



Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment

Bassam A. Y. Alqaralleh¹ · Thavavel Vaiyapuri² · Velmurugan Subbiah Parvathy³ · Deepak Gupta⁴ · Ashish Khanna⁴ · K. Shankar⁵

Received: 21 October 2020 / Accepted: 16 February 2021

© The Author(s), under exclusive licence to Springer-Verlag London Ltd. part of Springer Nature 2021

Abstract

In recent days, the Internet of Medical Things (IoMT) is commonly employed in different aspects of healthcare applications. Owing to the increasing necessities of IoT, a huge amount of sensing data is collected from distinct IoT gadgets. To investigate the generated data, artificial intelligence (AI) models plays an important role to achieve scalability and accurate examination in real-time environment. However, the characteristics of IoMT result in certain design challenges, namely, security and privacy, resource limitation, and inadequate training data. At the same time, blockchain, an upcoming technology, has offered a decentralized architecture, which gives secured data transmission and resources to distinct nodes of the IoT environment and is stimulated for eliminating centralized management and eliminates the challenges involved in it. This paper designs deep learning (DL) with blockchain-assisted secure image transmission and diagnosis model for the IoMT environment. The presented model comprises a few processes namely data collection, secure transaction, hash value encryption, and data classification. Primarily, elliptic curve cryptography (ECC) is applied, and the optimal key generation of ECC takes place using hybridization of grasshopper with fruit fly optimization (GO-FFO) algorithm. Then, the neighborhood indexing sequence (NIS) with burrow wheeler transform (BWT), called NIS-BWT, is employed to encrypt the hash values. At last, a deep belief network (DBN) is utilized for the classification process to diagnose the existence of disease. An extensive experimental validation takes place to determine the analysis of the optimal results of the presented model, and the results are investigated under diverse aspects.

Keywords Blockchain · Security · Hash value encryption · Deep learning · IoMT

1 Introduction

In recent times, the Internet of things (IoT) and related clinical applications have been developed progressively and facilitated as an effective and efficient system for the users where the

medical resources are available automatically. Remote patient management (RPM) has been deployed with diverse medical services like prominent signal observation using implantable sensors, arrhythmia detection, fall investigation, oxygen maintenance, observing the pregnant women, chemotherapy

✉ K. Shankar
drkshankar@ieee.org

Bassam A. Y. Alqaralleh
alqaralleh@ahu.edu.jo

Thavavel Vaiyapuri
t.thangam@psau.edu.sa

Velmurugan Subbiah Parvathy
s.p.velmurugan@klu.ac.in

Deepak Gupta
deepakgupta@mait.ac.in

Ashish Khanna
ashishkhanna@mait.ac.in

¹ Associate Professor, Computer Science Department—IT Faculty, AL-Hussein Bin Talal University, Ma'an, Jordan

² College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj, Kingdom of Saudi Arabia

³ Department of Electronics and Communication Engineering, Kalasalingam Academy of Research and Education, Srivilliputhur, Tamil Nadu 626128, India

⁴ Department of Computer Science & Engineering, Maharaja Agrasen Institute of Technology, Delhi, India

⁵ Department of Computer Applications, Alagappa University, Karaikudi, India

response, regularization of glucose level, and so on [1]. Although IoT is facilitated with a massive number of resources, complete proficiency is lagging because of the inexistence of stability, fault-tolerant, and security. In e-health, the biological details of the patients are collected with the help of medical IoT machines, and the received details are forwarded to edge or cloud units which are consumed by hackers and resulted in security problems. Finally, the systems are highly vulnerable under specific points, in particular, while handling massive information. The cyberattacks namely ransomware, denial-of-service (DoS), and additional attacks degrade the proficiency of classical e-health methods and disrupt the clinical services [2].

Nowadays, the intruders highly interrupt the clinical details from all medical centers. Based on the survey of the US Health and Human Services (HHS) department, over 2000 data violations were carried out in the last decades. Moreover, the caretakers like medical professionals and staffs were relevant to incomplete data breaches. The IoT architecture is endangered for eavesdropping intrusions using Bluetooth, Zigbee, or WiFi links, DoS, and attacks. In addition, traditional edge or cloud processes are defective in maintaining the patient details and eliminate hackers and intruders. Even though a massive number of benefits are embedded in this method, it suffers from numerous issues that require an effective method for resolving these problems named Big Data analysis for IoT model namely inexistence of accuracy, minimum delay, privacy, and centralization. In order to overcome these problems, the blockchain model has been applied due to enormous benefits. It is a protective, decentralized, and shared database method. Each node in a blockchain is linked in a distributed fashion in which transactions and timestamps are saved robustly and distributed transactions without an intruder.

Blockchain method is capable of attaining better results in diverse applications like the economy, data privacy, agriculture, and medical care in IoT. Followed by, the data recorded in the block is connected by a chain using a hash function. As the block is connected consecutively, it is prevented from hacking. The conjunction of blockchain and artificial intelligence (AI) for IoT is composed of maximum approaches which reduce the issues like decentralized, digital signature, distributed, verified, and general digital ledger. Recently, the IoT gadgets find useful for collecting numerous details in a centralized manner; then, security, as well as space issues, is produced. These problems can be resolved under the application of a decentralized database executed in the merging of Blockchain and AI in IoT.

When a person decides to distribute the transaction with a neighbor in IoT, then the transaction ought to be immutable, protective, definable, digitally signed, and verified. Such modules offer a manageable quantity of data which has been employed for several applications like medical, smart home,

armed forces, government, and modern transportation. Initially, the smart contract concept has been applied to the blockchain system for security purposes that is recorded in the digital ledger. Next, the combination of Blockchain and AI shows maximum advantages in several aspects. The database present in a blockchain model is composed of transactions which are digitally signed hash value. Also, AI models are employed in resolving these complicated problems. Under the application of decentralization, automated and robust data verification in a blockchain network is performed which resolves small issues in a cloud server for big data analytics.

This paper introduces novel deep learning with blockchain-assisted secure image transmission and diagnosis model for the Internet of Medical Things (IoMT) environment. The presented model comprises few processes specifically data collection, secure transaction, hash value encryption, and data classification. Firstly, elliptic curve cryptography (ECC) is employed, and the optimal key generation of ECC is carried out by hybridization of grasshopper with fruit fly optimization (GO-FFO) algorithm. Followed by, neighborhood indexing sequence (NIS) with burrow wheeler transform (BWT), called NIS-BWT, is employed to encrypt the hash values. Finally, a deep belief network (DBN) is utilized for the classification process to diagnose the existence of the disease. An extensive experimental validation takes place to determine the optimal result analysis of the presented model, and the results are investigated under diverse aspects.

2 Related works

Rahman et al. [3] introduced a secured therapy model named blockchain at MEC and cloud. The therapeutic details collected from the physicians and patients have been processed with the help of cloud and mobile edge computing (MEC) blockchain nodes to ensure the permanent, unspecified, protective, and transparent distribution. In this method, blockchain preserves the hashes of therapy multimedia as well as original multimedia with images, audios, text, and videos under different databases. Although this method is composed of MEC blockchain which helps in eliminating the disadvantages of high bandwidth and computation, Griggs et al. [4] offered an automatic remote patient observing model by means of the modern contract of Ethereum. A smart device like mobile and laptop collects the data transmitted by body sensors. Then, the smart devices forward the gathered information to the previous smart contract recorded on Ethereum. Moreover, the Electronic Health Record (EHR) is saved in the blockchain system. Therefore, the intelligence results in a single point of failure and insignificant for the DoS attack. But, this method ensures the privacy of processing medical details.

Chen et al. [5] implemented a blockchain-based clinical data accessing model along with a cloud in order to save the

clinical data. Liang et al. [6] developed a blockchain and personal medical data distributing method where mobile application collects the information from portable sensors and enclose with cloud and blockchain hyperledger for validation of data security. Zhang et al. [7] applied a blockchain-related infrastructure termed as Fast Healthcare Interoperability Resources (FHIR) Chain for protective and reliable distribution healthcare data. The requirements are defined under the application of “Shared Nationwide Interoperability Roadmap.” Brogan et al. [8] focused on the role of the decentralized ledger for advanced EHR and assure the authority and data security. Developers have demonstrated the usage of IoTA protocol which is applied for authenticating confidential sharing, preservation, and retrieval of encryption details by means of a tamper-proof distributed ledger. A service of blockchain in patient-centric interoperability is presented in [9] using medical data utilities, collection, liquidity, affinity, and immutability. Rupasinghe et al. [10] discovered 2 types of risk factors like clinical factors and environmental factors. Such risk factors are termed as low, medium, and high that depend upon proof and expert recommendations. Here, 4 types of users in consortium blockchain to guarantee the interoperability, authentication, and simple data application for examining the likelihood of aged people. In addition, a smart contract is used for registering the user and the inclusion of data with blockchain and fall detection.

Dwivedi et al. [1] proposed blockchain-related e-health models deployed by Dorri et al. [11], which has been implied from lightweight blockchain for IoT. An overlay system has been considered for peer-to-peer networks where the nodes are linked in a virtual way. Here, IoT medical devices offer a block that has to be confirmed using cluster head (CH). Followed by, researchers have employed massive lightweight and standard security protocols for executing the security and preserve patient’s details in e-health. A static CH verifies blockchain security. Therefore, the removal of complete consensus eliminates the maintenance of blockchain-based e-health system. The e-health mechanism has been extended under the implementation of lightweight consensus method on peer to peer fog system. The CH selection for certain time intervals on nodes’ attributes. In addition, the essential blocks applied in monitoring the patient gathered as PA, and PA is triggered at 3 stages such as smartphone, fog, and cloud levels.

Gaetani et al. [12] projected a blockchain with 2 layers in the CC environment. The blockchain in a primary layer that retains the events carried out and used in a decentralized database while removing costlier computation for proof of work (PoW). Next, blockchain in a second layer preserves the logged actions generated from the primary layer database using PoW. Novo [13] developed a blockchain-based distributed structure to manage the control at memory and power IoT machines. The major purpose of this structure is composed of a manager hub between IoT devices and blockchain. The

manager hub is applied for accessing the blockchain node saved under certain wireless sensor network (WSN). The smart contract was executed to add the access policy with blockchain.

3 The proposed methodology

The overall working principle of the presented model is shown in Fig. 1. At the primary stage, the patient details are gathered using IoT gadgets, which are then encrypted using the GO-FFO algorithm. Besides, hash values in blockchain are encrypted and compressed by the NIS-BWT technique. Finally, the classification process is carried out using the DBN model. The detailed working process of these components is discussed in the subsequent sections.

3.1 ECC with GO-FFO technique

Normally, screening is a significant process in medical diagnosis. Once the medical image gets captured, a secure data transmission process is initiated. ECC is a novel model used for resolving the public key cryptography by means of the mathematical structure of elliptical bends with restricted field. It is an effective module with minimal key sizes for image privacy, and it is remarkably interesting with respect to

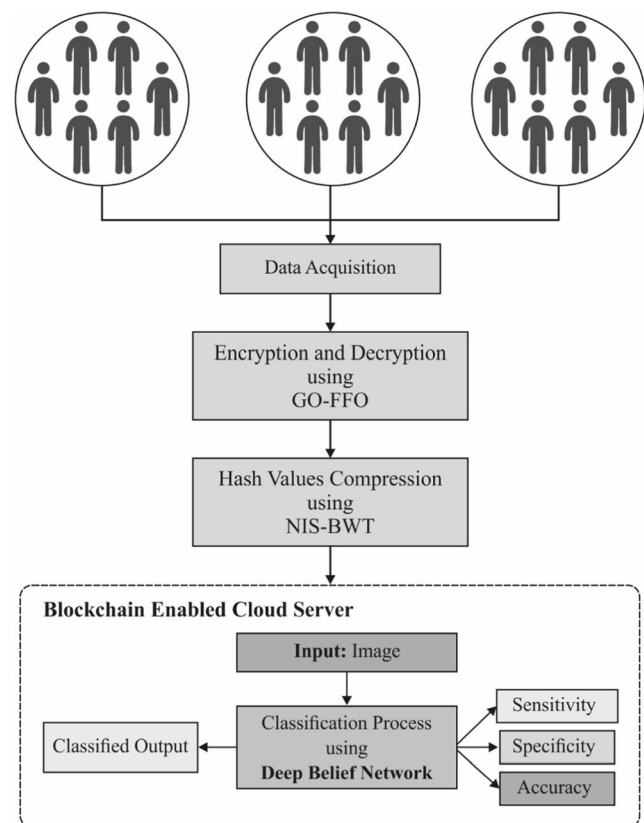


Fig. 1 The overall process of proposed method

breaking time. Moreover, the IoT clinical images are included with ECC [14]. This cryptographic security method is comprised of key generation, encryption, decryption, and prediction as demonstrated in Fig. 2. In order to improve the privacy of IoMT, optimization technology has been assumed for key generation. ECC is essential to achieve efficient implementation.

3.1.1 Key generation stage

The performance of ECC is divided into 2 phases, namely, prime stage and binary stage. In case of cryptographic events, a considerable module was selected with minimum points. Initially, prime stage operations decide a prime value, and restricted substantial quantities are developed on EC. Developing public as well as private keys are highly complicated for “ECC,” and the keys are obtained from prime numbers. Next, the sender encrypts the images using the public key of the receiver, and then decryption takes place by the use of the private key.

3.1.2 Optimal key selection process

The arithmetic optimization model which is suitable for the selection of elements among the collection of alternatives is applied in sectors like computer science, mathematics, and operation study. It helps in identifying the accessible value of the target function from various applications. The ECC security method is optimized using the key generation stage. Followed by, hybrid swarm-centric optimization is correlated with the integration of GO and FFO. Under the application of an optimization mechanism, the key solution is accomplished with private and public keys. Here, the sender will encrypt the image using the public key of the receiver, while the beneficiary decrypts the data with the help of a private key [15]. The GO model defines the grasshopper’s behavior. The mathematical approach reflects the swarming nature of grasshoppers as well as the FFO method.

At the time of initialization, once the key solution is induced, prime numbers are used for generating novel population size for the ideal key selection process.

$$Input_Sol = \{S1, S2, S3, \dots S_n\} \quad (1)$$

Here, the optimum set of keys are chosen by assuming the “fitness function” as the max key using PSNR for data scrambling and unscrambling data from clinical images. The organization has been developed with the help of hybrid optimization. It is demonstrated in condition (2).

$$Fitness = MAX\{PSNR\} \quad (2)$$

3.1.3 Grasshopper optimization (GO)

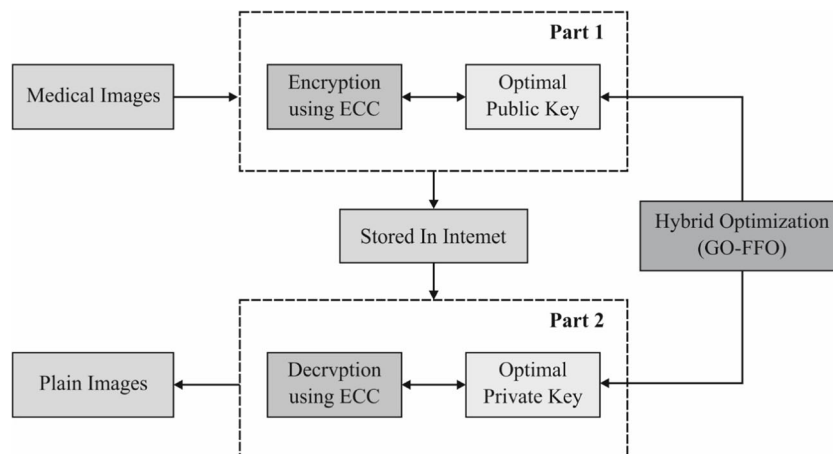
Grasshoppers are creepy crawlies and divided as a bug. Typically, the plant harvest is failed as it consumes every plant crops. The grasshopper swarm is comprised of exceptional trademark, where the swarming nature of nymph and adults [16] are presented. The swarm nymph has considerable deployment in a larval stage. The main location of the grasshopper is depicted by Eq. (3).

$$G_i = Soc_i + Gravity_i + Wind_i \quad (3)$$

where Soc_i shows social communication, $Gravity_i$ implies the gravity force on i th grasshopper, and $Wind_i$ refers a wind advection. In order to resolve the grasshopper function, few operations are evolved from social communication, gravitational force, and wind advection.

1. **Social interaction:** With limited advantages, it is not possible to create diverse solid energy among grasshoppers with wider isolations among them. This problem is resolved using the separation among grasshoppers and mapped with respect to [1, 4]; hence, the social interaction is depicted as,

Fig. 2. Process of GO-FFO



$$Soc_i = \sum_{j=1, j \neq i}^N S(p_{ij}) \hat{p}_{ij} \quad (4)$$

Therefore, $\hat{p}_{ij} = \frac{q_j - q_i}{p_{ij}}$; $p_{ij} = |q_j - q_i|$ where p_{ij} denotes the distance from i th and j th grasshopper, Soc represents the function which defines the efficiency of social forces, and \hat{p}_{ij} implies a unit vector from i th grasshopper to j th grasshopper. N refers to the count of grasshoppers. The s function describes the social forces as determined by the applied function:

$$Soc_force = f e^{-k/l} - e^{-k} \quad (5)$$

where f represents the intensity of attraction, l signifies the attractive length scale, and its ability is demonstrated.

2. Gravity force and wind advection: The gravitational force ($Gravity_i$) of grasshopper can be processed under the application of Eqs. (6) and (7). A nymph grasshopper does not have wings, and the deployments exceed the wind direction.

$$Gravity_i = -gr_con_g \quad (6)$$

$$Wind_i = zlgr_drift \quad (7)$$

where g denotes the gravitational constant, gr_con implies a unit vector, l refers a constant drift, and gr_drift represents a unit vector towards the wind direction. To overcome the optimization problems, the stochastic method should implement exploration and exploitation for selecting accurate approximation of global optimum which has been illustrated by

$$G_i = \sum \left\{ S(|q_j - q_i|) \frac{q_j - q_i}{p_{ij}} - gr_con_g + zlgr_drift \right\} \quad (8)$$

In GOA, it is ensured that grasshopper with optimal objective esteem is considered as the fittest grasshopper. The numerical method is efficient with exclusive parameters for exploration and exploitation under diverse optimization stages.

3.1.4 FFO algorithm

FFO is defined as a novel swarm intelligent (SI) model which was evolved from the fruit fly's foraging nature that comes under the interactive evolutionary processing. In general, fruit flies are tiny creatures that consume fruits and rotten plants. These types of creatures exist in high temperate as well as tropical climate zones globally. These species have effective

optical and olfactory senses when compared with alternate creatures. It is capable of identifying diverse aroma carried out in air using the olfactory organ even if the food source is placed far away. Followed by, it flies towards the food location using the vision property. Therefore, food searching process of a fruit fly is given in the following: (1) first, smell the food source using olfactory organ; (2) then, fly closer to the food position using the sensitive visions; and (3) finally, fruit flies' flocking location and fly towards the concerned direction. Figure 3 [17] illustrated the flowchart of FFO method.

Based on the food searching principle, the FFO is classified into 7 steps as given below.

Step 1. Initializing parameters: overall evolution value, population size pop , and initial fruit fly swarm position (X_0, Y_0).

Step 2. Initializing population:

$$\begin{aligned} X_i &= X_0 + rand, \\ Y_i &= Y_0 + rand. \end{aligned} \quad (9)$$

Step 3. Estimation of distance (D_i) and smell (S_i):

$$\begin{aligned} D_i &= \sqrt{X_i^2 + Y_i^2}, \\ S_i &= \frac{1}{D_i}. \end{aligned} \quad (10)$$

Step 4. Estimation of fitness function (f_i):

$$f_i = f(S_i). \quad (11)$$

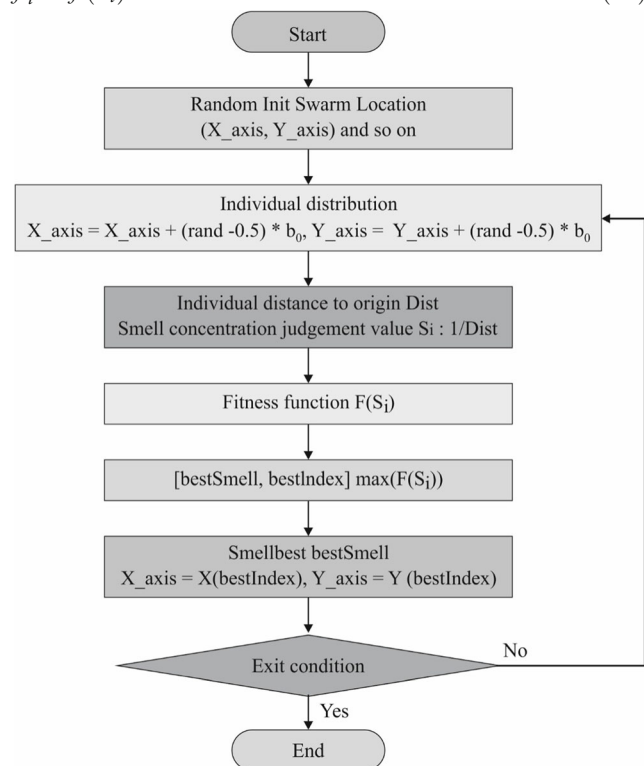


Fig. 3. Flowchart of FFO

Step 5. Identify the minimum individual fruit fly with optimal fitness function (f_b) when compared with other fruit flies:

$$[bestXbestindex] = \min (f(S_i)). \quad (12)$$

Step 6. Selection operation: Retain the optimal fitness function and coordinate points (X_b, Y_b). Next, fruit fly swarm move towards the position with effective fitness function value under the application of sensitive vision:

$$\begin{aligned} f_b &= bestX, \\ X_b &= X (bestindex), \\ Y_b &= Y (bestindex). \end{aligned} \quad (13)$$

Step 7. Decide whether the stopping criteria are satisfied or not. Else, jump to Step 2; else, terminate the circulation.

3.1.5 Encryption and decryption process

The hybridization of GO with FFO takes place for resolving the optimal key of ECC with extreme key, where PSNR is developed with the principles mentioned above. The evolutionary strategy of GO, with intensive organic product flies in searching limited course where a brief optimization model has been presented. Encryption is defined as the procedure of encoding images or text for the purpose of security issue. If the input image is forwarded by a sender through a curve, then the curvature point is found for scrambling the plain images and transform into ciphered image under the application of selected public keys. On the other hand, decryption is an inverse function of encryption where the encrypted details are decrypted with specific key given to the authenticated receiver. Then, scrambled data or image is appeared and remaining details are dropped. Hence, under the application of ECC, image would be decrypted, where ciphering the image with the help of private key.

3.2 NIS-BWT-based hash value encryption

The newly presented NIS-BWT method is referred to as an individual character encoding model which is operated on the basis of “data traversal between 0’s and 1’s.” It declares the low sized codewords for all characters in an input sequence using valuable data from closer bits of input character. When compared with 2 tiny codewords created by 0’s and 1’s traversal as well as best codeword have been chosen based on the needed bits. For an input sequence in length N , the NIS-BWT approach demands for C_{bits} which has to be recorded and compress the data and expressed as given below:

$$C_{bits} = \sum_{i=1}^N NIS_{opt}(i) + controlbits \quad (14)$$

where NIS_{opt} implies the existence of bits in codeword. Additionally, the presented method requires excess of 8 control bits to exhibit the best counts in compressed data. Then, massive bits are required for preserving a single character using NIS-BWT technology is formalized in Eq. (15).

$$NIS_{ch_av} = \frac{C_{bits}}{N}, \quad 1 \leq NIS_{ch_av} \leq 4 \quad (15)$$

While the rate of C_{bits} and NIS_{ch_av} becomes lower then, the compression function is improved. Particularly, Eq. (15) shows that the NIS-BWT technique requires 4 bits which helps for recording even a single character. Hence, it demands for 1 bit to save an individual character with enhanced compressed function.

The term “Thank you” has been depicted as illustration. Initially, the newly developed technology consumes the input as text with alphanumeric characters and special symbols. Followed by, the applied character has been examined and converts them into ASCII rates. Then, ASCII values are converted into the binary form. The bit traversal is applied using primary bits in a binary form of the input characters and identifies the bits from 0 or 1. Following, 0’s based traversal undergoes loading and preserves the control bit as 00 while the primary bit is 1. Under the application of the first bit, a model starts the traversing from the second bit; hence 0’s is found and conserve the positions at the time of exploring the value of 0. Once the value of 0 has been found, the position (x) is saved in code-word (00-x) and computed until reaching the 7th bit. When the traversal reaches the consequent bit, the neighboring code-word is preserved. Afterward, 1’s based traversal has been processed. The computation involved in 0’s and 1’s based traversal is assumed to be similar which results in the exploration of binary digits. The 2 codewords were generated; hence the projected model selects a codeword with the least count of bits and declares as an optimal codeword. At last, an optimized codeword and encoded characters are integrated with control bits to generate a compressed file. NIS-BWT method uses symmetrical compression where decompression is assumed as an exact reverse task of the compression process [18].

It is a reversible transformation that generates a permutation of input string where the symbols intend to perform a clustering operation. In prior to performing clustering, BWT compression is carried out, and pre-processing takes place in data compression. Data compression is considered as a major operation in BWT. BWT is considered as a major portion of self-indexes that has been applied in bioinformatics and data retrieval. For data compression, it is feasible to divide massive

input and develop BWT for tiny blocks, as decoding and encoding were performed simultaneously. Therefore, it is impossible for self-indexes as the optimal search needs BWT. At this point, the runtime and memory are highly essential for BWT development. Theoretical worst-case time complexity, real-time runtime, and memory footprint were enhanced. Therefore, $n \log n$ bits are composed of low memory bound for rapid suffix array development. Besides, the memory bound is not valid for BWT execution, as the above-mentioned models are not viable in constructing BWT; however, it is based on the input size. Then, external models have been projected for computing suffix array. Using this model, the issues relevant to storage space can be resolved which represents that BWT has better significance.

3.3 DBN-based classification

In general, DBN is comprised of numerous restricted Boltzmann machines (RBMs) where each layer is composed of visible layer v as well as hidden layer h . The vector w has been employed for developing layer connection among the RBMs, and units present in the similar layers are autonomous [19]. The energy performance is described and steady state of a system corresponds to low-energy consumption. Therefore, the energy function is depicted as:

$$E(v, h) = - \sum_{i=1}^m a_i v_i - \sum_{j=1}^n b_j h_j - \sum_{j=1}^n \sum_{i=1}^m v_i h_j w_{ij}, \quad (16)$$

where a and b refer to the bias vector of the visible layer and hidden layer. Followed by, the units of visible layer and hidden layer are denoted by m and n . The joint distribution as well as conditional distribution for every layer is determined using the given function:

$$P(v, h) = \frac{e^{-E(v, h)}}{\sum_{v, h} e^{-E(v, h)}}, \quad (17)$$

$$P(v|h) = \frac{P(v, h)}{P(h)} = \frac{e^{-E(v, h)}}{\sum_v e^{-E(v, h)}}, \quad (18)$$

$$P(h|v) = \frac{P(v, h)}{P(v)} = \frac{e^{-E(v, h)}}{\sum_h e^{-E(v, h)}} \quad (19)$$

When the units are not connected with one another, then the conditional probabilities of units are estimated using the given expression:

$$\begin{aligned} P(h_j = 1|v) &= \frac{P(h_j = 1, v)}{P(h_j = 1, v) + P(h_j = 0, v)} \\ &= \sigma \left(\sum_{i=1}^m a_i + w_{ij} v_i \right), \end{aligned} \quad (20)$$

$$\begin{aligned} P(v_i = 1|h) &= \frac{P(v_i = 1, h)}{P(v_i = 1, h) + P(v_i = 0, h)} \\ &= \sigma \left(\sum_{j=1}^n b_j + w_{ij} h_j \right), \end{aligned} \quad (21)$$

$$\sigma(x) = \frac{1}{1 + e^{-x}}. \quad (22)$$

The training procedures of RBM on the basis of contrast divergence method as consolidated below:

Initialization of parameters The RBM has a visible layer v as well as a hidden layer h as developed and applied along with w , a , b , while learning rate e has reduced randomness. The batches and epochs of RBM are fixed on the basis of test knowledge. Followed by, training samples are emerged in the primary visible layer v .

Update parameters The conditional probability of primarily hidden layer $h1$ could be estimated using the above-mentioned equations. Next, the Gibbs sampling model was employed for reformation of $h1$ and v . According to the reconstruction error among actual v and reconstructed v , the stochastic gradient descent (SDG) model has been utilized for parameter updating w , a , b .

While providing input to visible layer y , the RBMI is developed using y and hidden layer $h1$. Likewise, RBM2 is comprised of equipped $h1$ as well as hidden layer $h2$. Once the greedy layer-wise pre-training of RBMI and RBM2 has been completed then, the unsupervised training of DBN is performed. Followed by, a sigmoid layer is employed for sample matching and extracts the features for determining the error among output as well as the real label. Using the supervised back-propagation technology, model parameters are fine-tuned for accomplishing the least classification error.

4 Performance validation

The simulation of the presented technique takes place using Python-3.6.5 in a PC Processor-i5-8600 k Graphics Card-GeForce 1050Ti 4GB RAM-16GB OS Storage-250GB SSD File Storage-1 TB HDD. The parameter setting of the presented model is given as follows. Batch size. 30; learning rate, 0.001; input node, 100; hidden layer, 50; average activation, 0.5; weight decay, 0.0001; particle size, 100; and inertia weight, 0.9–0.4. In addition, fivefold cross-validation is applied to split the dataset into training and testing parts.

The performance of the proposed model is analyzed using the skin lesion image ISIC dataset [20], which contains a set of images under different class labels. In addition, the results are

investigated in terms of different aspects such as image quality, compression performance, and classification outcome.

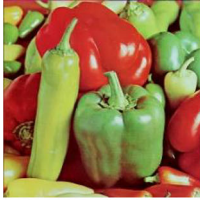






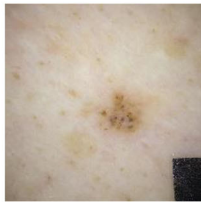
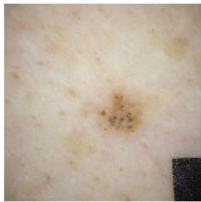



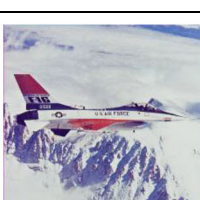
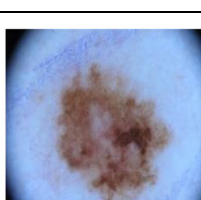
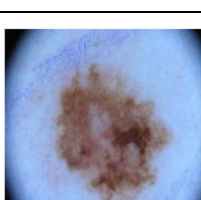
Table 1 investigates the performance of the GO-FFO algorithm with respect to PSNR. The table values denoted that the GO-FFO algorithm has showcased better results on all the applied images. For instance, on the applied image 1, the proposed GO-FFO algorithm has reached a higher PSNR of 46.14 dB. Similarly, on the applied images 2–5, the GO-FFO algorithm has obtained a maximum PSNR of 45.89 dB, 46.24 dB, 47.66 dB, and 47.51 dB, respectively.

Figure 4 investigate the performance of the GO-FFO algorithm with other methods with respect to PSNR. On the applied image 1, the GO-FFO algorithm has resulted in a higher PSNR of 46.14 dB, whereas the GO-PSO and GWO

algorithms have obtained a lower PSNR of 44.72 dB and 42.09 dB, respectively. Similarly, on the applied image 2, the GO-FFO algorithm has attained a maximum PSNR of 45.89 dB, whereas the GO-PSO and GWO algorithms have resulted in a minimum PSNR of 43.82 dB and 41.76 dB, respectively. Likewise, under all the applied images, the presented GO-FFO algorithm has outperformed the compared methods with the maximum PSNR.

Figure 5 examine the performance of the NIS-BWT model in terms of compression performance under a varying number of transactions. Under the transaction count of 500, the NIS-BWT model has compressed the original data of 620 bytes into 303 bytes, whereas the LZW and LZWA models have led to the higher compressed file size of 501 bytes and 486 bytes,

Table 1 Experimental result analysis of proposed GO-FFO model interms of PSNR

	Input Images	Reconstructed Images	PSNR (dB)
			46.14
			45.89
			46.24
			47.66
			47.51

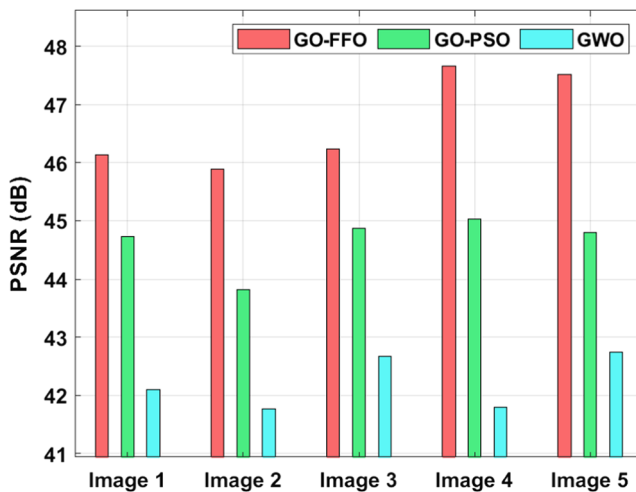


Fig. 4 PSNR analysis of different models

respectively. Moreover, under the transaction count of 1000, the NIS-BWT method has compressed the original data of 1180 bytes into 664 bytes, but the LZW and LZMA approaches have led to the superior compressed file size of 953 bytes and 764 bytes correspondingly. Furthermore, under the transaction count of 1500, the NIS-BWT approach has compressed the original data of 1793 bytes into 1152 bytes, while the LZW and LZMA models have led to the higher compressed file size of 1356 bytes and 1287 bytes, respectively. Along with that, under the transaction count of 2000, the NIS-BWT model has compressed the original data of 2354 bytes into 1478 bytes whereas the LZW and LZMA methods have led to the higher compressed file size of 1742 bytes and 1693 bytes correspondingly. In the same way, under the transaction count of 2500, the NIS-BWT model has compressed the original data of 2985 bytes into 1983 bytes, but the LZW and LZMA methods have led to the superior compressed file size of 2184 bytes and 2084 bytes correspondingly.

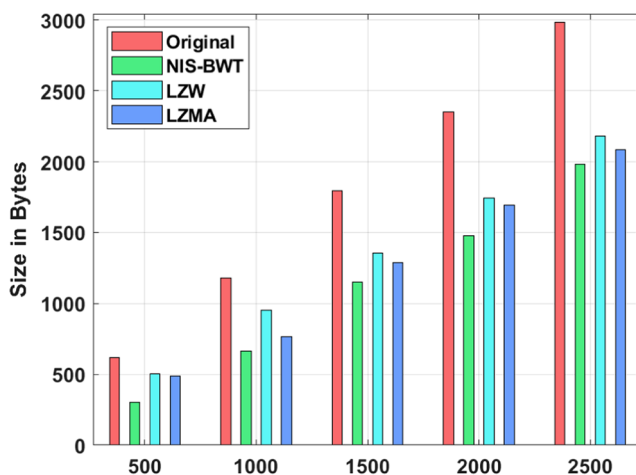


Fig. 5 Compression performance analysis of NIS-BWT with other methods

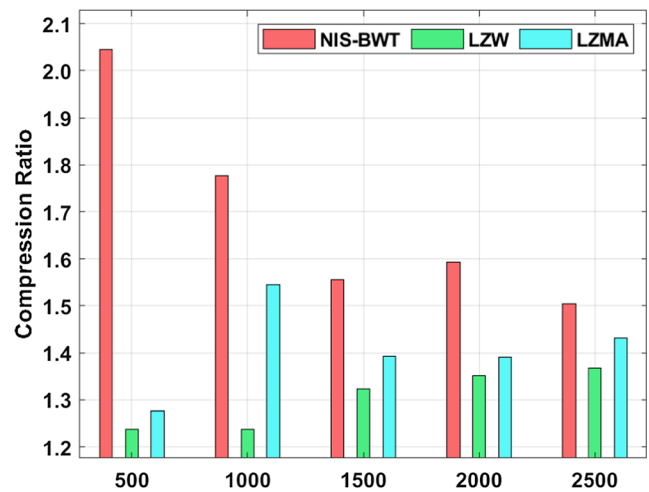


Fig. 6 CR analysis of NIS-BWT with other methods

Figure 6 showcases the CR analysis of the NIS-BWT model over the compared methods under varying transaction count. The presented model displays that the NIS-BWT model has resulted in a higher CR over the LZW and LZMA models. For instance, on the transaction count of 500, the NIS-BWT model has attained a higher CR of 2.046, whereas the LZW and LZMA models have obtained a slightly lower CR of 1.238 and 1.276, respectively. Simultaneously, on the transaction count of 1000, the NIS-BWT method has obtained a superior CR of 1.777, while the LZW and LZMA models have attained a somewhat lower CR of 1.238 and 1.545 correspondingly. Concurrently, on the transaction count of 1500, the NIS-BWT model has reached a higher CR of 1.556, but the LZW and LZMA methods have obtained a slightly minimum CR of 1.322 and 1.393, respectively. In line with, on the transaction count of 2000, the NIS-BWT approach has achieved a maximum CR of 1.593, while the LZW and LZMA methods have reached a somewhat minimum CR of 1.351 and 1.390 correspondingly. At the same time, on the transaction count of 2500, the NIS-BWT model has reached a higher CR of 1.505, while the LZW and LZMA methods have achieved a slightly lower CR of 1.367 and 1.432 correspondingly.

Figure 7 and Table 2 illustrate the SS analysis of the NIS-BWT method over the compared methods under varying transaction count. The projected method shows that the NIS-BWT model has resulted in a maximum SS over the LZW and LZMA models. For instance, on the transaction count of 500, the NIS-BWT model has achieved a superior SS of 51.129%, but the LZW and LZMA models have attained a somewhat lower SS of 19.194, and 21.613% correspondingly. At the same time, on the transaction count of 1000, the NIS-BWT model has attained a higher SS of 43.729%, whereas the LZW and LZMA models have achieved a somewhat minimum SS of 19.237 and 35.254%, respectively. Along with, on the transaction count of 1500, the NIS-BWT model has reached

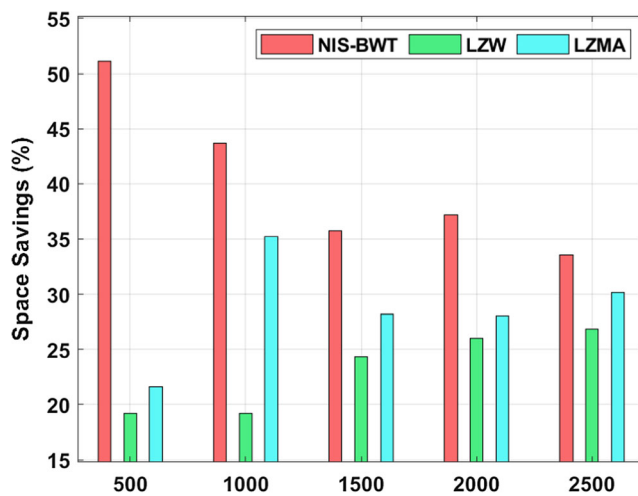


Fig. 7 SS analysis of NIS-BWT with other methods

a higher SS of 35.750%, while the LZW and LZMA approaches have obtained a somewhat minimum SS of 24.373 and 28.221%, respectively. Similarly, on the transaction count of 2000, the NIS-BWT approach has reached a higher SS of 37.213%, but the LZW and LZMA methods have obtained a somewhat lower SS of 25.998 and 28.080%, correspondingly. Simultaneously, on the transaction count of 2500, the NIS-BWT model has reached a higher SS of 33.568, while the LZW and LZMA methods have achieved a slightly lower SS of 26.834 and 30.184, respectively.

Figure 8 had undergone a detailed comparative analysis of different classifier models such as ResNet-50, VGG19-SVM, VGG-19, YOLO-GC, deep full resolution convolutional networks (DFRCN), deep learning networks (DLN), convolutional-deconvolutional networks (CDNN), and ResNet in terms of different measures. The simulation values denoted that the ResNet-50 model has failed to showcase effective outcome with the minimum sensitivity of 90%, specificity of 61%, and accuracy of 75.5%. At the same time, the VGG-19 SVM model has displayed slightly better results with the sensitivity of 93%, specificity of 69%, and accuracy of 80.7%. Simultaneously, the VGG-19 model has surpassed

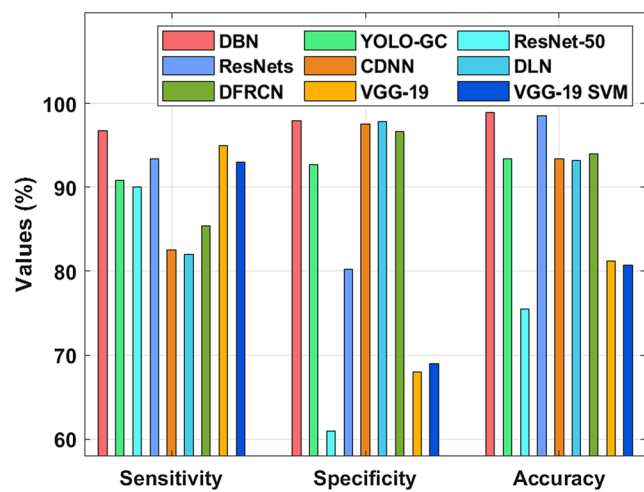


Fig. 8 Comparative analysis of NIS-BWT with existing methods

the earlier models with the sensitivity of 95%, specificity of 68%, and accuracy of 81.2%. Next to that, the DLN model has exhibited even better results with the sensitivity of 82%, specificity of 97.8%, and accuracy of 93.2%. Afterward, the YOLO-GC model has demonstrated moderate results with the sensitivity of 90.82%, specificity of 92.68%, and accuracy of 93.39%. Followed by, the CDNN model has exhibited manageable results with the sensitivity of 90%, specificity of 61%, and accuracy of 75.5%.

Concurrently, the DFRCN model has portrayed somewhat satisfactory results with the sensitivity of 85.4%, specificity of 96.69%, and accuracy of 94.03%. On continuing with, the ResNet model has resulted to a near optimal performance with the sensitivity of 93.4%, specificity of 80.2%, and accuracy of 98.5%. But the proposed DBN model has classified effective performance with the maximum sensitivity of 96.73%, specificity of 97.91%, and accuracy of 98.96%. The presented model has outperformed the other methods due to the following reasons: optimal key generation, effective compression, and encryption of hash values.

5 Conclusion

This paper has introduced an effective model for secure blockchain enabled intelligent IoT and healthcare diagnosis model. At the initial stage, data collection process is executed to collect details of the patient using IoT gadgets. Followed by, GO-FFO algorithm with ECC is used for secret image transmission. Next, the NIS-BWT technique is employed for hash value encryption. Finally, the DBN model is applied for disease diagnosis purposes. Extensive set of simulations were carried out to identify the goodness of the proposed model. The experimental outcome indicated the effective classification performance of the presented model with the sensitivity of 96.73%, specificity of 97.91%, and accuracy of 98.96%. As

Table 2 Space savings analysis original vs compression of blockchain hash values

No. of transactions	Space savings (%)		
	NIS-BWT	LZW	LZMA
500	51.129	19.194	21.613
1000	43.729	19.237	35.254
1500	35.750	24.373	28.221
2000	37.213	25.998	28.080
2500	33.568	26.834	30.184

a part of future work, the parameter tuning of the DBN model can be done to improvise the classification performance.

Acknowledgment The author K. Shankar sincerely acknowledge the financial support of RUSA–Phase 2.0 grant sanctioned vide Letter No. F. 24-51/2014-U, Policy (TNMulti-Gen), Dept. of Edn. Govt. of India, Dt. 09.10.2018.

Declarations

Conflict of interest The authors declare that they have no conflict of interest. The manuscript was written through contributions of all authors. All authors have given approval to the final version of the manuscript.

References

- Dwivedi AD, Srivastava G, Dhar S, Singh R (2019) A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors* 19(2):326
- Abdolkhani R, Gray K, Borda A, DeSouza R (2019) Patient-generated health data management and quality challenges in remote patient monitoring. *JAMIA Open* ooz036. <https://doi.org/10.1093/jamiaopen/ooz036>
- Rahman MA, Hossain MS, Loukas G, Hassanain E, Rahman SS, Alhamid MF, Guizani M (2018) Blockchain-based mobile edge computing framework for secure therapy applications. *IEEE Access* 6:72469–72478
- Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T (2018) Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J Med Syst* 42(7):130
- Chen Y, Ding S, Xu Z, Zheng H, Yang S (2019) Blockchain-based medical records secure storage and medical service framework. *J Med Syst* 43(1):5
- Liang X, Zhao J, Shetty S, Liu J, Li D (2017) Integrating blockchain for data sharing and collaboration in mobile healthcare applications, in: *Proceedings of the 28th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–5, <https://doi.org/10.1109/PIMRC.2017.8292361>.
- Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST (2018) Fhircain: applying blockchain to securely and scalably share clinical data. *Comput Struct Biotechnol J* 16:267–278
- Brogan J, Baskaran I, Ramachandran N (2018) Authenticating health activity data using distributed ledger technologies. *Comput Struct Biotechnol J* 16:257–266
- Gordon WJ, Catalini C (2018) Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Comput Struct Biotechnol J* 16:224–230
- Rupasinghe T, Burstein F, Rudolph C, Strange S (2019) Towards a blockchain based fall prediction model for aged care, in: *Proceedings of the Australasian Computer Science Week Multiconference*, ACM, p. 32.
- Dorri A, Kanhere SS, Jurdak R (2017) Towards an optimized blockchain for IoT. *ACM*, pp 173–178
- Gaetani E, Aniello L, Baldoni R, Lombardi F, Margheri A, Sassone V (2017) Blockchain-based database to ensure data integrity in cloud computing environments, in: *Italian Conference on Cybersecurity*, Venice, Italy. 17 – 20 Jan 2017, p. 10.
- Novo O (2018) Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet Things J* 5(2):1184–1195
- Rathore S, Pan Y, Park JH (2019) BlockDeepNet: a Blockchain-based secure deep learning for IoT network. *Sustainability* 11(14):3974
- Elhoseny M, Shankar K, Lakshmanaprabu SK, Maselena A, Arunkumar N (2018) Hybrid optimization with cryptography encryption for medical image security in Internet of Things. *Neural Comput & Applic*:1–15
- Neve AG, Kakandikar GM, Kulkarni O (2017) Application of grasshopper optimization algorithm for constrained and unconstrained test functions. *Int J Swarm Intell Evol Comput* 6(165):2
- Xiao C, Hao K, Ding Y (2015) An improved fruit fly optimization algorithm inspired from cell communication mechanism. *Math Probl Eng*:2015
- Uthayakumar J, Vengattaraman T, Dhavachelvan P (2019) A new lossless neighborhood indexing sequence (NIS) algorithm for data compression in wireless sensor networks. *Ad Hoc Netw* 83:149–157
- Yu J, Liu G (2020) Knowledge-based deep belief network for machining roughness prediction and knowledge discovery. *Comput Ind* 121:103262
- The International Skin Imaging Collaboration, ISIC Archive, <https://isic-archive.com/>, Accessed on June 14, 2020.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.