Computers, Materials & Continua
DOI: 10.32604/cmc.2022.028275
Article

Tech Science Press

Privacy Preserving Image Encryption with Deep Learning Based IoT Healthcare Applications

Mohammad Alamgeer[1], Saud S. Alotaibi[2], Shaha Al-Otaibi[3], Nazik Alturki[3], Anwer Mustafa Hilal[4,*], Abdelwahed Motwakel[4], Ishfaq Yaseen[4] and Mohamed I. Eldesouki[5]

[1]Department of Information Systems, College of Science & Art at Mahayil, King Khalid University, Muhayel Aseer, 62529, Saudi Arabia
[2]Department of Information Systems, College of Computing and Information System, Umm Al-Qura University, Saudi Arabia
[3]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, 11671, Saudi Arabia
[4]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, Al-Kharj, 16278, Saudi Arabia
[5]Department of Information System, College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Al-Kharj, 16278, Saudi Arabia
*Corresponding Author: Anwer Mustafa Hilal. Email: a.hilal@psau.edu.sa
Received: 06 February 2022; Accepted: 10 March 2022

Abstract: Latest developments in computing and communication technologies are enabled the design of connected healthcare system which are mainly based on IoT and Edge technologies. Blockchain, data encryption, and deep learning (DL) models can be utilized to design efficient security solutions for IoT healthcare applications. In this aspect, this article introduces a Blockchain with privacy preserving image encryption and optimal deep learning (BPPIE-ODL) technique for IoT healthcare applications. The proposed BPPIE-ODL technique intends to securely transmit the encrypted medical images captured by IoT devices and performs classification process at the cloud server. The proposed BPPIE-ODL technique encompasses the design of dragonfly algorithm (DFA) with signcryption technique to encrypt the medical images captured by the IoT devices. Besides, blockchain (BC) can be utilized as a distributed data saving approach for generating a ledger, which permits access to the users and prevents third party's access to encrypted data. In addition, the classification process includes SqueezeNet based feature extraction, softmax classifier (SMC), and Nadam based hyperparameter optimizer. The usage of Nadam model helps to optimally regulate the hyperparameters of the SqueezeNet architecture. For examining the enhanced encryption as well as classification performance of the BPPIE-ODL technique, a comprehensive experimental analysis is carried out. The simulation outcomes demonstrate the significant performance of the BPPIE-ODL technique on the other techniques with increased precision and accuracy of 0.9551 and 0.9813 respectively.

Keywords: Internet of things; healthcare; decision making; privacy preserving; blockchain; deep learning

1 Introduction

Latest advances in communication and computing techniques are allowed the development of connected health care systems that depends mainly on Edge and IoT techniques [1]. The medical field is globally emerging as advanced digital solution is being executed for accommodating the rise in health care cost when preserving care quality and sending access to each potential health care service. This field is under great pressure to offer high-quality services to patients and regulate expenses [2]. Extensive information is presented in the health care sector in the form of therapeutic research, medical analysis, clinical preliminaries, complex billing, patient medical records, and so on. This information is a useful resource for wide-ranging medical analysis, research, and patients nowadays are concerned with health care data privacy and confidentiality. In addition, unauthorized access to health care information results in privacy and security problems. Further, continued progress has been made in IoT, resultant in an urgent need to analyse current IoT capabilities and requirements. E-Health is a stimulating IoT application [3]. For handling information with other organizations, this architecture demands secured data transmission. Healthcare information is extremely private and data transmission might increase the exposure possibility. Additionally, the present scheme of data transmission employs a centralized framework that needs centralized trust [4,5].

Encryption of sensitive data is the essential and primary approach in cryptography regarding patients' historical information. Considering the digital health care scheme as the environment for receiving and transferring patients' medical data [6]. The transmission of medical information to authorized users is a crucial requirement of effective health care. But the current system lacks security techniques since majority of these cases lack appropriate access control and encryption method. Most significantly, blockchain (BC) offers a decentralized network and peer-to-peer systems. A global forecasting estimate that the open direction is available to utilize BC technique for managing IoT device in healthcare system [7]. BC-assisted IoT devices could assist patient privacy and recover ownership of healthcare data by leveraging its property including decentralization, persistence, anonymity, and auditability [8]. BC technique in the medical sector is in its earlier developmental stage, and for its effective operation, there are multiple challenges ahead. BC technique offers strength against data exposure and failure. The BC is a communal data structure accountable to store each transaction detail [9,10].

This article introduces a Blockchain with privacy preserving image encryption and optimal deep learning (BPPIE-ODL) technique for IoT healthcare applications. The proposed BPPIE-ODL technique encompasses the design of dragonfly algorithm (DFA) with signcryption technique to encrypt the medical images captured by the IoT devices. Moreover, BC can be utilized as a distributed data saving approach for generating a ledger, which permits access to the users and prevents third party's access to encrypted data. Furthermore, the classification process includes SqueezeNet based feature extraction, softmax classifier (SMC), and Nadam based hyperparameter optimizer. In order to investigate the improved encryption as well as classification performance of the BPPIE-ODL technique, a comprehensive experimental analysis is carried out.

2 Literature Review

Dwivedi et al. [11] presented architecture of adapted BC model applicable for IoT devices that relies on distributed nature and security and privacy properties of the system. This further security and privacy property in this method depend on innovative cryptographic primitive. In [12], BC as a distributed database was presented with a homomorphic encryption approach for ensuring a secured search and keywords-based access to database. In addition, the presented method offers a secured key

revocation method and update different policy consequently. Consequently, a secured patient medical data access system is developed, that incorporates trust chain and BC to satisfy the security and efficiency problems in the existing systems. Hamza et al. [1] presented a privacy preserving chaos-based encryption cryptosystem for protecting patient privacy. The presented cryptosystem could defend patient image in compromised broker. Particularly, it can be proposed a fast probabilistic cryptosystem for securing healthcare key frame which are extracting in wireless capsule endoscopy process with a prioritization technique.

Alassaf and Gutub [13] proposed a comparative study of efficiency metrics of three trusted candidate encryption methods such as SIMON, AES, and SPECK, that is compared and simulated in detail for distinguishing has the optimal performance that designated for a healthcare application. This encryption algorithm is evaluated and implemented regarding the power consumption, execution time, speed, and memory occupation. In [14], a privacy-preserving DSSE system for IIoTH has been introduced. An initial DSSE system developed to personal health record (PHR) dataset with forwarding security. Once the user implements searching operation, he/she gets corresponding attribute values rather than the entire files.

Denis and Madhubala [15] present a hybridization of data encryption method for sheltering the diagnoses information in healthcare image. The projected method was designed by integrating 2D-DWT-2 L or 2D-DWT-1 L steganography using the presented hybrid encryption system. The hybrid encryption system was constructed by employing Rivest–Shamir–Adleman (RSA) and Advanced Encryption Standard (AES) approaches for securing diagnoses information that embed with RGB channel of healthcare cover images. In [16], Evolutionary Algorithms, such as the Memetic Algorithm are utilized to encrypt the text message. Then, the encoded data is injected into the healthcare image with DWT 1 level and 2 levels. The reverse approach of the Memetic Algorithm was executed once removing hidden messages in the encrypted letter.

3 The Proposed Method

In this study, a new BPPIE-ODL technique has been developed to accomplish security and classification on IoT healthcare applications. The major goal of the BPPIE-ODL technique is to securely transmit the encrypted medical images captured by IoT devices and performs classification process at the cloud server. The proposed BPPIE-ODL technique follows several subprocesses namely IoT based data acquisition, signcryption, DFA based optimal key generation, SqueezeNet feature extractor, Nadam hyperparameter optimizer, and SMC. Fig. 1 illustrates the overall process of BPPIE-ODL technique.

3.1 Image Encryption: Signcryption with Optimal Key Generation Process

Initially, the IoT devices can be utilized for capturing the medical images which are then encrypted by the use of signcryption approach before transmitting to the cloud server. An important function of this work is for developing mutually authenticated data broadcast protocols which offer secret, integrity, and authenticity of information [17]. Primarily, the typical data is assumed for security procedure which is encrypted and decrypt technique, at this point DFA based signcryption approach was presented. The drive of optimally key selective from security method was selecting optimum private as well as public keys from both senders as well as receiver sides. Afterward, the data is encrypted, it's saved from the cloud or relevant region, then optimally private key was employed to data decryption technique, at this point the optimally key was achieved dependent upon the main function as maximal PSNR value and this presented technique was executed from MATLAB platform.

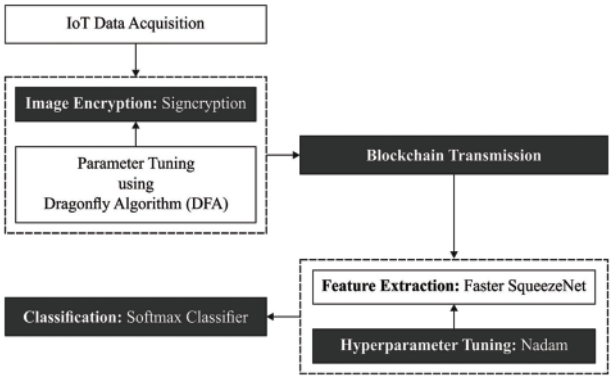

Figure 1: Overall process of BPPIE-ODL technique

A novel approach to public key cryptography was Signcryption that concurrently fulfills both the element of digital signatures and open key encryption with minimum cost. The property contained from signcryption is Non-repudiation, Secret, Integrity, and Unforgeability. Any signcryption has more elements namely Public verifiability and forwarding confidentiality of secret communication [17]. The communication forwarded of past encoding data was extremely secured by presented DFA signcryption with optimum key selective.

3.1.1 Key Generation

The signcryption signifies the public-key primitive that constitute 2 essential cryptographic gadget that is able of making sure the non-repudiation, privacy, and honesty. This initialized method initializes the prime number, hash function (HF) with key. It can develop the private as well as public keys to both the sender and receiver. For increasing the data security, the projected approach employs the ideal private key by optimized approach.

Initialization:- L_P refers the large prime numbers, L_f signifies the large prime factors, I denotes the integer with order L_f modulo L_P, certain arbitrarily in $[1\ ,\ \ldots L_P - 1]$, Hash One way HF, whose outcome is a minimum128 bit, L_P Keyed one way HF D Value, elected arbitrarily $\left[1,\ \ldots\ L_f - 1\right]$.

Sender Key pair $((M_{k1},\ N_{k1}))$

$$M_{k1} = Q^{A_{k1}} \bmod L_P \tag{1}$$

Receiver key pairs $(M_{k2},\ N_{k2})$

$$N_{k2} = Q^{A_{k2}} \bmod L_P \tag{2}$$

3.1.2 Optimal Key Generation Process

For effectively choosing the optimal keys involved at the sender and receiver sides, the DFA can be utilized. DFA is stimulating the swarming behavior of dragonflies [18]. The purpose for swarming is hunting or migration (static swarm or dynamic swarm, correspondingly). During static swarm, smaller group of dragonflies moves over a smaller region for hunting other insects. This type of swarming Behavior includes abrupt changes and local movements. During dynamic swarming, a large number of dragonflies create an individual group and move in one direction for a long distance [19]. The abovementioned behaviors are considered the primary motivation of DFA. For directing artificial dragonfly to different paths, five weights have been applied, that is alignment weight (a), separation

weight (s), enemy factor (e), cohesion weight (c), the inertia weight (w) and food factor (f). To exploit the searching space, lower-cohesion weights and higher alignment can be utilized, but to explore the searching space higher-cohesion weights and lower alignment are utilized. Tuning the swarming weights ($s,\ a,\ c, f, e, and\ w$) adoptively in the optimization method is alternative method for balancing exploitation and exploration.

$$S_i = -\sum_{j=1}^{N} X - X_j \tag{3}$$

Here, X shows the location for the existing individual, X_j indicates the location for the j^{th} neighboring dragonfly, N represent the amount of individual neighbours of the dragonfly swarm, and S shows the separation movement for i^{th} individual:

$$A_i = \frac{\sum_{j=1}^{N} V_j}{N} \tag{4}$$

whereas V denotes the velocity of j^{th} neighboring dragonfly and A_i represent the alignment movement for i^{th} individual. Cohesion can be formulated by:

$$C_i = \frac{\sum_{j=1}^{N} X_j}{N} - X \tag{5}$$

In which N indicates the neighbourhood size, C_i represent the cohesion for i^{th} individual, X indicates the present dragonfly individual, and X_j represents the location of the j^{th} neighboring dragonfly. The attractive movement towards food can be calculated by:

$$F_i = X^+ - X \tag{6}$$

Now X^+ denotes the location of the source of food, F_i signifies the attraction of food for i^{th} dragonfly and X represent the location of the existing dragonfly individual. Distraction outward predator can be evaluated by:

$$E_i = X^- + X \tag{7}$$

where X represent the location of existing dragonfly individual, E_i means the enemy distraction movement for i^{th} individual, and X^- shows the enemy location. For location update in the searching space, artificial dragonfly uses position vector X and step vector ΔX. The step vector is correspondence to the velocity vector in PSO approach. Also, the location update is mainly depending on the PSO approach:

$$\Delta X_{t+1} = (sS_i + aA_i + cC_i + fF_i + eE_i) + w\Delta X_t \tag{8}$$

In which w represent the inertia weight; C_i shows the cohesion for i^{th} dragonfly; A_i indicates the alignment for i^{th} dragonfly; E_i implies the place of enemy for i^{th} dragonfly; F_i characterizes the food source for i^{th} individual; S_i shows the separation for i^{th} dragonfly; and t denotes the amount of iterations.

Once the step vector estimation is completed, the estimation for the location vector starts by:

$$X_{t+1} = X_t + \Delta X_{t+1} \tag{9}$$

In which t designates the existing iteration. The DFA derives a fitness function for optimal key generation process, as given below.

$$fitness\ function = \max\{PSNR\} \tag{10}$$

The objective of the DFA is to select the optimal keys for the signcryption process in such a way that the PSNR can be maximized.

3.2 Blockchain Technology

In this work, BC can be utilized as a distributed data saving approach for generating a ledger, which permits access to the users and prevents third party's access to encrypted data. The BC is an immutable distributed data base for that novel time-stamped transaction was append and group as to hash-chain of blocks [19]. The fundamental BC protocols determine that several copies of such blocks are created and maintained in a distributed fashion. An important aspect of this protocol was decided that network of participants, recognized that miners, is found consensus on existing state of BC. It can be various kinds of BC structures (that is, permission-less, permissioned, public, and private). There are 2 main approaches to the similar such as Proof of Work (PoW) and Proof of Stake (PoS). When these tasks are done, a novel transaction is together with the BC. All blocks have of unique code named as hash that also comprises the hash of preceding block from the chains, and is utilized for connecting the block composed from a particular order. Some miner has to execute a group of calculations for establishing their credibility as a leader. This computation resolves a puzzle for mapping arbitrarily size data to set size.

Generally, a leader is selected from one of these 2 approaches. In PoW, several miners try for solving the puzzles, and the one that finishes primary transmits to the group proof that the work was complete. Another miner then validates that the work completed is correct. If all confirm this, it can be choose that specific miner as leader. An initial drive of block is for maintaining a list of verified transactions utilizing a cryptographic hash function. The hash function was effectual due to the subsequent properties:

- It creates a resultant of set length irrespective of length of the input.
- It can be deterministic that represents that it makes a similar result to a provided input.
- It can be irreversible signifies that obtaining a similar input in the outcome is not feasible.
- Some slight perturbation to the original input creates novel output.
- The hash computation is quick with lesser overhead.

The block from the BC was connected to first of all genesis blocks and is verified by hashes. Fig. 2 illustrates the structure of BC. Every block was related to the connections of every hash that implies all the blocks comprise the preceding hash, and these obtain more hashed from the next blocks. Some modify to hash because the chain that broken as the novel hash was until attach by next block from the chain. Recalculate the novel hash for restoring the chain needs several counts of computing powers. Besides, nonce was more than the miner is role with data for producing a hash that outputs 3 leading zeroes. If the miners establish a nonce which outcomes from its block's hash being under the complexity threshold, the block was lastly assumed that valid, and it could be transmitted to network with miner taking a reward to its efforts.

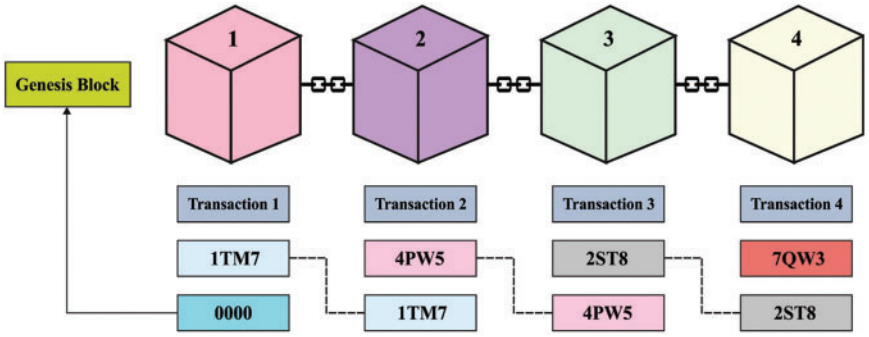

Figure 2: Framework of blockchain

3.3 Image Classification

Once the encrypted images are available at the cloud server, the decryption process is carried out followed by classification process, which involves Faster SqueezeNet feature extractor, Nadam hyperparameter optimizer, and SMC. The working of each module is elaborated in the succeeding sections.

3.3.1 Faster SqueezeNet

During feature extraction process, the Faster SqueezeNet model can be applied to derive a useful collection of feature vectors. To enhance the real-time performance and accuracy of image classification, Fast SqueezeNet has been introduced [20]. To avoid overfitting, we add residual and BatchNorm models. Simultaneously, as DenseNet, we utilized concat for connecting distinct layers to improve the expressiveness of the initial layer in the network. Fast SqueezeNet contains three-block layers, four convolutional layers, a global average pooling layer and1 BatchNorm layer. Fast SqueezeNet is largely enhanced in a subsequent manner. Further, to enhance the data flow among layers, it can be imitated the DenseNet architecture and presented a distinct connection mode. This comprises a fire module and pooling layer, and lastly, the two concat layers are interconnected with the following convolutional layer. The existing layer receives each feature map of the previous layer, and utilize $x_0, \ldots, x_{l-1}$ as input;

$$x_l = H_l\ ([x_0,\ x_1,\ \ldots,\ x_{l-1}]) \tag{11}$$

whereas $[x_0,\ x_1,\ \ldots,\ x_{l-1}]$ represent the connection of feature graph created in layer $0, 1, \ldots, l-1$ and H_l concatenate many inputs. Now, x_0 signifies the max pooling layer, x_1 signifies the Fire layer, and x_l shows the concat layer. Without extremely improving the amount of network variables, the efficiency of the system can be improved in the earlier phases, and simultaneously, two-layer networks could communicate directly data.

To guarantee good network convergence, it is learn in the ResNet architecture and present distinct components that comprise a fire module and a pooling layer. At last, afterward, the two layers are summed, it is interconnected to the following convolution layers.

3.3.2 Nadam Optimizer

To optimally adjust the hyperparameter values of the SqueezeNet model, the Nadam optimizer can be utilized. The Nadam optimizer combines Nesterov-accelerated adaptive moment estimation into the Adam [21]. The great advantage of this combined technique is that employed adaptive moment

estimating helps in carry out high precision step in the gradient direction through update of model parameters with momentum step beforehand the computation of gradient. The upgrading rule of Nadam can be described by the following:

$$w_t = w_{t-1} - \alpha \times \frac{\bar{m}_t}{\sqrt{\hat{v}_t} + \varepsilon} \tag{12}$$

whereas

$$\bar{m}_t = \left(1 - \beta_{1,t}\right) \hat{g}_t + \beta_{1,t+1} \hat{m}_t$$

$$\hat{m}_t = \frac{m_t}{1 - \prod_{i=1}^{t+1} \beta_{1i}}$$

$$\hat{g}_t = \frac{g_t}{1 - \prod_{i=1}^{t+1} \beta_{1i}} \tag{13}$$

3.3.3 Softmax Classifier

At the final stage, the SMC model is utilized to allot proper class labels. The SMC layer could forecast the label probability of input data x_j with the help = the feature learned from the 3rd hidden state depiction $h_i^{(3)}$. The amount of nodes existing in SMC layer was selected as corresponding to the amount of labels. Although classifiers like SVM could also be utilized, softmax LR permits users to improve the entire deep networks via fine-tuning [22]. The subsequent objective function was minimalized for fine-tuning the network along with softmax layer.

$$J_{SSAE-SMC}\left(W,\ b,\ x, \hat{z}\right) = \min_{W,b} J\left(x, \hat{z}\right)\ + \lambda^{smc} \| W^{smc} \|_2^2 \tag{14}$$

whereas W and b represent the weights and bias of the entire deep networks, $J\left(x, \hat{z}\right)$ denotes the LR cost amongst the classification attained by input feature x and the unsupervised results $\hat{z}$, W^{smc} stands for the weight and λ^{smc} indicates the weight decay variable on SMC layer. The SMC layer is utilized for classification. Here, y_i signifies label of trained instance x_i. Likelihood of x_i belonging to the k^{th} class is equated by the following equation

$$p\left(y_j = k | x_j; W_{smc},\ b_{smc}\right) = \frac{e^{W_{smc}^{(k)^T} x_i + b_{smc}^{(k)}}}{\sum_{j=1}^{N} e^{W_{smc}^{(j)^T}, x_i + b_{smc}^{(j)}}} \tag{15}$$

In which $W_{smc}^{(k)}$ and $b_{smc}^{(k)}$ denotes the distribution of weight as well as bias from k^{th} class. N shows the overall amount of classes, that correspond to 5 grade groups. As per the maximum probability, we could calculate the grade group of instance x_j as follows:

$$Grade\ \ (x_i) = arg_k \tag{16}$$

4 Result and Discussion

The experimental result analysis of the BPPIE-ODL model is validated utilizing the ISIC dataset [23]. The dataset includes dermoscopic images under distinct classes like Angioma, Nevus, Lentigo NOS, Solar Lentigo, Melanoma, Seborrheic Keratosis, and Basal Cell Carcinoma. A few sample images are illustrated in Fig. 3.

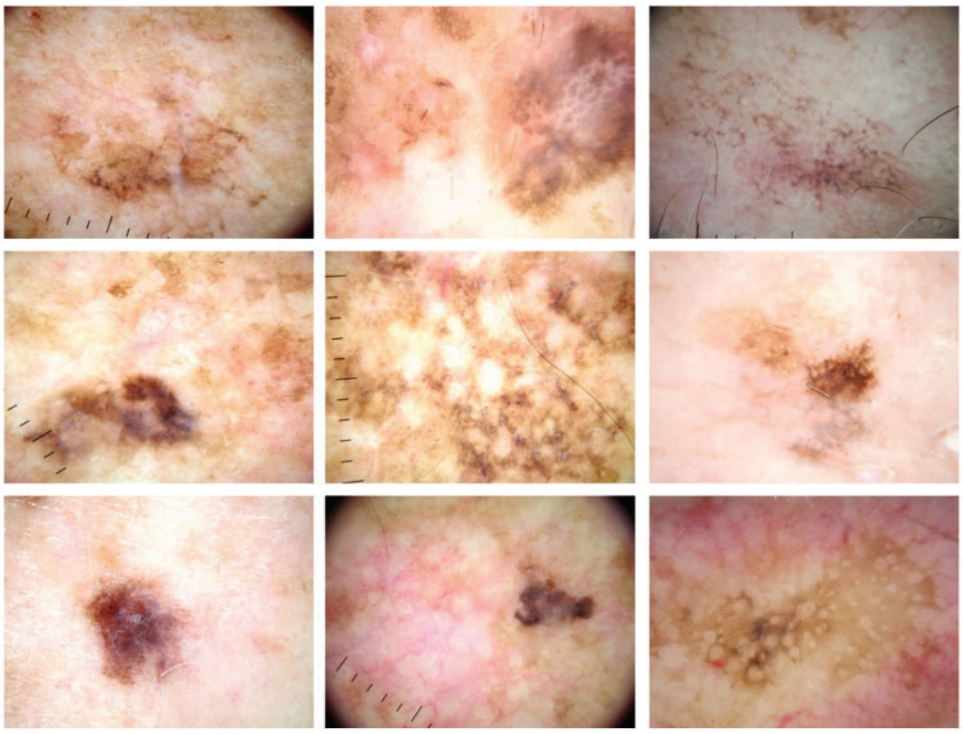

Figure 3: Sample images

Fig. 4 visualizes the result analysis of the BPPIE-ODL model. The first column indicates the input medical images and the respective encrypted versions are offered in second column. Finally, the histogram of these images is provided in the third column.

An extensive MSE analysis of the BPPIE-ODL approach with compared algorithms is provided in Fig. 5. The outcomes specified that the BPPIE-ODL method has depicted effectual outcomes with minimal values of MSE. For instance, with test image 1, the BPPIE-ODL model has reached decreased MSE value of 0.081 whereas the BEEPO, hybrid-CE, PSOECC, and CO-ECC techniques have achieved higher MSE values of 0.088, 0.127, 1.147, and 1.281 respectively. Additionally, with test image 5, the BPPIE-ODL model has accomplished least MSE value of 0.066 whereas the BEEPO, hybrid-CE, PSOECC, and CO-ECC techniques have accomplished increased MSE values of 0.075, 0.140, 1.249, and 2.784 respectively.

Fig. 6 depicts the comparative PSNR examination of the BPPIE-ODL approach with recent models. The results have shown the supremacy of the BPPIE-ODL model with maximum PSNR values under every test image. For instance, with test image 1, the BPPIE-ODL model has attained maximum PSNR value of 59.046 dB whereas the BEEPO, hybrid-CE, PSOECC, and CO-ECC techniques have obtained lower PSNR values of 58.686 dB, 57.093 dB, 47.535 dB, and 47.055 dB respectively.

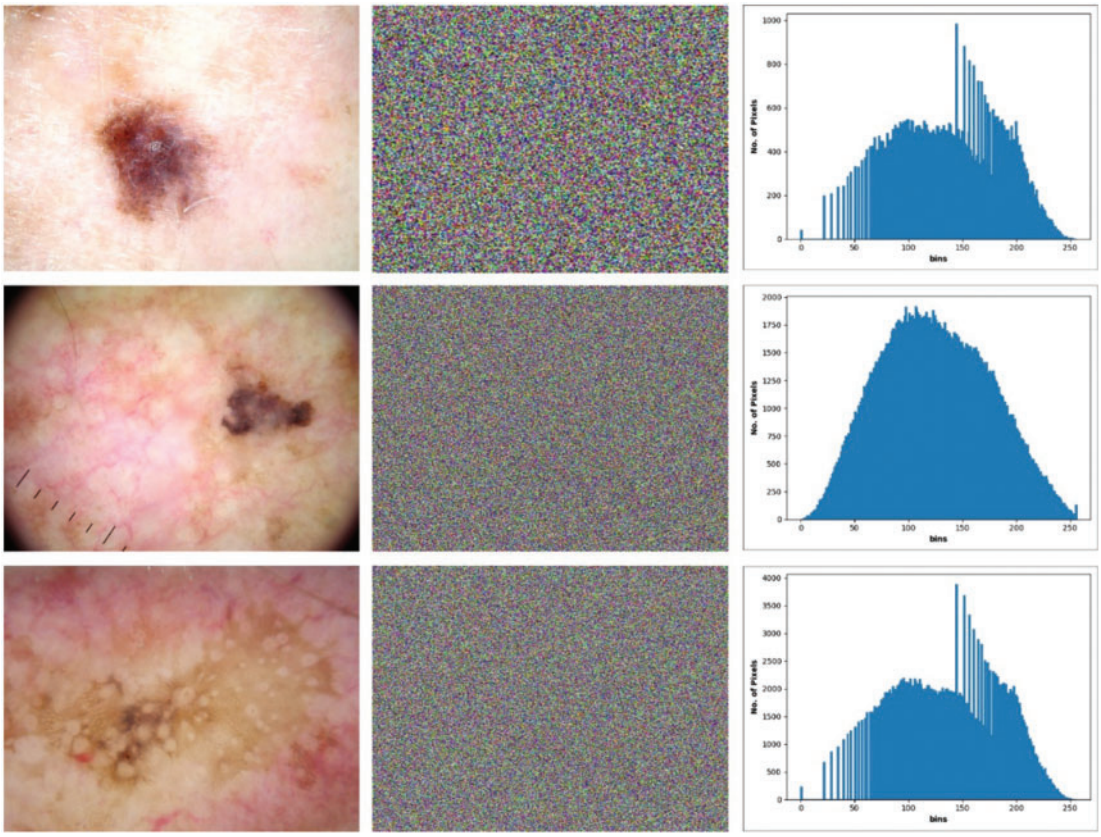

Figure 4: Sample results: first column original images second column encrypted image third colum histogram of encrypted image

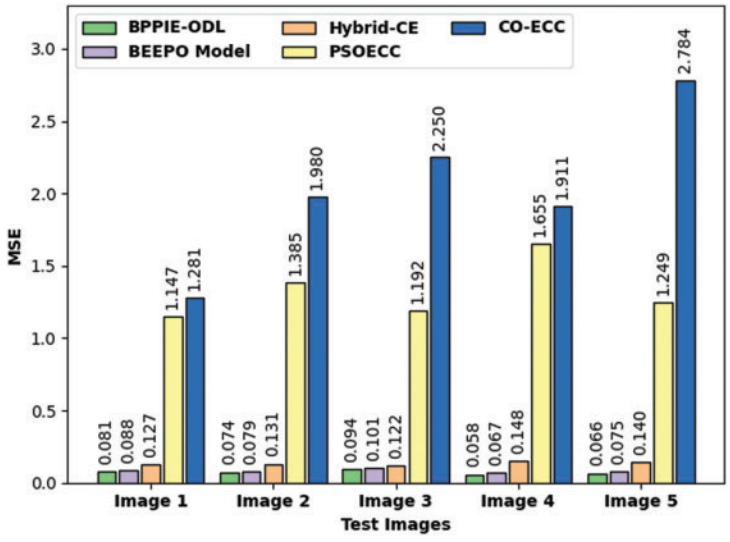

Figure 5: MSE analysis of BPPIE-ODL technique with different images

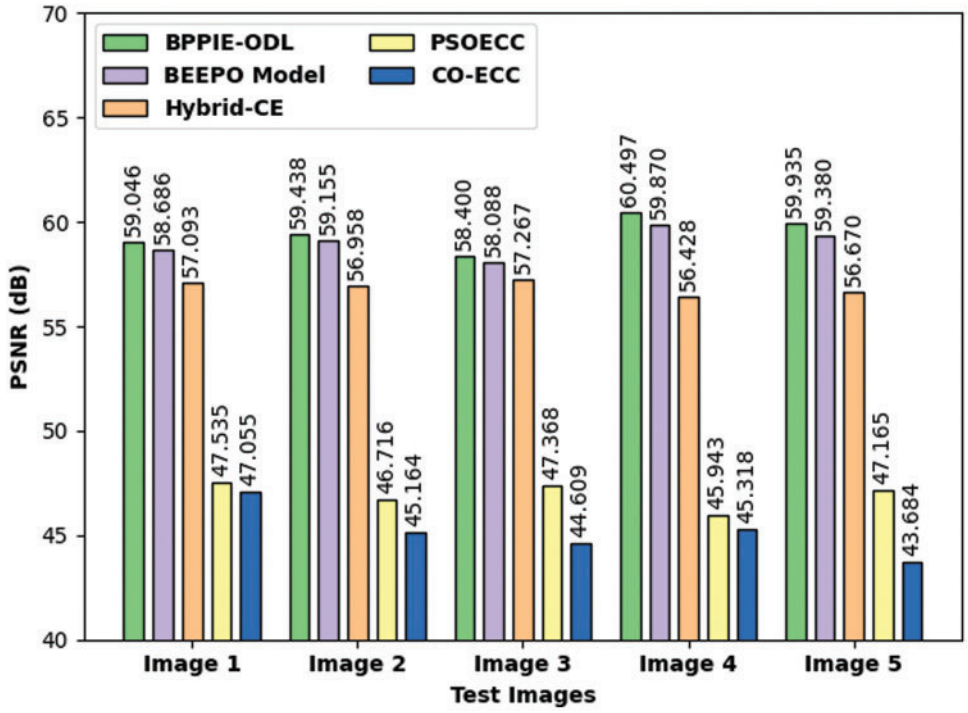

Figure 6: PSNR analysis of BPPIE-ODL technique with different images

Furthermore, with test image 5, the BPPIE-ODL model has resulted in increased PSNR value of 59.935 dB whereas the BEEPO, hybrid-CE, PSOECC, and CO-ECC techniques have reached decreased PSNR values of 59.380 dB, 56.670 dB, 47.1635 dB, and 43.684 dB respectively.

Tab. 1 and Fig. 7 depict the comparative CC examination of the BPPIE-ODL approach with existing models. The results outperformed the supremacy of the BPPIE-ODL technique with maximal CC values under every test image. For instance, with test image 1, the BPPIE-ODL technique has reached increased CC value of 99.82% whereas the BEEPO, hybrid-CE, PSOECC, and CO-ECC methodologies have obtained decreased CC values of 99.74%, 99.54%, 99.21%, and 99.10% respectively. In addition, with test image 5, the BPPIE-ODL technique has resulted in maximum CC value of 99.95% whereas the BEEPO, hybrid-CE, PSOECC, and CO-ECC techniques have gained lower CC values of 99.91%, 99.81%, 99.41%, and 99.34% correspondingly.

Table 1: CC analysis of BPPIE-ODL technique with recent approaches

Test images	BPPIE-ODL	BEEPO model	Hybrid-CE	PSOECC	CO-ECC
Image 1	99.82	99.74	99.54	99.21	99.10
Image 2	99.94	99.91	99.75	99.41	99.08
Image 3	99.91	99.84	99.63	99.33	99.13
Image 4	99.97	99.95	99.72	99.52	99.26
Image 5	99.95	99.91	99.81	99.41	99.34

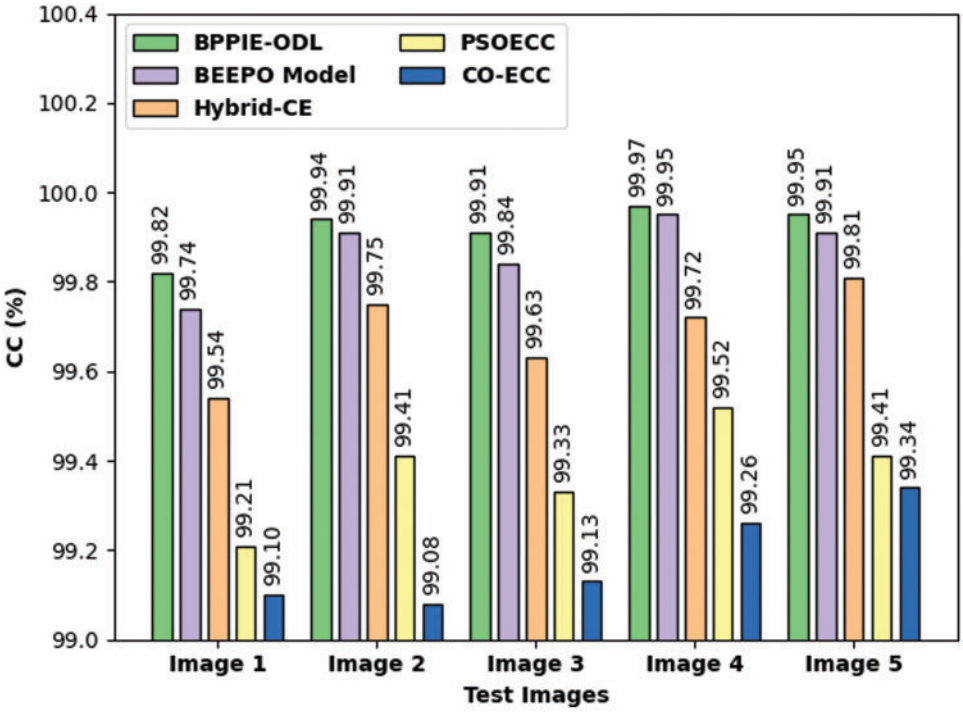

Figure 7: CC analysis of BPPIE-ODL technique with different images

A detailed CT analysis of the BPPIE-ODL model with compared approaches is provided in Tab. 2 and Fig. 8. The outcomes specified that the BPPIE-ODL technique has depicted effectual outcomes with lower values of CT. For instance, with test image 1, the BPPIE-ODL model has gained minimal CT value of 42.84 s whereas the BEEPO, hybrid-CE, PSOECC, and CO-ECC techniques have achieved superior CT values of 54.60 s, 65.40 s, 101.40 s, and 111.00 s correspondingly. Moreover, with test image 5, the BPPIE-ODL model has accomplished least CT value of 41.35 s whereas the BEEPO, hybrid-CE, PSOECC, and CO-ECC techniques have accomplished higher CT values of 48 s, 58.80 s, 129.60 s, and 154.80 s correspondingly.

Table 2: Computation time (sec) analysis of BPPIE-ODL technique with recent approaches

Computation time (sec)					
Test images	BPPIE-ODL	BEEPO model	Hybrid-CE	PSOECC	CO-ECC
Image 1	42.84	54.60	65.40	101.40	111.00
Image 2	36.11	40.20	57.60	116.40	120.00
Image 3	32.24	39.60	41.40	127.20	146.40
Image 4	49.87	63.00	76.80	138.00	148.80
Image 5	41.35	48.00	58.80	129.60	154.80

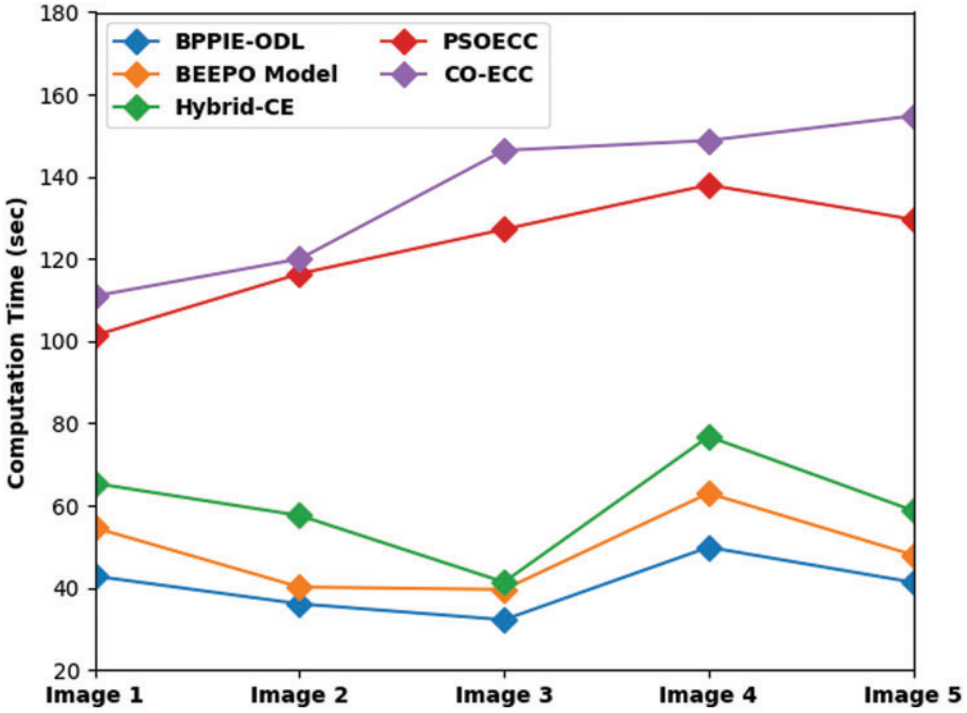

Figure 8: CT analysis of BPPIE-ODL technique with different images

Tab. 3 reports the comparative classification result analysis of the BPPIE-ODL approach with existing algorithms [24–26]. Fig. 9 showcases comparison study of the BPPIE-ODL model interms of precision and accuracy. The results referred that the EBT model has resulted to lower performance with the precision and accuracy of 0.9092 and 0.8946 respectively. Next, the F-KNN, DT, and MC-SVM models have obtained slightly improved values of precision and accuracy. At the same time, the ELM model has shown competitive outcomes with the precision and accuracy of 0.9551 and 0.9813 correspondingly. However, the projected BPPIE-ODL approach has accomplished increased precision and accuracy of 0.9551 and 0.9813 respectively.

Table 3: Comparative analysis of BPPIE-ODL technique with existing approaches

Methods	Precision	FDR	Accuracy	Time (min)
MC-SVM	0.9086	0.0914	0.9311	3.5426
F-KNN	0.9077	0.0923	0.9070	2.8382
DT	0.9341	0.0659	0.9279	2.7264
Naïve Bayes	0.9262	0.0738	0.9769	3.4085
EBT	0.9092	0.0908	0.8946	2.6672
ELM	0.9418	0.0582	0.9502	2.2033
BPPIE-ODL	0.9551	0.0449	0.9813	1.8713

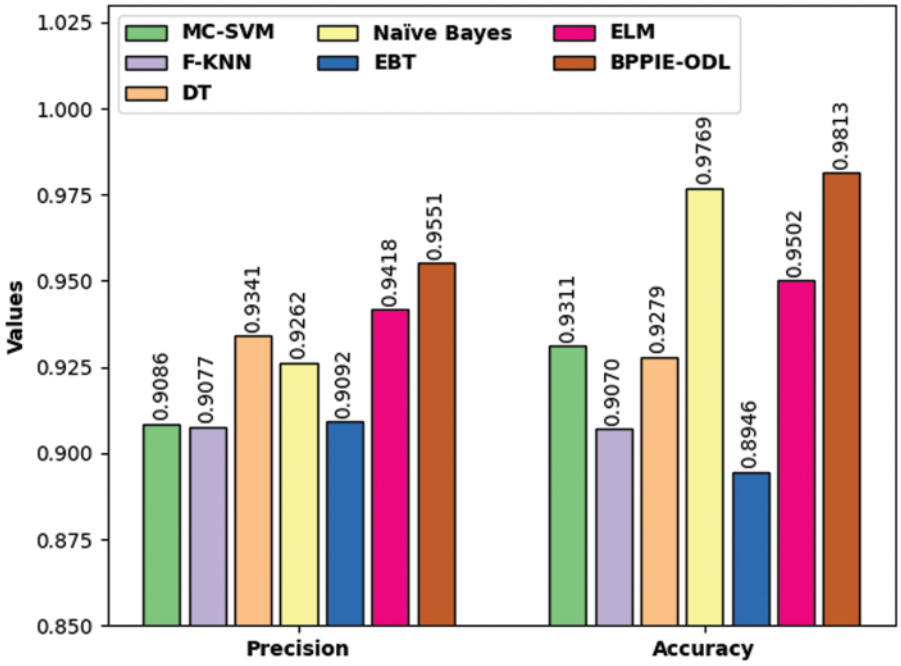

Figure 9: Comparative analysis of BPPIE-ODL technique with recent approaches

A brief computation time (CT) analysis of the BPPIE-ODL with recent models interms of CT as depicted in Fig. 10. The experimental results indicated that the MC-SVM and NB models have obtained higher CTs of 3.5426 min and 3.4085 min. In line with, the F-KNN, DT, EBT, and ELM techniques have obtained slightly reduced CT of 2.8382 min, 2.7264 min, 2.6672 min, and 2.2033 min respectively. However, the BPPIE-ODL methodology has outperformed the other techniques with the minimal CT of 1.8713 min. From these result analyses, it can be concluded that the BPPIE-ODL model has been found to be effective for security and classification in the IoT environment.

The accuracy outcome analysis of the BPPIE-ODL technique on the test data is illustrated in Fig. 11. The outcomes exhibited that the BPPIE-ODL system has accomplished improved validation accuracy compared to training accuracy. It is also observable that the accuracy values get saturated with the epoch count of epochs. The loss outcome analysis of the BPPIE-ODL system on the test data is demonstrated in Fig. 11. The figure exposed that the BPPIE-ODL approach has denoted the reduced validation loss over the training loss. It is additionally noticed that the loss values get saturated with the count of epochs.

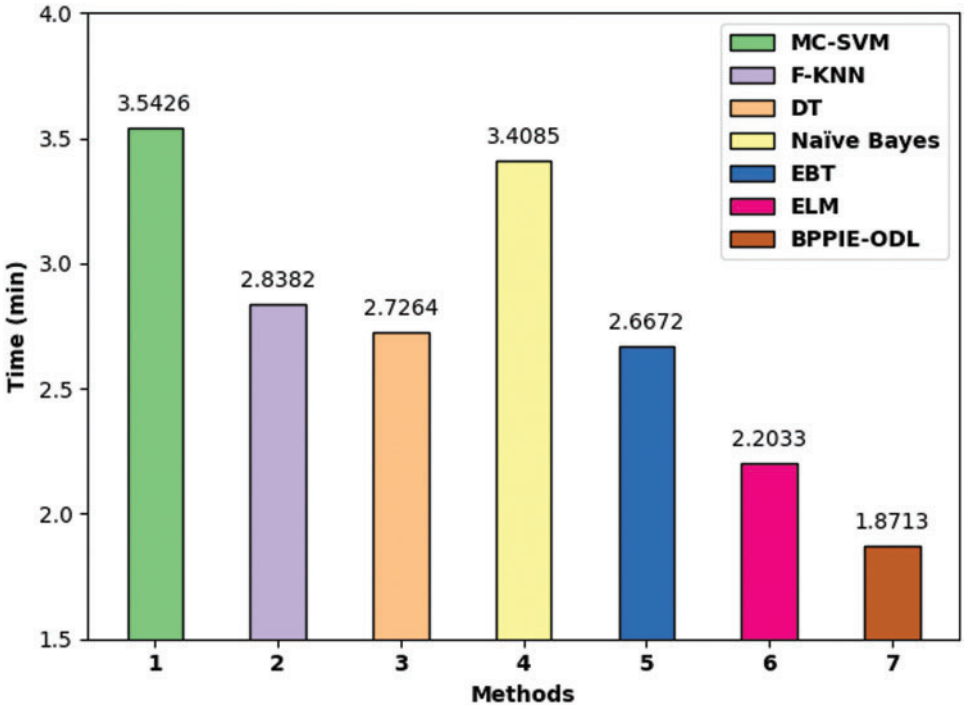

Figure 10: CT analysis of BPPIE-ODL technique with recent approaches

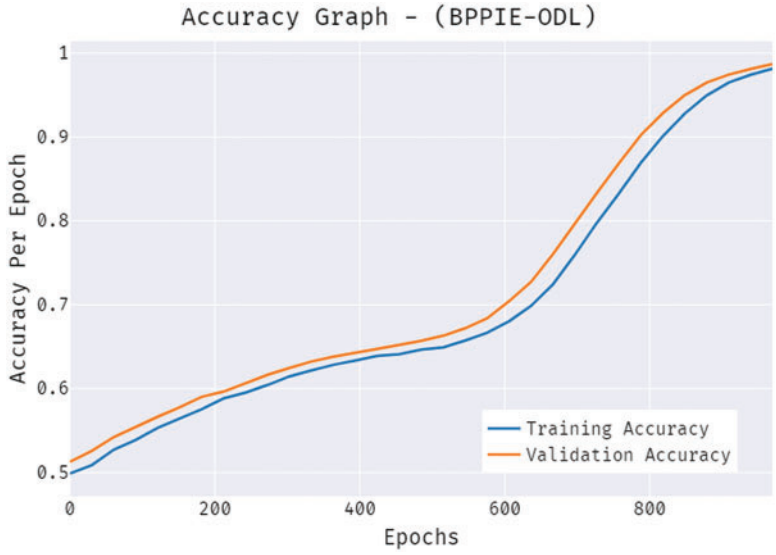

Figure 11: Loss graph analysis of BPPIE-ODL technique

5 Conclusion

In this study, a new BPPIE-ODL approach was developed to accomplish security and classification on IoT healthcare applications. The major goal of the BPPIE-ODL technique is to securely

transmit the encrypted medical images captured by IoT devices and performs classification process at the cloud server. The proposed BPPIE-ODL technique follows several subprocesses namely signcryption, DFA based optimal key generation, Faster SqueezeNet feature extractor, Nadam hyperparameter optimizer, and SMC. The design of DFA assists in effectively determining the keys for encryption and decryption processes. In order to investigate the improved encryption as well as classification performance of the BPPIE-ODL technique, a comprehensive experimental analysis is implemented. The simulation outcomes demonstrate the significant performance of the BPPIE-ODL technique over the other methods with increased precision and accuracy of 0.9551 and 0.9813 respectively. In future, the performance of the BPPIE-ODL technique can be improvised by hybrid metaheuristic algorithms.

Acknowledgement: The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: (22UQU4210118DSR03).

Funding Statement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work under Grant Number (RGP.1/283/43). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R136), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista and F. Titouna, "A Privacy-preserving cryptosystem for IoT E-healthcare," *Information Sciences*, vol. 527, pp. 493–510, 2020.

[2] W. Li, C. Jin, S. Kumari, H. Xiong and S. Kumar, "Proxy re-encryption with equality test for secure data sharing in internet of things-based healthcare systems," *Transactions on Emerging Telecommunications Technologies*, 2020, https://doi.org/10.1002/ett.3986.

[3] Y. Winnie, U. E. and D. M. Ajay, "Enhancing data security in IoT healthcare services using fog computing," in *2018 Int. Conf. on Recent Trends in Advance Computing (ICRTAC)*, Chennai, India, pp. 200–205, 2018.

[4] X. R. Zhang, W. F. Zhang, W. Sun, X. M. Sun and S. K. Jha, "A robust 3-D medical watermarking based on wavelet transform for data protection," *Computer Systems Science & Engineering*, vol. 41, no. 3, pp. 1043–1056, 2022.

[5] X. R. Zhang, X. Sun, X. M. Sun, W. Sun and S. K. Jha, "Robust reversible audio watermarking scheme for telemedicine and privacy protection," *Computers, Materials & Continua*, vol. 71, no. 2, pp. 3035–3050, 2022.

[6] G. Srivastava, J. Crichigno and S. Dhar, "A light and secure healthcare blockchain for IoT medical devices," in *2019 IEEE Canadian Conf. of Electrical and Computer Engineering (CCECE)*, Edmonton, AB, Canada, pp. 1–5, 2019.

[7] J. A. Alzubi, "Blockchain-based lamport merkle digital signature: Authentication tool in IoT healthcare," *Computer Communications*, vol. 170, pp. 200–208, 2021.

[8] A. Sharma, S. Kaur and M. Singh, "A comprehensive review on blockchain and internet of things in healthcare," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 10, pp. e4333, 2021.

[9] S. Shukla, S. Thakur, S. Hussain, J. G. Breslin and S. M. Jameel, "Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model," *Internet of Things*, vol. 15, pp. 100422, 2021.

[10] O. A. Alzubi, J. A. Alzubi, K. Shankar and D. Gupta, "Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in internet of things," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 12, pp. e4360, 2021.

[11] A. Dwivedi, G. Srivastava, S. Dhar and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, pp. 326, 2019.
[12] A. Ali, M. A. Almaiah, F. Hajjej, M. F. Pasha, O. H. Fang *et al.,* "An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network," *Sensors*, vol. 22, no. 2, pp. 572, 2022.
[13] N. Alassaf and A. Gutub, "Simulating light-weight-cryptography implementation for iot healthcare data security applications," *International Journal of E-Health and Medical Communications*, vol. 10, no. 4, pp. 1–15, 2019.
[14] Y. Liu, J. Yu, J. Fan, P. Vijayakumar and V. Chang, "Achieving privacy-preserving dsse for intelligent IoT healthcare system," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 2010–2020, 2022.
[15] R. Denis and P. Madhubala, "Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems," *Multimedia Tools and Applications*, vol. 80, no. 14, pp. 21165–21202, 2021.
[16] S. Doss, J. Paranthaman, S. Gopalakrishnan, A. Duraisamy, S. Pal *et al.,* "Memetic optimization with cryptographic encryption for secure medical data transmission in iot-based distributed systems," *Computers, Materials & Continua*, vol. 66, no. 2, pp. 1577–1594, 2021.
[17] K. Shankar, M. Elhoseny, E. Perumal, M. Ilayaraja and K. S. Kumar, "An efficient image encryption scheme based on signcryption technique with adaptive elephant herding optimization," in *Cybersecurity and Secure Information Systems, Advanced Sciences and Technologies for Security Applications Book Series (ASTSA)*, Springer, Cham, pp. 31–42, 2019.
[18] Y. Meraihi, A. R. Cherif, D. Acheli and M. Mahseur, "Dragonfly algorithm: A comprehensive review and applications," *Neural Computing and Applications*, vol. 32, no. 21, pp. 16625–16646, 2020.
[19] J. Li, J. Wu, G. Jiang and T. Srikanthan, "Blockchain-based public auditing for big data in cloud storage," *Information Processing & Management*, vol. 57, no. 6, pp. 102382, 2020.
[20] Y. Xu, G. Yang, J. Luo and J. He, "An electronic component recognition algorithm based on deep learning with a faster SqueezeNet," *Mathematical Problems in Engineering*, vol. 2020, pp. 1–11, 2020.
[21] N. D. Hoang, "Automatic impervious surface area detection using image texture analysis and neural computing models with advanced optimizers," *Computational Intelligence and Neuroscience*, vol. 2021, pp. 1–17, 2021.
[22] B. Abraham and M. S. Nair, "Computer-aided classification of prostate cancer grade groups from MRI images using texture features and stacked sparse autoencoder," *Computerized Medical Imaging and Graphics*, vol. 69, pp. 60–68, 2018.
[23] https://challenge.isic-archive.com/data/. 2021.
[24] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maseleno and N. Arunkumar, "Hybrid optimization with cryptography encryption for medical image security in internet of things," *Neural Computing and Applications*, vol. 32, no. 15, pp. 10979–10993, 2020.
[25] U. Padmavathi and N. Rajagopalan, "Blockchain enabled emperor penguin optimizer based encryption technique for secure image management system," *Wireless Personal Communications*, 2021, https://doi.org/10.1007/s11277-021-08800-w.
[26] F. Afza, M. Sharif, M. A. Khan, U. Tariq, H. S. Yong *et al.,* "Multiclass skin lesion classification using hybrid deep features selection and extreme learning machine," *Sensors*, vol. 22, no. 3, pp. 799, 2022.