Neural Computing and Applications (2024) 36:17467–17482
https://doi.org/10.1007/s00521-024-10039-y

ORIGINAL ARTICLE

Deep neural network-based secure healthcare framework

Abdulaziz Aldaej[1] · Tariq Ahamed Ahanger[2] · Imdad Ullah[3]

Received: 29 December 2023 / Accepted: 28 April 2024 / Published online: 20 June 2024

Abstract
Healthcare stands out as a critical domain profoundly impacted by Internet of Things (IoT) technology, generating vast data from sensing devices as IoT applications expand. Addressing security challenges is paramount for a successful IoT healthcare framework, with blockchain technology offering a decentralized structure for robust data protection and secure data exchange within multi-node IoT networks. The research introduces a secure IoT healthcare diagnostic model empowered by deep neural networks, emphasizing encryption, safe transactions, and healthcare diagnostics as key components. Notably, the model incorporates innovative techniques like the orthogonal particle swarm optimization algorithm for sharing medical images and a neighborhood indexing sequence method for hash value encryption. The development of an optimized deep neural network-based classification model for illnesses, validated through extensive trials, demonstrates superior performance metrics compared to existing decision-making techniques, with significant improvements in *f*-Measure (96.25%), sensitivity (93.26%), specificity (94.26%), and accuracy (93.26%). This study's scientific contribution lies in its innovative approach to securing IoT-healthcare diagnosis models, validated performance enhancements using real-world datasets, and insightful recommendations for future research directions, fostering advancements in healthcare technology for enhanced patient care and system efficiency.

Keywords Security · Blockchain · Internet of Things · Particle swarm optimization

1 Introduction

Internet of Things (IoT) technology-based healthcare applications have been significantly explored such that medical decision-making is automatically provided to every user [1, 2]. These include remote patient management (RPM), which comprises a variety of clinical applications, such as frequent signal observation utilizing implanted sensors, arrhythmia prediction and fall detection, oxygen regularization, and healthcare vitals tracking [3, 4]. However, the approach is not frequently adopted since it lacks stability, fault tolerance, and security [5, 6]. Electronic health applications use medical IoT equipment to obtain physiological data from patients, which can be used by attackers, causing data protection concerns [7, 8]. In certain instances, the systems are quite fragile, especially when dealing with a large number of specialized interactions [9, 10].

1.1 Research domain

Traditional e-Health models can suffer efficiency reductions and service interruptions due to cyberattacks like ransomware and denial of service (DoS) [11]. Medical data have recently piqued the curiosity of cybercriminals [1]. A study by the US Department of Health and Human Services (HHS)[1] found that between 2009 and 2018, there were

✉ Tariq Ahamed Ahanger
t.ahanger@psau.edu.sa

Abdulaziz Aldaej
a.aldaej@psau.edu.sa

Imdad Ullah
imdad.ullah@sydney.edu.au

[1] College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, 11942 Al-Kharj, Saudi Arabia

[2] Management Information Systems Department, CoBA, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia

[3] School of Computer Science, Faculty of Engineering, The University of Sydney, Sydney, NSW 2006, Australia

[1] Source: https://www.hhs.gov/.

almost 2000 data breaches. There were partial data breaches involving doctors, medical professionals, and caregivers. Hackers can eavesdrop by using Bluetooth, Zigbee, Wi-Fi, DoS, or insider attacks [5]. Moreover, conventional edge and cloud operations exhibit inefficiencies in securing patient data against unauthorized access [12]. The utilization of blockchain technology for storing and processing patient data eliminates the need for centralized fog or cloud authentication [13]. The potential of blockchain technology has spurred developers to create privacy-preserving e-health modules. Uddin et al. [14] illustrated the assessment of user memory, permissions, and security through a patient agent (PA) integrated into an intelligent gateway, facilitating the secure uploading of medical information to a tailored blockchain. The PA is responsible for selecting blockchain providers for scheduling clinical data, processing tasks, and managing memory space. Uddin et al. [15] expand the PA's role to include maintaining several blockchain and storage media, such as a local computer or the cloud, to maintain security. Tuli et al. [16] developed a fog-computing paradigm based on a lightweight blockchain infrastructure termed a fog bus. Medical sensors and other edge devices can be integrated with the blockchain using universal broker software. The broker's primary function is to distribute work among the fog's other tools. E-Health can be compromised due to concerns about privacy and security because of the presence of the universal broker module. Figure 1 shows some of the vital healthcare parameters that can be acquired using the IoT technology.[2]

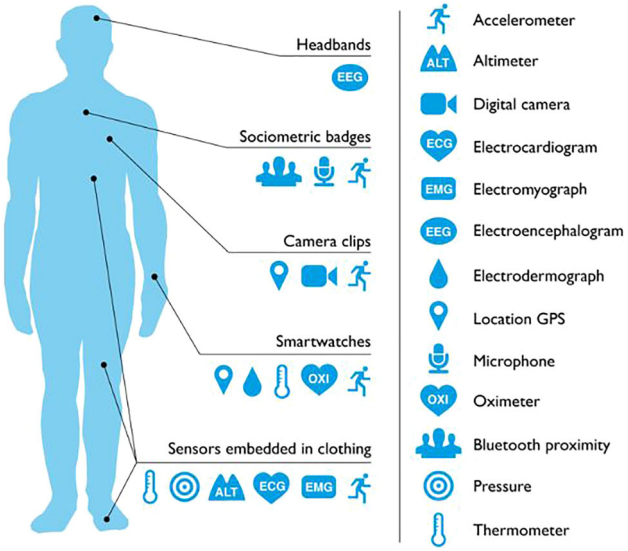

Fig. 1 Smart Healthcare Parameters by IoT

1.2 Blockchain technology fundamentals

Blockchain technology is described as a collection of blocks. There are 4 sub-sections to a single block including *transaction data*, *hash value of the previous block*, *current block*, and *time-stamp* of the transaction. Blockchain has been used to record transactions in the past as a common digital ledger. Because each block carries a cryptographic measure of the previous block, an attacker will be unable to recover the data. A cryptographic hash value is used to access all transactions in this method, which is validated by every miner. As seen in Fig. 2, it is made of blocks for each transaction and has identical values across the whole ledger. As a result of the blockchain, it is possible to communicate detailed records in a way that is both open and private. One of the sources in the blockchain is decentralized storage, and a huge amount of data can be kept and linked via the last block by utilizing an intelligent contract code. In recent years, decentralized databases such as Swarm, Litecoin, Monero, Siacoin, Interplanetary File System (IPFS), and BigchainDB have emerged. Internet-based, sensor-based, and knowledge-based categories for IoT were defined by Pham et al. [17]. Specifically, *IoT is a collection of devices linked together via the internet to generate large amounts of data.* The use of RFID and other sensor-dependent services is referred to as sensor-based IoT. Knowledge-based IoT is a collection of data used in meaningful fields. IoT technology refers to a new approach in which a variety of devices with unique identifiers communicate with one another through the internet. IoT security, privacy, and fault tolerance issues increase as the number of data sources increases. Using a blockchain approach for the IoT can alleviate these issues. A distributed framework for vulnerability assessment, trust, and security is provided by several blockchain approaches. Based on the aforementioned aspects, specific research challenges in the current study domain include

1. Security challenges in IoT healthcare systems due to the vast amount of data generated by sensing devices.
2. The need to protect sensitive patient information and ensure data integrity in IoT healthcare frameworks.
3. Secure exchange of data and resources across multi-node IoT networks poses a significant challenge.
4. Safeguarding the transmission of medical data between interconnected devices within the healthcare infrastructure is crucial.
5. Implementing robust security measures to mitigate risks and vulnerabilities in IoT-enabled healthcare systems.
6. Maintaining a secure environment for data transmission, storage, and processing in complex interconnected healthcare networks.

[2] Source: https://www.cbinsights.com/research/internet-of-medical-things-5g-edge-computing-changing-healthcare/.

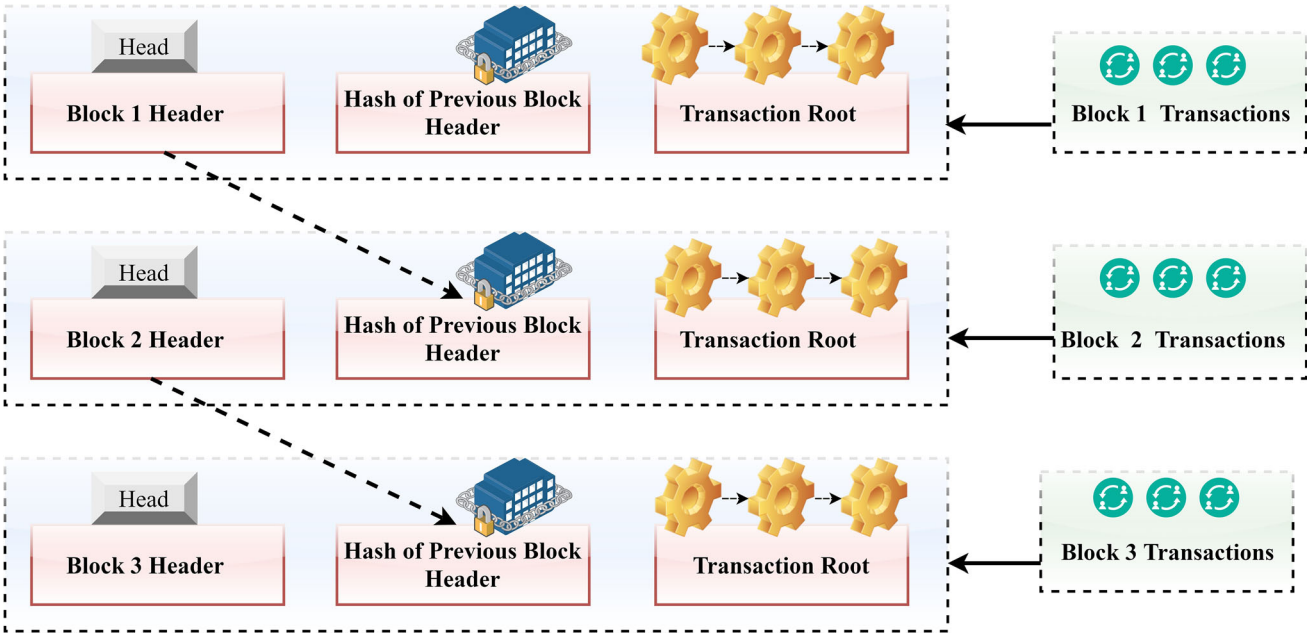

Fig. 2 Blockchain Structure

7. Building trust in IoT healthcare solutions by addressing security challenges to protect patient privacy and confidentiality.

1.3 Major contribution

In IoT applications such as smart homes, smart cities, the medical industry, and farming, blockchain offers additional advantages such as lower power consumption, decreased processing strain, faster response times, and increased security. A peer-to-peer network for administration and attack resistance is created using blockchain technology. Conspicuously, blockchain and IoT can be used to manage and build a wide range of products and services. Based on the aforementioned aspects, some of the major contributions of the presented model are as follows;

1. Deep neural network (DNN)-inspired secure intelligent IoT-medical diagnosis models are the primary focus of the current research.
2. A secure transaction employing picture steganography, hash value encryption, and medical diagnostics is presented as the vital components of the proposed model.
3. Medical images are secretly shared using an orthogonal particle swarm optimization technique.
4. A neighborhood indexing sequence technique is used to encrypt hash values.
5. An optimized DNN is employed as a classification model to assist in an illness diagnosis.

Figure 3 shows the generic view of blockchain-inspired healthcare architecture [18]. The study adds scientific value by introducing a novel method to secure IoT-healthcare diagnosis models, showcasing performance enhancements, validating results with real-world datasets, and suggesting future research pathways. *Paper Organization* Sect. 2 presents a state-of-the-art literature review in the current domain of study. Section 3 presents the proposed model for secure disease diagnosis. The presented model is validated for performance assessment in Sect. 4. Finally, Sect. 5 concludes the paper with future research directions.

2 State-of-the-art healthcare frameworks: blockchain perspective

Mavrogiorgou et al. [26] suggested a framework that enables all organizations in the health ecosystem to get multimodal, actionable information from heterogeneous data. These data are then managed, combined, and aggregated to create new data structures, such as Holistic Health Records (HHRs). In contrast, the mechanism develops various data management techniques covering the entire data path, from data acquisition and cleaning to data integration, modeling, and interpretation, to effectively construct the HHRs. However, the scalability and interoperability of the framework across different healthcare settings and systems may be a challenge. Benaich et al. [27] offered a novel solution that strengthens EHR systems by utilizing the decentralized and immutable nature of blockchain technology in conjunction with cutting-

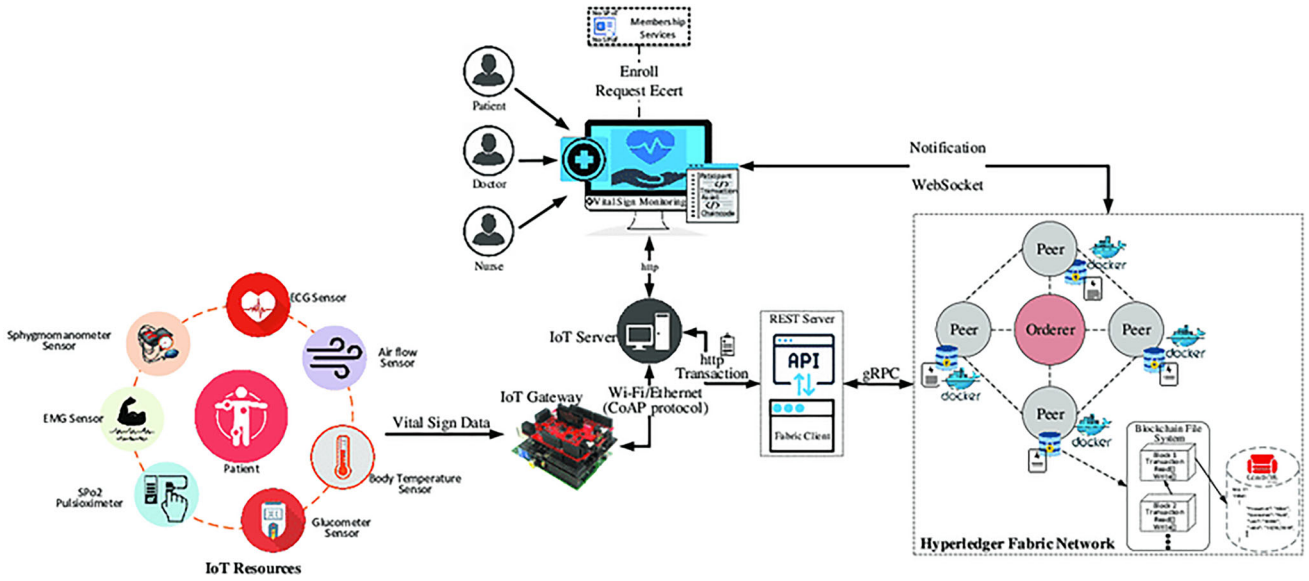

Fig. 3 Conceptual View of Blockchain-inspired Smart Healthcare

edge encryption methods like the Advanced Encryption Standard and Zero Knowledge Proof Protocol. According to the authors, blockchain technology can effectively address major challenges with electronic health records (EHRs), such as fragmented data and interoperability issues. This can be achieved by facilitating secure and transparent data exchange, which can improve care coordination, quality, and cost-effectiveness among healthcare facilities. While the use of blockchain technology and encryption methods strengthens EHR systems, the potential limitations in terms of scalability, energy consumption, and integration with existing healthcare infrastructure need to be addressed for widespread adoption. Singh et al. [28] provides a comprehensive discussion on how to adapt blockchain to satisfy the specific needs of IoT to develop blockchain-based IoT (BIoT) applications. Several elements that affect the planning, creation, and implementation of a BIoT application are discussed, along with current challenges and future directions for advancement. Finally, a set of suggestions is given to assist future BIoT researchers and developers in comprehending some of the issues that must be resolved before the implementation of the next wave of BIoT applications. Challenges related to data privacy, scalability, and interoperability between diverse IoT devices and platforms need to be carefully considered for successful implementation. A blockchain-based therapeutic strategy combining mobile edge computing (MEC) and cloud computing was proposed by Alqaralleh et al. [19]. MEC-Cloud-based blockchain nodes were used to calculate the therapeutic data gathered from doctors and patients, enabling fixed, unspecified, secure, and visible sharing. Images, music, text, and video files recorded in multiple databases were hashed and stored on the blockchain. Experimental implementation showed that energy consumption is higher with MEC blockchains that remove bandwidth and analytical compute requirements of the cloud. Challenges related to energy consumption, scalability, and efficient integration with existing healthcare systems may impact its practical implementation. Using the smart contract, Kakkar et al. [20] created a framework for an automated remote patient monitoring system. A laptop or mobile device with intelligence collects the data acquired by body sensors. Ethereum-based smart contracts were used to store the data acquired from the IoT device. Moreover, electronic health records are recorded on the blockchain for security purposes. While the automated remote patient monitoring system using Ethereum-based smart contracts enhances data security, ensuring the compatibility of smart contracts with diverse IoT devices and addressing potential vulnerabilities in the system's design are critical aspects to consider for robust implementation. Security measures in healthcare and IoT are both a problem and a solution, according to Tariq et al. [29]. Egala et al. [21] advocated for the use of a blockchain-based healthcare information accessing strategy with a centralized cloud for storing medical data. However, the advocacy for blockchain-based healthcare information accessing strategy with centralized cloud storage raises concerns about data centralization, potential single points of failure, and the scalability of the system to handle large volumes of medical data securely. To examine the vulnerability of the network routing process, Sagu et al. [22] established a multi-level model for secure processing in IoT healthcare. However, the complexity of implementing and maintaining such a model across diverse IoT devices and networks may pose challenges for practical

deployment. Soni et al. [30] implemented a customized healthcare information distribution framework in which an application is used to collect information from IoT devices. Blockchain technology of hyperledgers was used to verify the integrity of the data.

Kumar et al. [25] utilized the FHIR chain to distribute healthcare data in a safe and scalable manner. Decentralized ledger modules, according to Gorbunova et al. [23], are responsible for maintaining authentication and data integrity in the emergency medical response. Confidential information can be shared, saved, and retrieved using a tamper-proof distributed ledger. Moreover, IoT protocol was used to cover the extension of authentication messages. In terms of medical information liquidity, aggregation, utility, similarity, and immutability, Attaran [24] defined the applicability of blockchain in patient-specific interoperability. There are 2 types of fall risk variables identified by Lu et al. [31] including medical and ecological. Based on data and expert recommendations, these vulnerability factors are categorized from low to high. Consortium blockchain was used to secure data to ensure that data are interoperable, authenticated, and accessible for older individuals who are at high risk of falling. Using a lightweight blockchain for IoT, Pal et al. [32] suggested an IoT-based e-Health solution. The assumption is made that a peer-to-peer computer system built with virtual nodes is an overlay network. A cluster head (CH) of an overlay network validates the IoT medical equipment before data is sent to cloud servers. Numerous lightweight security mechanisms were implemented by authors to protect the patient's trust in the e-Health system. Based on node characteristics, the CH was picked for a limited period. Two levels of a cloud computing-based blockchain were proposed by Duan et al. [33]. The primary level of the blockchain is used to keep track of all the actions, avoiding the need for expensive proof-of-work processing. In the presented technique, once the data have been logged, the second level of the blockchain performs data storage. To govern access to storage and power of IoT devices, Abdi et al. [34] developed a distributed framework based on blockchain. There is a management hub connecting IoT devices and blockchain in the presented technique. Moreover, access to wireless sensor network policies is restricted to a certain blockchain node in the management hub. The blockchain's access policy is implemented via smart contracts. Based on the aforementioned works, a minimal number of studies focused on block-enabled IoT approaches in healthcare. To enhance security, a more effective hash value encryption method is required. Conspicuously, an IoT-based healthcare diagnostic paradigm is built on a secure deep neural network (DNN)-based blockchain technology. DNN is an effective classifier as it is capable of performing feature engineering. As a result, it can learn at a quicker rate without the need for an explicit representation of these traits. Moreover, based on the comprehensive literature review, Table 1 is formulated to depict the novel aspects of the proposed model in comparison with the state-of-the-art literature works.

2.1 Research gaps

Based on the aforementioned aspects, the following research gaps have been identified.

1. Limited focus on block-enabled IoT approaches in healthcare: Despite the growing interest in blockchain technology and IoT applications in healthcare, there is a scarcity of studies that specifically explore the integration of blockchain with IoT devices to enhance security and interoperability in healthcare settings.
2. Lack of emphasis on more effective hash value encryption methods: While security is a critical aspect in healthcare data management, there is a need for research to develop and implement improved hash value encryption methods to enhance data protection and confidentiality in IoT-based healthcare systems.
3. Inadequate exploration of the application of deep neural network (DNN)-based blockchain technology in healthcare diagnostics: The potential of utilizing DNN-based blockchain technology for healthcare diagnostics remains underexplored, highlighting a gap in research focusing on leveraging advanced classifiers like DNNs for enhancing diagnostic accuracy and efficiency in healthcare settings.
4. Limited research on comprehensive models combining blockchain technology with deep neural networks for healthcare applications: The integration of secure DNN-based blockchain technology for healthcare diagnostics presents a novel approach, indicating a gap in the existing literature regarding the development and evaluation of comprehensive models that leverage both technologies for improved healthcare outcomes.

3 Proposed model

Figure 4 depicts the conceptual model for secure healthcare data processing using blockchain technology [35]. Initially, IoT devices receive data from end-users. The proposed technique is used to secretly share healthcare images. Moreover, the NIS algorithm is used to hash the acquired data measures. Finally, the diagnosed condition is identified using the proposed neural network model. The detailed functionality has been explained ahead.

Table 1 State-of-the-art comparison (1 available, – not available)

References	Alqaralleh et al. [19]	Kakkar et al. [20]	Egala et al. [21]	Sagu et al. [22]	Gorbunova et al. [23]	Attaran [24]	Kumar et al. [25]	Proposed
Security	1	1	1	1	1	1	1	1
IoT	–	1	1	–	1	–	–	1
Quantification	1	1	1	1	1	–	1	1
Healthcare	1	1	1	1	1	1	1	1
Data visualization	–	–	–	–	–	–	–	1
Performance analysis	–	–	–	–	–	1	1	1
Prediction	–	–	1	–	1	–	–	1
Anomaly prediction	–	–	–	–	–	–	–	1
Stability	–	–	–	–	–	1	–	1
Accuracy	–	–	–	–	–	–	–	1

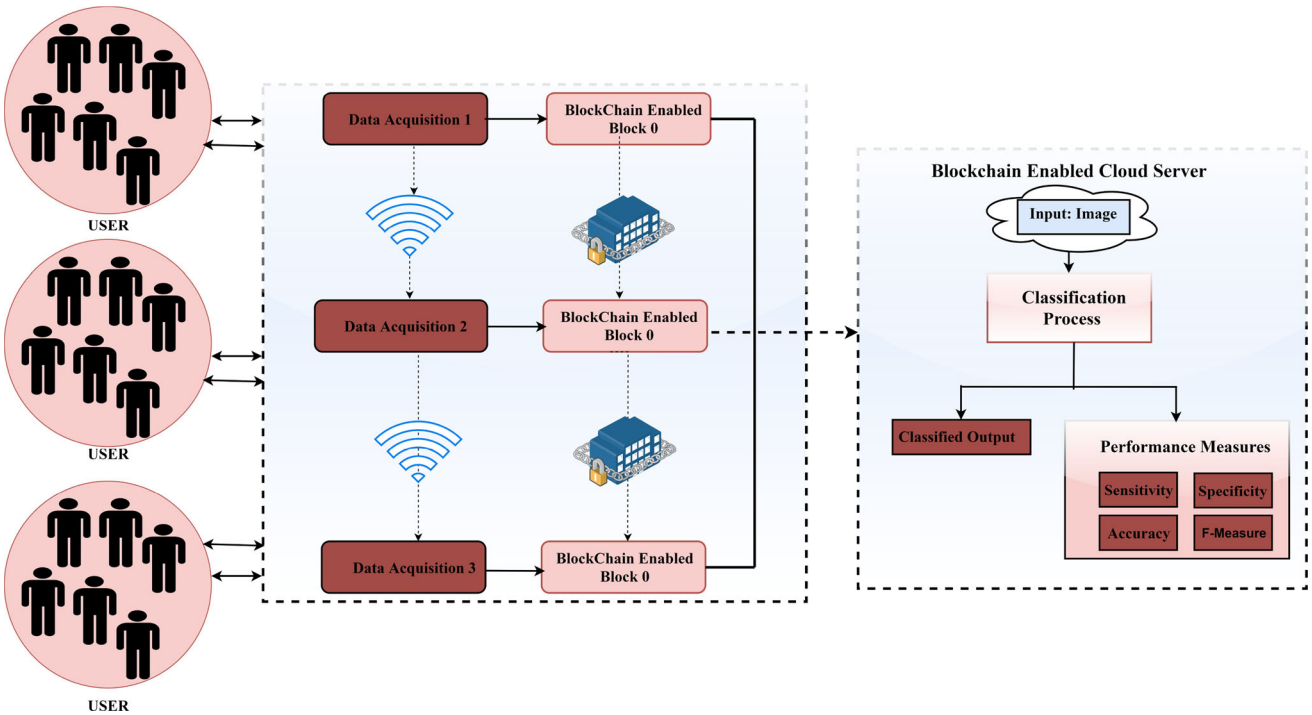

Fig. 4 Blockchain Procedure

3.1 Fundamentals of optimized particle spam algorithm (OPSA)

The particle spam algorithm (PSA) includes a random collection of particles to find the optimal outputs. Specifically, every particle's position in the search space, as well as its distance from the swarm's ideal particle, is considered for computation. As a result of an optimization problem, all particles' features are processed from the global optimum. Individual best and global best are 2 modules based on PSA. A particle's location can be used to determine the original model. The best particles in the swarm are used in the global best selection procedure, which gains comprehensive knowledge. The essential aspect of upgrading the convergence rate of optimization algorithms is OBL (opposition-based learning). Efficient implementation of OBL can identify optimal candidate solutions to a given problem by taking into account both

the current and previous populations. Mathematically, let M be a real number represented as M[y, z]. M_0 is the inverse number, and its representation is as follows:

$$M_0 = y + z - M$$

The following explanation applies to an e-dimensional search space.

$$M_{0_j} = y_j + z_j - M_j$$

such that M_j varies from M_1,..., M_e, and M_j is the number of dimensions in that search space.

3.2 OPSA-inspired security technique

OSPA enables the transmission of an encrypted message from the sender to many recipients using picture steganography. By using the proposed OPSA technique, a private picture can be used for security purposes. In the presented strategy, the placements of the embedding points are carefully chosen to maximize the PSNR (peak signal-to-noise ratio). Steganography can be used to share hidden images with the proposed OPSA. Figure 5 shows the steps that make up the proposed OPSA approach. Optimal embedding spots can be acquired after the maximal iterations are achieved. A secure input picture can be created by using the private shares that have been created.

3.3 Encryption technique

A newly designed character encoding scheme is presented to operate on traversal data by employing 0 and 1. It uses valid data from nearby bits of the input character to assign the minimal code words for each character contained in the input sequence. However, it is necessary to compare the 2 resulting code words to determine the optimal measure for the given bit count (i.e., 0 s or 1 s). The proposed model requires D bits to record compressed information for input sequences of length O, as demonstrated below:

$$D_{\text{bits}} = \sum_{j=1}^{O} \text{NIS}_{\text{opt}}(j) + \text{control} - \text{bits}$$

where NIS_{opt} indicates an optimal coding word containing bits. To get the best compression ratio, the suggested method requires 8 extra control bits. Using the proposed approach, the maximum bits required to preserve a unique character are computed as follows.

$$\text{NIS}_{ch-av} = \frac{D_{\text{bits}}}{O}, 0 < \text{NIS}_{ch-av} < 5$$

Compression efficiency improves with lower D_{bits} and $\text{NIS}_{\text{ch-av}}$ rates. The presented approach uses a maximum of 4 bits to store a single character. To store a character, it uses minimally one bit and hence delivers the best compression possible.

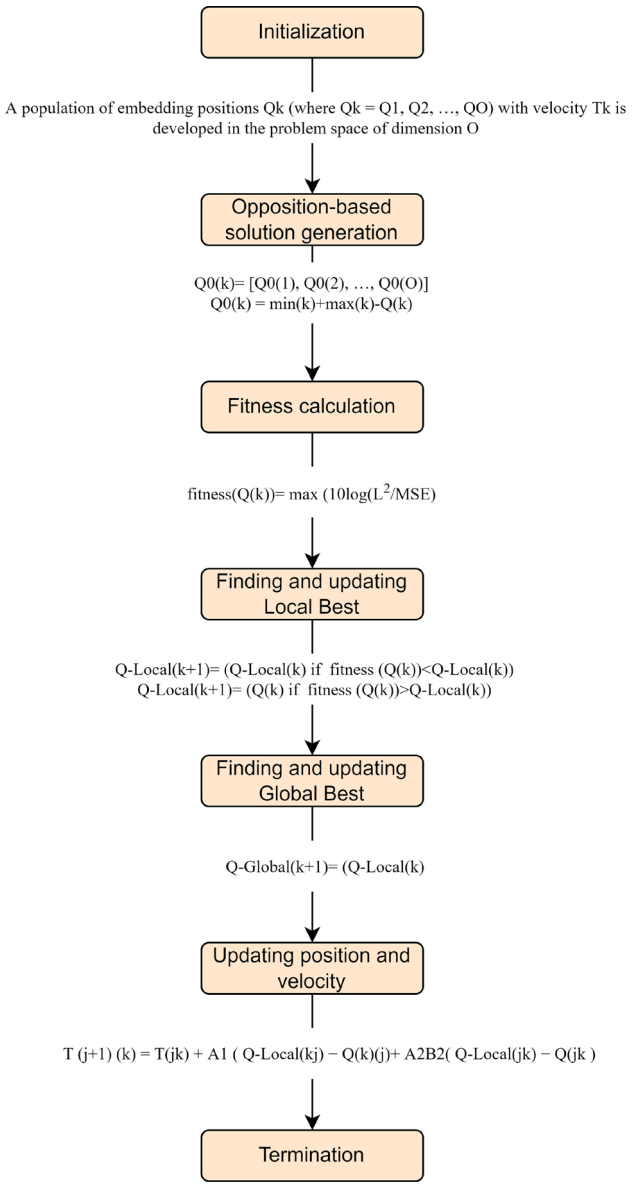

Fig. 5 OPSA-inspired Security Technique (variables are defined accordingly)

3.3.1 Encryption technique: working procedure

The detailed working principle of the proposed technique is presented in the current section. Alphanumeric letters and special symbols are used to begin the text in the presented framework. Characters are learned by the model and converted to ASCII rates. Binary values are generated from the ASCII values. The binary equivalent of the input character is used to initiate the bit traversal, which then defines each bit as either 0 or 1. Moreover, the control bit is saved as either 00 or 10 depending on whether the first bit identified

is 0 or 1. The presented technique begins traversing assessing the second bit as a reference so that 0 s may be identified and their places recorded. Code words 00-x are used to record the position of the 0 s, and the procedure is repeated until all 7 0 s have been identified. The following codeword is recorded if the traversal reaches the final bit. Once the 0-based processes have been traversed, the 1-based processes are subsequently traversed. Similar to 0-based traversal, the procedure is the same for the 1-based. 2 words serve as a code. When comparing the two, the presented technique selects the one with the minimal bits. Conspicuously, each encoded character is joined with the control bits to generate the compressed file.

Compression and decompression are the same in the presented approach, which utilizes symmetrical compression. Decoding does not require any additional data to be sent along with the compressed data. A compressed file is first learned using binary code of 0 and 1, and transformation is carried out. When 00 is set as the control bit, it means that the initial 7 bits are 0, and the compression procedure begins. If the code is 0-specific, the measure of 0 s occupies the matching reference point. The first bit is reconstructed from control bits to pick a printable character. In the next step, the remaining spots are filled with values of 1 s. Similarly, in 1-based traversal, the code word is placed in the 1 s position and the other locations are filled with 0 s. The ASCII values of each character's codewords are then revised. Finally, the ASCII values are transformed into alphanumeric characters, and the original text is reformatted without affecting its contents.

3.3.2 Medical diagnosis model

Deep neural networks (DNN) are used to control the presented framework's hidden and output components for medical diagnosis for imagery data. At the time of implementation, a DNN consists of pre-training and fine-tuning phases for healthcare images. Deep belief networks (DBN) are used at the beginning of the training phase and feed-forward phase where input transmits from the initial layer to the output layer via intermediary layers, resulting in multi-level architecture. System optimality is provided by the hidden units, as it enables the system to give the necessary initiations. Numerous researchers have developed the RBM (restricted Boltzmann machine) to reduce the constraints of DNN. Specifically, RBM is composed of stochastic hidden and final units. The final units are assigned to the training vector during the startup step. Mathematically, it is represented as

$$G(w,i) = -\sum_{j=1}^{J}\sum_{k=1}^{K} OpTG_{jk} w_k i_k - \sum_{j=1}^{J} \beta_j w_j - \sum_{k=1}^{K} \alpha_k i_k$$

where $OpTG_{jk}$ indicates the communication between w_k and hidden unit i_k, β, α are the normalization bias. J, K represents the visible and non-visible nodes. Numeration of hidden nodes in RBM can be obtained from the intermediary measure of $(W_j, i_k)_{data}$ without direct impact.

$$P\left(i_k = \frac{1}{w}\right) = \sigma\left(\sum_{j=1}^{m} OpTG_{jk} w_j + \beta_k\right)$$

The normalization function $\sigma(y)$ indicates the sigmoid function $\frac{1}{(1+e^y)}$; w_k and i_k indicate unbiased samples. At the verification level, the intermediary nodes are expanded to deploy the steepest function in the probabilistic log as follows

$$\delta OpTG_{jk} \phi(w_k i_k)_{\text{data}} - (w_k i_k)_{\text{reconstruction}}$$

In the training method, a multi-layered RBM is constructed in a variety of configurations. By rearranging current weights and biases, the RBM layers can incorporate the behaviors. The basic back-propagation approach is used in the tuning phase. The normal layer of the DNN can be used to classify the dataset. O best features are used as input and the hidden layers are used to project the DNN. Similarly, the back-propagation procedure begins with the weight load gained in the beginning phase, and the resulting ideal weight is structured by training phases utilizing systematic data gathering. The OPSA method is used during the fine-tuning stage of the DNN to tune the parameters and thereby improve classification performance for disease analysis. Figure 6 shows the overall working procedure.

4 Experimental validation

4.1 Experimental design

The presented model was tested using a benchmark dataset of ELCAP Public Lung Image Database[3] on a PC with an i7-9700 CPU processor, an Nvidia 2060 graphics card, 32 GB of RAM, and 512 GB of SSD storage with 1 TB of HDD disc space. From the entire collection, 3000 images are selected. Figure 7 shows some of the samples of images from the acquired database.

4.2 Simulation environment

The proposed model is validated using the following configuration. The input node of DNN has 100 neurons, the

[3] http://www.via.cornell.edu/lungdb.html.

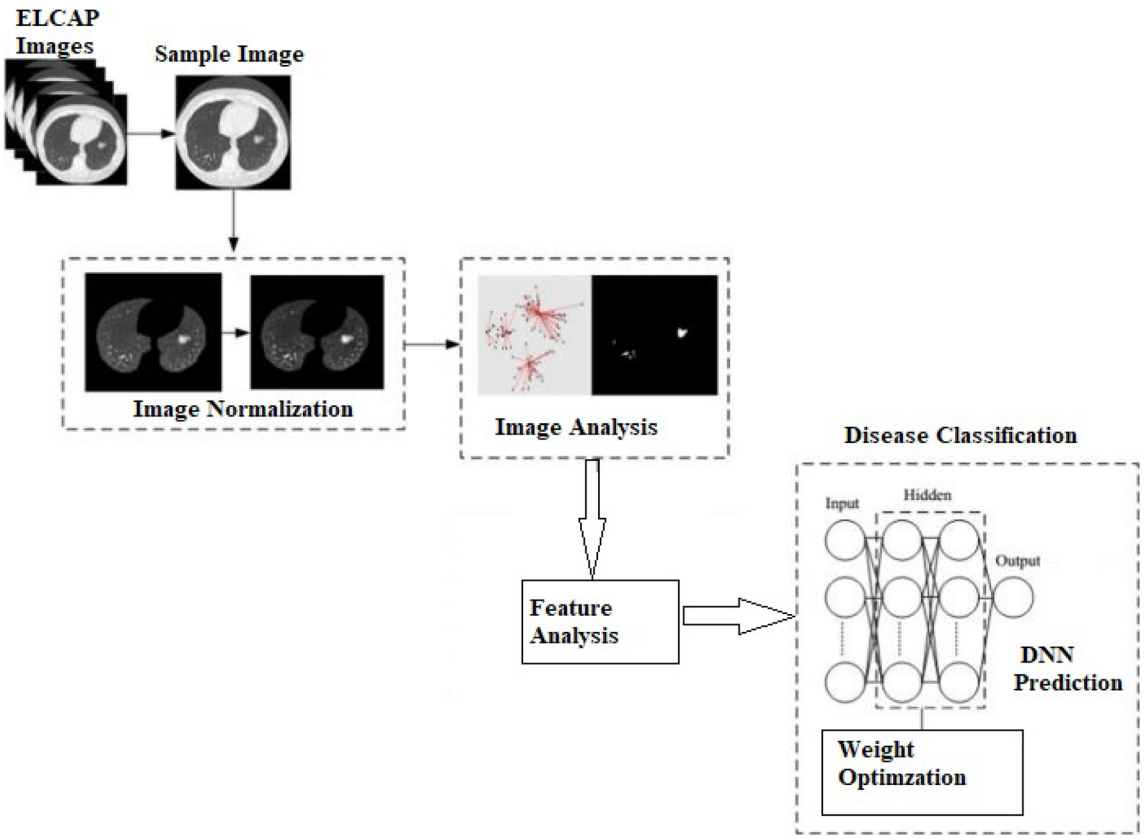

Fig. 6 Medical Image-based Diagnosis procedure

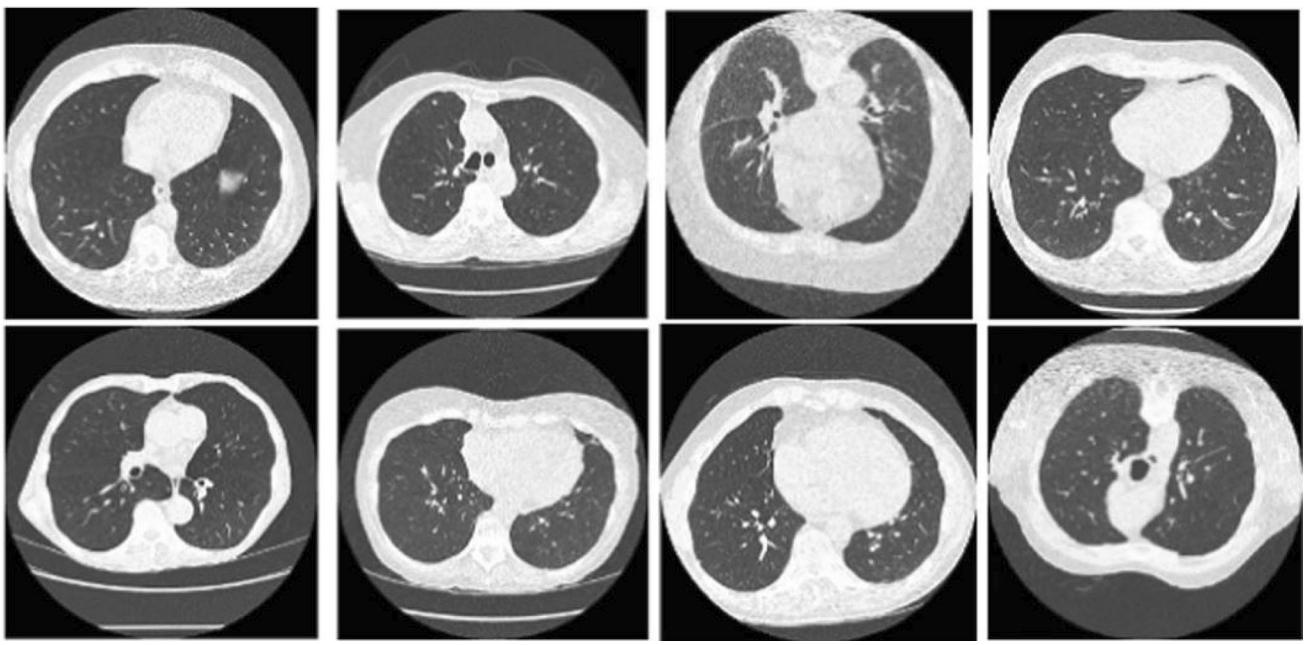

Fig. 7 ELCAP Public Lung Sample Image

hidden layer is comprised of 50 neurons, and the average activation is set to 0.6 with a weight decay of 0.02%. The particle size is set to 99 with inertia weights between 0.8 and 0.2. Cross-validation is also used to divide the dataset into train and test classes. Space savings (SS) and

compression ratio (CR) are 2 metrics used to validate a file's compression efficiency.

4.3 Statistical analysis

A framework's compression ratio is determined by dividing its uncompressed data by its compressed data. For performance assessment, 5 images have been represented as Image A, Image B, Image C, Image D, and Image E. For comparative analysis, baseline techniques of grey wolf optimization (GWO) and particle swarm optimization (PSO) were used. Numerous statistical parameters were estimated including accuracy, *f*-measure, specificity, and precision. Additionally, PSNR analysis, encryption technique analysis, and space save analysis were carried out for performance validation.

4.4 PSNR Analysis

The OPSA algorithm's output and the reconstructed pictures are shown in Fig. 8. Specifically, the generic image is discreetly used to communicate the medical image as it results in superior PSNR values for all of the test photos. As shown in Table 2, the OPSA algorithm's PSNR is higher than that of other approaches. Average PSNR values of 30.21 and 31.48 were obtained by the PSO and GWO algorithms, respectively, for Image A, while 34.87 was achieved by the OPSA method. The proposed model achieved a PSNR value of 35.65 dB for Image B, whereas the PSO and GWO techniques achieved PSNR values of 30.25 and 32.65 dB, respectively. A similar trend was observed for Image C where the proposed model registered an enhanced measure of PSNR value (36.59), whereas PSO and GWO techniques produced lower PSNR values of 29.65 and 33.56, respectively. PSNR values of 37.98 and 32.65 dB were achieved by the OPSA and PSO algorithms, respectively, on test Image D, whereas GWO obtained PSNR values of 34.48 dB. PSNR for Image E has been calculated by the OPSA algorithm to be 38.48dB, whereas the PSNRs for the PSO and GWO algorithms are numerated to 28.65 dB and 34.15 dB, respectively. Figure 9 shows the graphical results of the proposed approach. Henceforth, based on the aforementioned results, it can be concluded that the presented technique is more effective in image analysis as compared to state-of-the-art decision-making techniques.

4.5 Encryption technique analysis

The proposed ETA analysis is performed using statistical significance analysis. The null hypothesis was defined as compression of data is not effective in the proposed model. Therefore, the alternate hypothesis is defined as data compression is effective. It is shown in Table 3 that the outcomes of the proposed (NIS) algorithm under varied transaction counts are compared with the state-of-the-art LZW (Lempel-Ziv-Welch) and LZMA (Lempel-Ziv-Markov chain) technique. The compressed iterations should be less in size than the original Iterations. The proposed technique has successfully compressed 600 iterations with an initial size of 700 bytes to 350 bytes. With a compressed size of 590 bytes for LZW and 575 bytes for LZMA, the proposed model is better in terms of compression analysis. The presented technique achieved enhanced compression by compressing 1200 iterations with an initial size of 1380 bytes to 520 bytes. On the other hand, the LZW and LZMA techniques performed less optimally, with maximum compressed sizes of 1082 and 950 bytes, respectively. Similarly, for 1800 iterations with an initial size of 2015 bytes, LZW and LZMA models produced less compression with 1654 bytes and 1546 bytes. In comparison, the proposed technique was able to obtain a compressed size of 950 bytes. A compressed size of 1650 bytes has been reached by the presented technique with 3000 Iterations at a size of 3520 bytes. On the other hand, the compressed sizes of 2952 bytes and 2645 bytes were achieved by the LZW and LZMA models, respectively. These results are mapped with the p-value of 0.02 which is less than the 0.05 value for statistical significance analysis. Henceforth, the null hypothesis is rejected. Therefore, data compression is effective in the proposed model.

4.6 Compression ratio (CR) analysis

Blockchain hash values are analyzed for estimating the compression ratio measure. The findings are shown in Table 4 (Figs 10 and 11). It is important to mention that a greater CR number indicates enhanced performance. The suggested method has a CR of 1.99 after 600 iterations, while the CRs of the LZW and LZMA models are only 1.15 and 1.26, respectively. The proposed method generated a CR of 1.85 for 1200 iterations, while the LZW and LZMA models had CRs of 1.02 and 1.20, respectively. While the LZW and LZMA algorithms generated compression ratios for 1800 iterations numerated to 1.005 and 1.15, respectively, the presented method produced a better CR measure of 1.175. The proposed method has a CR of 1.65, whereas the LZW and LZMA models have CRs of 1.0023 and 1.102, respectively, after 2400 iterations. Similarly, the presented method has a CR of 1.55, whereas the LZW and LZMA models have a CR of 1.001 and 1.095, respectively, after 3000 iterations. Conspicuously, it can be concluded that the presented technique is more effective in data compression in comparison with other techniques.

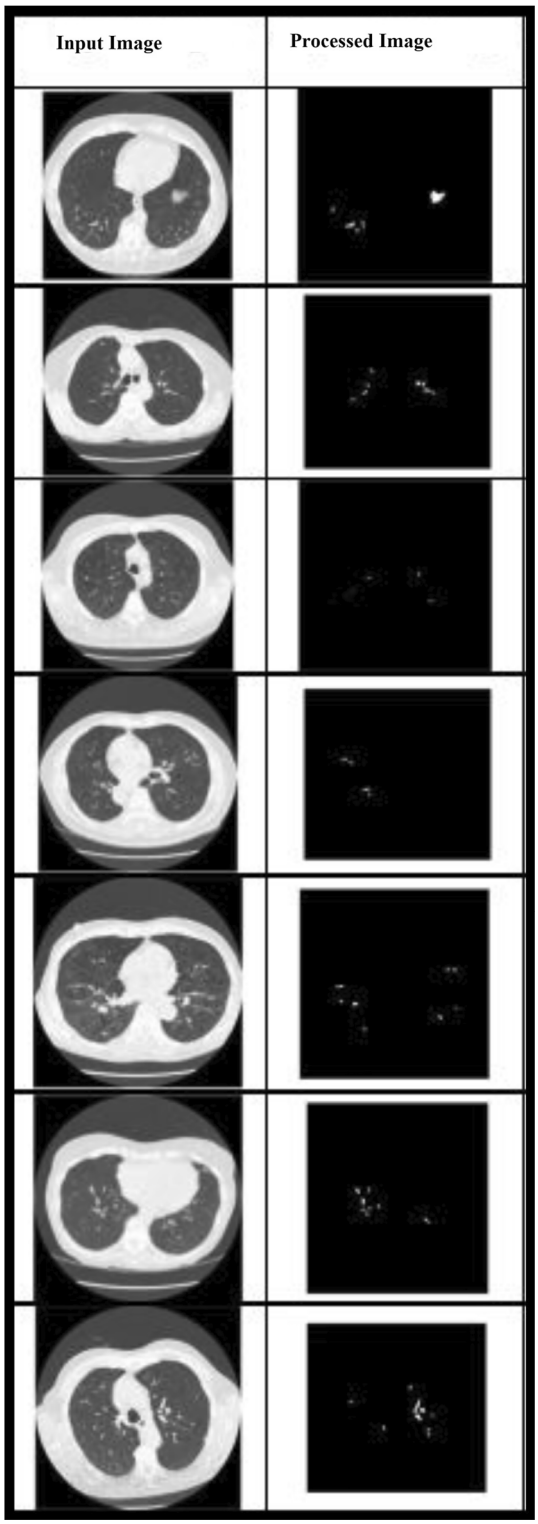

Fig. 8 Segmented Image

4.7 Space save analysis

The proposed model results for space savings (SS) are shown in Table 5 (Fig. 12). It demonstrates the effectiveness of SS in reducing the amount of space required by the blockchain hash values. Better performance is associated with a higher SS. The proposed method has a high SS of 48.65%, whereas the LZW and LZMA models have a substantially lower SS of 12.48% and 16.25%, respectively, after 600 iterations. While LZW and LZMA models have yielded lesser scores of 18.25 and 22.36%, the proposed technique has obtained a score of 42.36% in 1200

Table 2 PSNR ratio

Image	PSO	OPSA	GWO
Image A	30.21	34.87	31.48
Image B	30.25	35.65	32.65
Image C	29.65	36.59	33.56
Image D	32.65	37.98	34.48
Image E	28.65	38.48	34.15

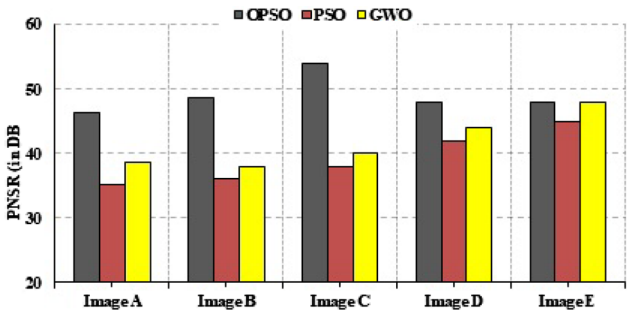

Fig. 9 Comparative Analysis: PSNR

Table 3 Comparative analysis

Iterations	Original	Proposed	LZW	LZMA
600	700	350	590	575
1200	1380	520	1082	950
1800	2015	950	1654	1546
2400	2780	1350	2658	2454
3000	3520	1650	2952	2645

Table 4 Comparative analysis: compression ratio

Iterations	Proposed	LZW	LZMA
600	1.99	1.15	1.26
1200	1.85	1.02	1.20
1800	1.75	1.005	1.15
2400	1.65	1.0023	1.102
3000	1.55	1.001	1.095

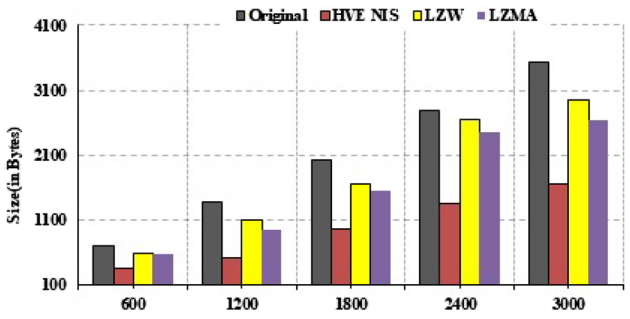

Fig. 10 Comparative Analysis: Size Ratio

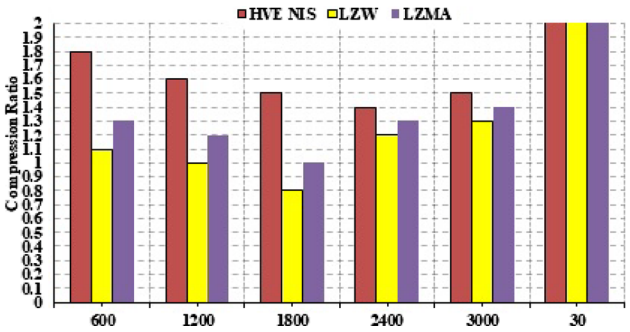

Fig. 11 Comparative Analysis

Table 5 Save space analysis

Iterations	Proposed	LZW	LZMA
600	48.65	12.48	16.25
1200	42.36	18.25	22.36
1800	35.65	25.26	28.25
2400	32.26	24.25	26.56
3000	28.45	22.26	24.15

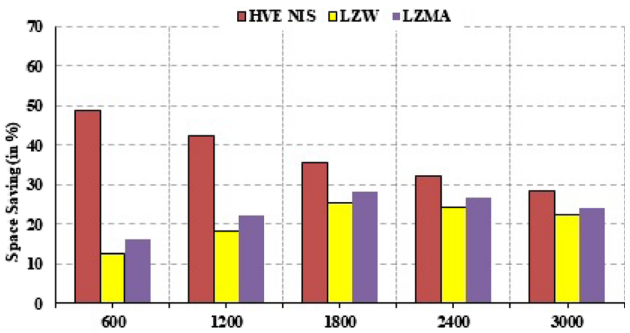

Fig. 12 Comparative Analysis: Space Saving

iterations. In the case of 1800 iterations, the proposed algorithm generated an SS of 35.65%, whereas the LZW and LZMA models generated SS of 25.26% and 28.25%, respectively. While the LZW and LZMA models yielded SS of 24.25% and 26.56%, the presented technique has yielded an SS of 32.26%. Similar trends were observed in the case of 3000 iterations where the proposed technique obtained superior results. Therefore, it can be concluded that in the current scenario, the proposed model is better and more effective in SS in comparison with the state-of-the-art techniques.

4.8 Statistical analysis

Figures 13, 14, 15, and 16 compare the classifier findings based on statistical metrics of accuracy, sensitivity, specificity, and *F*-Measure. Mathematically, these statistical metrics are computed based on True positive (TP), True negative (TN), False negative (FN), and False positive (FP). The mathematical formulation is represented as

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

$$\text{Sensitivity} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$\text{Specificity} = \frac{\text{TN}}{\text{FP} + \text{TN}}$$

$$F - \text{Measure} = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} = \frac{2 * TP}{2 * TP + FP + FN}$$

1. *Accuracy Assessment:* The proposed DNN-based classification model achieved an accuracy of 93.26% when compared to the linear regression model, which achieved an accuracy of 82.36%. With accuracy rates of 89.56% and 79.56%, the MLP and RBF algorithms are superior to the linear regression model but less optimal than the proposed model. The accuracy levels of the ANN (86.25%) and DNN (88.25%) models are also considerably higher. At 75.15%, the KNN model is less optimal for accuracy analysis.
2. *Sensitivity Assessment:* In comparison with the proposed DNN-based classifier's sensitivity analysis (93.26%), KNN's simulation output has the lowest level of sensitivity (76.21%), which was used to rank the models. With sensitivity levels of 81.95% and 86.21%, the RBF and DNN approach outperformed the linear regression model (81.45%). There are even better results using the ANN, which has achieved a sensitivity of 85.98%. Henceforth, the proposed model is more sensitive in accurately classifying data.
3. *Specificity Assessment:* The linear regression model does averagely in comparison with the proposed DNN-based classification model (94.26%) in terms of specificity, achieving 83.26%. On the other hand, RBF and MLP approaches have achieved a higher degree of specificity of 86.32% and 84.65%, respectively. The ANN and KNN models have yielded

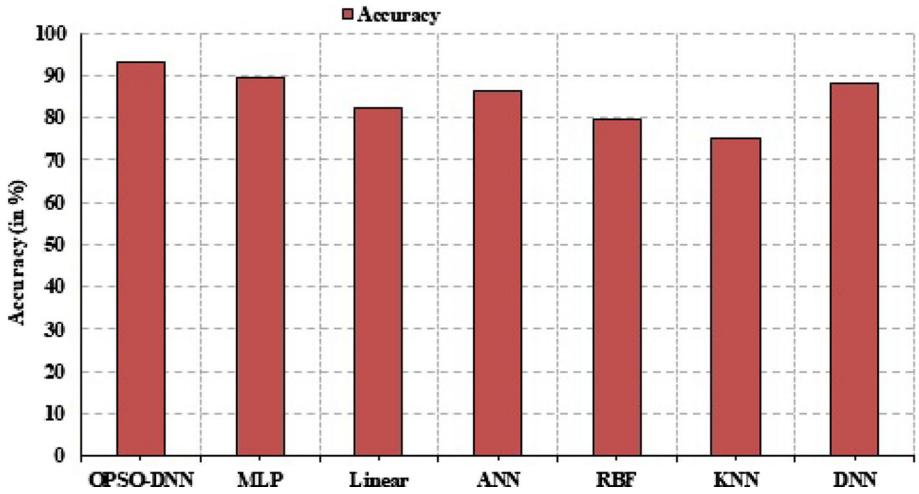

Fig. 13 Accuracy Analysis

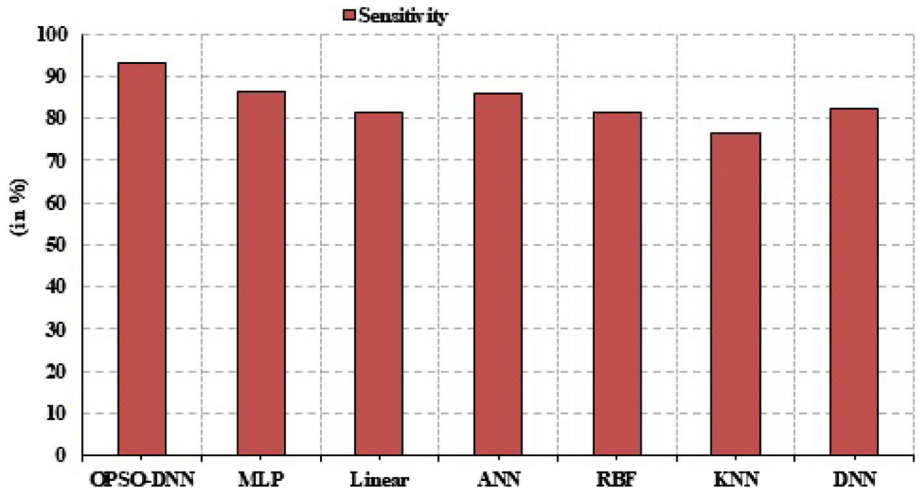

Fig. 14 Sensitivity Analysis

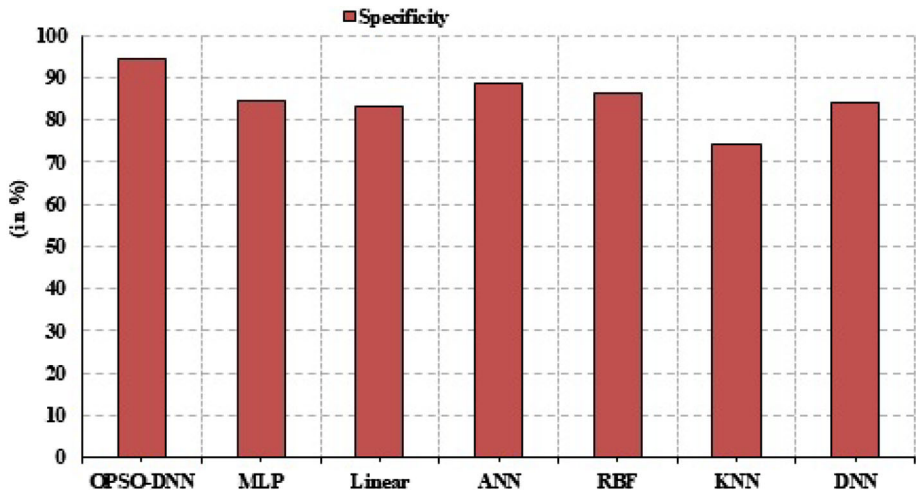

Fig. 15 Specificity Analysis

88.44% and 74.32% specificity, respectively. A specificity of 84.15% was achieved using the DNN approach.

4. *F-Measure Assessment:* A similar trend was seen for the *F*-Measure analysis for the proposed approach. Specifically, the presented technique registered an enhanced measure of 96.25% in comparison with

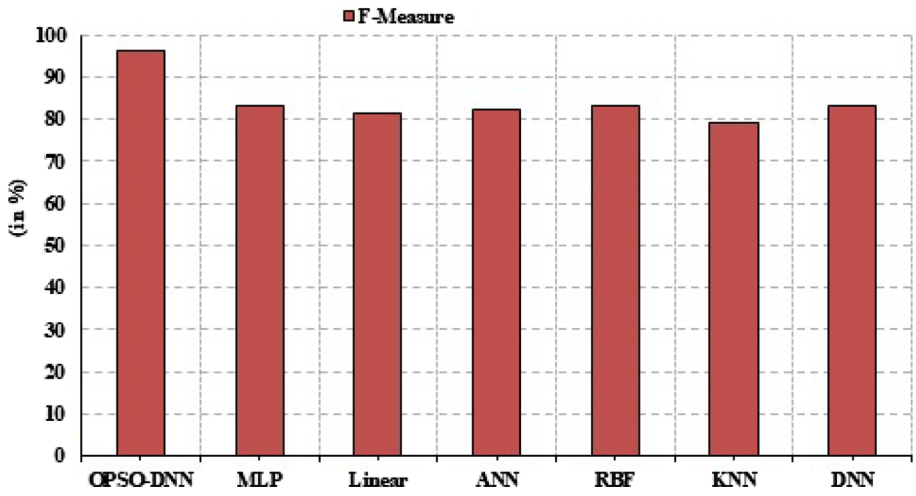

Fig. 16 *F*-Measure Analysis

83.26% (MLP), 81.14%(Linear regression), 82.22%(ANN), 83.14%(RBF), 79.25% (KNN), and 83.14% (DNN).

Several factors have contributed to the model's success, including the use of OPSA for secret sharing, an effective hash value encryption mechanism, and the parameter tweaking of the DNN model. Henceforth, it can be concluded from Table 6 that the presented approach is better than the state-of-the-art classification technique for healthcare data.

4.9 Research implications

The research contributions can be emphasized both practically and academically as follows:

4.9.1 Practical contributions

1. Enhanced Security Measures: The utilization of deep neural network (DNN)-driven secure intelligent IoT-medical diagnosis models enhances the security of healthcare data, ensuring patient privacy and confidentiality.
2. Secure Data Transmission: The incorporation of secure transactions involving picture steganography, hash value encryption, and medical diagnostics facilitates safe and confidential data exchange, crucial for maintaining the integrity of sensitive medical information.
3. Advanced Image Sharing Techniques: The use of orthogonal particle swarm optimization for secret sharing of medical images enhances data privacy and security, enabling efficient and secure transmission of critical healthcare visuals.
4. Robust Encryption Methods: The implementation of a neighborhood indexing sequence technique for hash value encryption strengthens data protection, safeguarding against unauthorized access and ensuring the integrity of medical data.
5. Improved Diagnostic Accuracy: The optimized DNN classification model aids in illness diagnosis, contributing to enhanced accuracy in identifying and categorizing medical conditions, thereby improving patient care outcomes.

Table 6 Performance analysis

Method	Accuracy	Sensitivity	Specificity	*F*-Measure
OPSA-DNN	93.26	93.26	94.26	96.25
MLP	89.56	86.25	84.65	83.26
Linear	82.36	81.45	83.26	81.14
ANN	86.25	85.98	88.44	82.22
RBF	79.56	81.95	86.32	83.14
KNN	75.15	76.21	74.23	79.25
DNN	88.25	86.21	84.15	83.14

4.9.2 Academic contributions

1. Innovative Research Focus: The primary focus on DNN-inspired secure intelligent IoT-medical diagnosis models contributes to the academic field by introducing innovative approaches to healthcare data security and diagnosis.
2. Novel Methodologies: The presentation of novel methodologies such as picture steganography, orthogonal particle swarm optimization, and neighborhood indexing sequence techniques adds to the academic discourse on secure data transmission and encryption in healthcare settings.
3. Algorithmic Contributions: The utilization of advanced algorithms in the proposed model, including DNN

optimization for classification tasks, offers insights into the application of cutting-edge technologies for medical diagnosis within academic research.

4. Validation through Trials: The validation of the model through extensive trials provides empirical evidence of its effectiveness, contributing to the academic literature by demonstrating practical applications of secure IoT-medical diagnosis models in real-world scenarios.
5. Potential for Future Research: The research sets a foundation for further academic exploration in the areas of secure IoT applications in healthcare, encryption techniques, and advanced diagnostic models, paving the way for future research advancements in the field.

5 Conclusion

The current paper delves into the development of a secure IoT healthcare diagnosis model that leverages IoT devices for data collection, the OPSA algorithm for secure medical image sharing, and hash value encryption for data protection. Scientifically, the study contributes to advancing secure IoT-healthcare diagnosis models by showcasing improved decision-making, data protection, and compression capabilities, setting a foundation for enhanced healthcare outcomes through innovative technology integration. The OPSA-DNN-based illness diagnosis model was proposed for effective decision-making and validated using a large-scale benchmark dataset of lung disease. The results showcased the model's ability to secure medical image transmission, achieve a high PSNR value, and outperform existing decision-making models in terms of statistical measures like f-Measure (96.25%), sensitivity (93.26%), specificity (94.26%), and accuracy (93.26%). Additionally, the NIS model demonstrated superior compression capabilities for blockchain-hashed data. Future research endeavors should delve deeper into the proposed technique by exploring dictionary-based encoding approaches to further enhance its performance. It is imperative to address the limitations encountered in the current study, such as scalability issues, interoperability challenges, and real-world implementation constraints. Recommendations for future studies include conducting more extensive testing across diverse datasets, refining the model's algorithmic components, and considering practical implications for seamless integration into healthcare systems. By addressing these aspects in-depth and incorporating valuable insights from the study's limitations, future research can advance the field of secure IoT healthcare diagnosis models and contribute to improved healthcare outcomes.

Acknowledgements The authors extend their appreciation to Prince Sattam bin Abdulaziz University for funding this research work through the project number PSAU/2024/R/1445.

Data availability The data used to support the findings of this study are available from the corresponding author upon request.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Zaman S, Khandaker MR, Khan RT, Tariq F, Wong KK (2022). IEEE Access
2. Bhatia M, Sood SK (2016) J Med Syst 40:1
3. Singh S, Rathore S, Alfarraj O, Tolba A, Yoon B (2022) Futur Gener Comput Syst 129:380
4. Bhatia M, Sood SK (2017) Comput Ind 92:50
5. Raghuvanshi A, Singh UK, Joshi C (2022) Advanced healthcare systems: empowering physicians with IoT-enabled technologies pp 43–58
6. Bhatia M, Sood SK (2019) Mobile Netw Appl 24:1392
7. Qahtan S, Yatim K, Zaidan A, Alsattar H, Albahri O, Zaidan B, Alamoodi A, Zulzalil H, Osman M, Mohammed R (2022) Novel multi security and privacy benchmarking framework for blockchain-based IoT healthcare industry 4.0 systems. IEEE Trans Ind Inform. 18(9):6415–23
8. Bhatia M (2020) Microprocess Microsyst 78:103227
9. Bhatia M, Kaur S, Sood SK, Behal V (2020) Artif Intell Med 107:101913
10. Olaniyan OT, Adetunji CO, Adeniyi MJ, Hefft DI (2022) In deep learning, machine learning and IoT in biomedical and health informatics (CRC Press,), pp 297–310
11. Bhuiyan MN, Rahman MM, Billah MM, Saha D (2021) Internet of things (IoT): a review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. IEEE Int Things J 8(13):10474–98
12. Torres P, Catania C, Garcia S, Garino CG (2016) An analysis of recurrent neural networks for botnet detection behavior. In: 2016 IEEE Biennial congress of Argentina (ARGENCON) (IEEE,), pp. 1–6
13. Canedo J, Skjellum A (2016) In: 2016 14th annual conference on privacy, security and trust (PST) (IEEE,), pp 219–222
14. Uddin MA, Stranieri A, Gondal I, Balasubramanian V (2018) IEEE Access 6:32700
15. Uddin MP, Mamun MA, Hossain MA (2021) IETE Tech Rev 38(4):377
16. Tuli S, Basumatary N, Gill SS, Kahani M, Arya RC, Wander GS, Buyya R (2020) Futur Gener Comput Syst 104:187
17. Pham QV, Dev K, Maddikunta PKR, Gadekallu TR, Huynh-The T, et al (2021) arXiv preprint arXiv:2101.00798
18. Jamil F, Ahmad S, Iqbal N, Kim DH (2020) Sensors 20(8):2195
19. Alqaralleh BA, Vaiyapuri T, Parvathy VS, Gupta D, Khanna A, Shankar K (2021) Personal and ubiquitous computing pp 1–11
20. Kakkar B, Johri P (2021) Blockchain: a healthcare perspective. In: 2021 10th International conference on system modeling and advancement in research trends (SMART) IEEE, pp 373–379
21. Egala BS, Pradhan AK, Badarla V, Mohanty SP (2021) IEEE Internet Things J 8(14):11717

22. Sagu A, Gill NS, Gulia P (2022) Hybrid deep neural network model for detection of security attacks in IoT enabled environment. Int J Adv Comput Sci Appl 13(1):1
23. Gorbunova M, Masek P, Komarov M, Ometov A (2021) Distributed ledger technology: state-of-the-art and current challenges. Comput Sci Inform Syst 1:65–85
24. Attaran M (2022) Int J Healthc Manag 15(1):70
25. Kumar R, Tripathi R (2021) J Ambient Intell Humaniz Comput 12(2):2321
26. Mavrogiorgou A, Kiourtis A, Manias G, Symvoulidis C, Kyriazis D (2023) Emerg Sci J 7(2):339
27. Benaich R, El Mendili S, Gahi Y (2023) HighTech Innov J 4(3):630
28. Singh S, Rosak-Szyrocka J, Tamàndl L (2023) HighTech Innov J 4(1):134
29. Tariq N, Khan FA, Asim M (2021) Proced Comput Sci 191:425
30. Soni SK, Manimaran D, Thomas SB, Thomas B (2023) Microstructure and mechanical characterization of Al6061 based composite and nanocomposites prepared via conventional and ultrasonic-assisted melt-stirring techniques. Mater Today Commun 34:105222
31. Lu L, Liang C, Gu D, Ma Y, Xie Y, Zhao S (2021) Technol Soc 67:101786
32. Pal K (2022) In: Prospects of blockchain technology for accelerating scientific advancement in healthcare (IGI Global,), pp 158–188
33. Duan W, Jiang Y, Xu X, Zhang Z, Liu G (2022) An edge cloud data integrity protection scheme based on Blockchain. Secur Commun Netw 1:5016809
34. Abdi AI, Eassa FE, Jambi K, Almarhabi K, Khemakhem M, Basuhail A, Yamin M (2022) Electronics 11(5):711
35. Veeramakali T, Siva R, Sivakumar B, Senthil Mahesh P, Krishnaraj N (2021) J Supercomput 77(9):9576