles is conducted by Enrichment Bounding (EB). The mathematical expression for EB is given below:

$$EB = \frac{\sum_{c=1}^{q} N_c}{q}, c = 1,2,..., q. \qquad (6)$$

where, EB is the enrichment bound and $N_c$ indicates the level of neutron enrichment of the $c^{th}$ particle.

***Step iv) Stability level***

In the next step, the particle's stability level is determined and is formulated as follows:

$$Z_c = \frac{N_c - A}{B - A}, c = 1,2,..., q \qquad (7)$$

where $A$ and $B$ are the best and worst stability level available in the search space, $Z_c$ is the stability level of the $c^{th}$ particle.

***Step v) Generate Alpha indexes***

Here, to boost the stability level of the product in the physical reaction, $\alpha$ rays are emitted. This can be expressed as one of the scheme where a novel solution is produced. Therefore, in this phase, Alpha Index I of range [1, k], and Alpha Index II of range [1, Alpha Index I] are generated, k represents the number of emitted rays and this is mathematically represented as below.

$$Y_c^{n_1} = Y_c(Y_A(y_c^d)), \begin{cases} c = 1,2,\ldots,q. \\ d = AlphaIndexII. \end{cases} \quad (8)$$

Where, $Y_c$ indicates the current vector position of the $c^{th}$ particle, $YA$ indicates the best stability level, $y_c^d$ indicates the $d^{th}$emitted ray, and $Y_c^{n1}$ is the freshly generated particle in the search space.

***Step vi) Generate Gamma indexes***

Here, to enhance the excited particles' stability level, γ rays are emitted and are expressed as an additional position-updating procedure of EVO in which a novel solution is produced. Therefore, Gamma Index I in the range of [1, k ], and Gamma Index II in the range of [1, Gamma Index I] are developed, k corresponds to the number of emitted photons, The entire distance involving the measured particle and the other ones are evaluated as given below:

$$G_c^p = \sqrt{(y_2 - y_1) + (x_2 - x_1)^2} \ , \begin{cases} c = 1,2,\ldots, q. \\ p = 1,2,\ldots, q-1. \end{cases} \quad (9)$$

where, $(x_2, y_2)$ and $(x_1, y_1)$ symbolize the coordinates of the particles, and $G_c^p$ is the overall distance between the $K^{th}$ neighboring particle and $c^{th}$ particle.

In this phase, for generating the next particle, a position updating process is performed and is formulated mathematically as follows:

$$Y_c^{n_2} = Y_c(Y_Q(y_c^d)), \begin{cases} c = 1,2,\ldots, q. \\ d = GammaIndexII. \end{cases} \quad (8)$$

Where $Y_c$ indicates the current vector position of the $c^{th}$ particle,

$Y_c^{n_2}$ indicates the freshly generated particle, $Y_Q$ is the vector position of the nearby particle around the $c^{th}$ particle, and $Y_c^d$ denotes the $d^{th}$ discharged photon.

***Step vii) Centre of particles***

If $Z_c \leq EB$, beta decay is occurred. According to the physics principles, to boost the stability level of the particle β rays from the particles are excluded. Then, a position updating process for the particles because of the superior levels of instability in the particles is carried out, here a controlled movement in the direction of the particle or candidate with the best stability level $(Y_Z)$ and the centre of particles $(Y_R)$ is carried out. This is expressed beneath;

$$Y_R = \frac{\sum_{c=1}^{q} Y_c}{q}, c = 1,2,\ldots, q. \quad (10)$$

$$Y_c\ (n_1 + 1) = Y_c + \frac{(m_1 \times Y_A - m_2 \times Y_R)}{Z_c} \quad (11)$$

Where $Y_R$ is the vector position for the center of particles, $Y_c(n_1 + 1)$ and $Y_c$ represents the forthcoming and current position vectors of the $c^{th}$ particle in search space, $Z_c$ denotes the stability level of the $c^{th}$ particle, $Y_A$ represents the particle with the best stability level, $m_1$ and $m_2$ are the random numbers in the range [0, 1].

***Step viii) Determine best stability level***

As mentioned above, to progress the exploration and exploitation levels of the algorithm, a new position updating procedure is performed.

$$Y_c\ (n_1 + 1) = Y_c(n_1) + (m_3 \times Y_A - m_4 \times Y_Q) \quad (12)$$

Where $Y_Q$ denotes the vector position of the nearby particle around the $c^{th}$ particle, $Y_c\ (n_1 + 1)$, $Y_c\ (n_1)$ are the approaching and current position vectors of the $c^{th}$ particle, $m_3$ and $m_4$are the random numbers of range[0, 1] which decide the quantity of particles' movement.

The convergence of EVO can be enhanced by including DOX, and from DOX [13],

$$\vec{H}(j+1) = \vec{H}h(j) - \vec{E}.\vec{F}(f) \quad (13)$$

where, $$\vec{F}(f) = \left| \vec{C}.\vec{H}h(Y) - \vec{H}(j) \right| \quad (14)$$

Assume, $$\vec{C}\vec{H}h(j) > \vec{H}(j)$$
(15)

Let, $$\vec{H}(j+1) = Y_c(n_1 + 1)$$

$$\vec{H}(j) = Y_c(n_1)$$

$$\vec{E} = E$$

$$\vec{H}h(j) = Yh_c(n_1)$$

Thus the equation (13) becomes;

$$Y_c(n_1 + 1) = Yh_c(n_1) - E(C.Yh_c(n_1) - Y_c(n_1)) \quad (16)$$

$$Y_c(n_1 + 1) = Yh_c(n_1)(1 - E.C) + E.Y_c(n_1) \quad (17)$$

$$Y_c(n_1) = \frac{Y_c(n_1 + 1) - Yh_c(n_1)(1 - E.C)}{E} \quad (18)$$

Substituting equation (17) in equation (11);

$$Y_c(n_1+1) = \frac{Y_c(n_1+1) - Yh_c(n_1)(1-E.C)}{E} + (m_3 \times Y_A - m_4 \times Y_Q) \qquad (19)$$

$$Y_c(n_1+1) - \frac{Y_c(n_1+1)}{E} = \frac{Yh_c(n_1)(C.E-1) + (m_3 \times Y_A - m_4 \times Y_Q)}{E} \qquad (20)$$

$$\frac{(E-1)Y_c(n_1+1)}{\cancel{E}} = \frac{Yh_c(n_1)(C.E-1) + (m_3 \times Y_A - m_4 \times Y_Q)}{\cancel{E}} \qquad (21)$$

$$Y_c(n_1+1) = \frac{Yh_c(n_1)(C.E-1) + E(m_3 \times Y_A - m_4 \times Y_Q)}{E-1} \qquad (22)$$

Where $Y_A$ is the best solution, m$_3$, and m$_4$ are the random numbers of range [0,1], $Y_Q$ is the neighbor solution, $C = 2 * \tau_1$, $\tau_1$ is a constant, $Yh_c(n_1)$ is the position of the prey vector, and $E$ is the coefficient matrix.

***Step ix) Feasibility check***

After the completion of the entire tasks, if the fitness of the current best solution is superior to the previous one, the current best solution is retained. Otherwise, the best solution in the preceding iteration will be utilized as the new one

***Step x) Termination***

The above mentioned steps are continued until the best solution is attained. By combining these two techniques an optimal PU coefficient value is produced using which the linear polarized data matrix is generated, which is then subjected to the next process.

### 4.3. Cumulative Linear polarized data

Once the linear polarized data $L$ is generated to create the coefficients of the key matrix, the Cumulative Linear polarized data is produced via the summation of separate columns of Linear polarized data

$$T = \sum_{I=1}^{U} W_{kl^*} \qquad (23)$$

Where $W$ notes the individual element of Linear polarized data matrix of size $[r \times l]$

### 4.4. Develop key matrix

The key matrix performs a vital task in deciding the data privacy. The combination of key matrix and original data $S$ enables conservation of the confidential details. The developed key matrix is specified beneath:

$$V = [a \ \ b] \qquad (24)$$

where,$a$ and $b$ are the key coefficients.

The entity in $a$ holds the value between 1 and W, the adding up of single elements in the form of Cumulative Linear polarized data (CLPD), $a$ is expressed beneath;

$$a = \{Mg\}; \qquad 1 \le g \le W\mu W < X \qquad (25)$$

where, $a$ indicates the key coefficient 1 and Mg acquires the value as given below;

$$Mg = \sum_{s^*=g}^{X-Wg} R_k \qquad (26)$$

where, the size of $a$ is $\frac{1}{2}$ and $R_k$represents the CLDP matrix.

### 4.5. Construct the Cumulative Key Matrix (CKM)

As of the key matrix, CKM is generated to examine the next key coefficient, thus CKM relies on the PU coefficient and key coefficient 1. The CKM can be formulated as below;

$$J = K^{1\sigma} * a * a^O \qquad (27)$$

where $K^{1\sigma}$ denotes the one-dimensional element of PU coefficient.

Then, the key coefficient 2 is calculated as the overall column elements in CKM and it is expressed as follows;

$$l = \sum_{e=1}^{o} V_e \qquad (28)$$

where $V_e$ is the column element of the CKM.

### 4.6. Construct the privacy-preserved data by using the generated key

For establishing the privacy preserved medical data $S^*$ with the intermediate element $S^O$ the key matrix is utilized, with the key matrix $l$ , This is formulated as;

$$S^* = \frac{S^O}{l} \qquad (29)$$

where $S^O$is the intermediate element and $l$ is the key matrix.

$$S^O = S \oplus a \qquad (30)$$

By executing the EX-OR matrix ($\oplus$) on S and key coefficient 1, that is $a$ , $S^O$ is generated.

### 4.6.1. Extraction of original data

The original data extraction from the cloud's privacy preserved data is expressed as follows;

$$S^* \times l = S^{O^*} \qquad (31)$$

$$S^{0^*} \oplus l = S^* \qquad (32)$$

here, $S^*$ is the retrieved data.

### 4.7. Privacy preserved medical data classification

In order to perform the classification, the retrieved data $s^*$ is fed to the DNFN as input. The DNFN training is carried out by DEVO, which is produced by the incorporation of EVO and DOX. DNFN is a kind of artificial intelligence that incorporates Neural Network (NN) and Fuzzy concept. Here, the learning capability of the Deep Neural Network (DNN) and the reasoning ability of Fuzzy systems are utilized. The deep structures relied on the fuzzy model was effective in image analysis. The layers in this network are stacks of two operations namely, fuzzy inference and fuzzy pooling. The structural drawing of the DNFN for classification is exhibited in figure 4.

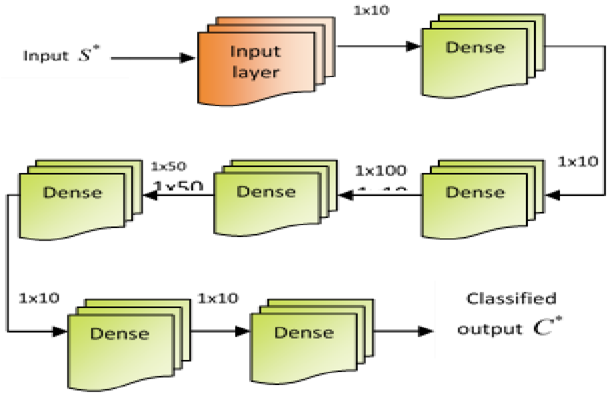

**Fig 4.** The structural diagram of DNFN.

### 4.7.2. Training using DEVO algorithm

The DEVO model is devised for the training of DNFN by combining EVO [12] and DOX [13]. The EVO is incorporated to the DOX in order to safeguard the cloud medical data privacy by generating the privacy utility coefficient matrix. The privacy-preserved medical data classification is carried out using the DNFN [14], which is trained by the proposed DEVO algorithm. The phases carried out in this process are detailed in the section 4.2.1.

As the EVO is used here to train the DNFN, the fitness of the particles in the search space is mathematically expressed in terms of the Mean Squared Error (MSE) as mentioned beneath.

$$MSE = \frac{1}{\bar{b}} \sum_{\bar{a}=1}^{\bar{b}} \left( C_{\bar{a}}^{*} - C_{\bar{a}} \right)^2$$

where $C_{\bar{a}}^{*}$ implies the expected outcome, $C_{\bar{a}}$ denotes the DNFN's output and $\bar{b}$ denotes the amount of training samples.

## 5. Results and Discussion

The DEVO-DNFN is contrasted with prevailing strategies and the assessment carried out for this system are detailed in the subsequent section.

### 5.1. Experimental setup

The devised DEVO-DNFN is executed on a PC with a Python tool implementation.

### 5.2. Dataset description

The heart disease database [25] is utilized in this model for acquiring the medical data. This repository holds 76 features, but all the available works refer to using a division of 14 of them. This dataset supplies the multivariate characteristics of Health and Medicine in Cleveland, Hungary, and Switzerland.

### 5.3. Evaluation measures

The DEVO-DNFN model's performance is assessed in terms of TNR, TPR, and accuracy.

***a) Accuracy:*** It is the ratio of the accurately classified medical data to the overall medical data fed to the model. It is expressed as below,

$$Accuracy = \frac{v'_{11} + r'_{11}}{v'_{11} + r'_{11} + v'_{12} + r'_{12}}$$

(39)

where $v'_{11}$, represents true positive and $v'_{12}$ represents false positive and $r'_{11}$ terms true negative and false negative is specified by $r'_{12}$.

***b) TNR:*** It is the ratio of the amount of true positive data classification to the amount of all positive data classification of medical data in the model.

$$TNR = \frac{r'_{11}}{r'_{11} + r'_{12}} \tag{40}$$

***c) TPR:*** It is the ratio of the amount of true negative data classification to the amount of all negative classification of medical data in the model.

$$TPR = \frac{v'_{11}}{r'_{11} + r'_{12}} \tag{41}$$

### 5.4. Comparative methods

The conventional methods taken for the assessment of devised DEVO-DNFN are ACNN [1], DA-PMLM [2], POMIC [3], and PPMD [4].

### 5.5. Comparative assessment

Here, the DEVO-DNFN is examined for it proficiency in medical data classification considering three datasets, such as Hungary, Cleveland, and Switzerland, and this is explicated in the subsequent sections.

### 5.5.1. Using Hungary dataset

The performance of the DEVO-DNFN is analyzed comparatively with training data by utilizing Hungary dataset. This assessment is portrayed in figure 6. The assessment on accuracy for the DEVO-DNFN is exhibited in figure 6a. The attained accuracy by the techniques ACNN, DA-PMLM, POMIC, PPMD and the DEVO-DNFN with 90% training data is 0.741, 0.798, 0.866, 0.870 and 0.912 correspondingly. The accuracy of DEVO-DNFN is enhanced by 4.54% than the PPMD. Figure 6b exhibits the analysis of DEVO-DNFN in term of TPR. The obtained TPR values of the applied methods ACNN, DA-PMLM, POMIC, PPMD and the proposed DEVO-DNFN when the training data is 90% are 0.740, 0.844, 0.873, 0.878 and 0.915 correspondingly. The TPR value of DEVO-DNFN is improved by 4.07% than the PPMD framework. The assessment on the basis of TNR is exhibited in Figure 6c. The attained TNR values of the applied techniques ACNN, DA-PMLM, POMIC, PPMD and the DEVO-DNFN with 90% training data is 0.855, 0.821, 0.778, 0.751, and 0.915 correspondingly. The TNR values of the developed DEVO-DNFN are enhanced by 5.10% than the ACNN

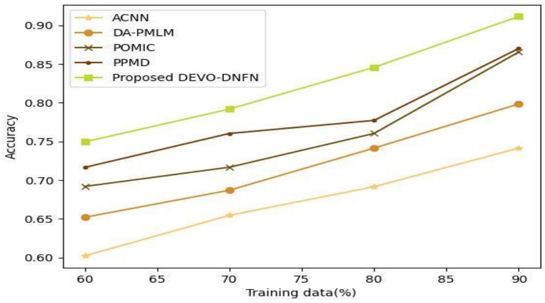

**Fig 6a**

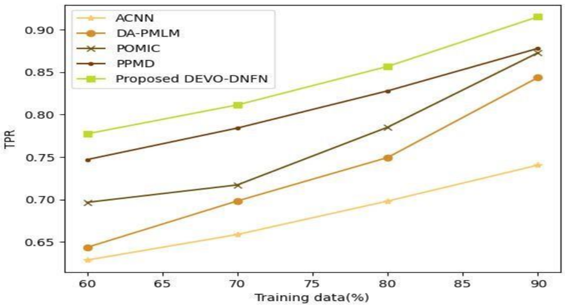

**Fig 6b**

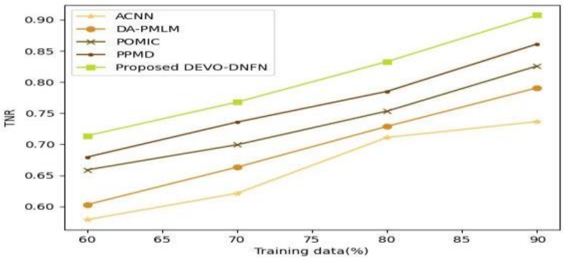

**Fig 6c**

**Figure 6.** Comparative assessment of a) accuracy, b) TPR, and c) TNR of the DEVO-DNFN with other methods based on training data using Hungary dataset.

### 5.5.2. Using Cleveland dataset

The performance of the DEVO-DNFN is analyzed comparatively with training data by utilizing Cleveland dataset. This analysis is exhibited in the figure 7. The analysis of the of DEVO-DNFN on the basis of accuracy is exhibited in figure 7a The accuracy obtained in the techniques ACNN, DA-PMLM, POMIC, PPMD and the DEVO-DNFN with 90% training data is 0.783, 0.842, 0.888, 0.891 and 0.911 correspondingly. The accuracy of DEVO-DNFN is enhanced by 2.18% than the PPMD. Figure 7b portrays the performance of the DEVO-DNFN in terms of TPR. The obtained TPR values of the methods ACNN, DA-PMLM, POMIC, PPMD and the proposed DEVO-DNFN when the training data is 90% are 0.785, 0.843, 0.883, 0.892 and 0.915 correspondingly. The TPR value of DEVO-DNFN is improved by 2.56% than the PPMD framework. The assessment of the DEVO-DNFN based on TNR is exhibited in Figure 7c. The attained TNR values of the techniques, such as ACNN, DA-PMLM, POMIC, PPMD and the DEVO-DNFN with 90% training data is 0.782, 0.841, 0.883, 0.889, and 0.907 correspondingly. The TNR value of the developed DEVO-DNFN is improved by 2.05% than the ACNN.

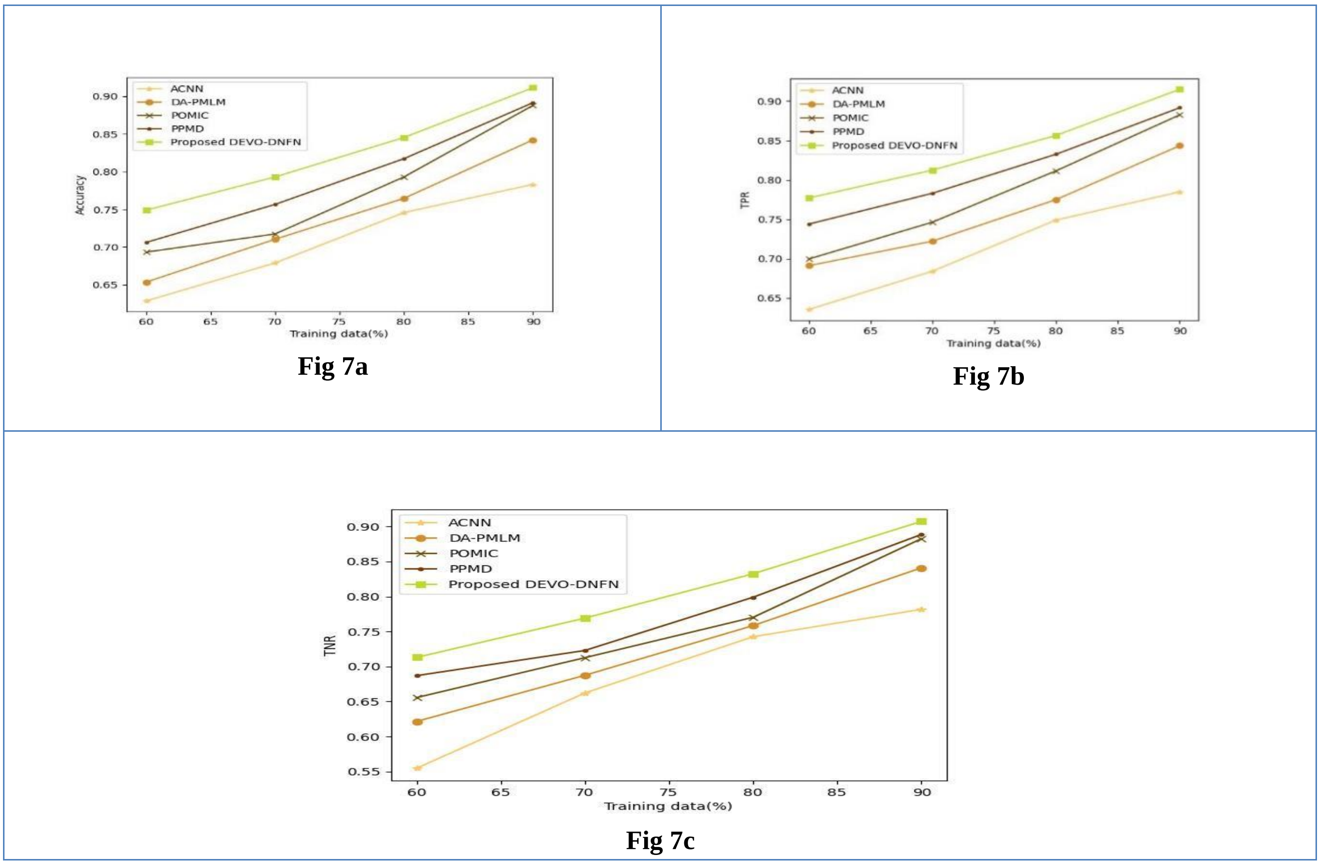

Fig 7a

Fig 7b

Fig 7c

**Fig 7.** Comparative assessment of a) accuracy, b) TPR, and c) TNR of the DEVO-DNFN with other methods with training data using Cleveland dataset.

### 5.5.3. Using Switzerland dataset

The performance of the DEVO-DNFN is analyzed comparatively with training data by utilizing Switzerland dataset. This assessment is exhibited in the figure 8. The accuracy-based assessment of the DEVO-DNFN is exhibited in figure 8a. The techniques, like ACNN, DA-PMLM, POMIC, PPMD and the DEVO-DNFN with 90% training data acquired accuracy of 0.754, 0.838, 0.882, 0.890 and 0.909, correspondingly. The accuracy of DEVO-DNFN is enhanced by 2.03% than the PPMD. Figure 8b exhibits the assessment of the DEVO-DNFN on the basis of TPR. The obtained TPR values of the methods ACNN, DA-PMLM, POMIC, PPMD and the proposed DEVO-DNFN when the training data is 90% are 0.757, 0.840, 0.886, 0.892 and 0.913 correspondingly. The TPR value of DEVO-DNFN is improved by 2.31% than the PPMD framework. The assessment of the DEVO-DNFN in terms of TNR is exhibited in Figure 8c. The TNR values attained by ACNN, DA-PMLM, POMIC, PPMD and the DEVO-DNFN with 90% training data is 0.731, 0.813, 0.868, 0.879, and 0.895. correspondingly. The TNR value of the developed DEVO-DNFN is improved by 1.69% than the ACNN.

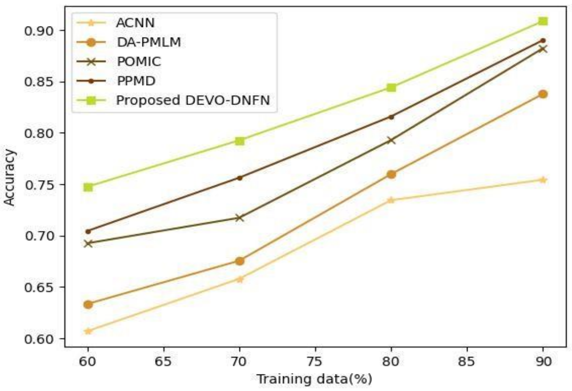

**Fig 8a.**

-PMLM

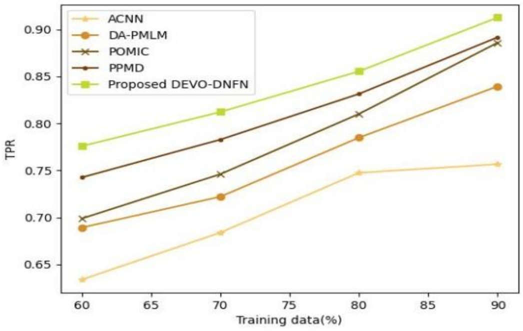

**Figure 8b**

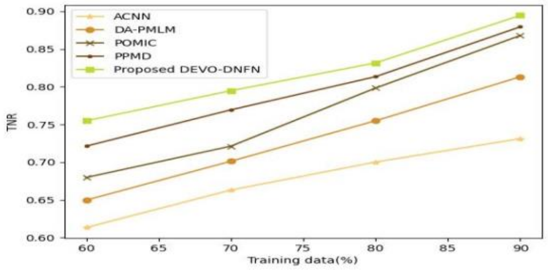

**Figure 8c.**

**Fig 8.** Comparative assessment of a) accuracy, b) TPR, and c) TNR of the DEVO-DNFN with other methods with training data using Switzerland dataset.

### 5.6. Comparative discussion

Table 1 describes the comparative discussion of DEVO-DNFN, here; the performance of the DEVO-DNFN is estimated in terms of metrics like, TPR, TNR and accuracy with the comparison of prevailing medical data classification techniques. The prevailing methods ACNN, DA-PMLM, POMIC, PPMD, and the proposed DEVO-DNFN attained high accuracy of 0.783, 0.842, 0.888, and 0.912, TPR of 0.785, 0.843, 0.886, 0.892 and 0.915, and TNR of 0.782, 0.841, 0.883, 0.889, and 0.907 correspondingly. The established DEVO-DNFN shows high accuracy, TPR, and TNR, due to the incorporation of DEVO for structurally optimizing the DNFN employed for data classification. Further, the conversion of the input data into a linear polarized form enhanced the privacy preservation.

| *Dataset* | *Metric* | *ACNN* | *DA-PMLM* | *POMIC* | *PPMD* | *Proposed DEVO-DNFN* |
|---|---|---|---|---|---|---|
| ***Hungary*** | ***Accuracy*** | 0.741 | 0.798 | 0.866 | 0.870 | **0.912** |
| | ***TPR*** | 0.740 | 0.844 | 0.873 | 0.878 | **0.915** |
| | ***TNR*** | 0.736 | 0.791 | 0.826 | 0.861 | **0.907** |
| ***Cleveland*** | ***Accuracy*** | 0.783 | 0.842 | 0.888 | 0.891 | 0.911 |
| | ***TPR*** | 0.785 | 0.843 | 0.883 | 0.892 | 0.915 |
| | ***TNR*** | 0.782 | 0.841 | 0.883 | 0.889 | 0.907 |
| ***Switzerland*** | ***Accuracy*** | 0.754 | 0.838 | 0.882 | 0.890 | 0.909 |
| | ***TPR*** | 0.757 | 0.840 | 0.886 | 0.892 | 0.913 |
| | ***TNR*** | 0.731 | 0.813 | 0.868 | 0.879 | 0.895 |

**Table 1.** Comparative discussion of DEVO-DNFN

## 6. Conclusion

This paper developed a DNFN model optimized with DEVO for the classifying the privacy preserved medical data. Here, the DEVO is established by integrating EVO and DOX. At first, the input medical data is obtained from the dataset. Then, the privacy of the cloud data is conserved by producing the privacy utility coefficient matrix with the usage of the proposed DEVO. Then, the linear polarized data is generated to create the coefficients of the key matrix. Afterwards, to determine the privacy of the data a key matrix is built. From the built key matrix, the cumulative key matrix is generated to determine the second key coefficient and the data privacy is preserved and the data is stored up in cloud. Finally, the DNFN performs the medical data classification. Here, DNFN is trained by the developed DEVO. It attained higher values in terms of accuracy as 0.912, TPR as 0.915 and TNR as 0.909, the proposed DEVO-DNFN outperformed other methods. The further goals include, incorporating advanced deep learning and optimization techniques and employing large dataset is a part of the future research direction

### Acknowledgements

We thank our colleagues from MIT Art Design and Technology University who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations of this paper. We thank Hiren Dand, PhD Guide for assistance with optimization Techniques that greatly improved the manuscript.

### Author contributions

**Suruchi Nannaware:** Conceptualization, Methodology, Software, Field study, Data curation, Writing-Original draft preparation, Software, Field study Visualization,

**Hiren Dand:** Validation., Investigation, Writing-Reviewing and Editing.

### Conflicts of interest

The authors declare no conflicts of interest.

## References

[1] Subramaniyam, A., Mahapatra, R.P. and Singh, P., "Taylor and gradient descent-based actor critic neural network for the classification of privacy preserved medical data", Big data, vol.7, no.3, pp.176-191, 2019.

[2] Gupta, R. and Singh, A.K., "A differential approach for data and classification service-based privacy-preserving machine learning model in cloud environment", New Generation Computing, vol.40, no.3, pp.737-764, 2022.

[3] Yu, Q., Zhang, H., Xu, H. and Kong, F., "POMIC: Privacy-Preserving Outsourcing Medical Image Classification Based on Convolutional Neural Network to Cloud", Applied Sciences, vol.13, no.6, pp.3439, 2023.

[4] Singh, A.K. and Gupta, R., "A privacy-preserving model based on differential approach for sensitive data in cloud environment", Multimedia Tools and Applications, vol.81, no.23, pp.33127-33150, 2022.

[5] Li, J., Kuang, X., Lin, S., Ma, X. and Tang, Y., "Privacy preservation for machine learning training and classification based on homomorphic encryption schemes", Information Sciences, vol.526, pp.166-179, 2020.

[6] Kim, Y.K., Kim, H.J., Lee, H. and Chang, J.W., "Privacy-preserving parallel kNN classification algorithm using index-based filtering in cloud computing", Plos one, vol.17, no.5, pp.e0267908, 2022.

[7] Du, J. and Bian, F., "A privacy-preserving and efficient k-nearest neighbor query and classification scheme based on k-dimensional tree for outsourced data", IEEE Access, vol.8, pp.69333-69345, 2020.

[8] Park, J. and Lee, D.H., "Parallelly Running and Privacy-Preserving k-Nearest Neighbor Classification in Outsourced Cloud Computing Environments", Electronics, vol.11, no.24, pp.4132, 2022.

[9] Xu, S., Yang, G., Mu, Y. and Deng, R.H., "Secure fine-grained access control and data sharing for dynamic groups in the cloud", IEEE Transactions on Information Forensics and Security, vol.13, no.8, pp.2101-2113, 2018.

[10] Gomathi, N. and Karlekar, N.P., "Ontology and hybrid optimization based SVNN for privacy preserved medical data classification in cloud", International Journal on Artificial Intelligence Tools, vol.28, no.03, pp.1950009, 2019.

[11] Xu, L., Tian, C., Zhang, G., Li, L., Tian, W. and Zhang, Y., "PPDRM: Privacy-Preserving DRM Training and Classification on the Cloud", Available at SSRN 4460902, 2023.

[12] Azizi, M., Aickelin, U., A. Khorshidi, H. and Baghalzadeh Shishehgarkhaneh, M., "Energy valley optimizer: a novel metaheuristic algorithm for global and engineering optimization", Scientific Reports, vol.13, no.1, pp.226, 2023.

[13] Bairwa, A.K., Joshi, S. and Singh, D., "Dingo optimizer: a nature-inspired metaheuristic approach for engineering problems", Mathematical Problems in Engineering, pp.1-12, 2021.

[14] Javaid, S., Abdullah, M., Javaid, N., Sultana, T., Ahmed, J. and Sattar, N.A., "Towards buildings energy management: using seasonal schedules under time of use pricing tariff via deep neuro-fuzzy optimizer", In Proceedings of 15th international wireless communications & mobile computing conference, IWCMC, pp. 1594-1599, IEEE, June 2019.

[15] Gayathri, S. and Gowri, S., "CUNA: A privacy preserving medical records storage in cloud environment using deep encryption" Measurement: Sensors, vol.24, pp.100528, 2022.

[16] Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y. and Vasilakos, A.V., "Security and privacy for storage and computation in cloud computing", Information sciences, vol.258, pp.371-386, 2014.

[17] Stergiou, C. and Psannis, K.E., "Efficient and secure big data delivery in cloud computing", Multimedia Tools and Applications, vol.76, pp.22803-22822, 2017.

[18] Pulido-Gaytan, B., Tchernykh, A., Cortés-Mendoza, J.M., Babenko, M., Radchenko, G., Avetisyan, A. and Drozdov, A.Y., "Privacy-preserving neural networks with homomorphic encryption: C hallenges and opportunities", Peer-to-Peer Networking and Applications, vol.14, no.3, pp.1666-1691, 2021.

[19] Zhu, H., Liu, X., Lu, R. and Li, H., “Efficient and privacy-preserving online medical prediagnosis framework using nonlinear SVM”, IEEE journal of biomedical and health informatics, vol.21, no.3, pp.838-850, 2016.

[20] Shokri, R. and Shmatikov, V., “Privacy-preserving deep learning”, In Proceedings of the 22nd ACM SIGSAC conference on computer and communications security, pp. 1310-1321, October, 2015.

[21] Liang, J., Qin, Z., Xue, L., Lin, X. and Shen, X., “Efficient and privacy-preserving decision tree classification for health monitoring systems”, IEEE Internet of Things Journal, vol.8, no.16, pp.12528-12539, 2021.

[22] Qi, Z., MaungMaung, A. and Kiya, H., “Privacy-Preserving Image Classification Using ConvMixer with Adaptative Permutation Matrix and Block-Wise Scrambled Image Encryption”, Journal of Imaging, vol.9, no.4, pp.85, 2023.

[23] Chenthara, S., Ahmed, K., Wang, H. and Whittaker, F., “Security and privacy-preserving challenges of e-health solutions in cloud computing”, IEEE access, vol.7, pp.74361-74382, 2019.

[24] Yang, P., Xiong, N. and Ren, J., “Data security and privacy protection for cloud storage: A survey”, IEEE Access, vol.8, pp.131723-131740, 2020.

[25] The heart disease dataset is taken from “**https://archive.ics.uci.edu/ml/datasets/heart+disease”** accessed on October 2023.