Section A -Research paper
ISSN 2063-5346

AN EFFICIENT DEEP LEARNING BASED DISTRIBUTED LEDGER TECHNOLOGY FOR SECURING COVID-19 MEDICAL IMAGES

Chandini Avula Gopalakrishna
REVA University, Bangalore, Karnataka, India
SJC Institute of Technology, Karnataka, India
chandinimegu@gmail.com
Prabhugoud I. Basarkod
Department of ECE, REVA University, Bangalore
Karnataka, India

DOI: 10.48047/ecb/2023.12.si4.1674

Abstract

Internet of Medical Things (IoMT) is a study field that is in high demand and is used in most medical applications. When dealing with medical data or images on a decentralized site, security is a hard problem to solve. To improve the security of medical images in IoMT, a deep learning-based blockchain framework that works well and has lower transaction costs is suggested. The suggested study has four steps: getting the image, encrypting it, finding the best key, and storing it safely. In the picture acquisition stage, the input images are gathered in the first step. Then, the gathered medical images are encrypted using coupled map lattice (CML). This encryption process helps keep medical pictures from being seen by attackers. The optimal keys are made by using the opposition-based sparrow search optimization (O-SSO) method. This makes the encrypted images more private. Distributed ledger technology (DLT) and smart contract-based blockchain technology are used to store these pictures that have been encrypted. This blockchain technology improves the integrity and authenticity of the data and makes it possible to send medical pictures securely. In the classification step, the disease is found by using the proposed Recurrent Generative Neural Network (RGNN) model. This is done after the image has been decrypted. For the simulation analysis in the suggested study, a Python tool was used, and the medical images came from CT images in the COVID-19 dataset.

Index terms: Secure image transmission, Blockchain technology, coupled map lattice, Recurrent Generative Neural Network, opposition-based sparrow search optimization.

1. Introduction

Recently, Internet of Things (IoT)-based healthcare applications have reached a point where medical treatments are automatically accessible for all users [1]. This is a significant milestone in the evolution of healthcare technology. A form of healthcare known as remote patient monitoring (RPM), sometimes known as telehealth, is a concept that requires both patients and medical professionals to make use of

IoT-connected, lightweight medical devices. RPM can be used for a variety of medical purposes, including the prediction of heart arrhythmia, the maintenance of normal glucose levels, the monitoring of chemotherapy, and the regularization of oxygen levels [2]. On the other hand, RPM monitoring is not frequently used because faults can arise, there is a lack of security, and the system is not stable [3].

In an electronic health care application, medical Internet of Things devices are used to collect a patient's physiological data, which is subsequently sent to cloud and edge servers. This presents a problem to the security system because it can be easily accessible by potential intruders and hackers [4]. Conventional E-health technology can have its robustness significantly reduced by cyberattacks such as Man-in-the-middle attacks, denial of service (DoS) assaults, and ransomware attacks, which can also cause significant disruptions to medical services. Based on the report of the United States Department of health service, nearly 2000 data contraventions occurred between 2010 and 2020 [5]. The Internet of Things model is vulnerable to eavesdropping attacks via Zigbee, as well as insider attacks, Wi-Fi, and Bluetooth. In addition, traditional edge and cloud computing are not very efficient to protect the data [6].

IoMT has the potential to successfully improve the efficacy and accessibility of illness treatment, while also reducing the likelihood of errors, enhancing the patient experience, and ensuring that costs are kept to a minimum. In these modern times, a pandemic sickness known as COVID-19 has broken out, posing a challenge to traditional models of medical identification [7]. Therefore, the development of new technology that can provide data on healthcare detection that is dependable, accurate, and up-to-date is crucial. As a result, IoMT is thought to be employed for collecting and analyzing the key symptoms of COVID-19 affected individuals to locate the sources of the COVID-19 outbreak and ensure a massive amount of authentic data. However, there is a risk that personal information could become public, which would be a significant obstacle and diminish the patient's motivation to participate in the IoMT [8] [9].

Motivation

In recent years, Internet of Things devices have grown increasingly important in the field of healthcare applications. Due to the huge increasing requirement of IoT, the sensitive information of patients is being collected and used for further diagnostic processes. The Internet of Medical Things (IoMT) is vital because of its practical applications in hospitals and throughout the entire healthcare network. At this time, the most important solutions are implemented by first gathering information through testing and then waiting for the outcomes of those tests. After the patients have received the results, they need to wait for the decision that will be made by the doctors. Nevertheless, additional time is required for appropriate decision-making and therapy. IoMT is a superior method for connecting, exchanging data made by different IoT devices, and doing analysis on that data to cut down on the amount of time spent waiting and processing information. Because of the proliferation of new technologies and rapid digitalization, such as IoT, the applications of deep learning (DL) algorithms are developing as an important category of algorithms. Recently, during COVID-19, several researchers focused their attention on combining blockchain technology with deep learning models to advance digital healthcare. To ensure the security of medical data, blockchain technology has been developed and it is a decentralized structure. By this motivation, this research work introduces a blockchain with DL based model for secure data transmission and diagnostic model. The major contribution of the proposed study is given as,

To introduce an efficient Internet of medical things (IoMT) with deep learning (DL) based blockchain model for securing COVID-19 medical images:

1. To introduce coupled map lattice (CML) method for encrypting the images with opposition-based sparrow search optimization (O-SSO).
2. To design blockchain-based hash value encryption using distributed ledger technology (DLT) and smart contract based on blockchain.
3. To perform disease classification using Recurrent Generative Neural Network (RGNN) for diagnosing the presence of disease.

The remaining sections of the paper are structured as follows: Section 2 deals with the literature review of various studies on secured transmission using blockchain mechanisms, Section 3 presents the suggested methodology for this paper, Section 4 discusses the simulation results and analysis of the suggested framework, and Section 5 highlights the overall conclusion as well as the potential application in the future.

Related works

Some of the related works based on blockchain with the Internet of medical things (IoMT) is discussed in this section.

A blockchain architecture that is built on fog was presented by Shukla et al. [18] as a solution for authentication in IMoT. The study described here built a three-tier fog model for the purpose of transmitting trustworthy and protected data between medical professionals, fog nodes, Internet of Things devices, and patients. After that, a blockchain paradigm that is decentralized and relies on fog for safe data transactions and transmissions in IoMT. With the assistance of a private blockchain, this model was able to execute identification, the verification of certificates, and the generation of keys for IoT devices and fog nodes. In the end, Advanced Signature Encryption (ASE) was responsible for both the homogeneous and heterogeneous identification of IMoT devices. Several different cryptographic functions and a private blockchain were utilized in order to encrypt and decrypt the data. The accuracy of malicious node detection was 91%, while detection accuracy in the cloud was 87%.

Griggs et al. [20] presented a blockchain paradigm for the healthcare industry that makes use of smart contracts (SCs) for automated RPM. For the purpose of carrying out SCs, this architecture made use of a blockchain that was consortium-based and permissioned. This architecture offered improved service availability as well as fault tolerance, and Practical Byzantine Fault Tolerance (PBFT) was utilized to manage any failures that occurred. By delivering messages to both medical professionals and patients, this SC system would facilitate medical intervention and real-time monitoring of patients. Additionally, it would remove a variety of security concerns that are associated with RPM.

Keshk et al. [21] introduced blockchain and the DL model to protect smart power networks. This model has two stages like privacy stage and the anomaly detection stage. Enhance Proof of Work (E-PoW) was used for verifying data integrity and identify the attacks. Then the DL model Variational Auto Encoder (VAE) was used for transferring data to prevent inference attacks. Then the DL model Long Short-Term Memory (LSTM) was utilized to train and validate the result of the privacy stage. This model achieved a better detection rate of 99.8% on the UNSW-NB 15 dataset.

A Blockchain and deep learning approach was published by Kumar et al. [22] for the purpose of securing data sharing and detecting CT images. The primary objective of this work was to improve the DL model and get the data ready for more accurate prediction by using SCs. For the purpose of ensuring the integrity of shared data between many data sources, a specialized SCs was developed. In the beginning, the bat algorithm (BA) and data augmentation were utilized in order to get rid of noise and prevent problems with over-fitting. After that, an estimation of the region of interest (ROI) was performed with the help of a recurrent convolutional neural network (RCNN). The findings of the experiments supported the hypothesis that this model correctly identified cancer at an early stage and recognized malignancy.

Neelakandan et al. [23] integrated blockchain technology with a DL model for the purpose of ensuring the secure transmission of data in the healthcare and diagnostic model industries. The image was encrypted in the beginning using elliptic curve cryptography (ECC) in conjunction with moth flame optimization (MFO). After that, the blockchain was utilized for the purpose of storing the photographs. The diagnostic model was first segmented using a histogram, then a deep learning (DL) model called ResNet-Inception was used to extract features, and finally, the model was classified using a support vector machine (SVM). The testing revealed that this model achieved a specificity of 98.3 percent and an accuracy of 95.2 percent, respectively.

Based on the FL and blockchain concept, Poap et al. [24] suggested a multi-agent framework (MAF) for the Internet of Things (IoT). This paper presented a novel IoMT model, in which the safety of the data and its processing were separated into separate components. The separate components were given to the intermediaries who oversaw exchanging the information. Innovative agent procedures for medical care that made it possible to delegate certain responsibilities to the agent’s unit. Additionally, the MAF made use of blockchain technology to facilitate the sharing and protection of personal data. After that, an agent equipped with a consortium model will classify the results obtained from the FL model. This methodology improved both accuracy and security, while also reducing the amount of time needed to carry out operations.

Problem statement

In recent years, IoMT has become increasingly commonplace in a variety of applications pertaining to medical treatment. Because IoMT places such high demands on its components, a substantial quantity of monitoring data is produced by a wide variety of sensing devices. Real-time data analysis that is both accurate and scalable can be made possible thanks to the application of artificial intelligence (AI) techniques. Despite this, the components of IoMT give rise to distinct design issues, such as concerns over privacy and security, limitations on available resources, and improper data for training. Blockchain technology is being implemented in several recently published research to solve the problems with IoMT's security. Based on blockchain technology, numerous methods have already been established in the present day to allow for the transmission of medical images in a secure manner within the medical profession. However, they were not successful in delivering ideal results because of several limitations, including data leakage, increased processing complexity, sensitive to attacks, limited battery life, and so on. As a result, the purpose of the proposed research is to create a reliable system for archiving medical photos of the IoMT platform that is based on blockchain technology and deep learning. The following are some of the currently available studies, along with the limitations of each.

Table 1 Comparison of existing state-of-the-art methods

Author	**Methods**	**Purpose**	**Parameters**	**Limitations**
Shukla, S et al. [18]	ASE, Fog computing based blockchain framework	Affording authentication, identification, and verification for securely transmitting IoT based healthcare. data	Execution time, packet error, CPU time, reliability, processing time, running time, detection. accuracy	System complexity is enhanced while using high amount of IoT data.
Unal, D et al. [19]	Federated learning (FL), Context Triggered Piece-wise Hash (CTPH)	Mitigating attacks on FL techniques processing in IoT platform through blockchain mechanism	Processing time, end-to-end delay, energy consumption, packet overhead	□ Failed to detect the variations in trained model. □ Computational cost is high.
Griggs, K.N et al. [20]	Smart contract based blockchain	Affording secure remote patient monitoring in an automatic manner	To prove the efficacy of the system, the security parameters like confidentiality, traceability, availability, speed, transparency etc are analysed.	□ Facing several challenges while maintaining security at each specific node.
Keshk, M et al. [21]	VAE, LSTM, E-PoW	To design a robust blockchain mechanism for preserving smart power networks	False positive ratio (FPR), detection rate processing time	This study cannot investigate the scalability and utility of the developed system.

Kumar, R et al. [22]	RCNN, BA	To provide secured data transmission and diagnosis of CT images for the	Accuracy, loss, power ratio, average transaction	It needs more amount of training data to make accurate decision.

2. Proposed Methodology:

In today's world, the Internet of medical things (IoMT) is rapidly becoming into a requirement for a wide variety of applications, notably those pertaining to medical care. As a result of the presence of patients' personally identifiable information, medical image transmission presents a significant problem in terms of data security. In addition, the analysis of the patients' health records (PHR) requires the use of these photographs, which are an integral part of the data in the medical system. The use of artificial intelligence plays a significant part in ensuring that the analysis of data is both accurate and scalable. The development of blockchain technology has made it possible to operate in a decentralized manner. This research paper presents a deep learning (DL) based blockchain model for the secure transmission of image and diagnostic model for use in healthcare applications. The task is broken down into its major steps, which include the gathering of data, the safe transaction of hash value, the encryption of hash value, and the classification of data. Initially, the input photographs are gathered, and then coupled map lattice (CML), an encryption algorithm, is applied to the images. In addition, for the purpose of increasing the effectiveness of CML, the ideal key is created by employing a technique known as opposition-based sparrow search optimization (O-SSO). This optimization is utilized in order to reduce the amount of time spent on computing while simultaneously improving image quality. The blockchain technology is applied here in order to store the encrypted versions of the photographs. That is, medical data is shared via distributed ledger technology (DLT), and a smart contract based on blockchain is used to keep patient data. This model will make a method that is efficient for the exchange of medical information, will enhance the data integrity, and will decrease the cost of the transaction. The picture is deciphered on the receiver's end of the transmission. The workflow of the suggested methodology is illustrated in Figure 1

Figure 1 Block diagram of the proposed framework

2.1 Image Acquisition

Acquiring input images is the first step of the proposed framework. The aim of this step is to gather the input medical images from the provided dataset. The proposed study adopts CT images in the COVID-19 dataset and collects the data for further processing. The collected medical images are then fed as the input of the encryption stage to attain higher security. Some of the collected input images are shown in Figure 2.

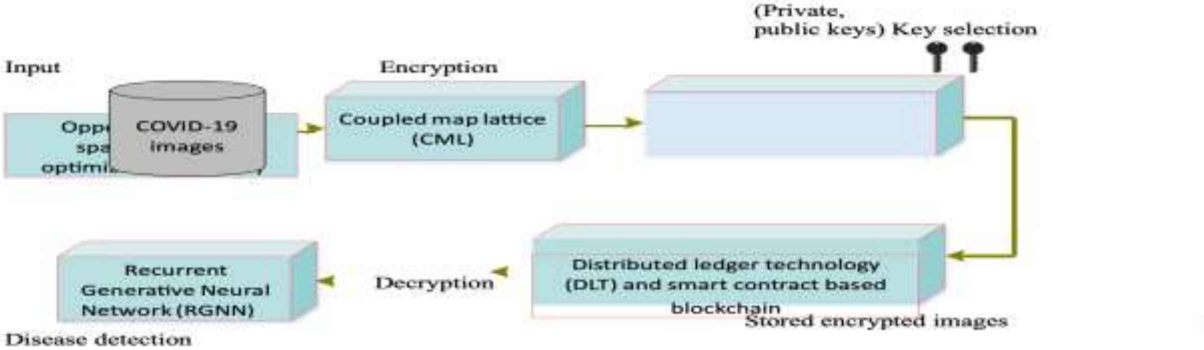


Figure 2 Input Images

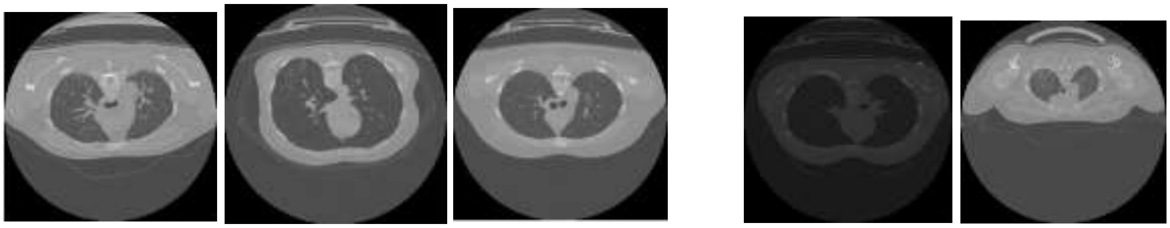


Image encryption using CML

The input private images transmitted over healthcare organizations are not as secure due to the enormous number of attackers who trace sensitive medical images. Thus, encryption is necessary to preserve the patient’s private medical images. For providing more security to the input images, the proposed study introduced the CML approach for the process of encryption. In existing, several encryption schemes are developed to enhance security, but they failed because of an increased computational time.

CML holds the benefits of both one-dimensional and high-dimensional systems hence it attains more attention nowadays. CML is a kind of chaotic function which utilizes the logistic map for creating its sequences. As compared with a one-dimensional chaotic system, the proposed CML approach involves an efficient chaotic strategy, a high number of parameters, optimal pseudo-random chaotic sequences, and minimal periodic windows in bifurcation layouts. Hence, the generation of pseudo-random chaotic sequences from the proposed CML system is highly protective than the fundamental chaotic system. In the encryption process, the random series that generated by the chaotic map is executed. This chaotic map has played an optimal role for encrypting the images depending on the strategies like sensitivity to initial terms, and sensitivity to limit parameters. In the chaotic map, a logistic map is easier to encrypt the medical images. It is given as,

The term ε represents the control parameter. The pseudo-random sequences are generated by using a logistic map for encoding the input medical images into binary. In general, the logistic map is a dynamic scheme employed for generating pseudo-random sequences. It is mentioned as,

Where, the process of period-doubling bifurcation is represented as λ ∈(0, 4). For CML, the chaotic space-time system is employed. The proposed CML exhibits spatiotemporal chaos depending on the spatial coupling between maps local. The expression of CML is given as

$$k_{m+1}(i) = (1-\alpha)\, h\,(k_m(i)) + \alpha . h\,(k_m(i-1))$$

Where, i (i = 1, 2, ...P) mentions the lattice index site, the time index m indicates coupling parameter km (0) = km (P)as the boundary periodic case, the local mapping function is specified as h (k) which

$k_{i+1} = \varepsilon k_i\,(1-k_{i)}$

(1)

ki and *ki*+1 mentions the *i* th and *i* + 1st

can choose the logistic map.

$h\,(k) = \varepsilon . k_m .(1-k_m)$ $k0 \in {}^{(}0,1^{)}$and ε = (3.5599456.3)

$z_{m+1} = \lambda * z_m\,(1-z_{m)\, zm} \in (0,1)$ and $m = 0,1,2$, $\lambda \in (0, 4)$

The chaotic state is in CML with the initial case. The dual-point variable is initiated to convert CML into integers for performing encryption of medical images.

$$(k.10^{12} - [k.10^{12}]).10^{3}, 64)$$

Where, mod (k, v) turns back the rested value after the completion of division and the term [k] rounds the neighbouring integer like or lower than k. Depending on the produced chaotic sequences, the sequences of random numbers are attained using the above equation (5). Thus, the proposed CML approach effectively encrypts the provided medical images with reduced complexity. To enhance the efficiency of CML, optimal key generation is essential, and it is described in the next section. During the key generation process, the receiver can decrypt the medical images with a private key and encrypt them with a public key.

Optimal key selection using O-SSO

To afford higher authentication to the encrypted images, key generation is highly required. In the encryption process, the keys are randomly generated. The randomly generated keys may lead lack of security and it affects the entire efficiency of the developed system. Thus, to select optimal keys, the proposed study adopts the O-SSO approach. The introduced SSO approach is one of the swarm optimization algorithms inspired by the foraging strategies of sparrows. The proposed O-SSO algorithm chooses the optimal keys based on the fitness function.

Fitness function = Max (PSNR)

To determine the optimal keys, a virtual search agent is needed. The following matrix mentions the position of search agents in the search space.

Where *m* represents the number of search agents and dim mentions the variable's dimension to be optimized. The below vector specifies the fitness value of each search agent.

Where *m* represents the number of search agents, and the fitness value of each search agent is indicated as the value of every row in *Fz*. The search agents with appropriate fitness functions have the preference to attain better keys in the searching process. This is because the search agents are more responsible for exploring optimal keys and governing the movement of the whole individuals. Hence, the search agents can explore for optimal keys in a large area and the location of the search agent is updated as,

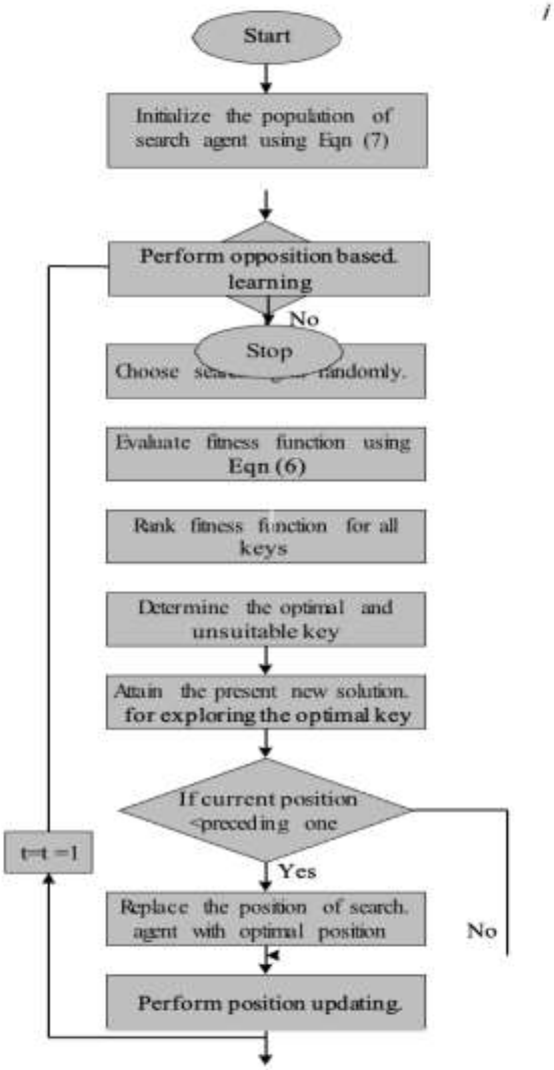
Where *z* best mentions the present optimal location. The step size limited parameter is specified η, the random normal distribution is represented as Q ∈[−1,1]. The fitness of the present search agent is signified as *fi*, the optimal fitness value is mentioned as *fl* and the worst fitness value is represented as *fw* correspondingly. The constant terms that neglect zero-division error are mentioned as ε. The direction that moves by the search agent is mentioned as Q and also it is defined as the coefficient of

$$F = \begin{bmatrix} f([z_{1,1} & z_{1,2} & \square & \square & z_{1,dim}]) \\ f([z_{2,1} & z_{2,2} & \square & \square & z_{2,dim}]) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ f([z_{m,1} & z_{m,2} & \square & \square & z_{m,dim}]) \end{bmatrix} \quad (8)$$

step size control. The fitness value is evaluated for each iteration and the obtained outcome is compared to each other. The optimal solution is attained by finding the best fitness value. To enhance the capability of the SSO approach, the proposed study develops an opposition-based learning mechanism in which the SSO approach is gets modified. The formulation of opposition-based learning in the O-SSO algorithm is given as

$$Y^{0} = U^{b} + L^{b} - Y$$

Where, Y^{0} be an opposite value for the original value. The opposite value


Start
Initialize the population of search agent using Eqn (7)
Perform opposition based learning
No
Stop
Choose search agent randomly.
Evaluate fitness function using Eqn (6)
Rank fitness function for all keys
Determine the optimal and unsuitable key
Attain the present new solution for exploring the optimal key
If current position <preceding one
Yes
No
t=t =1
Replace the position of search agent with optimal position
Perform position updating.

DLT and smart contract-based blockchain framework:

Blockchain technology is utilized for both transmission and storage. This technology stores the sensitive images in a ledger composed of a set of blocks. In this, all the blocks are connected to the preceding block to design a chain of blocks. With the assistance of a peer-to-peer network, the data transmission gets secured. Therefore, blockchain is referred to as a distributed ledger transmitted in a safe and decentralized way. The blockchain mechanism stores the medical images in a distributed network confiding several nodes instead of a central node is termed a distributed ledger. Once the medical images are stored in the blockchain, the blocks cannot be eliminated or renovated. When the updating of the ledger occurs, all nodes in the network makes new transaction and the nodes are voted by a consensus mechanism through verification. Figure 3 mentions the proposed blockchain technology for the process of medical image sharing.

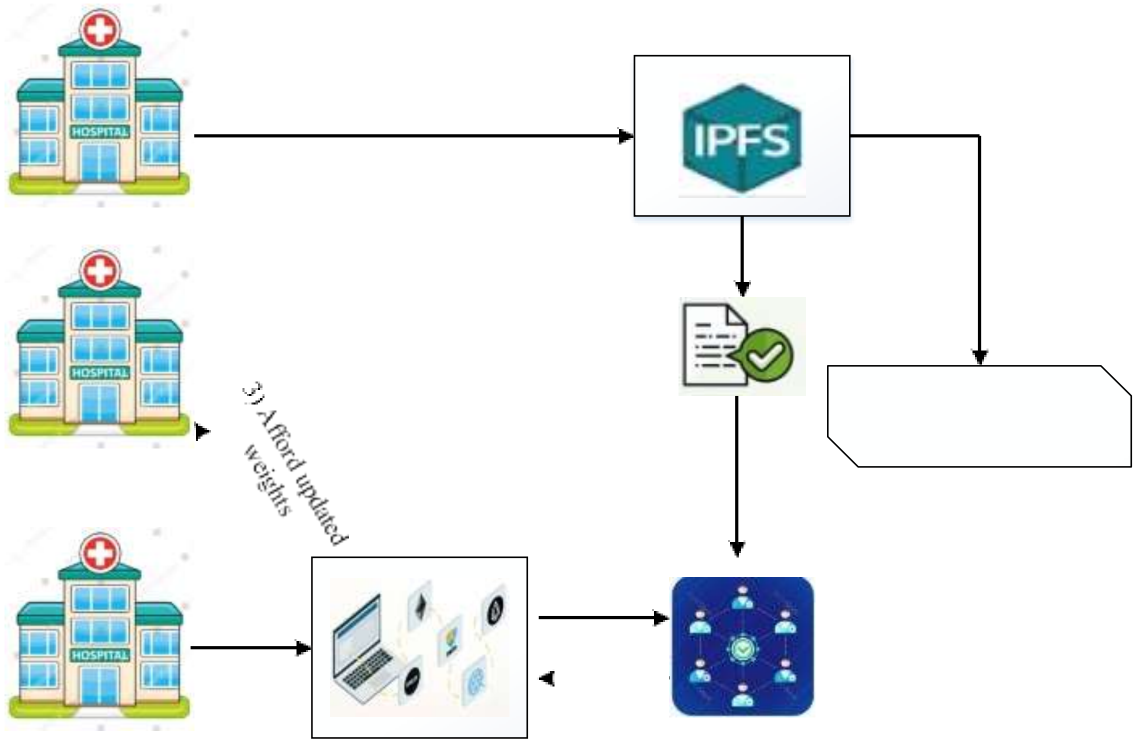


Figure 3 Proposed DLT and smart contract technology for secure medical image transmission for transacting the medical images between two parties, the DLT mechanism cannot demand a central authority. Because of the useful features such as distributed, decentralized and secured, the blockchain mechanism becomes more popular. Due to the decentralized network, the requirement of central authority is minimized to manage the network. The ledger is shared and is controlled by each node presented in the network. A distributed ledger is a kind of shared dataset that considers the availability of nodes with the motive of attack. DLT and smart contracts provide a chance to limit their digital identity. The legal identity mentions the transaction of personal smart contracts and obtains several personal data like reputation, medical records, credit records and validating obligations.

After encrypting the medical images, blockchain is employed to store such encrypted images for enhancing confidentiality, authenticity, and integrity. The proposed study used DLT and a smart contract mechanism for storing medical images. To ensure the patient's medical images, an effective smart contract is developed. The major intention of smart contracts is to provide increased security with minimized costs. Smart contract technology is publicly presented over the network for maintaining communication between users. Moreover, the smart contract assures the secured transmission by automatically verifying the stored medical images. Also, it can trace and gather medical images from the actual destination. The parameters that are needed to share the images via smart contract are the name of the data provider, hospital address and data description.

The stored local model weights along with hash values in the IPFS are stored in the database of the blockchain. Authorized healthcare centres distribute the trained weights of deep learning mechanisms via smart contracts. This smart contract allows to distribute the deep learning models on the blockchain system. Hence, only authorized hospitals can be able to access the distributed weights (medical images). The blockchain over the distributed nodes ensures reliability and transparency. The smart contract-based hospital registration is shown in Table 2

Table 3 Medical image sharing through smart contract.

Table 2 Hospital registration algorithm through smart contract

```
Step 1: State of contract □generated.
Step 2: State of Hospital □Qualified to Upload Medical Images
Step 3: h □is the group of Registered Hospitals (Q)
Step 4: h1 □Comes under the catalogue of hospitals
Step 5: Limited access to only h □ Q
Step 6: if (Registered Hospital and IPFS hash= =true) then
Step 7: State of contract □1 sign for success
Step 8: State of hospital □ success Authorized.
Step 9: For each hospital, generate validation message
Step 10: end if.
Step 11: if (Registered Hospital and IPFS hash! = true) then
Step 12: Return State of contract exhibit an error
Step 13: end if
```

An example smart contract based medical image sharing is illustrated in the above-mentioned algorithm. In this case, the smart contract affords the condition to distribute the medical information between hospitals. In the blockchain ledger, the token is created, and the smart contract mechanism ensures the distributed images belongs to a trustworthy source. In the blockchain system, the smart contract transfers the data along with the sign of authorized medical centres. The smart contract distributes the stored medical images to the healthcare centres without exhibiting the actual information. The proposed DLT and smart contract based blockchain assures the transmission of medical images by improving the data integrity with reduced transaction cost. The decryption stage obtains the medical images using private key. Then, the disease available in the input medical image is analysed using deep learning model.

Proposed recurrent generative neural network (RGNN) for disease diagnosis

After decrypting the medical image, it is important to detect the disease in the input medical image. For this purpose, the proposed study used the RGNN model, where the recurrent neural network (RNN) is hybridized with a generative adversarial network (GAN). The RNN method has the ability to learn temporal features of input images and it allows to solve prediction problems. The GAN analyses the different characteristics of each image and improves the classification.
accuracy. Because of the benefits of these two deep learning models, the proposed study hybridized GAN with RNN for diagnosing disease in the provided medical images. The GAN model contains two networks a generator and a discriminator.

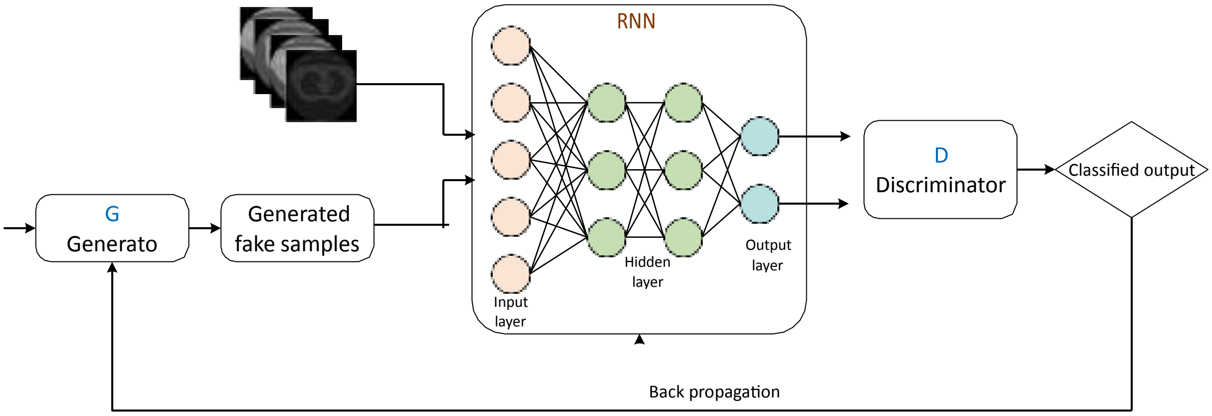


Figure 4 RGNN structure

The generator is responsible for mimicking input images with the aim of spoofing the discriminator by portraying the generated images are original diseased ones. The discriminator attempts to detect whether the input images are healthy or unhealthy. The generator creates fake samples from the random input and the output of the generator is fed to the RNN model. The generator contains both healthy and unhealthy samples which are given as the input of the RNN model. The layers presented in the RNN network extract the useful features and provide the extracted features to the discriminator. Then, the discriminator generates a classified output. The min-max game of GAN with value function $VF\ (Gr\ , Dr\ )$ is given as, min-max $V_F(G_r, D_r) = E_{Z\sim q\ data(z)}[\log D_r(z)] + E_{y\sim q\ (y)}[\log(1 - D_r(G_r(y)))]$

This GELU provides an optimal convergence rate to the neural network as compared with the sigmoid function. When training is done for both generator and discriminator, then the RGNN model is qualified to generate samples. Based on this, the disease in the input images is detected in the proposed RGNN model.

Results and discussion

This section provides the simulation result and analysis of the proposed framework. The efficacy of the proposed approaches is evaluated by analyzing the performance of both proposed and existing techniques. For simulation purposes, the proposed study used a Python tool and CT images in the COVID-19 dataset is utilized in the experimental setup. The performance is measured through different parameters like accuracy, sensitivity, specificity, compression ratio, PSNR and space savings.

Performance Metrics:

The evaluation of performance metrics exhibits the effectiveness of the proposed methodologies. The following metrics are employed to measure the performance of the proposed model.

Accuracy: Accuracy is an essential metric utilized to measure the efficacy of the proposed classifier. The ratio of correctly predicted images to the entire medical images in the dataset is termed as accuracy. It is computed as,

$$Accuracy = \frac{Tp + Tn}{Tp + Tn + Fp + Fn}$$

Specificity: It is the ratio of the entire amount of non-diseased images which are correctly detected to the entire non-diseased images from the dataset. The specificity measure is also called a True Negative Rate. The expression of specificity is represented as

$$Specificity = \frac{T_n}{T_n + F_p}$$

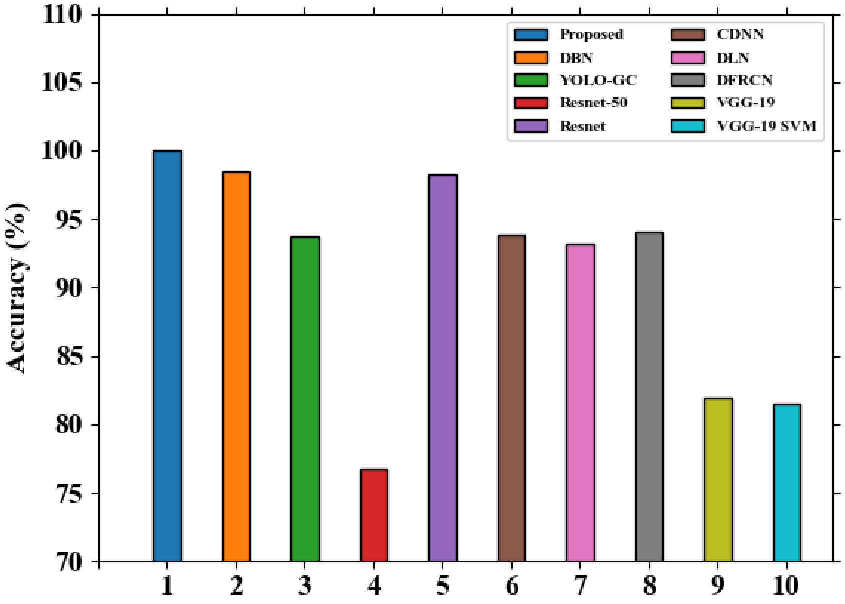
Sensitivity: Sensitivity measures the number of accurately classified images by the proposed RGNN classifier of all perfect predictions that could have been done. The term sensitivity is also called recall and it portrays the missed correctly classified image. The formulation of sensitivity is given as,

$$Tp\ Tp + Fn$$

PSNR: The term PSNR measures the inaudibility of each image and also it indicates the quality of the image. The PSNR is mentioned in terms of decibels (dB) and its value is proportional to the nearest cover image to the stego image. With the help of the PSNR measure, the peak error is detected.

Performance Comparison Analysis

The comparison analysis is necessary to prove the efficacy of the proposed techniques. For comparison analysis, the proposed study used several existing techniques [25] and shows the efficacy of the proposed framework. The accuracy performance of the proposed RGNN and existing techniques are shown in Figure 5



The above graphical representation shows that the proposed model brings higher detection accuracy as compared with others. The existing techniques attained reduced detection accuracy due to several drawbacks like low learning ability, increased computational complexity, overfitting issues etc. But the proposed study has a higher ability to learn the features using a hybrid deep learning model. Also, the effective encryption and key generation process makes the system avoid computational complexity. The attained accuracy of proposed RGNN is 99.9% and the existing DBN is 98.5%, YOLO-GC is 93.7%, Resnet-50 is 76.7%, Resnet is 98.3%, Convolutional- deconvolutional networks (CDNN) is 93.8%, Deep learning networks (DLN) is 93.17%, Deep full resolution convolutional networks (DFRCN) is 94.04%, VGG-19 is 81.93% and VGG-19 SVM is 81.5%. This analysis reveals that the proposed deep learning model is highly suitable for detecting diseases in the given input images. The specificity comparison of both proposed and existing techniques are illustrated in Figure 6

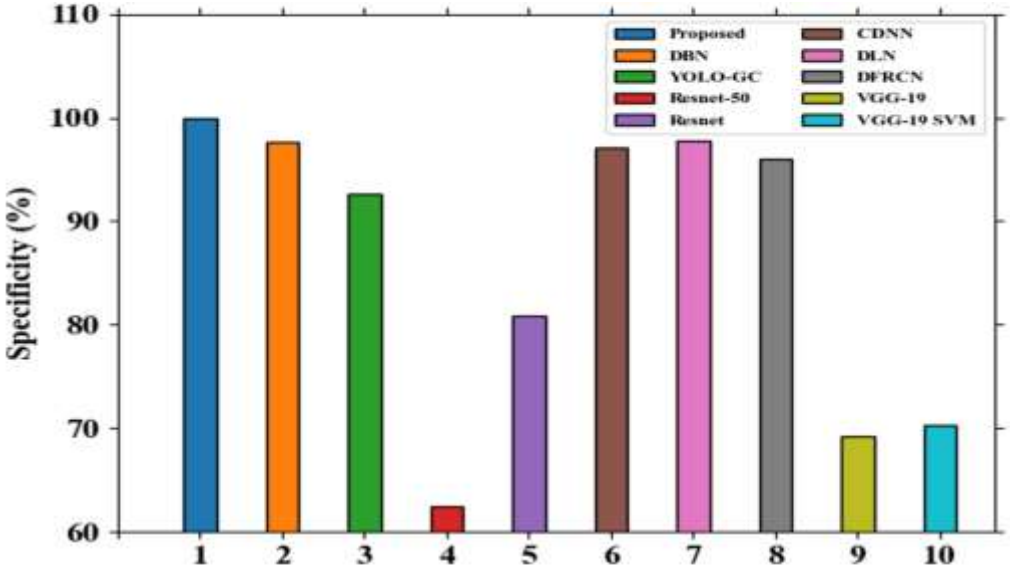
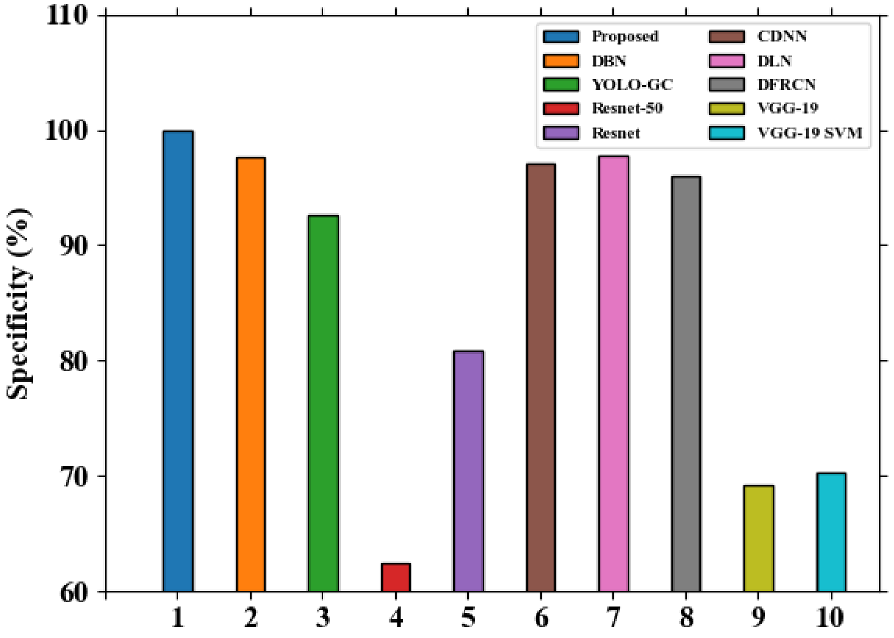


Figure 6 Specificity comparison analysis

The attained specificity of the proposed model is compared with several existing models. The comparison analysis clearly shows that the proposed RGNN model attained a higher specificity value than other techniques. The RGNN model attained a specificity of 98% and the specificity of existing DBN is 97.67%, YOLO-GC is 92.68%, Resnet-50 is 62.49%, Resnet is 80.92%, CDNN is 97.12%, DLN is 97.76%, DFRCN is 96.06%, VGG-19 is 69.25% and VGG-19 SVM is 70.31%



Hence, it shows that the proposed RGNN is highly effective than other existing techniques. The comparison analysis in terms of sensitivity measure is depicted in Figure 7

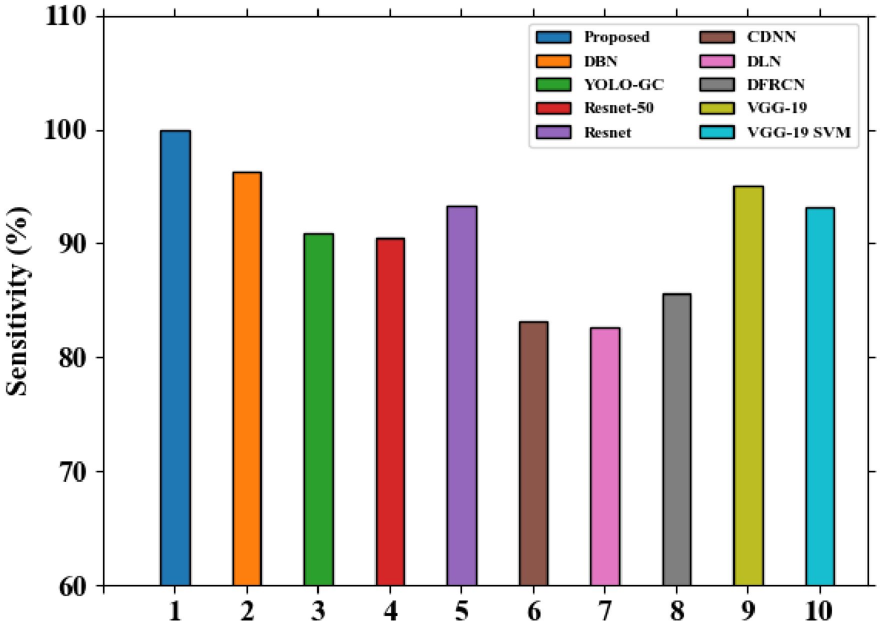


Figure 7 Sensitivity comparison analysis

The sensitivity comparison analysis is shown in the above graphical representation. The sensitivity performance of proposed RGNN is compared with varied existing deep learning models. The attained sensitivity of existing techniques is reduced due to several limitations. But the proposed RGNN gains increased sensitivity of 97%. The obtained sensitivity of DBN is 96.22%, YOLO-GC is 90.92%, Resnet-50 is 90.49%, Resnet is 93.35%, CDNN is 83.18%, DLN is 82.65%, DFRCN is 85.61%, VGG-19 is 95.03% and VGG-19 SVM is 93.12%. Thus, it apparently represents that the proposed RGNN is more efficient than others. The PSNR analysis of both proposed and existing optimized key generation is highlighted in Figure 8

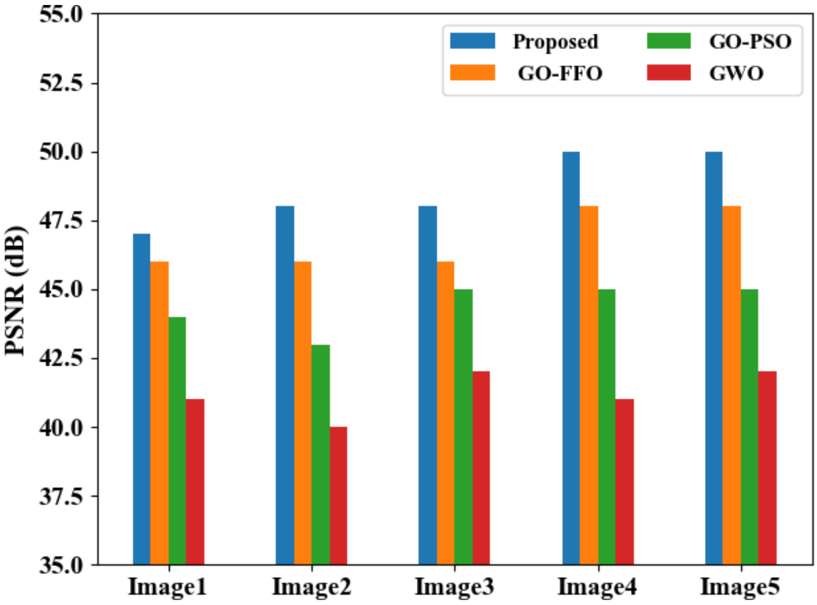


Figure 8 PSNR comparison analysis

The above figure investigates the efficiency of the proposed O-SSO algorithm with other existing algorithms in terms of PSNR. Here, the PSNR is analyzed for varied input images and the analysis shows that the proposed O-SSO achieved higher PSNR value than others. In the first image, the attained PSNR of O-SSO is 47 dB, Grasshopper with fruit fly optimization (GO-FFO) is 46 dB, Grasshopper with particle swarm optimization (GO-PSO) is 44 dB and (Grey wolf optimizer) GWO is 41 dB. By applying a second medical image, the attained PSNR of the proposed O- SSO is 48 dB, GO-FFO is 46 dB, GO-PSO is 43 dB and GWO is 40 db. Using the third image, the PSNR of the proposed O-SSO is 48 dB, GO-FFO is 46 dB, GO-PSO is 45 dB and GWO is 42 dB. Applying the fourth image, the proposed O-SSO algorithm attained the PSNR of 50 dB, GO-FFO is 48 dB, GO-PSO is 45 dB and GWO is 41 dB. Similarly, the PSNR attained from the fifth image is 50 dB for O-SSO algorithm. The PSNR of existing GO-FFO is 48 dB, GO-PSO is 45 dB and GWO is 42 dB. Thus, the analysis clearly shows that the proposed O-SSO approach outperformed the compared other optimized key generation algorithms. The compression performance analysis of both proposed and existing encryption approaches is depicted in Figure 9

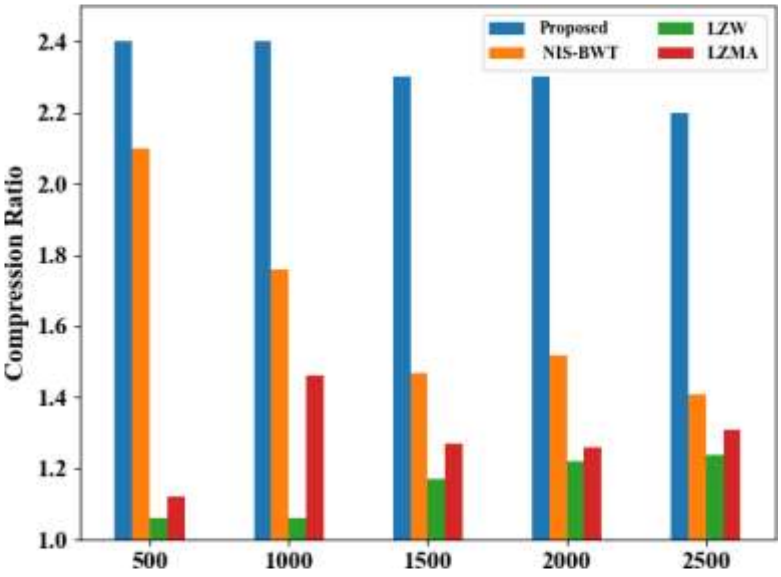


Figure 9 Compression ratio analysis of proposed CML with other existing approaches

The compression ratio analysis of CML model is compared with other existing encryption approaches. The above figure states that the proposed CML approach obtains a higher compression ratio than other compared approaches. Here, the compression ratio is analyzed for varying the transactions from 500 to 2500. When the number of transactions is 500, the proposed CML attained the higher compression ratio of 2.4 and the existing (Neighborhood indexing sequence (NIS) with burrow wheeler transform (BWT)) NIS-BWT is 2.1, LZW is 1.06 and LZMA is 1.12. Similarly, on the transaction amount of 1000, the compression ratio of the proposed CML is 2.4, NIS-BWT is 1.76, LZW is 1.06 and LZMA is 1.46. When the number of transactions is increased to 1500, the obtained compression ratio of the proposed CML is 2.3, whereas the existing approaches obtained the reduced compression ratio of NIS-BWT is 1.47, LZW is 1.17 and LZMA is 1.27. Concurrently, on the transaction amount of 2000, the attained compression ratio of proposed CML is 2.3 and the existing NIS-BWT is 1.52, LZW is 1.22 and LZMA is 1.26. When the transaction count is of 2500, the proposed CML obtained an increased compression ratio of 2.2 whereas, the existing key approaches achieved a reduced compression ratio i.e.) NIS-BWT is 1.41, LZW is 1.24 and LZMA is 1.31. This analysis proves that the proposed encryption algorithm is more robust than the other existing encryption approaches. The compression performance analysis of the proposed encryption approach with other existing approaches is shown in Figure 10

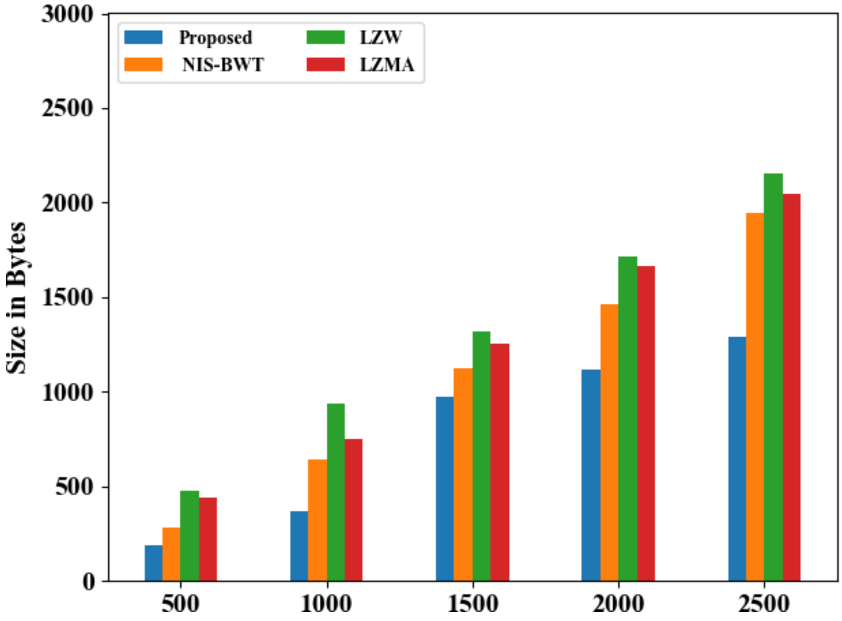


Figure 10 Comparison analysis of compression performance

The compression performance is analysed for proposed CML and other existing approaches like NIS-BWT, LZW and LZMA. By varying the number of transactions, the compression performance is determined. When the number of transactions is 500, the proposed CML compresses the original image into 190 bytes, whereas the existing approaches like NIS-BWT, LZW and LZMA have a higher compressed file size of 285 bytes, 477 bytes and 444 bytes. Under the transaction number of 1000, the proposed CML has reduced the compressed file size to 370 bytes. But the existing NIS-BWT, LZW and LZMA have increased compressed file size of 643 bytes, 935 bytes and 750 bytes. When the number of transactions is 1500, the proposed CML has compressed the actual file into 974 bytes, while the existing NIS-BWT, LZW and LZMA have led to the increased compressed file size of 1128 bytes, 1320 bytes and 1254 bytes. Moreover, when the transaction count is varied in 2000, the proposed approach obtained a minimal compressed file size of 1120 bytes. But the existing NIS-BWT, LZW and LZMA obtained higher compressed file sizes of 1460 bytes, 1712 bytes and 1665 bytes. Under the transaction number of 2500, the proposed CML compresses the actual file size into 1292 bytes, while the existing NIS-BWT, LZW and LZMA have increased compressed file size of 1944 bytes, 2157 bytes and 2044 bytes. The space savings analysis of both proposed and existing approaches is shown in Figure 1.

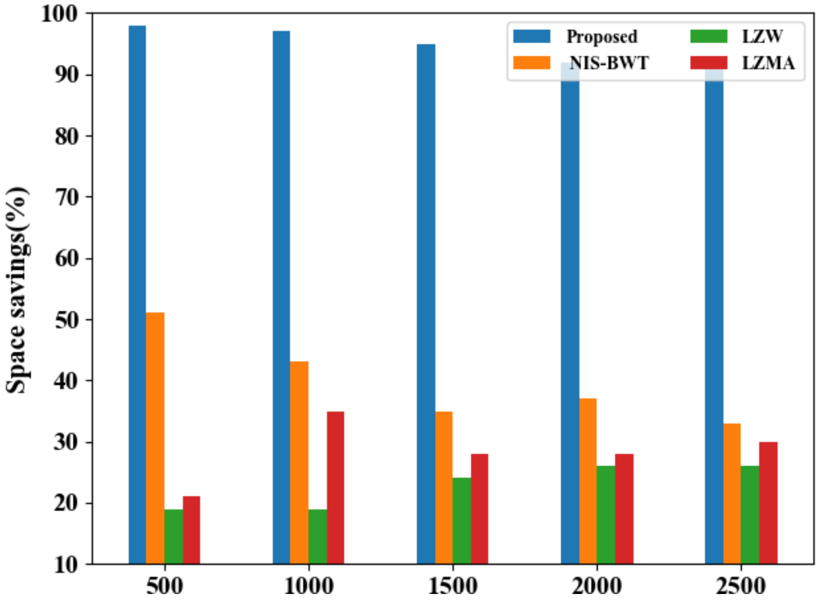


Figure 11 Space savings analysis of both proposed CML with other existing approaches

The above figure investigates the space savings analysis of the proposed encryption approach with other existing encryption approaches. The result analysis apparently shows that the proposed CML approach obtains higher space savings than other compared approaches. When the transaction number is 500, the space savings of the proposed CML is increased to 98%, but the existing techniques NIS-BWT, LZW and LZMA obtained reduced space savings of 51%, 19% and 21%. When the amount of transaction is 1000, the space savings of CML is 97%, NIS-BWT is 43%, LZW is 19% and LZMA is 35%. On the transaction count of 1500, the space savings of CML is 85%, NIS-BWT is 35%, LZW is 24% and LZMA is 28%. Similarly, the transaction is enhanced to 2000, and the proposed CML obtains the increased space savings of 92%, whereas NIS- BWT is 37%, LZW is 26% and LZMA is 28%. When the transaction amount is 2500, the space savings of CML is 91%, NIS-BWT is 33%, LZW is 26% and LZMA is 30%. Therefore, the obtained results of the proposed framework and the comparison over other existing techniques prove that the proposed framework is more efficient than others.

Conclusion:

The proposed framework introduced an efficient model for securing medical images through blockchain technology. In recent decades, security is becoming a major challenging task while transmitting medical images to several healthcare centres. Thus, to provide secure transmission of medical images, the proposed study develops a deep learning-based blockchain model. Initially, the input data are collected from the provided dataset. Then, an encryption process is performed to improve the security through the CML approach. The authenticity of the encrypted images is improved by generating optimal keys with the assist of the O-SSO approach. This approach selects optimal keys for the encryption and decryption

process, and it helps to enhance the confidentiality of the image. After encrypting the image with the optimal public key, the DLT and smart
contract-based blockchain technology is adopted to store encrypted images. Hence, the input medical images are highly secured during transmission. Finally, the medical images are decrypted with a private key and the disease is detected using the proposed RGNN model. The experimental results show that the proposed deep learning model obtained higher detection performance in terms of accuracy 99.9%, sensitivity 97% and specificity 98% over other compared methods. Also, the analysis of PSNR, compression ratio and space savings show that the proposed approaches are highly suitable for secure image transmission. In future, the parameters of deep learning will be tuned to attain more classification performance. Furthermore, hybrid encryption approaches will be developed to afford more security.

References

[1] Dwivedi, A.D., Srivastava, G., Dhar, S. and Singh, R., 2019. A decentralized privacy- preserving healthcare blockchain for IoT. Sensors, 19(2), p.326.

[2] Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A. and Hayajneh, T., 2018. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of medical systems, 42(7), pp.1-7.

[3] Ratta, P., Kaur, A., Sharma, S., Shabaz, M. and Dhiman, G., 2021. Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives. Journal of Food Quality, 2021.

[4] Abdolkhani, R., Gray, K., Borda, A. and DeSouza, R., 2019. Patient-generated health data management and quality challenges in remote patient monitoring. JAMIA open, 2(4), pp.471-478.

[5] Tuli, S., Mahmud, R., Tuli, S. and Buyya, R., 2019. Fogbus: A blockchain-based lightweight framework for edge and fog computing. Journal of Systems and Software, 154, pp.22-36.

[6] Baker, T., Asim, M., Samwini, H., Shamim, N., Alani, M.M. and Buyya, R., 2022. A blockchain-based Fog-oriented lightweight framework for smart public vehicular transportation systems. Computer Networks, 203, p.108676.

[7] Lin, H., Garg, S., Hu, J., Wang, X., Piran, M.J. and Hossain, M.S., 2020. Privacy-enhanced data fusion for COVID-19 applications in intelligent Internet of medical Things. IEEE Internet of Things Journal, 8(21), pp.15683-15693.

[8] Wang, R., Liu, H., Wang, H., Yang, Q. and Wu, D., 2019. Distributed security architecture based on blockchain for connected health: architecture, challenges, and approaches. IEEE Wireless Communications, 26(6), pp.30-36.

[9] Tang, W., Ren, J., Deng, K. and Zhang, Y., 2019. Secure data aggregation of lightweight E- healthcare IoT devices with fair incentives. IEEE Internet of Things Journal, 6(5), pp.8714-8726.

[10] Mohanta, B.K., Jena, D., Satapathy, U. and Patnaik, S., 2020. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 11, p.100227.

[11] Miglani, A. and Kumar, N., 2021. Blockchain management and machine learning adaptation for IoT environment in 5G and beyond networks: A systematic review. Computer Communications, 178, pp.37-63.

[12] Kumar, P., Gupta, G.P. and Tripathi, R., 2021. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. Journal of Systems Architecture, 115, p.101954.

[13] Shafay, M., Ahmad, R.W., Salah, K., Yaqoob, I., Jayaraman, R. and Omar, M., 2022. Blockchain for deep learning: review and open challenges. Cluster Computing, pp.1-25.

[14] Shah, D., Patel, D., Adesara, J., Hingu, P. and Shah, M., 2021. Exploiting the capabilities of blockchain and machine learning in education. Augmented Human Research, 6(1), pp.1-14.

[15] Li, D., Han, D., Weng, T.H., Zheng, Z., Li, H., Liu, H., Castiglione, A. and Li, K.C., 2022. Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey. Soft Computing, 26(9), pp.4423-4440.

[16] Srivastava, G., Parizi, R.M. and Dehghantanha, A., 2020. The future of blockchain technology in healthcare internet of things security. Blockchain cybersecurity, trust and privacy, pp.161-184.

[17] Gadekallu, T.R., Manoj, M.K., Kumar, N., Hakak, S. and Bhattacharya, S., 2021. Blockchain- based attack detection on machine learning algorithms for IoT-based e-health applications. IEEE Internet of Things Magazine, 4(3), pp.30-33.

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

[19] Unal, D., Hammoudeh, M., Khan, M.A., Abuarqoub, A., Epiphaniou, G. and Hamila, R., 2021. Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things. Computers & Security, 109, p.102393.

[20] Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A. and Hayajneh, T., 2018. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of medical systems, 42(7), pp.1-7.

[21] Keshk, M., Turnbull, B., Moustafa, N., Vatsalan, D. and Choo, K.K.R., 2019. A privacy- preserving-framework-based blockchain and deep learning for protecting smart power networks. IEEE Transactions on Industrial Informatics, 16(8), pp.5110-5118.

[22] Principal, S. H. M., Mishra, A., Sharma, J. K., Aarif, M., & Arwab, M. SMART AND INNOVATIVE IDEAS TO PROMOTE TOURISM FOR GLOBAL TRADE AND ECONOMIC GROWTH.

[23] Ebrahimi, M., Attarilar, S., Gode, C., Kandavalli, S. R., Shamsborhan, M., & Wang, Q. (2023). Conceptual Analysis on Severe Plastic Deformation Processes of Shape Memory Alloys: Mechanical Properties and Microstructure Characterization. Metals, 13(3), 447.

[24] J. K. S. Al-Safi, A. Bansal, M. Aarif, M. S. Z. Almahairah, G. Manoharan and F. J. Alotoum, "Assessment Based On IoT For Efficient Information Surveillance Regarding Harmful Strikes Upon Financial Collection," 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2023, pp. 1-5, doi: 10.1109/ICCCI56745.2023.10128500.

[25] Khan, S.I., Kaur, C., Al Ansari, M.S. et al. Implementation of cloud based IoT technology in manufacturing industry for smart control of manufacturing process. Int J Interact Des Manuf (2023). https://doi.org/10.1007/s12008-023-01366-w

[26] M, Arun and Alalmai, Ali and Aarif, Mohd, Student's Anticipation in Procuring Post Graduation Programme in Hotel Management through Distance Learning (March 1, 2022). ANWESH: International Journal of Management & Information Technology (2022), Available at SSRN: https://ssrn.com/abstract=4072674

[27] Tidake, Vishal & Mazumdar, Nilanjan & Kumar, A. & Rao, B. & Fatma, Dr Gulnaz & Raj, I.. (2023). Sentiment Analysis of Movie Review using Hybrid Optimization with Convolutional Neural Network in English Language. 1668-1673. 10.1109/ICAIS56108.2023.10073750.

[28] Kaur, C., Panda, T., Panda, S., Al Ansari, A. R. M., Nivetha, M., & Bala, B. K. (2023, February). Utilizing the Random Forest Algorithm to Enhance Alzheimer's disease Diagnosis. In 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS) (pp. 1662-1667). IEEE.

[29] Kandavalli, S. R., Wang, Q., Ebrahimi, M., Gode, C., Djavanroodi, F., Attarilar, S., & Liu, S. (2021). A brief review on the evolution of metallic dental implants: history, design, and application. Frontiers in Materials, 140.

[30] C. Kaur, T. Panda, S. Panda, A. Rahman Mohammed Al Ansari, M. Nivetha and B. Kiran Bala, "Utilizing the Random Forest Algorithm to Enhance Alzheimer's disease Diagnosis," 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2023, pp. 1662-1667, doi: 10.1109/ICAIS56108.2023.10073852.

[31] M. A. Tripathi, R. Tripathi, F. Effendy, G. Manoharan, M. John Paul and M. Aarif, "An In-Depth Analysis of the Role That ML and Big Data Play in Driving Digital Marketing's Paradigm Shift," 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2023, pp. 1-6, doi: 10.1109/ICCCI56745.2023.10128357.

[32] A. Siddiqua, A. Anjum, S. Kondapalli and C. Kaur, "Regulating and monitoring IoT controlled solar power plant by ML," 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2023, pp. 1-4, doi: 10.1109/ICCCI56745.2023.10128300.

[33] M. Lourens, A. Tamizhselvi, B. Goswami, J. Alanya-Beltran, M. Aarif and D. Gangodkar, "Database Management Difficulties in the Internet of Things," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 322-326, doi: 10.1109/IC3I56241.2022.10072614.

[34] Dhas, D. S. E. J., Raja, R., Jannet, S., Wins, K. L. D., Thomas, J. M., & Kandavalli, S. R. (2023). Effect of carbide ceramics and coke on the properties of dispersion strengthened aluminium□silicon7□magnesium hybrid composites. Materialwissenschaft und Werkstofftechnik, 54(2), 147-157.

[35] Prabha, C., Arunkumar, S. P., Sharon, H., Vijay, R., Niyas, A. M., Stanley, P., & Ratna, K. S. (2020, March). Performance and combustion analysis of diesel engine fueled by blends of diesel+ pyrolytic oil from Polyalthia longifolia seeds. In AIP Conference Proceedings (Vol. 2225, No. 1, p. 030002). AIP Publishing LLC.

[36] Abd Algani, Y. M., Caro, O. J. M., Bravo, L. M. R., Kaur, C., Al Ansari, M. S., & Bala, B. K. (2023). Leaf disease identification and classification using optimized deep learning. Measurement: Sensors, 25, 100643.

[37] Ratna, K. S., Daniel, C., Ram, A., Yadav, B. S. K., & Hemalatha, G. (2021). Analytical investigation of MR damper for vibration control: a review. Journal of Applied Engineering Sciences, 11(1), 49-52.

[38] Abd Algani, Y. M., Ritonga, M., Kiran Bala, B., Al Ansari, M. S., Badr, M., & Taloba, A. I. (2022). Machine learning in health condition check-up: An approach using Breiman's random forest algorithm. Measurement: Sensors, 23, 100406. https://doi.org/10.1016/j.measen.2022.100406

[39] Mourad, H. M., Kaur, D., & Aarif, M. (2020). Challenges Faced by Big Data and Its Orientation in the Field of Business Marketing. International Journal of Mechanical and Production Engineering Research and Development (IJMPERD), 10(3), 8091-8102.

[40] Ruban, S. R., Jayaseelan, P., Suresh, M., & RatnaKandavalli, S. (2020, December). Effect of textures on machining of carbon steel under dry cutting condition. In IOP Conference Series: Materials Science and Engineering (Vol. 993, No. 1, p. 012143). IOP Publishing.

[41] Naidu, K. B., Prasad, B. R., Hassen, S. M., Kaur, C., Al Ansari, M. S., Vinod, R., ... & Bala, B. K. (2022). Analysis of Hadoop log file in an environment for dynamic detection of threats using machine learning. Measurement: Sensors, 24, 100545.

[42] Suman, P., Bannaravuri, P. K., Baburao, G., Kandavalli, S. R., Alam, S., ShanthiRaju, M., & Pulisheru, K. S. (2021). Integrity on properties of Cu-based composites with the addition of reinforcement: A review. Materials Today: Proceedings, 47, 6609-6613.

[43] Kandavalli, S. R., Rao, G. B., Bannaravuri, P. K., Rajam, M. M. K., Kandavalli, S. R., & Ruban, S. R. (2021). Surface strengthening of aluminium alloys/composites by laser applications: A comprehensive review. Materials Today: Proceedings, 47, 6919-6925.

[44] Sharma, Nisha, Anil Kumar Yadava, Mohd Aarif, Harishchander Anandaram, Ali Alalmai, and Chandradeep Singh. "Business Opportunities And Challenges For Women In The Travel And Tourism Industry During Pandemics Covid-19." Journal of Positive School Psychology (2022): 897-903.

[45] Raja, R., Jegathambal, P., Jannet, S., Thanckachan, T., Paul, C. G., Reji, S., & Ratna, K. S. (2020, November). Fabrication and study of Al6061-T6 reinforced with TiO2 nanoparticles by the process of friction stir processing. In AIP Conference Proceedings (Vol. 2270, No. 1, p. 030002). AIP Publishing LLC.

[46] Kumar, B., & Kumar, P. (2022). Preparation of hybrid reinforced aluminium metal matrix composite by using ZrB2: A systematic review. Materials Today: Proceedings.

[47] Kandavalli, S. R., Khan, A. M., Iqbal, A., Jamil, M., Abbas, S., Laghari, R. A., & Cheok, Q. (2023). Application of sophisticated sensors to advance the monitoring of machining processes: analysis and holistic review. The International Journal of Advanced Manufacturing Technology, 1-26.

[48] Aarif, Mohd, and Ali Alalmai. "Importance of Effective Business Communication for promoting and developing Hospitality Industry in Saudi Arabia." A case study of Gizan (Jazan) (2019).

[49] Abd Algani, Y. M., Ritonga, M., Kiran Bala, B., Al Ansari, M. S., Badr, M., & Taloba, A. I. (2022). Machine learning in health condition check-up: An approach using Breiman's random forest algorithm. Measurement: Sensors, 23, 100406. https://doi.org/10.1016/j.measen.2022.100406

[50] Mourad, H. M., Kaur, D., & Aarif, M. (2020). Challenges Faced by Big Data and Its Orientation in the Field of Business Marketing. International Journal of Mechanical and Production Engineering Research and Development (IJMPERD), 10(3), 8091-8102.

[51] Kumar, R., Wang, W., Kumar, J., Yang, T., Khan, A., Ali, W. and Ali, I., 2021. An integration of blockchain and AI for secure data sharing and detection of CT images for the hospitals. Computerized Medical Imaging and Graphics, 87, p.101812.

[52] Neelakandan, S., Rene Beulah, J., Prathiba, L., Murthy, G.L.N., Irudaya Raj, E.F. and Arulkumar, N., 2022. Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model. International Journal of Modeling, Simulation, and Scientific Computing, p.2241006.

[53] Połap, D., Srivastava, G. and Yu, K., 2021. Agent architecture of an intelligent medical system based on federated learning and blockchain technology. Journal of Information Security and Applications, 58, p.102748.

[54] Alqaralleh, Bassam AY, Thavavel Vaiyapuri, Velmurugan Subbiah Parvathy, Deepak Gupta, Ashish Khanna, and K. Shankar. "Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment." Personal and ubiquitous computing (2021): 1-11.