IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 10 May 2023, accepted 29 May 2023, date of publication 7 June 2023, date of current version 23 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3283930

RESEARCH ARTICLE

Enhancing Breast Cancer Classification in Histopathological Images through Federated Learning Framework

JYOTHI PETA AND SRINIVAS KOPPU
School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu 632014, India
Corresponding author: Srinivas Koppu (srinukoppu@vit.ac.in)

This work was supported by the School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India.

ABSTRACT In recent decades, the mortality rate of breast cancer in females is rapidly increasing because of unawareness and failed to detect in earlier stages. In existing, several studies are attempted to develop a robust mechanism for detecting breast cancers from the given input samples. However, they are not as much effective because of several limitations and the secured sharing of sensitive medical images is still a challenging problem faced by medical sector. Thus, the proposed study aims to introduce an automated disease diagnosis system using federated learning and deep learning which automates and speed up the process efficiently. The five crucial steps that involved in the proposed study are image acquisition, encryption, optimal key generation, secured data storing and disease classification. Initially, the required input medical images are gathered in the image acquisition stage. Then, to afford more confidentiality, the gathered medical samples are encrypted through an Extended ElGamal Image Encryption (E-EIE) method. Here, the efficiency of encryption process is enhanced by generating the suitable keys in optimal manner with the help of Improved Sand Cat Swarm Optimization (I-SCSO) algorithm. Next, the security of encrypted images are improvised by utilizing federated learning flower (FLF) framework for storage purpose. This framework has the ability to transmit the medical images with higher security. Finally, the stored images are decrypted and performs disease classification by using convolutional capsule twin attention tuna optimal network (C^2T^2Net) model. The available loss in the proposed classifier is reduced by fine-tuning the parameters using chaotic tuna swarm optimization (CTSO) algorithm. For simulation analysis, the proposed study used Python software and the experimental analysis is carried out by using BreakHis Database. The simulation results shows that the proposed study obtained higher performance in terms of accuracy (95.68%), recall (95.6%), precision (95.66%), F-measure (95.63%), specificity (95.6%) and kappa coefficient (95.26%).

INDEX TERMS Breast cancer classification, federated learning framework, extended ElGamal image encryption, improved sand cat swarm optimization, convolutional capsule twin attention tuna optimal network.

I. INTRODUCTION

In recent years, an advancement of Artificial Intelligence (AI) technologies has been enhanced and it can be mainly utilized in smart medical detection process [1]. An effectiveness of smart medical detection is based on a high volume of enhanced quality data attained from the learning model [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Shuangqing Wei.

Nevertheless, data confidentiality and patient privacy are the challenging issues for securely accessing the medical information [3]. Thus, affording security and privacy of data are the two major concerns while using AI to smart medical detection [4]. Nowadays, the growth of federated learning in data security has been increasing day by day because of its higher efficiency [5]. This federated learning assists the data owners for locally train their techniques and collect the specific parameters instead of combining data directly [6], [7],

[8]. In order to provide more security to the provided medical data, the proposed study used federated learning flower (FLF) framework. From the past decades, the rate of breast cancer among women has been increasing and also the mortality rate is enhanced because of its high severity [9], [10]. Due to the varied morphological features, the breast cancer is considered as one of the large heterogeneous disease [11]. Therefore, the proposed study used breast cancer related medical data for affording security through federated learning.

Among the varied categories of cancer, breast cancer is considered as the top list among women around the globe [12]. In order to reduce the mortality rate due to breast cancer, early detection of tumor is highly important [13]. In existing, several techniques have been proposed to detect breast cancer in earlier stage [14]. However, detecting breast cancer in earlier stage is still a challenging issue faced by medical experts [15]. Depending on the breast cancer histopathological dataset, an advanced detection techniques have been developed to perform the process of cancer detection. The existing studies developed both machine learning and deep learning model for classifying the breast cancer disease. However, the machine learning methods generates reduced classification results as compared with deep learning models. Some of the deep learning models that existed to categorize breast cancer are convolutional neural network (CNN) [16], deep neural network (DNN) [17], deep belief network (DBN) [18], ResNet [19], DenseNet, Recurrent neural network (RNN), etc.

Most recently, the deep convolutional network is widely used for the cancer categorization task on BreakHis database. Moreover, using histopathological data is highly complicated in the experimental scenario. To successfully train the learning model, adequate improved quality data is more important [20]. Because of an inadequate and uneven distribution of data, medical datasets involves several issues. Thus, it results the contradiction among sufficient data fusion demands and privacy protection is an important obstacle to the growth of smart healthcare system. In this case, the techniques that combine knowledge obtained from data rather than combining data themselves, federated learning is highly applicable for the growth of smart medical detection systems.

Recently, the ever-enhancing world-wide requirement for early diagnosis of breast cancer at several hospitals and screening sites has leads in the demand of new research avenues. The great advancement in deep learning models plays a vital role in detecting breast cancer from the provided input images. Also, federated learning concept have becoming an interesting mechanism for affording security to the given input samples. Thus, it motivates the author to design a robust FLF framework along with deep learning model for affording security and making efficient decision in classification. The major objectives of the proposed study are,

- ➢ To develop an automated medical image diagnosis model using federated and deep learning framework for securing the Breast Cancer histopathology images.
- ➢ To perform secure transmission, privacy and effective storage of medical images using Extended ElGamal Image Encryption (E-EIE) algorithm.
- ➢ To introduce a new FLF framework for storing the encrypted breast cancer images securely.
- ➢ To accurately identify and categorize the disease classes using the new deep learning model called as Convolutional Capsule Twin attention Tuna Optimal Network (C2T2Net).

The rest of this research paper is well organized as follows, Section II discussed about the recent existing works that carried out on breast cancer classification using different techniques, Section III portrays the proposed methodologies that introduced for diagnosing breast cancer in proposed work, Section IV describes the simulation results and analysis to determine the performance of proposed techniques and Section V highlighted the overall conclusion of this work along with suitable future recommendations.

II. RELATED WORK

Li et al. [21] designed a federated learning framework for classifying breast cancer through histopathological images. In order to solve the security issues, this existing study introduces a federated learning concept which can performs knowledge fusion attained by distributing the patient's model parameters. Thus, by using federated learning, the sharing of data was neglected and the experiment was carried out by using BreakHis dataset. The simulation analysis shows that the developed federated learning model attained optimal classification performance as similar to centralized learning.

Abunasser et al. [22] developed a deep learning based Xception model for performing breast cancer detection and classification. Initially, the dataset was gathered from Kaggle depository and then pre-processing was performed to eliminate the unwanted noises. Then, the dataset was divided into three categories like training, validation and testing. The developed exception model was trained with the divided training dataset. During the stage of training, data augmentation scheme was performed to avoid the overfit issue. The layers presented in the exception model extracts the most significant features and the final softmax classification categorizes the breast cancer. The simulation analysis shows that the developed model gained high performance, however processing time is enhanced.

Jabeen et al. [23] presented the breast cancer classification through probability based optimal deep learning feature fusion framework. Initially, the needed data are gathered from the provided dataset. In order to enhance the dataset size, data augmentation was initiated and then the developed model was trained through transfer learning. The pooling layer presented in the transfer learning network assisted to extract the most discriminative features. Then, the feature dimensionality issue was avoided by selecting the most optimal features through two enhanced optimization approaches such as reformed gray wolf (RGW) and reformed differential evaluation (RDE). The chosen features are then combined through a probability based serial method and the classification was performed by varied machine learning approaches. The simulation results show that the classification performance is not as much improved because of an increased computational complexity.

Jiménez-Sánchez et al. [24] introduced a memory-aware curriculum federated learning framework for detecting and classifying breast cancer disease. This existing study is intended to develop a model for fulfilling the inconsistent prediction of previous techniques. To enhance the multi-site breast cancer categorization in a federated setting, the curriculum learning (CL) mechanism was introduced. Using a data scheduler, the developed CL was executed and it applied a concept of local training sample prioritization. In this existing study, the data scheduler was integrated with federated adversarial learning and exhibits that the combination was effective for the classification.

Ogundokun et al. [25] utilized a hyper parameter based optimized neural network model for detecting breast cancer through medical Internet of Things (IoT). To mitigate the difficulty in detecting cancer at early stage, this existing study introduces a medical IoT based detection system. Here, artificial neural network (ANN) was integrated with CNN and the hyper parameter of this developed scheme was optimally tuned through the utilization of an optimization algorithm. The developed model categorizes whether the given input data is benign tumor or malignant tumor. To analyze the performance of developed classifiers, the comparison analysis was done over Multilayer Perceptron (MLP) and Support Vector Machine (SVM) methods. The feature dimensionality issue was solved by applying particle swarm optimization (PSO) in the feature selection stage. The simulation results exhibits that the developed models achieved optimal performance as compared with others.

Tan et al. [26] have designed a transfer learning method for classifying breast cancer from the given samples. In this existing study, the federated learning framework is adopted for enhancing the classification performance. Here, the transfer learning method was utilized to fetch the required features from the inputs. For reducing the class imbalance issue, synthetic minority oversampling technique (SMOTE) was employed. Also, the utilization of MobileNet and FeAvg-CNN in a federated learning assured the privacy and security of user's data. The simulation results shows that the developed mechanism is suitable for artificial intelligence (AI) healthcare applications.

Manikandan et al. [27] have introduced an ensemble machine learning models for categorizing breast cancer from the provided SEER dataset samples. For removing the unnecessary noises, pre-processing was initially performed. Then, the most useful features from the pre-processed samples were selected through a Variance Threshold and Principal Component Analysis method. Finally, the varied machine learning classifiers like Ada Boosting, Gradient Boosting, XG Boosting and Decision Tree were utilized for generating an ensemble classification process. The developed classification process categorizes the breast cancer disease from the dataset images. The experimental analysis shows that the utilized Decision Tree method produced superior results than other machine learning models.

Ogier du Terrail et al. [28] have developed a machine learning model for predicting triple negative breast cancer through a federated learning framework. For affording high data privacy, the developed study utilized federated learning concept. With the support of federated learning, the patient's data was gets secured. The developed study represents that the normal machine learning techniques were mainly confides on entire slide images, which has the ability to detect responses to NACT. But, the collaborative training of machine learning techniques enhances the performance in triple cancer detection. Also, this study conveys that the federated learning model is sufficient for utilizing in real-time scenarios.

Problem statement: The World Health Organization (WHO) declares that the detection of cancer disease in earlier stage can improves the feasibility of taking the accurate decision on an effective treatment plan. By concerning this, several existing studies have attempted to develop an efficient detection mechanism for minimizing the mortality rate due to breast cancer. However, the existing methods cannot provide better classification outcomes because of several limitations like computational complexity, overfitting issues, increased misclassifications, etc. Along with disease detection, affording security of medical data is also a primary concern. Because of varied unauthorized parties in the network, the privacy of sensitive data is gets affected. Hence, to provide secure medical data transmission and accurate breast classification, an effective methodology is highly required. Thus, the proposed study designed a robust encryption algorithm with federated learning concept for securing the patient's data. Also, for mitigating the classification issues, the proposed study utilizes a new deep learning mechanism.

III. PROPOSED METHOD

Breast Cancer is one of the most fatal diseases among women and it is the second leading cancer type across the world. Nowadays, in females the rate of breast cancer is increasing rapidly as a result of unawareness and not diagnosed at its early stages. Therefore, proper treatment is provided only by early disease detection and classification. The quick detection and diagnosis is essential to reduce the mortality rate by identifying the disease at its initial stages. However, the manual cancer diagnosis from the histopathological images are still challenging due to the excessive time consumption, inaccurate detection at high probability which may occur due to human error. Traditional methods used for diagnosis procedure involves the participation of medical professionals, with the risks of subjective diagnosis and treatment delay. Thus, to overcome these defects this work presents an automated disease diagnosis system using FLF and deep learning which automates and speed up the process efficiently. Figure 1 shows the workflow of proposed methodology.

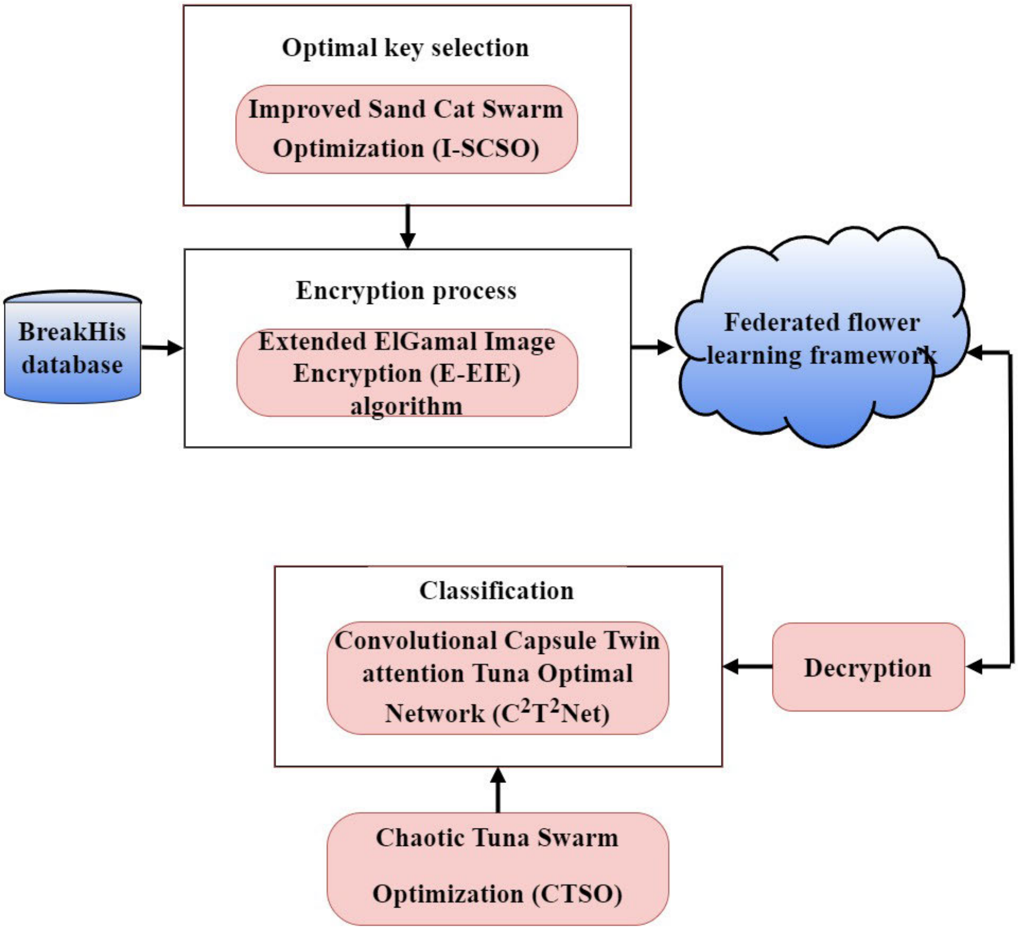


FIGURE 1. Workflow diagram.

In this work, an effective detection of breast cancer from histopathological images is performed using a FLF framework and deep learning. Currently, federated learning is emerged as an effective framework for the classification of breast cancer and offers secure data sharing of sensitive medical data among various healthcare providers. The proposed work includes five different stages like image acquisition, encryption process, optimal key generation, secured data storing and disease classification. Initially, the input images are collected in the image acquisition stage. Then, the collected medical images are encrypted using Extended ElGamal Image Encryption (E-EIE) algorithm. This encryption process assists to preserve the input medical images from the attackers. In order to provide more confidentiality to the encrypted images, optimal keys are generated using Improved Sand Cat Swarm Optimization (I-SCSO) algorithm. These encrypted images are stored using FLF framework. This technology enhances the data integrity as well as authenticity and allows secured transmission of medical images. After decrypting the image, the disease is identified in the classification stage using Convolutional Capsule Twin attention Tuna Optimal Network (C^2T^2Net) model. The loss minimization is performed using the Chaotic Tuna Swarm Optimization (CTSO) algorithm.

A. IMAGE ACQUISITION

Image acquisition is the first step that performed in the proposed framework. Initially, the input images are acquired from the publicly available BreakHis Database (https://web.inf.ufpr.br/vri/databases/breast-cancer-histopathological-database-breakhis/). After collecting the data, the further stages are executed to enable secure breast cancer classification.

B. MEDICAL IMAGE ENCRYPTION THROUGH E-EIE APPROACH

In order to afford more security to the input breast images from an authorized users, an efficient encryption algorithm is highly required. The encryption algorithm has the ability to covert the input images into encrypted form. For encryption purpose, the proposed study used E-EIE [29] algorithm, which is an effective cryptographic mechanism utilized for securing medical images. In existing different encryption schemes are established. Nevertheless they are not as much effective because of lower efficiency. The proposed encryption scheme utilizes a large computing process and it helps to attain superior encryption results. Because of its higher efficiency, making key predictions to the attackers has become more difficult. The proposed E-EIE algorithm processes the encryption flow based on the evaluation of discrete logarithms. Thus, it produce effective encryption process and secures the input images from attackers. The mathematical formulation of elliptic curve over finite filed is represented as,

$$E : x^2 = z^3 + lz + m \mod q \tag{1}$$

where, $q = 3 \mod 4$, q mentions a maximum prime number, the terms l and m denotes constants and $4l^3 + 27m^2 \neq 0$. The encryption process is performed by utilizing the coordinates that compromise the elliptic curve formulation. To create $N(z_n, x_n)$, the following points $L(z_l, x_l)$ and $M(z_m, x_m) \in E$ are adds up. It is newly observed as, utilizing $L(z_l, x_l) \in E$ and $M(z_m, x_m) \in or \notin E$, then the point addition is initiated to obtain $N(z_n, x_n) \in or \notin E$. During the process of point addition, it is necessary to analyze that $z_l \neq z_m$ to reduce point at infinity condition, if it is not in a point doubling condition. After completing the point subtraction process of $L(z_l, x_l)$ from $N(z_n, x_n)$ if $z_l \neq z_n$. It is mathematically expressed as,

$$M(z_m, x_m) = N(z_n, x_n) - L(z_l, x_l) \tag{2}$$

The coordinates z_m and x_m for M while the process of encryption should be lower than q. Utilizing an E-EIE, q_a is selected as any coordinate $\in$ or $\notin E$. The proposed E-EIE makes the conventional ElGamal cryptosystem as simpler with its higher efficiency and large embedding degree. The following requirements are important while using E-EIE method.

Minimize point at infinity condition by checking whether that the z coordinates of q_a and kq_m are varied, if not a state of point doubling while the process of encryption. If it happens, the random value k should be changed by,

$$q_{no} = \{k\alpha, (q_a + kq_m)\} \tag{3}$$

where, q_{no} mentions the cipher data's coordinates, k denotes the random integer among 1 and $b - 1$, the term α indicates the pubic data and q_a denotes plain input image mentioned on E coordinates through Koblitz embedding method.

The generated z_n in the below equation should not be equivalent to z-coordinate of kq_n. If it is same, then the range of k is changed.

Utilizing proposed E-EIE method, any (z, x) coordinates, the terms z and x are minimal than q can mention q_a keeping into account that it cannot became into a point at infinity condition. At infinity condition, the occurred probability is infinitesimally and it happens the range of random integer k is required to change. Also, as compared with conventional ElGamal method, the proposed E-EIE method utilizes both z and x coordinates to maintain the plain image and it assists to solve the data expansion issue. In addition, the embedding degree of proposed E-EIE method is higher than the conventional ElGamal algorithm and the embedding degree of E-EIE is represented as, $A < q$.

In order to encrypt the input dataset images, a 3D image from several 2D images are generated by piling up on top of each input image. The 3D images can be visible, but it is made up of various number of pixels that have a specific numerical value mentioning its intensity. To minimize the dimension of cipher data, each execution utilizes a particular one $k\alpha$ value. Various q_a in every execution distribute a single $k\alpha$. When one $k\alpha$ is employed for several q_a, there has a feasibility of familiar plain data attack exist. Hence, $k\alpha$ is forwarded to the another communicating user as encrypted form $k\alpha'$.The steps that included in the proposed encryption process are,

→ Initially attain the 3D input image's pixel values in the form of bytes.

→ The generated pixel values from preceding step 1 are gets XORed with the support of Mersenne Twister pseudo-random number generator. For Mersenne Twister system, the x-coordinate of $k\alpha$ is generated as the seed value.

→ Integrate all 64-pixel values in preceding step 1 with base conversion through 256 as a base.

→ For all q_a, evaluate q_{no} through the below given equation.

$$q_{no} = \{k\alpha, (z_{no}, x_{no})\} \tag{4}$$

where, z_{no} and x_{no} mentions the coordinates after the process of point addition of $(q_a + kq_m)$.

→ Convert the vales of (z_{no} and x_{no}) to 3D cipher image. To enable this, it is need to return back the byte value range (0, 255) by alternation with 256 as a base. Using 64 values, maintain a constant fixed length of disintegrated z_{no} and x_{no} by padding with zero to leftmost side if compulsory. 3D cipher image is created by securing the 3D plain image's dimension.

→ Transfer the cipher 3D image and the encrypted $k\alpha$.

Thus, by utilizing E-EIE method, the input images are encrypted through random keys. In order to make effective encryption, selecting optimal keys are more important and it has been described in the next section.

C. OPTIMAL KEY SELECTION THROUGH I-SCSO ALGORITHM

To encrypt the input images, suitable keys are highly required so that the proposed study used I-SCSO algorithm for choosing optimal keys. The keys like private and public are utilized for encrypting and decrypting the input dataset images. The proposed I-SCSO algorithm is one of the metaheuristic algorithm which imitates the hunting strategy of sand cat. Based on the frequency of sound, the sand cats can search their foods or prey and also its goal is to attain the best prey. Thus, depending the strategy of I-SCSO algorithm, the proposed study selects the better keys for encryption process. Using the below mentioned fitness function, the proposed I-SCSO algorithm chooses the optimal keys.

$$Fitness = Max\ (Network\ throughput) \tag{5}$$

❖ *Population initialization:* Initially, the population of keys are gets initialized, where each key is a 1 × dim array in the dimension optimization issue. In a group of variable values $(Pk_1, Pk_2, \ldots, Pk_{\dim})$, all Pk should lie from lower to upper boundary. Here, Pk is represented as position of keys. In this stage, an initialization matrix is generated based on the dimension of problem $(M \times \dim)$. In each iteration, the respected solution will be the resultant outcome. If the next resultant value is superior, then the present solution will be changed into the next. When there is no superior solution in the next iteration, the present iteration's solution will not be preserved. The population initialization is mathematically expressed in a matrix form. It is given as,

$$Keys = \begin{bmatrix} Pk_{1,1} & Pk_{2,1} & Pk_{1,\dim} \\ Pk_{2,1} & Pk_{2,1} & Pk_{2,\dim} \\ \vdots & \vdots & \\ Pk_{M,1} & Pk_{N,2} & Pk_{N,\dim} \end{bmatrix} \tag{6}$$

$$Pk_{i,j} = \left(UB_j - LB_j\right) \times rand + LB_J \tag{7}$$

where, UB_j mentions the upper bound of i^{th} key in j^{th} dimension, LB_j represents the lower bound of i^{th} key in j^{th} dimension and the random number ranges from 0 to 1 is termed as $rand$.

- *Exploration phase:* In this phase, the search agents chooses the keys based on the sensitivity range s_H as described in equation (8). Here, the search agents can analyze the ability of each keys and selects the best one.

$$s_H = T_N - \left(\frac{T_N \times l}{L}\right) \tag{8}$$

$$S = 2 \times s_H \times rand\ (0.1) - s_H \tag{9}$$

where, the value of T_N is considered as 2, L denotes the maximum number of iteration, l mentions the present iteration number and S denotes the parameter. This parameter is attained based on the aforementioned equation (9). A new location is determined by each search agent within the range of sensitivity while the process of exploring optimal keys. The global local optimum issue is avoided by utilizing varied range of sensitivity keys. This is expressed as,

$$s = s_H \times rand\ (0.1) \tag{10}$$

where, the term s_H is utilized for the guidance factor s. Each search agent will explore for the position of keys based on the best candidate solution Pk_{bc}, present position $Pk_c(l)$ and its range of sensitivity (s). It is mathematically represented as,

$$Pk\ (l+1) = s \times (Pk_{bc}\ (l) - rand\ (0.1) \times Pk_c\ (l)) \tag{11}$$

- *Exploitation phase:* To simulate the search agent's key attacking strategy is described in the below equation (12). Let us consider the range of sensitivity of the search agent is a circle and the movement direction utilizes the Roulette Wheel selection method to choose a random angle (β). Whereas, the selection of random angle is from the degree of 0 to 360 and its value is ranged between -1 and 1. According to the equation (13), the key is selected by the search agent.

$$Pk_{rand} = |rand\ (0.1 \times Pk_b\ (l) - Pk_c\ (l))| \tag{12}$$

$$Pk\ (l+1) = Pk_b\ (l) - s \times Pk_{rand} \times \cos(\beta) \tag{13}$$

By managing the adaptive parameters like s_H and S, the proposed optimization algorithm regularize both exploration and exploitation stage. The parameter s is a random value ranges from -4 to 4 and the search agent will acquire the keys when s is smaller than or equivalent to 1. Or else, the search agent will explore for keys as mentioned in equation (14).

$$Pk\ (l+1) \begin{cases} s \times (Pk_{bc}\ (l) - rand\ (0.1) \times Pk_c\ (l) \\ |L| > 1;\ \exp loration) \\ Pk_b\ (t) - Pk_{rand} \times \cos(\beta) \times s \\ |L| \leq 1;\ \exp loitation \end{cases} \tag{14}$$

The above equation represents the position updation of each search agent while exploration and exploitation phases. If $S \leq 1$, the search agent will catch its suitable key or else, the operation of search agent is to analyze a new key in the global area. In the proposed I-SCSO algorithm, the levy flight strategy is adopted to enhance the efficiency of conventional SCSO approach.

- *Levy flight walk behaviour:* When acquiring optimal keys, the search agent is nearer to its appropriate key. For affording random factors, the levy flight is highly efficient mathematical strategy. This strategy can render a walking scheme that confirms to levy distribution. Nevertheless, the step size pf levy's flight is too large and hence it consumes more time to complete the process. Thus, to obtain better performance of searching strategy, the constant $F = 0.35$ is included in levy flight. This helps the search agent to walk as nearer to its key as feasible. It is expressed as,

$$Pk_{new} = Pk_b\ (l) + (Pk_b\ (l) - Pk_c\ (l)) \times F \times Levy \tag{15}$$

Thus, by utilizing the proposed I-SCSO algorithm, an appropriate keys are selected and by using such keys the encryption process is performed through E-EIE method. Algorithm 1 mentions the pseudocode of proposed I-SCSO algorithm.

D. SECURED STORAGE USING FEDERATED LEARNING FLOWER FRAMEWORK

In order to securely store the encrypted input medical images, the proposed study used FLF framework. In general, the federated learning concept is arises from the requirement of distributing private medical data among varied healthcare providers. In the machine learning community, the federated learning procedure is an interesting research area because of its higher security and performance. The objective of federated learning is to train a distributed prediction model while securing the sensitive medical images. The three necessary steps that involved in the federated learning are, a) updation of local parameters to a distributed prediction model on every edge device b) transmitting the updated local parameter to a central server for the process of aggregation and c) attaining

Algorithm 1 Proposed I-SCSO: Pseudocode

Initialize the total number of keys using equation (7)
Evaluate the fitness function using equation (5)
Initialize the parameters like s, s_H and S
While ($l \leq$ max *imum number of iteration*)
  for all search agent
   Attain a random angle depending Roulette wheel selection $\left(0^0 \leq \beta \leq 360^o\right)$
   If (abs (S) > 1) **then**
    Perform position updation using equation (11)
    Update the position of each search agent using equation (13)
Execute levy flight walk strategy using equation (15) to attain an appropriate position
end
$L = l + 1$
end

the aggregated model back for the upcoming process of local parameter updation. The proposed FLF framework assists experimentation with system and algorithm based challenges in federated learning. The flower provides a stable, machine learning and language framework and also it affords larger level abstractions to execute efficient ideas. Also, the flower helps to improve the rate of transition and convergence. Moreover, the introduced FLF framework has the ability to mitigate the challenges of restricted computation, network bandwidth and memory in a cloud system. This proposed FLF can stores the encrypted images with more security. Figure 2 mentions the structure of proposed FLF framework.

E. DISEASE CLASSIFICATION USING PROPOSED C^2T^2NET MODEL

This section presents the classification process of input medical images using proposed deep learning mechanism. By exactly classifying the disease, the mortality rate due to breast cancer will gets reduced. Here, the classification process is performed by introducing a new C^2T^2Net model. In the proposed model, convolutional capsule network is designed by adopting a slice and excitation attention block. In the conventional capsule network, attention mechanism is not presented. The layers presented in the capsule network are responsible for fetching the rich information from the provided inputs. However, the conventional capsule network model failed to process in large dimension of data. Thus, it directly affects the performance of the network. Therefore, the proposed study hybridizes CNN with Capsule network model. Along with the hybrid network, a twin attention mechanism is introduced for generating better results. This attention mechanism helps to obtain more informative primary capsules. Also, the attention block assists to minimize the unwanted noises from the input samples and also ignores the irrelevant features by enabling salient feature propagation to larger level capsules.

Here, the routing coefficients are properly distributed by utilizing a modified factorized machines (FM) routing technique. The blocks that involved in the proposed C^2T^2Net model are input, convolutional block, primary capsule block, SE attention block and output block. Figure 3 mentions the architecture of proposed C^2T^2Net model.

Initially, the input images are obtained in the input block and then it is fed into the convolutional layers to capture the most essential features. Here, the convolutional layers involves the layers in the CNN method. The proposed study used CNN layers for extracts the significant features from the provided images. In the convolutional module, the layers like convolutional (13), pooling (5) and drop-out layers (0.15 and 0.25 rate) are presented. The initial convolutional layers has the ability to fetch the most unique features from the provided inputs. The feature extraction between various layers in CNN method is determined as follows,

$$F_i = \alpha \left(F_{i-1}\, \omega_i + b_i\right) \tag{16}$$

where, F_i mentions the total extracted features from CNN, the term α represents the activation function, ω_i denotes the weight and b_i mentions the bias. The next pooling layers are the most important features presented in the CNN method. In pooling layers, the size of features that attained in the convolutional layers are gets minimized and it assists to reduce the computational complexity issue. Then, the ability of proposed classifier is enhanced by the utilization of dropout layers. With the help of dropout layers, overfitting issue is reduced by diminishing the relationship among the neurons. At the end, the output of CNN layers are fed as the input of next primary caps layer.

The primary caps layer includes the convolutional layer along with ReLU activation and batch normalization. The convolution layer contains the suitable amount of filters to correspond the dimension. The features maps attained from the convolutional layers are fused together and forward to the ReLU activation function. After enabling batch normalization, the outcome is gets reshaped to generate primary capsules by the presented primary capsule layer. Then, non-linear squash activation function is presented to enhance the capability of primary capsule layer. The output of this layer is fed to the input of next SE attention block. The main intention of this attention block is to minimize the noisy and inappropriate features from the inputs. Thus, it highly helps the system to make accurate classification. The proposed attention block instructs the capsule for acquiring important features in the given image by guiding the attention network through deep features that attained by the capsules. Also, this block aids to enhance the channel inter-dependencies, and it leads to improvise the representation capability of the capsules. In the proposed SE block, the features are initially forwarded to enable squeeze operation. By using an average pooling process, each input features are gets squeezed to one numeric value and then it transmitted to the excitation process. This excitation block includes two fully convolutional layers and are activated through ReLU and sigmoid functions.

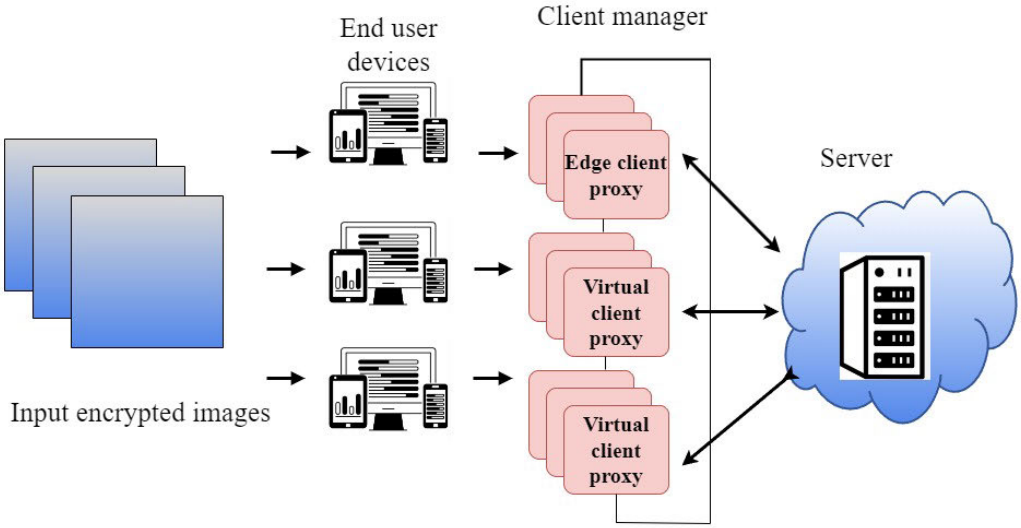


FIGURE 2. Architecture of FLF.

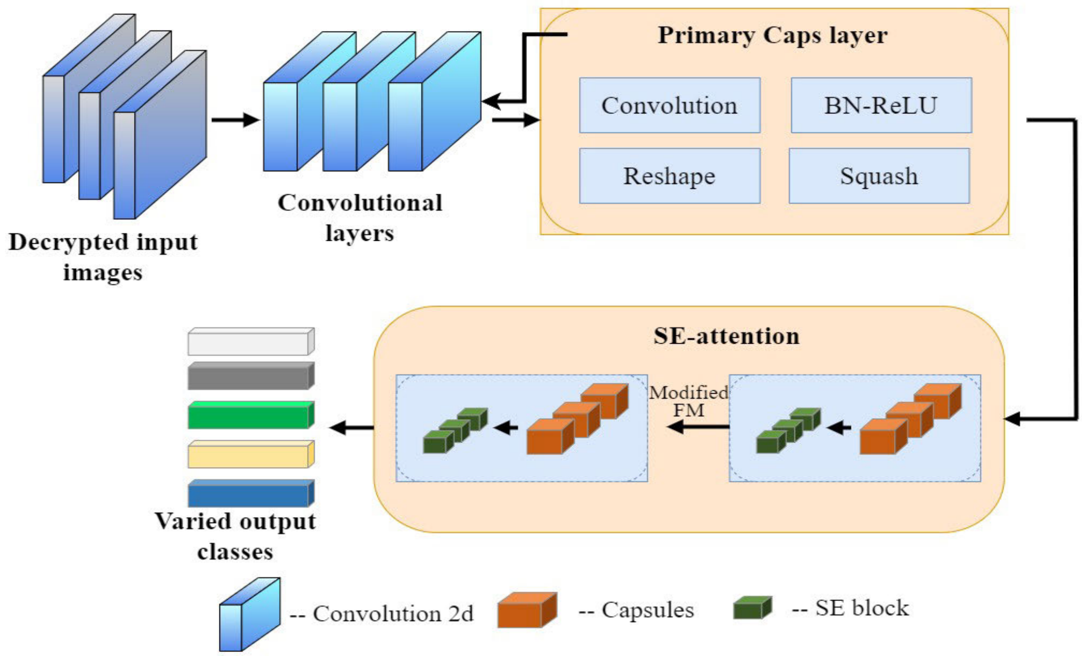


FIGURE 3. Proposed C^2T^2Net Model.

Finally, the output features are obtained by multiplying the SE attention block with input features. Figure 4 mentions the SE block structure.

The working process of proposed SE-attention block in the capsule network is given as,

$$G_{avg} = AveragePooling\ (G) \tag{17}$$

$$P_{RELU} = RELU\ \left(\omega_1 * G_{avg} + b_1\right) \tag{18}$$

$$N_{SE} = sigmoid\ (\omega_2 * P_{RELU} + b_2) \tag{19}$$

$$G' = G * N_{SE} \tag{20}$$

where, $RELU$ mentions the activation function, ω_1 and ω_2 represents the weight factors and b_1 and b_2 mentions the biases. The proposed C^2T^2Net model uses a modified FM routing mechanism to maintain the range of prediction vectors bounded and to attain efficient routing coefficients distribution to enhance the correlation among the parent and child capsules. Here, the softmax activation function is employed to attain the suitable features with higher value. Each capsule in the layer $m-1$ is represented by v_i and the prediction vector $\hat{v}_{j|i}$ for each capsule in the m^{th} layer is determined. Let us consider the prediction vector as $\left[\hat{v}_{j|0},\ \hat{v}_{j|1}, \ldots, \hat{v}_{j|k}\right]$, where the capsules agreement is composed via pairwise communication between the capsules in the similar layer. Here, the pairwise product is expressed as $\hat{c}_{j|i_1,\, i_2} = \hat{v}_{j|i_1} \otimes \hat{v}_{j|i2}$ in which the addition of all elements of $\hat{c}_{j|i_1,\, i_2}$ provides the agreement

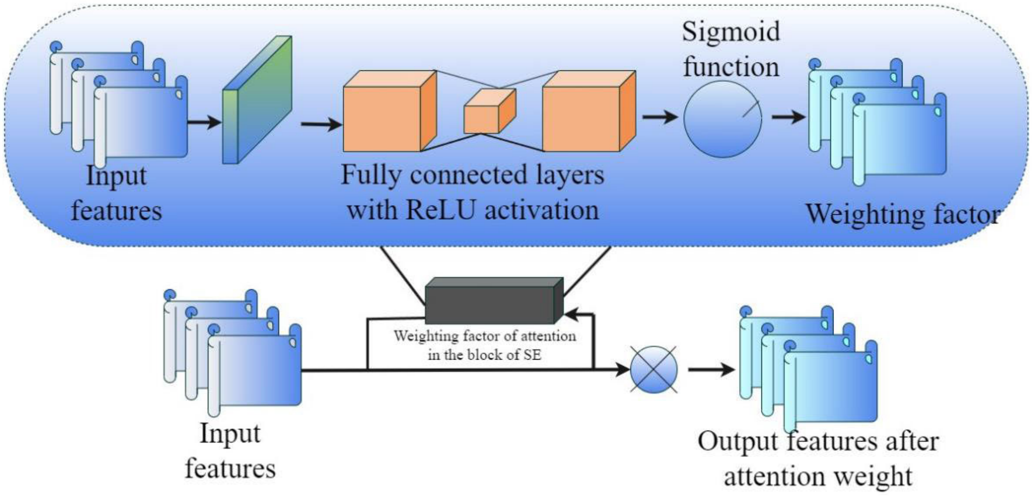


FIGURE 4. Structure of SE block.

magnitude. The pairwise communication of each capsules in $m-1$ layer to the j^{th} capsule of layer m is expressed as,

$$\hat{L}_j = \sum_{i_1=1}^{k} \sum_{i_2=i_1+1}^{k} \hat{v}_{j|i_1} \otimes \hat{v}_{j|i_2} \tag{21}$$

$$= \frac{1}{2}\left(\sum_{i=1}^{k} \hat{v}_{j|i} \otimes \sum_{i=1}^{k} \hat{v}_{j|i} - \sum_{i=1}^{k} \hat{v}_{j|i} \otimes \hat{v}_{j|i}\right) \tag{22}$$

where, $\hat{v}_{j|i} = \left[\hat{v}_{j|1}, \hat{v}_{j|2}, \ldots.., \hat{v}_{j|k}\right]$, $\hat{L}_j = \left[\hat{L}_{j,1}, \hat{L}_{j,2}, \ldots\ldots, \hat{L}_{j,k}\right]$, wherein $k$mentions the overall amount of prediction vectors. The resultant ofj^{th} capsule in l^{th}layer is represented as,

$$\hat{c}_j = \sum_{g=1}^{f} \hat{L}_{j,g} \tag{23}$$

The evaluation of agreement coefficient is performed by utilizing a softmax function on the output layer. It is expressed as,

$$\hat{o}_j = soft\max\left(\hat{c}_j\right) \tag{24}$$

Here, the definition of pose vector is given as, $\hat{U}_j = \frac{\hat{L}_j}{\|L_j\|}$, where the term $\hat{U}$mentions the pose, rotation, size, orientation, etc of a given entity. By performing summation operations, the gradient explosion issue is gets minimized and is given as,

$$\hat{L}_j = \frac{1}{2k}\left(\sum_{i=1}^{k} \hat{v}_{j|i} \otimes \sum_{i=1}^{k} \hat{v}_{j|i} - \sum_{i=1}^{k} \hat{v}_{j|i} \otimes \hat{v}_{j|i}\right) \tag{25}$$

Thus, the proposed C^2T^2Net model classifies the disease from the provided input medical image. However, the loss function attained in the proposed model reduces the working efficiency of entire system. Thus, the loss function in the proposed C^2T^2Net model is minimized by fine-tuning the parameters using CTSO algorithm. The loss function in C^2T^2Net model is given as,

$$LF = \frac{1}{K}\sum_{i=1}^{K}\left(a_i - c_i'\right)^2 \tag{26}$$

where, K denotes the maximum amount of iterations, $a_i$specifies the actual value and the classified value is mentioned as c_i'. The disease is detected according to the following fitness function using CTSO algorithm by,

$$Fitness\,function = Min\,[LF] \tag{27}$$

The CTSO algorithm is one of the new heuristic algorithm utilized for solving optimization issues by utilizing the hunting strategies of tuna. The CTSO method used levy flight concept to update the position of search agent to select the optimal parameters and is given as,

$$Z_i^{t+1} = \begin{cases} Z_{best}^t + \beta.Levy\,(p)\,.\left(Z_{best}^t - Z_i^t\right) \\ +tf\,.\,q^2.\,\left(Z_{best}^t - Z_i^t\right), \quad if\ rand < 0.5 \\ tf\,.\,q_i^2\,.\,Z_i^t, \\ if\ rand \geq 0.5 \end{cases} \tag{28}$$

Based on the above mentioned equation (28), the CTSO model explores the suitable parameters for enhancing the performance of proposed C^2T^2Net model. The simulation analysis of proposed techniques are discussed in the next section.

IV. SECURITY PROOF

A. EAVESDROPPING ATTACK

An eavesdropping attack is also called as snooping or sniffing attack. While eavesdropping, the private information is stolen by the malicious attacker as it is sent via network. To mitigate eavesdropping attack, the proposed study utilizes public key created by I-SCSO algorithm to encrypt the input images. Since, the provided input image is encrypted, initiating eavesdropping attack can be difficult to the attacker due to an unknown private key for decrypting the input. Hence, the proposed I-SCSO based encryption approach effectively avoids eavesdropping attack in the proposed system.

B. REPLAY ATTACK

The replay attack is also said as playback attack or repeat attack. The encryption process between transmitter and receiver can be eavesdropped via attacker. Thus, the encrypted images can effortlessly intercepted by the malicious attacker. To avoid this issue, the proposed study generates optimal keys for protecting the input medical images. To initiate replay attack, the attacker wants to have the knowledge about private keys that generated by I-SCSO algorithm. But, it is not viable by the malicious user to analyze the private keys because of the efficacy of proposed system. Therefore, the attacker transmits wrong information such that the receiver omits the intercepted images.

C. MAN IN THE MIDDLE ATTACK

The Man-in-the-Middle attack is prevented by developing secured encryption process. This attack is a usual cyber-attack, where the attackers intercepts and transmits information among to varied parties who confide they are interacting directly with each other. This attack can be prevented in the proposed system by developing robust encryption approach. The encrypted images ensures the security of the proposed system. Also, the selected private and public keys from I-SCSO algorithm are more effective. These keys provide higher security to the given input data and helps to avoid Man in the Middle attack.

V. SIMULATION RESULT ANALYSIS

This section presents the simulation results and analysis of proposed work using several performance parameters. The proposed study utilized Python tool for simulation and the implementation is done by using BreakHis dataset. By evaluating diverse parameters, the performance of proposed model is evaluated. Also, the comparative analysis over other existing methods proves the efficacy of proposed work. In the proposed work, the encryption and decryption process is implemented by utilizing a total key length of 1024. After the process of optimal key selection, it is reduced into 256. By using such keys, the encryption and decryption is done through E-EIE method. Table 1 shows the system configuration that supported for simulation. Also, the hyperparameter settings of proposed model is depicted in Table 2.

TABLE 1. System configuration.

Processor	Intel (R) Core ()TM i5-3570 CPU @ 3.40 GHz 3.40
Installed RAM	8.00 GB (7.89 GB usable)
Device ID	330431f3-8552-4664-BCAD-E0108D59137B
Product I.D	00330-80000-00000-AA440
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

TABLE 2. Hyperparameter settings.

No. of epochs	100
Batch size	60
Number of layers	15
Learning rate	0.01
Output layer	1

A. DATASET DESCRIPTION

By using BreakHis dataset, the implementation process is carried out. This dataset is constructed by using 9109 amount of microscopic images of breast tumor tissue, which is gathered from 82 varied patients utilizing several magnifying factors like 40x, 100x, 200x and 400x. This dataset involves two classes like benign and malignant, whereas the benign class contains the total of 2480 samples and malignant class involves totally 5429 samples. Thus, by using this dataset, the proposed study enables the disease classification process. In the proposed work, totally 7909 images are gathered from the mentioned dataset. Here, the dataset images are splitted into training and testing. From the total of 7909 images, 6327 images are used for training and 1582 images are used for testing. Also, the dimension of images that available in BreakHis dataset are 700*460 pixels. For better processing, the input images are reshaped in the pre-processing step by 256*256.

B. PERFORMANCE MEASURES

The evaluation of performance measures is more important to compute the performance of proposed techniques. In the proposed study, the performance measures like accuracy, precision, recall, specificity, kappa coefficient, MAE, MSE and RMSE are evaluated and the attained performance is compared with other existing methods to prove the strength of proposed work.

- *Accuracy:* Accuracy is a significant measure to compute the correctly classified images to the overall medical images in the provided dataset. This metric has the major role to analyze the performance of proposed C^2T^2Net model. The formulation of accuracy is given as,

$$Accuracy = \frac{TP + TP}{TP + TN + FP + FN} \tag{29}$$

- *Precision:* It is the rate of perfectly classified disease from the entire number of true positives. It is formulated as the sum of accurately classified images in a specific

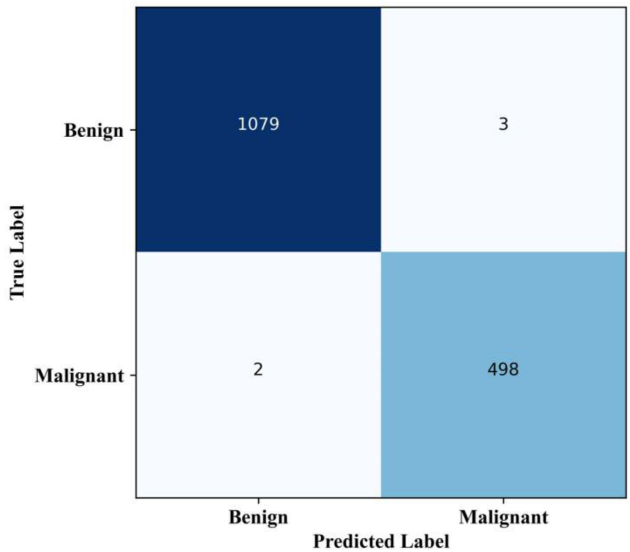


FIGURE 5. Confusion matrix analysis of C^2T^2Net model.

class divided by the entire classified medical images. It is represented as,

$$\Pr ecision = \frac{TP}{TP + FP} \tag{30}$$

➢ *Recall:* The recall metrics is the ratio of entire amount of true positives to the entire amount of both true positives and false negatives. The term recall is mathematically represented as,

$$Recall = \frac{TP}{TP + FN} \tag{31}$$

➢ *Specificity:* Specificity analyses the proportion of real negatives, which got classified as the negative. The perfectly classified disease in the provided images are determined in the specificity measure. It is evaluated as,

$$Specificity = \frac{TN}{TN + FP} \tag{32}$$

➢ *F-measure:* It is the harmonic mean of precision and recall. In f-score, an appropriate precision and recall is computed by one. If the value of recall or precision is zero, then the f-score value is also assumed as zero. The computation of F1-score is given as,

$$F - measure = 2 \times \frac{\Pr ecision \times Recall}{\Pr ecision + Recall} \tag{33}$$

➢ *Kappa coefficient:* Kappa defines the performance rate of the classifier i.e. it measures how much better the classifier is accurately classifying the output. This kappa measure provides the inter and intra rate reliability of classified samples.

$$K = \frac{P_{observed} - P_{chance}}{1 - P_{chance}} \tag{34}$$

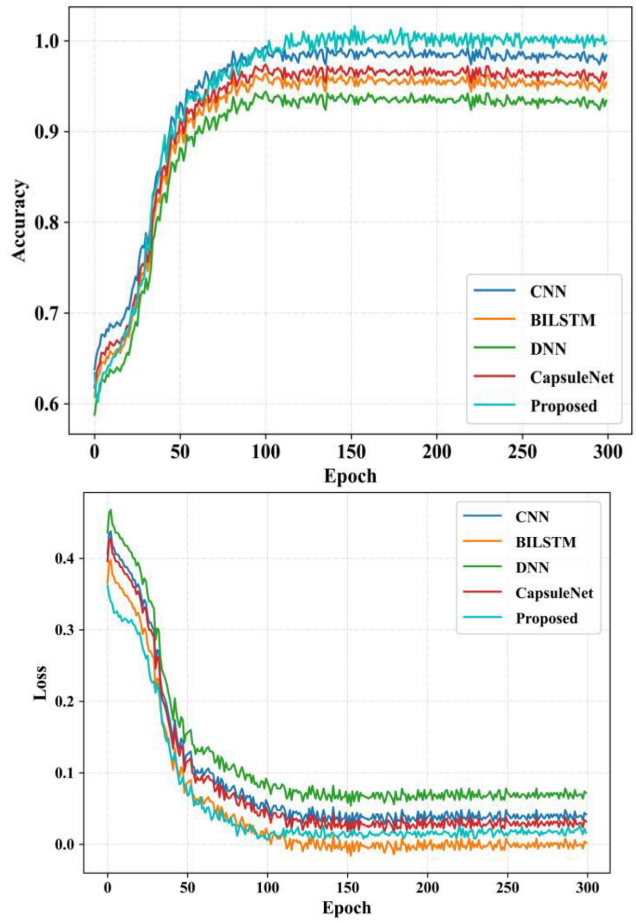


FIGURE 6. Analysis of accuracy and loss comparison.

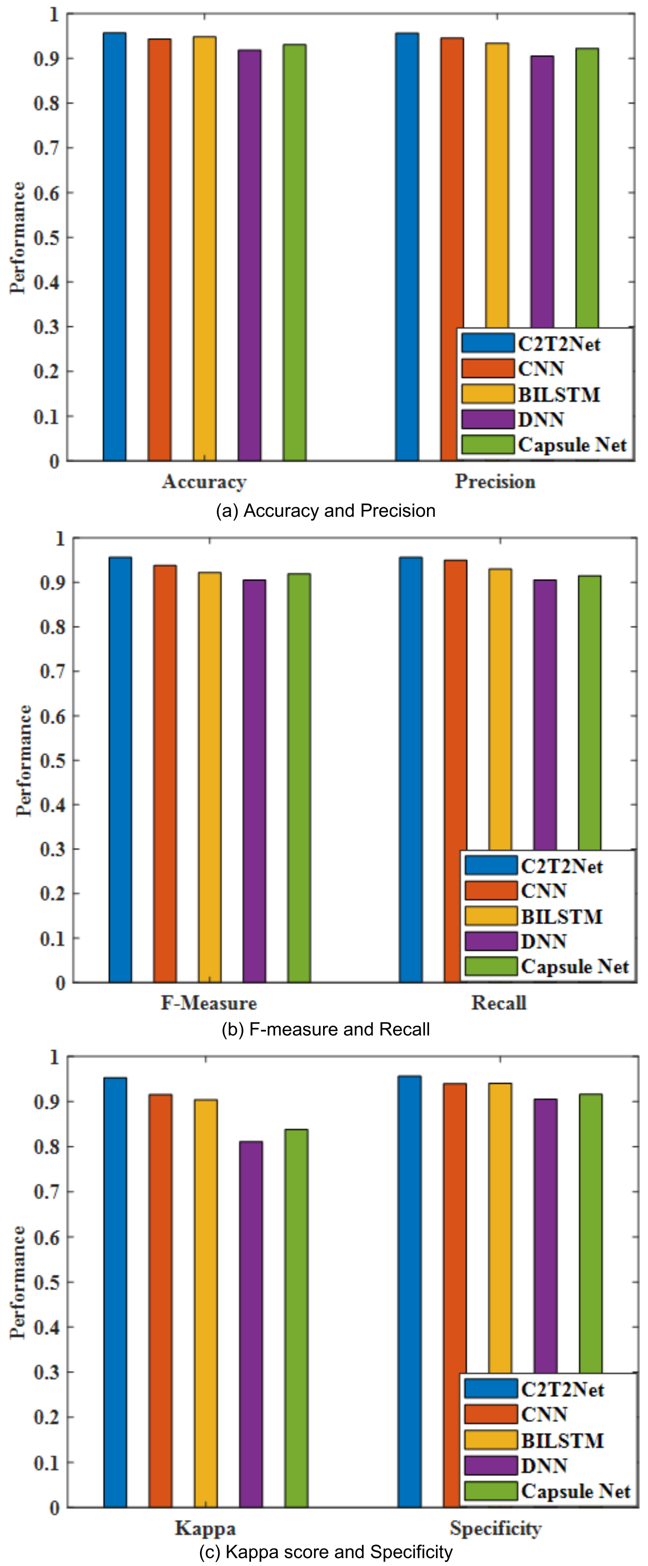
➢ *MAE:* It evaluates the average error magnitudes in a prediction set, without the consideration of their direction. This measure exhibits the average over the test input images of the absolute variations among prediction and real observation, where entire sample differences includes similar weight. The formulation of MAE is given as,

$$MAE = \frac{\left|(x_i - x_p)\right|}{m} \tag{35}$$

➢ *MSE:* The MSE metric provides the average squared variations among the predicted values and the original value. The technique with reduced MSE value is considered as an optimal one. The evaluation of MSE is given as,

$$MSE = \frac{1}{m}\sum_{i=1}^{m}\left(x_i - \hat{x}_i\right)^2 \tag{36}$$

➢ RMSE: This measure shows the error rate of proposed classifier very accurately. It is the square root of MSE



(a) Accuracy and Precision

(b) F-measure and Recall

(c) Kappa score and Specificity

FIGURE 7. **(a) – (c) Performance analysis using different metrics.**

and is expressed as,

$$RMSE = \sqrt{\sum_{i=1}^{m} \frac{(\hat{x}_i - x_i)^2}{m}} \tag{37}$$

TABLE 3. **Performance values for both proposed and existing methods.**

Performance	Proposed	CNN	BISTM	DNN	Capsule Net
Accuracy	0.9568	0.94333	0.948	0.9184	0.9304
Precision	0.9566	0.945	0.945	0.905	0.9223
F1-measure	0.9563	0.93781	0.9223	0.905	0.919
Recall	0.956	0.9497	0.93	0.9054	0.915
Kappa	0.9526	0.9155	0.904	0.8112	0.8379
Specificity	0.956	0.9397	0.9405	0.905	0.9158

TABLE 4. **Values attained for error metrics such as MAE, MSE and RMSE.**

Performance	Proposed	CNN	BISTM	DNN	Capsule Net
MSE	0.056	0.1914	0.202	0.285	0.2636
MAE	0.0031	0.0366	0.041	0.081	0.0695
RMSE	0.0031	0.036	0.041	0.081	0.069

where, TP mentions true positives, TN is considered as true negatives, FN signifies false negatives, FP signifies false positives, P is the probability of event, x_i represents actual values, m denotes the total number of dataset images, x_p and $\hat{x}_i$ are mentioned as predicted values.

C. PERFORMANCE COMPARISION ANALYSIS

This section discussed about the performance comparison of proposed study with other existing methods like CNN, BiLSTM, DNN and CapsuleNet [30]. By performing comparison analysis, the efficiency of proposed study is proved. The confusion matrix of proposed classification model is illustrated in Figure 5.

From the above confusion matrix, it is cleared that the proposed C^2T^2Net model effectively classified the given input images as benign or malignant. From the total of 1082 benign images, 1079 images are perfectly classified as benign by the proposed C^2T^2Net model and only 3 images are miss classified. Similarly, from the 500 number of malignant images, 498 images are accurately classified and two images are wrongly classified as benign. This analysis clearly mentions that the proposed classifier is most effective for classifying breast cancer disease from the provided samples. The accuracy and loss comparison during the stages of testing is shown in Figure 6.

The attained accuracy and loss of proposed and existing models are analyzed while testing process. Here, the accuracy and loss is determined by varying the epoch sizes from 0 to 300. At the epoch size of 100 to 300, the accuracy rate of proposed classifier is enhanced as compared with other competent methods. Similarly, the loss of proposed classifier is reduced from the epoch of 100 to 300. This shows that the proposed classifier outperforms than the other existing methods. The performance analysis in terms of several metrics are shown in Figure 7.

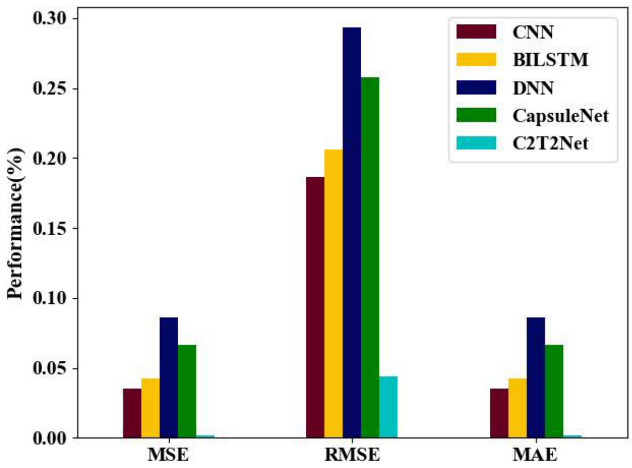


FIGURE 8. Error metrics comparison.

Here, the performance of proposed method is compared with several existing methods like CNN, BiLSTM, DNN and CapsuleNet. By measuring the metrics like accuracy, precision, recall, specificity, F-measure and kappa coefficient, the effectiveness of each model is analyzed. The analysis of accuracy and precision comparison represents that the proposed model obtains higher classification performance than others as shown in Figure 7 (a). This is because, the existing methods faces higher computational complexity and overfitting issues while classifying the breast cancer disease. Also, the existing methods highly troubles from computational complexity problem and hence the accuracy performance is gets affected, But, the proposed study used efficient classification method and it effectively reduces the computational complexity issue. Also, the higher ability of primary caps layer in the proposed C^2T^2Net model reduces the gradient explosion issue. Thus, the significant benefits in the proposed techniques makes the classification results as high.

Similarly, the F-measure and recall performance of proposed model is increased than the other comparable methods as illustrated in Figure 7 (b). As compared with others, the F-measure and recall performance of existing KNN is reduced because of its inefficiency. The specificity and kappa score performance portrays the higher efficacy of proposed model as mentioned in Figure 7 (c). According to this, the ability of proposed model is highly revealed and it states that the proposed model is highly suitable for detecting and classifying breast cancer disease from the input medical images. Table 3 mentions the performance values attained for both proposed and existing methods.

The mentioned graphical representation portrays the strength of proposed model by observing the improved performance. In order to clearly analyze the effectiveness of proposed classifier, evaluating the error metrics is more important. In the below Figure 8, the error metrics comparison is highlighted using different metrics.

The above graphical representation states the error metrics comparison of both proposed and existing methods.

TABLE 5. Performance comparison over recent research methods.

Methods	Proposed	ResNet-152	DenseNet-201	MobileNet-v2-100	EfficientNet-b7
Accuracy	95.68%	86.33 %	91.06%	87.38%	84.02%
F1-score	95.63%	73.95 %	84.97%	77.38%	72.78%
Diagnostics odd ratio	176.23	168.54	99.81	48.02	23
Kappa measure	95.26%	65.16 %	78.64	68.79%	61.58%

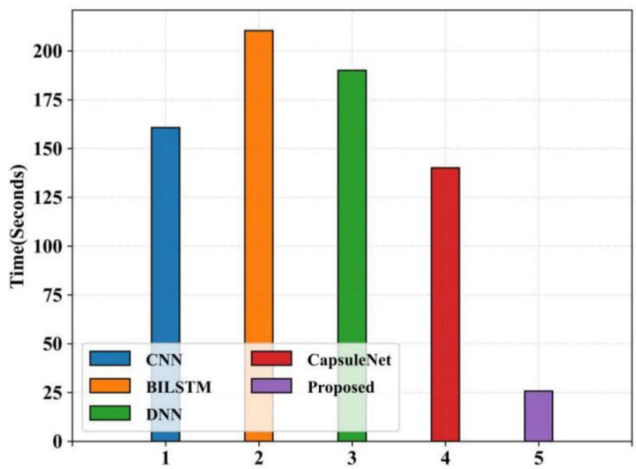


FIGURE 9. Overall processing time comparison.

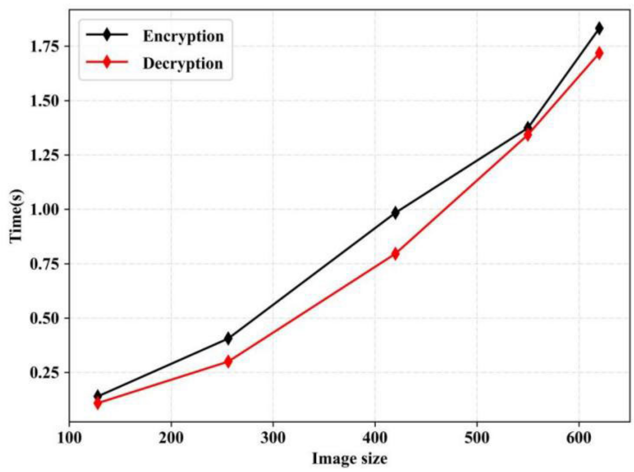


FIGURE 10. Encryption and decryption time.

As compared with other existing methods, the error rate of proposed classifier is highly reduced because of its enhancing learning ability. While, performing disease classification, the existing methods attained higher classification error due to reduced capability of performing exact classification. Figure 8 mentions the MAE comparison analysis, wherein

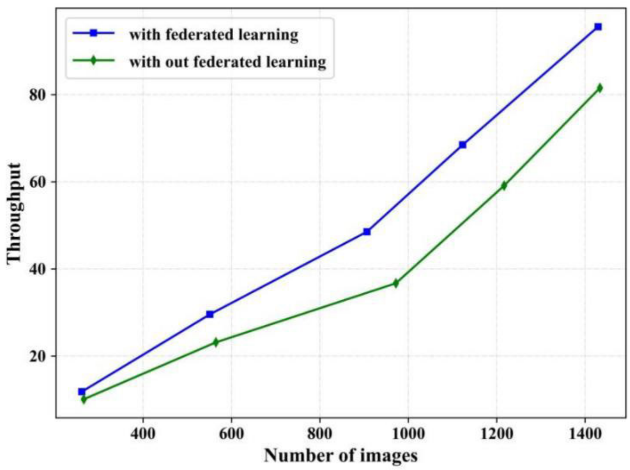


FIGURE 11. Throughput comparison.

the error rate of proposed classifier is highly gets minimized than others Similar to this, the MSE and RMSE analysis shown in Figure 8 portrays that the error rate of proposed model is reduced than the competent methods. Thus, it states that the proposed model is more efficient than the existing methods. The attained values in terms of MAE, MSE and RMSE is shown in Table 4.

To extend the performance analysis of proposed work, the proposed study also compares their work with other recent research results. Table 5 depicts the performance comparison of proposed work with recent existing studies [21].

The above analysis clearly exhibits that the proposed model obtained better classification results than the recent existing methods. The processing time is important to show the robustness of proposed model. The existing methods are failed to complete the classification with minimal time because of higher computation. The techniques that produce exact classification with reduced time is highly beneficial for medical sector while detecting the diseases. The overall processing time attained for both proposed and existing methods are shown in Figure 9.

The above figure shows that the processing time of proposed model is gets reduced than the other existing methods. This, this analysis proves that the proposed model is processed better than other existing methods. The processing time attained for proposed C^2T^2Net model is 21s, CNN is 160s, BiLSTM is 215s, DNN is 190s and CapsuleNet is 140s. Thus, it clearly exhibits the efficacy of proposed model. To know the strength of proposed FLF framework, the encryption and decryption time are analyzed and is highlighted in Figure 10.

From the above graph, the encryption and decryption time of proposed E-EIE method is analyzed. Here, the time is determined by varying the input images from 100 to 600. By enabling the encryption and decryption process, the time attained to complete the process is extremely reduced. Thus, it proves that the proposed E-EIE method is more effective for encrypting the medical images. Figure 11 shows the throughput performance comparison of with and without federated learning.

The above mentioned graph shows the throughput performance attained in the proposed work in two phases such as with federated learning and without federated learning. The comparison analysis clearly shows that the throughput performance is highly improved for utilizing federated learning. Thus, it reveals the need of utilizing FLF framework in the proposed work.

VI. CONCLUSION

This paper presents the secured breast cancer classification through a new FLF framework along with deep learning model. To make effective disease diagnosis, securing the medical data is highly required. Because, several unauthorized parties may influence the patient's medical data and it affects the exact classification. Thus, the proposed study intends to develop an efficient FLF with C2T2Net model for securely detecting and transmitting the medical images to authorized medical centres. For enhancing the confidentiality of patient's sensitive data, an effective encryption process is enabled by using E-EIE method. The encrypted images are then securely stored in the FLF framework for mitigating the unwanted attacks. This process helps to improve the network throughput because of attaining improved authentication. After decrypting the medical images, the breast cancer classification is performed through the proposed C2T2Net model. By fine-tuning the parameters of proposed classifier using CTSO algorithm, the entire performance of proposed model is gets enhanced. The proposed study utilized Python tool for implementation and the BreakHis dataset is chosen for simulation analysis. As compared with other existing methods, the proposed model gained higher performance in terms of accuracy (95.68%), precision (95.66%), recall (95.6%), specificity (95.6%), F-measure (95.63%), kappa coefficient (95.26%), MAE (0.0031%), MSE (0.056%) and RMSE (0.0031). Thus, the obtained higher performance in the proposed model states that the proposed work is highly sufficient for secured breast cancer detection. However, the proposed study utilized only one dataset for simulation and hence the evaluation is limited. Also, the utilization of publicly available dataset cannot reveals the worth of proposed work. Thus, it is considered as the drawback of this work. In future study, varied dataset will be employed for analysing the performance of proposed techniques. Furthermore, real-time data will be considered in the future study to exhibit the capability of proposed work. Also, to make effective encryption, hybrid cryptographic methods will be recommended in future.

REFERENCES

[1] R. F. Mansour, A. E. Amraoui, I. Nouaouri, V. G. Díaz, D. Gupta, and S. Kumar, "Artificial intelligence and Internet of Things enabled disease diagnosis model for smart healthcare systems," *IEEE Access*, vol. 9, pp. 45137–45146, 2021.

[2] S. Tian, W. Yang, J. M. L. Grange, P. Wang, W. Huang, and Z. Ye, "Smart healthcare: Making medical care more intelligent," *Global Health J.*, vol. 3, no. 3, pp. 62–65, Sep. 2019.

[3] S. Ahmed, M. F. Hossain, M. S. Kaiser, M. B. T. Noor, M. Mahmud, and C. Chakraborty, "Artificial intelligence and machine learning for ensuring security in smart cities," in *Data-Driven Mining, Learning and Analytics for Secured Smart Cities*. Cham, Switzerland: Springer, 2021, pp. 23–47.
[4] T. M. Ghazal, "Internet of Things with artificial intelligence for health care security," *Arabian J. Sci. Eng.*, Aug. 2021.
[5] D. C. Nguyen, Q.-V. Pham, P. N. Pathirana, M. Ding, A. Seneviratne, Z. Lin, O. Dobre, and W.-J. Hwang, "Federated learning for smart healthcare: A survey," *ACM Comput. Surveys*, vol. 55, no. 3, pp. 1–37, Mar. 2023.
[6] J. C. Jiang, B. Kantarci, S. Oktug, and T. Soyata, "Federated learning in smart city sensing: Challenges and opportunities," *Sensors*, vol. 20, no. 21, p. 6230, Oct. 2020.
[7] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, "Secure and provenance enhanced Internet of Health Things framework: A blockchain managed federated learning approach," *IEEE Access*, vol. 8, pp. 205071–205087, 2020.
[8] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, "A survey on federated learning," *Knowl.-Based Syst.*, vol. 216, Mar. 2021, Art. no. 106775.
[9] A. G. Waks and P. E. Winer, "Breast cancer treatment: A review," *Jama*, vol. 321, no. 3, pp. 288–300, 2019.
[10] M. F. Ullah, "Breast cancer: Current perspectives on the disease status," *Breast Cancer Metastasis and Drug Resistance*. New York, NY, USA: Springer, 2019, pp. 51–64.
[11] A. Conti, A. Duggento, I. Indovina, M. Guerrisi, and N. Toschi, "Radiomics in breast cancer classification and prediction," *Seminars Cancer Biol.*, vol. 72, pp. 238–250, Jul. 2021.
[12] B. Sahu, S. Mohanty, and S. Rout, "A hybrid approach for breast cancer classification and diagnosis," *EAI Endorsed Trans. Scalable Inf. Syst.*, vol. 6, no. 20, pp. 1–8, 2019.
[13] F. K. Al-Thoubaity, "Molecular classification of breast cancer: A retrospective cohort study," *Ann. Med. Surgery*, vol. 49, pp. 44–48, Jan. 2020.
[14] E. H. Houssein, M. M. Emam, A. A. Ali, and P. N. Suganthan, "Deep and machine learning techniques for medical imaging-based breast cancer: A comprehensive review," *Exp. Syst. Appl.*, vol. 167, Apr. 2021, Art. no. 114161.
[15] D. A. Ragab, O. Attallah, M. Sharkas, J. Ren, and S. Marshall, "A framework for breast cancer classification using multi-DCNNs," *Comput. Biol. Med.*, vol. 131, Apr. 2021, Art. no. 104245.
[16] F. F. Ting, Y. J. Tan, and K. S. Sim, "Convolutional neural network improvement for breast cancer classification," *Exp. Syst. Appl.*, vol. 120, pp. 103–115, Apr. 2019.
[17] M. Lamba, G. Munjal, and Y. Gigras, "A hybrid gene selection model for molecular breast cancer classification using a deep neural network," *Int. J. Appl. Pattern Recognit.*, vol. 6, no. 3, pp. 195–216, 2021.
[18] A. M. Abdel-Zaher and A. M. Eldeib, "Breast cancer classification using deep belief networks," *Exp. Syst. Appl.*, vol. 46, pp. 139–144, Mar. 2016.
[19] Q. A. Al-Haija and A. Adebanjo, "Breast cancer diagnosis in histopathological images using ResNet-50 convolutional neural network," in *Proc. IEEE Int. IoT, Electron. Mechatronics Conf. (IEMTRONICS)*, Sep. 2020, pp. 1–7.
[20] H. Yao, X. Zhang, X. Zhou, and S. Liu, "Parallel structure deep neural network using CNN and RNN with an attention mechanism for breast cancer histology image classification," *Cancers*, vol. 11, no. 12, p. 1901, Nov. 2019.
[21] L. Li, N. Xie, and S. Yuan, "A federated learning framework for breast cancer histopathological image classification," *Electronics*, vol. 11, no. 22, p. 3767, Nov. 2022.
[22] B. S. Abunasser, M. R. J. Al-Hiealy, I. S. Zaqout, and S. S. Abu-Naser, "Breast cancer detection and classification using deep learning xception algorithm," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 7, pp. 1–7, 2022.
[23] K. Jabeen, M. A. Khan, M. Alhaisoni, U. Tariq, Y.-D. Zhang, A. Hamza, A. Mickus, and R. Damaševičius, "Breast cancer classification from ultrasound images using probability-based optimal deep learning feature fusion," *Sensors*, vol. 22, no. 3, p. 807, Jan. 2022.
[24] A. Jiménez-Sánchez, M. Tardy, M. A. G. Ballester, D. Mateus, and G. Piella, "Memory-aware curriculum federated learning for breast cancer classification," *Comput. Methods Programs Biomed.*, vol. 229, Feb. 2023, Art. no. 107318.
[25] R. O. Ogundokun, S. Misra, M. Douglas, R. Damaševičius, and R. Maskeliūnas, "Medical Internet-of-Things based breast cancer diagnosis using hyperparameter-optimized neural networks," *Future Internet*, vol. 14, no. 5, p. 153, May 2022.
[26] Y. N. Tan, V. P. Tinh, P. D. Lam, N. H. Nam, and T. A. Khoa, "A transfer learning approach to breast cancer classification in a federated learning framework," *IEEE Access*, vol. 11, pp. 27462–27476, 2023.
[27] P. Manikandan, U. Durga, and C. Ponnuraja, "An integrative machine learning framework for classifying SEER breast cancer," *Sci. Rep.*, vol. 13, no. 1, pp. 1–12. 2023.
[28] J O. Du Terrail et al., "Federated learning for predicting histological response to neoadjuvant chemotherapy in triple-negative breast cancer," *Nature Med.*, vol. 29, pp. 1–12, Jan. 2023.
[29] D. S. Laiphrakpam and M. S. Khumanthem, "Medical image encryption based on improved ElGamal encryption technique," *Optik*, vol. 147, pp. 88–102, Oct. 2017.
[30] H. A. Khikani, N. Elazab, A. Elgarayhi, M. Elmogy, and M. Sallah, "Breast cancer classification based on histopathological images using a deep learning capsule network," 2022, *arXiv:2208.00594*.

JYOTHI PETA is currently a Research Scholar with the School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India, with more than seven years of experience in the IT industry and teaching. Her research interests include the IoT and AI/ML.

SRINIVAS KOPPU received the Bachelor of Technology degree in computer science and engineering from Jawaharlal Nehru Technological University Hyderabad, India, in 2006, the master's degree in information technology with specialization in human–computer interaction from the Indian Institute of Information Technology (IIIT) Allahabad, India, in 2009, and the Ph.D. degree from the Vellore Institute of Technology (VIT), Vellore, Tamil Nadu, India, in 2018. He has more than 14 years of experience in teaching. He was a Visiting Professor with the Neusoft Institute of Information Technology, China, in 2018. He is currently an Associate Professor Senior with the School of Information Technology and Engineering, VIT. He was a Co-Principal Investigator of the British Council Grant Industry-Academia Collaborative Grant 2022–2023 of the Project "Co-Designing a Smart Curriculum and Personalized Method of Delivery for Inclusive Value Added Courses" of INR 40 Lakhs which received from the University of Nottingham, U.K. He has published more than 30 international/national journals and conferences. His research interests include deep learning, federated learning, blockchain technologies, the IoT, data analytics, cryptography, medical image processing, image security analysis, video processing and computer vision, and high-performance computing. He is a Life Member of the Computer Society of India. He also acted as a Guest Editor of several reputed publishers, such as IEEE, Hindawi, and MDPI.