Svedberg Open
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Hybrid Optimization-Driven Multi-Attention Deep Learning Framework For Secure Authentication in Healthcare Iot Devices

S. Kumarappan[1*], Dr. K. Devasenapathy[2]

[1*]Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education
[1*]Assistant Professor, Department of CA & IT, Thiagarajar College.
[2]Associate Professor, Department of Computer Science, Karpagam Academy of Higher Education.
Corresponding Author Email: skumarappan928@gmail.com

ABSTRACT
The rapid growth of IoMT-enabled smart healthcare systems has significantly improved remote patient monitoring and medical image analysis; however, existing approaches suffer from critical limitations such as weak encryption robustness, high computational overhead, lack of secure access control, poor scalability in blockchain integration, and overfitting in deep learning-based diagnosis models. To address these challenges, this research proposes a novel IoMT–Blockchain Chaotic Encryption and Optimization-Driven Deep Learning Framework (IBCEODDLF) for secure medical image transmission and intelligent disease diagnosis. Initially, IoMT devices collect real-time patient data, which are securely managed using a blockchain framework incorporating BFT consensus, Merkle hashing, and smart contracts to ensure integrity and traceability. A Modified Logistic Map-based chaotic encryption scheme optimized via the American Zebra Optimization Algorithm (AZOA) enhances key sensitivity and diffusion strength. After secure transmission and decryption, DenseNet-169 with Hiking Optimization-based hyperparameter tuning extracts discriminative features, and final disease classification is performed using a Physics-Informed Neural Network (PINN) that integrates clinical data with physiological constraints for improved generalization. Experimental results demonstrate superior performance with 98.7% accuracy, 98.3% precision, 98.1% recall, 98.2% F1-score, AUC of 0.992, PSNR of 41.8 dB, entropy of 7.999, NPCR of 99.63%, average BFT consensus time of 2.3 s, and PINN final loss of 0.039, confirming enhanced security, efficiency, and diagnostic reliability.

Keywords: Internet of Medical Things, Blockchain Security, Chaotic Image Encryption, Deep Learning, Physics-Informed Neural Networks, Smart Healthcare Systems.

1. Introduction

Smart healthcare is the next phase of the development of the traditional healthcare system based on the utilization of the modern technologies and providing the ability to track the actual situation, make the effective decisions and to be supported by a doctor remotely [1]. Speedy development of the Internet of Medical Things (IoMT) has essentially enhanced the throughput of medical devices, their precision, and consistency by linking wearable sensors, diagnostic gadgets, and monitoring systems to the internet [2]. Remote health monitoring is necessary especially in the face of the global spread of the COVID-19, which has saved the needless visits to hospitals and minimized the risk of exposure [3]. The IoMT-enabled healthcare systems enable constant monitoring of health data of the patient, thus, making it possible to observe the abnormalities on time and prevent preventive measures [4].

In spite of these benefits, IoMT-based smart healthcare settings have severe security and privacy issues [5]. The entry of heterogeneous devices producing massive amounts of medical data in various formats poses a serious challenge in managed and safe storage, handling and transfer [6]. Healthcare repositories are becoming more susceptible to network attacks, software exploits, hardware violations and system level intrusions [7]. The medical data is very sensitive and therefore, any breach can jeopardize patient privacy and even lead to loss of life [8]. Thus, the need to keep healthcare information confidential, intact, and accessible has become one of the main research issues [9].

In order to overcome these barriers, Blockchain (BC) has become a prospective solution to safe and decentralized data management in the healthcare systems [10]. The blockchain technology allows the storage of data in a tamper-proof manner, verification of transactions and regulated access systems using

smart contracts [11]. It supports the exchange of safe patient data between the patient, healthcare provider, lab and pharmaceutical organization and maintains data integrity [12]. Blockchain can greatly improve trust, transparency, and dependability of IoMT-based healthcare systems by decentralizing storage and rendering the system unalterable [13].

Simultaneously, the Deep Learning (DL) methods applied into the IoMT settings have transformed the process of automatic disease diagnosis and medical image analysis [14]. Deep learning models are capable of identifying complicated trends in medical data, enhancing diagnostic performance, and providing personalized care [15]. Nevertheless, the DL models are extremely sensitive to their choice of hyperparameters, and trial-and-error hyperparameter optimization is both expensive and inefficient [16]. As a result, to automate hyperparameter optimization and improve the model efficiency, metaheuristic optimization algorithms have become a popular trend [17]. Moreover, reliable delivery of images involves the use of effective encryption algorithms with great key development techniques vital in ensuring that encrypted medical information is not attacked by cryptographers [18].

Inspired by these needs, this study presents an IBCEODDLF towards secure and intelligent smart healthcare. The medical images obtained through the IoMT devices are stored safely with the help of blockchain and access control with the help of smart contracts. An encryption scheme that is optimized with the AZOA is a Modified Logistic Map, which guarantees security in transmission. Hiking Optimization-based tuning of denseNet-169 is used to extract features and a PINN is used to classify diseases demonstrating robustness and physiological consistency. There are experimental outcomes that identify enhanced security and diagnostic performance. The novelty and contributions of this work are described below,

- Proposes a comprehensive IoMT-Blockchain-DL framework that combines secure data acquisition, encrypted transmission, optimal feature extraction, and physics-informed disease diagnosis in a single smart healthcare system.
- Presents a Modified Logistic Map-based chaotic encryption method with optimized key parameters through the AZOA, improving the security strength, randomness, and quality of reversible image reconstruction.
- Implements blockchain technology with BFT consensus, Merkle hashing, and smart contracts for secure and tamper-proof storage, transparent traceability, and patient-controlled access management of medical data.
- Uses DenseNet-169 with optimized hyperparameters through the Hiking Optimization Algorithm (HOA), improving the capability of deep feature representation and convergence speed for medical image classification.
- Combines PINN for disease prediction, including physiological constraints in the loss function to improve robustness, prevent overfitting, and provide physically consistent diagnoses.
- Simultaneously improves the overall reliability and security of the end-to-end healthcare system, along with the robustness of encryption strength, transmission integrity, and diagnostic accuracy compared to existing standalone approaches.

The remainder of this paper is organized as follows: Section 2 reviews related literature on IoMT security, blockchain integration, chaotic encryption, and deep learning models. Section 3 details the proposed methodology. Section 4 presents results and discussion. Section 5 concludes the paper.

2. Related Work

In 2025, Kateb, F., et al. [19] introduced an Enhanced Security Mechanism in Human-Centered Systems using Deep Learning with Jellyfish Search Optimizer (ESHCS-DLJSO) to Internet of Things (IoT)-enabled healthcare applications. The technique involves the use of minmax normalization to preprocess the data, Bacterial Foraging Optimization Algorithm (BFOA) to extract the features, Convolutional Neural Networklong short term memory with attention (CNN-LSTM-Attention) to detect and classify the disease and Jellyfish Search Optimizer (JSO) to tune the parameters. On an IoT healthcare security dataset, experimental results were 99.43% accurate. The method enhances safety in transmission of medical data and early diagnoses at the expense of higher computational costs and training.

In 2022, Kathamuthu, N. D., et al. [20] designed a Deep Q-Learning-based Neural Network with Privacy Preservation (DQ-NNPP) to safeguard healthcare data transmission under external threat. The deep- q-learning framework is combined with neural network model to optimize safe communication at the expense of minimum time spent on encryption and decryption. It is efficient in processing patient data, which lowers the network traffic and communication cost with transmission error. The experimental results demonstrated 93.74% accuracy, 92 sensitivity and 92.1 specificity, 67.08 communication overhead, 58.72 time encrypting and 62.72 decrypting time. Nevertheless, the approach is characterized by a moderate communication overhead and a low level of scalability in cases of large-scale deployments.

Ala, A., et al. [21] introduced an Artificial Intelligence (AI)- IoT-based Smart Healthcare System (SHS) framework to improve the quality of treatment and patient data processing. The paper proposed a superior version of a Particle Swarm Optimization--Long Short-Term Memory (PSO-LSTM) algorithm whereby PSO was used to optimize efforts to enhance classification of patient medical data. The model was benchmarked against standalone PSO on various benchmarks in order to realize maximum processing efficiency. Results of experiments showed an accuracy of 92.5% with low variation in prediction. This method is better in terms of reliability and patient satisfaction but can be affected by higher levels of computational complexity and sensitivity to the parameters.

In 2023, Devi, R. A., and Arunachalam, A. R. [22] designed a DL-based malware detection and prevention framework of secure data transmission in IoT networks. First, the use of trust values based on contextual features was done to differentiate attack nodes and normal nodes and the second was preprocessing and extraction of features to efficiently classify. Deep LSTM Malware detector was used. To prevent, there was the use of an Improved Elliptic Curve Cryptography (IECC) algorithm which had hybrid MA -BW optimization that was applied in the optimal selection of key. The results of the experiment revealed accuracy of 95, precision of 92, error of 5 and execution time of 6.02 s, however, the execution time is limited due to computational overhead.

In 2023, Irshad, R. R., et al. [23] introduced a new IoT-based monitoring system of health to track and predict diseases among communities in remote areas. This framework has three steps, which include data collection, which involves IoT sensor devices, secured storage, which involves Homomorphic Encryption (HE), and disease detection, which involves a Centered Convolutional Restricted Boltzmann Machines with Whale Optimization (CCRBM-WO) algorithm. The model was deployed on a cloud platform, Python based to test the performance. The experimental results obtained an accuracy of 96.87, precision of 97.45 and F1-measure of 97.78 and a recall of 98.57. The scheme is more secure and predictive than others but the computation becomes more complex and the size of the encryption is greater.

In 2023, Alamro, H., et al. [24] proposed a Blockchain Assisted IoT Healthcare System with Ant Lion Optimizer with Hybrid Deep Learning (BHS-ALOHDL) to provide secure medical data transmission and intrusion detection. The process implements the Feature Subset Selection (ALO-FSS) process that uses Ant Lion Optimizer to produce the best feature vectors. Intrusion detection is performed with the help of Hybrid DL model, which is a combination of Convolutional Neural Network (CNN) and LSTM models. Moreover, Flower Pollination Algorithm (FPA) is used to do hyperparameter tuning to improve detection performance. Experimental validation of benchmark datasets showed much better results, but a more complicated computation and implementation is one of the limitations.

Table 1: Comparative Analysis of Literature Survey

Ref.	Method / Model	Optimization Technique	Best Performance	Key Advantages	Key Disadvantages
[19]	ESHCS-DLJSO (CNN-LSTM-Attention)	BFOA + JSO	99.43% Accuracy	Very high accuracy, effective early diagnosis	High computational complexity and training time
[20]	DQ-NNPP	Deep Q-Learning	93.74% Accuracy	Reduced encryption/decryption time, lower traffic	Moderate communication overhead, scalability issues
[21]	PSO-LSTM	PSO	92.5% Accuracy	Improved reliability and patient satisfaction	Parameter sensitivity, increased complexity
[22]	Deep LSTM + IECC	Hybrid MA-BW	95% Accuracy	Effective malware detection and secure key selection	Higher computational overhead
[23]	CCRBM-WO	Whale Optimization	96.87% Accuracy	Strong security with high recall (98.57%)	Encryption overhead, increased processing time
[24]	BHS-ALOHDL (CNN-LSTM)	ALO + FPA	Superior detection rate	Secure blockchain integration, optimized feature selection	Implementation complexity and high resource consumption

Table 1 presents the comparison of recent healthcare security models that use DL and optimization techniques. ESHCS-DLJSO got the best accuracy (99.43%), and CCRBM-WO, Deep LSTM + IECC were both well-performing. Despite the fact that all the methods enhance the efficiency of security and detection, most of them have high computation complexity, encryption overhead, problem of scaling and high consumption of resources.

2.1 Problem statement

The fast implementation of the IoMT in intelligent healthcare has triggered serious issues connected with the secure transmission of the data, data privacy, and correct diagnosis of a disease, especially because of the massive amount of heterogeneous medical data produced by interconnected devices. Despite the applications of Blockchain to improve data integrity and decentralized data storage, most of the currently used solutions are oriented towards access control and record control at the expense of an efficient encryption scheme and optimal diagnostic performance. Likewise, traditional image encryption algorithms tend to be based on either low or fixed key generation policies, creating them susceptible to statistical and cryptographic attacks, and most deep learning-based diagnostics models are also overfit and poorly tuned in terms of hyperparameter selection and highly compute-intensive. Moreover, the earlier approaches tend to address the security and diagnostic issues as distinct modules instead of development of a unified framework that optimally strengths the encryption, key generation and classification. Thus, it is urgently needed to have an integrated, secure and optimization-oriented model of smart healthcare which will not only ensure strong encrypted transmission, best key generation, and high disease-detection accuracy in IoMT frameworks.

3. Methodology

The current study introduced a new IBCEODDLF to guarantee the safety of medical image transfer and intelligent disease diagnosis in the smart healthcare setting.

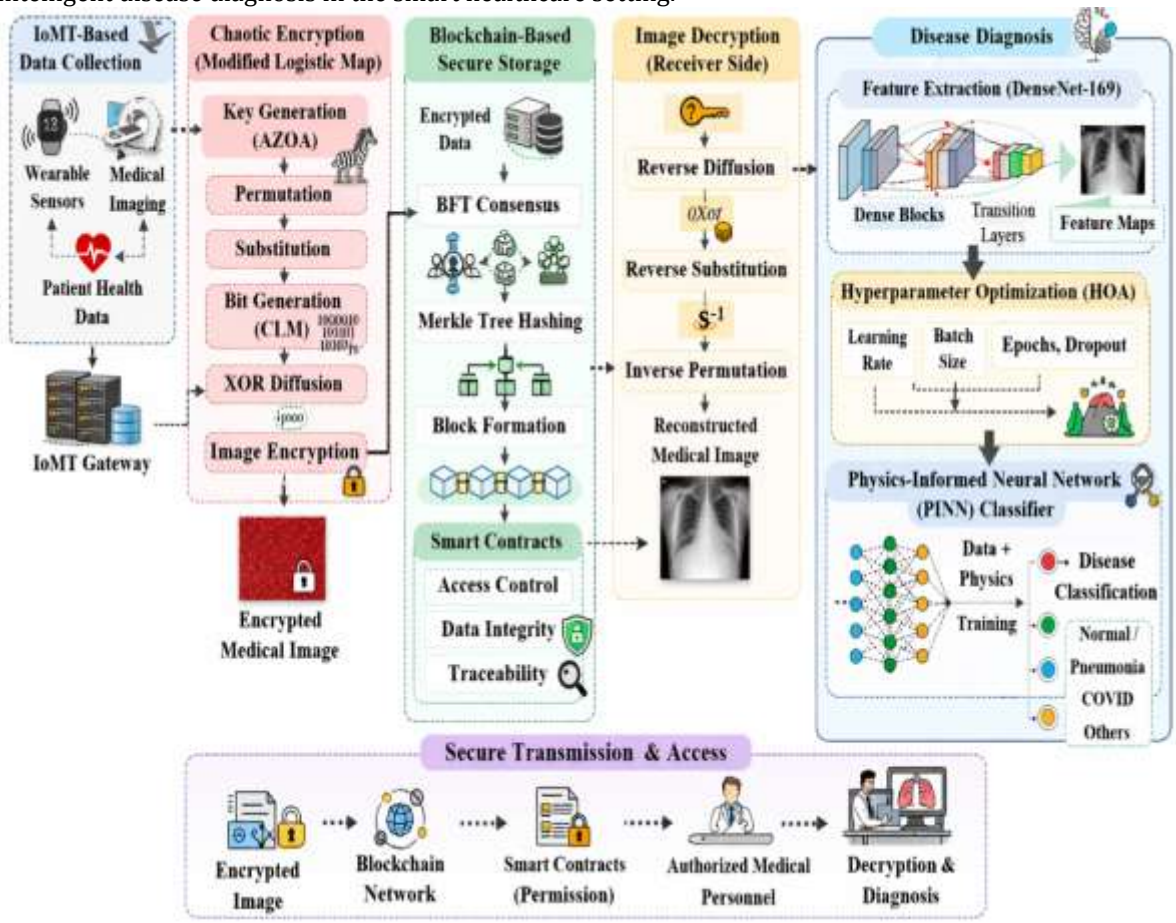


Figure 1: Schematic architecture of the developed model

First, the real-time patient data collected by IoMT devices are safely stored with blockchain based on BFT consensus, Merkle hashing and managed by smart contracts to allow limited access and trackability. To secure medical images, there is a chaotic encryption algorithm based on the Modified Logistic Map, and

the optimum key parameters are created by the application of the AZOA to achieve optimal security and reversible quality. The cipher text is sent via the blockchain network whereby it is decrypted at the authorized receiver location with synchronized chaotic parameters. Then, deep feature extraction is performed by DenseNet-169 and its hyperparameters are optimized with HOA to improve the performance of classification. Lastly, prediction of diseases is accomplished in a PINN providing the integration of clinical data with the physiological constraints to guarantee the sound, precise and physically coherent medical choices. The schematic architecture of the developed model is shown in figure 1.

3.1 IoMT-Based Data Collection

During this phase, the IoMT devices, such as wearable sensors and medical imaging devices are continuously capturing the health information of the patients as well as medical images. The IoMT devices are interconnected and transmit the captured information to the healthcare network for further processing and analysis. This allows for continuous remote monitoring and early detection of abnormalities, thus reducing the need for frequent visits to the hospital. Figure 2 illustrates the IoMT-enabled smart healthcare data acquisition and processing framework.

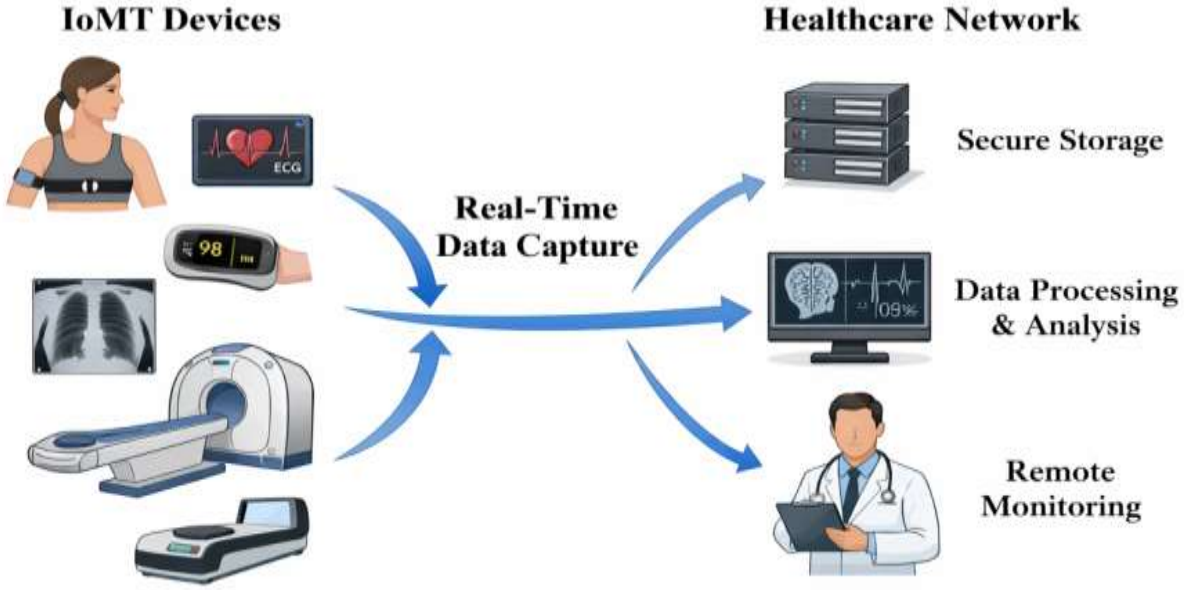


Figure 2: IoMT-Enabled Smart Healthcare Data Acquisition and Processing Framework

The above figure 2 depicts an IoMT-based smart healthcare system where patient data is captured in real-time by wearable sensors, ECG monitors, imaging devices, and diagnostic devices. The captured data is then sent to the healthcare network for secure storage, intelligent data processing, analysis, and remote monitoring by medical professionals.

3.2 Blockchain-Based Secure Data Storage

The Blockchain-Based Secure Data Storage is implemented through a blockchain coupling mechanism that involves the uploading of medical data by healthcare participants, such as IoMT devices, healthcare providers, laboratories, and monitoring authorities, into the blockchain network. The uploaded medical data in the form of images and patient records undergoes processing through smart contract workflows before being stored in the blockchain. The smart contracts enable the automatic selection of healthcare data, checks for consistency in formats, and initiates predetermined actions based on predefined conditions. In the event of any irregularity in the uploaded data, an alert system is initiated to alert the participants. For legitimate healthcare data, the process continues with consensus verification before storage. Figure 3 illustrates the blockchain structure.

Figure 3: Blockchain structure

3.2.1 Byzantine Fault Tolerant (BFT) Consensus Verification

The consensus verification procedure is based on the BFT algorithm to verify the transactions among the distributed nodes. The procedure involves a request phase where a node requests the validation of the medical information. The request is broadcasted to other blockchain nodes in the preparation and acknowledgement phase. The nodes verify the information and exchange acknowledgement messages. Consensus is reached when the number of agreeing responses exceeds the threshold condition ($N \geq 3f + 1$), and only then is the information accepted as valid for the creation of a block.

3.2.2 Merkle Tree Hashing and Block Formation

After that, the cryptographic hash values are created for the verified medical information. The hashes are then combined to create a Merkle Root. A new block is then formed by combining the Merkle Root, the previous block's hash, and the timestamp. This creates a chain where the blocks are linked by the previous hashes, forming a secure ledger system. Any attempt to alter the information in one block would mean that all the following blocks are also altered, thus maintaining the integrity of the data.

3.2.3 Smart Contract Supervision and Access Control

The blockchain technology uses various modules of smart contracts to handle healthcare information safely. Data Processing Contract authenticate uploaded records of patients, format information and derive key attributes to facilitate effective storage and retrieval. Data Judgement Contract assesses the uploaded medical data, and determines possible suspicious and abnormal activity because of the set healthcare policies. In case of violation, the Punishment Management Contract takes corrective measures like access control or reputation modification. Also, the Information Traceability Contract allows the specified healthcare professionals to access patient information using specific permission levels and maintain privacy without restricting the necessary access to medical information.

The blockchain-based storage system provides a secure, transparent and regulated data management framework of smart healthcare systems, which are IoMT-enabled, based on consensus-based validation, hierarchical hashing and multi-layer supervision of smart contracts.

3.3 Medical Image Encryption

Prior to the transmission of images to the healthcare network, the images are encrypted using an Encryption Algorithm Based on Modified Logistic Map. This algorithm combines permutation, substitution, chaotic bit generation, and diffusion processes to improve the randomness of the algorithm, increase the keyspace, and reduce the computational complexity.

3.3.1 Key Selection Using Modified Logistic Map

The encryption keys are generated using a Modified Chaotic Logistic Map (CLM). The classical logistic map is defined as follows in Equation (1).

$$b_{n+1} = \gamma b_n (1 - b_n) \quad (1)$$

where b_n indicates the chaotic state at iteration n, γ indicates the population growth (control parameter), and b_{n+1} indicates the next chaotic value. For chaotic behaviour, $3.6 < \gamma < 4$. To enhance randomness and generate unique permutations within the pixel range [0,255], the modified equation is expressed as follows in Equation (2).

$$y = (\gamma + 0.5)x(1 - x), \quad 0 \le x \le 255 \quad (2)$$

where x denotes the pixel intensity values, $\gamma \in Z^+$ (positive integers), and y denotes the generated chaotic output sequence. This modification enlarges the keyspace (greater than 2^{302}) and produces highly unique permutations for encryption. The parameters γ and initial value x_0 form the secret encryption key.

3.3.2 Chaotic Sequence Preprocessing

The produced chaotic sequences are subjected to preprocessing in order to remove the effects of transients. The initial iterations are removed to prevent predictability. The improved chaotic sequences are scaled to the intensity of pixels within the range [0,255]. The produced chaotic sequences are utilized to control the permutation, substitution, and bit generation processes.

3.3.3 Image Scrambling

Permutation: In the permutation stage, chaotic indices obtained from the modified CLM are used to reorder pixel places. The resulting permutation matrix is used to reorder the rows and columns of the medical image $I(i, j)$. This process maintains the histogram's properties while destroying the spatial correlation between neighboring pixels. The permuted image I_p is produced as follows if P stands for the permutation matrix produced from the chaotic sequence are given in Equation (3).

$$I_p(i, j) = I(P_i, P_j) \quad (3)$$

where P_i and P_j indicates the shuffled row and column indices.

Substitution: Pixel intensities are substituted with pseudorandom values produced by the modified CLM. The substituted value $S(i, j)$ for a pixel intensity $I_p(i, j)$ is calculated as follows in Equation (4).

$$S(i, j) = f_{CLM}(I_p(i, p)) \quad (4)$$

where f_{CLM} denotes the chaotic substitution function controlled by γ. This step obscures the direct relationship between original and encrypted pixel values.

3.3.4 Image Expansion

To improve the resistance against chosen-plaintext attacks, random matrices created using chaotic series are added to the boundaries of the image. If the size of the original image is M×N, then the size of the image will be in Equation (5).

$$I_e \in R^{(M+\Delta M)\times(N+\Delta N)} \quad (5)$$

where ΔM and ΔN represent additional rows and columns derived from chaotic values. This expansion increases entropy and improves structural complexity.

3.3.5 Confusion and Diffusion Operations

Binary Conversion and Bit Generation: Each substituted pixel intensity (0–255) is converted into an 8-bit binary sequence. Random binary bits are generated using the logistic map is given in Equation (6).

$$b_{n+1} = \gamma b_n (1 - b_n) \quad (6)$$

These bits form a one-time pad with strong randomness.

XOR Diffusion: The binary pixel sequence is combined with chaotic binary bits B_c using the XOR operation is given in Equation (7).

$$B_e = B_p \oplus B_c \quad (7)$$

where $\oplus$ denotes the XOR operation, and B_e indicates the encrypted binary output. In XOR, identical bits yield 0, and different bits yield 1.

Conversion to Encrypted Image: The resultant binary sequences are reconverted into pixel intensities is given in Equation (8).

$$I_{enc}(i, j) = BinaryToDecimal(B_e) \quad (8)$$

The final encrypted medical image I_{enc} exhibits uniform histogram distribution, high entropy, low pixel correlation, and strong resistance to brute-force and statistical attacks.
By permutation, substitution, chaotic bit generation, image expansion, and XOR diffusion, the Encryption Algorithm Based on Modified Logistic Map provides highly secure and efficient protection of medical images before their storage and transmission on the blockchain.

3.4 Key Generation Using American Zebra Optimization Algorithm

The parameters of the encryption key of the Modified Logistic Map are optimally generated by using the AZOA, a bio-inspired metaheuristic technique developed based on the life cycle of the American zebra. AZOA simulates the organization of the herd, the movement of the herd for feeding, the process of breeding, the control of leadership, and the transition of leadership. In the proposed system, each zebra represents a candidate encryption key containing chaotic parameters such as the initial value x_0 and control parameter γ. The objective is to determine the optimal parameter set that maximizes encryption strength while preserving reversible decryption quality.

3.4.1 Phase 1: Creation of Random Zebra Groups

Initially, the zebra population is randomly divided into groups. Let S denote the total zebra population and P represent the stallion probability. The total number of groups N is computed as follows in Equation (9).

$$N = S \times P \tag{9}$$

Each zebra's position in the j^{th} group is represented as follows in Equation (10).

$$Z_{i,j} = (Z_{\max} - Z_{\min}) \times rand + Z_{\min} \tag{10}$$

where $Z_{i,j}$ indicates the position (candidate solution) of the i^{th} zebra in the j^{th} group, $Z_{\min}$ and $Z_{\max}$ indicates the lower and upper parameter bounds of the encryption key, and $rand \in [0,1]$ is a uniformly distributed random number. These positions encode potential logistic map parameters for key generation.

3.4.2 Phase 2: Feeding Activity (Exploration Phase)

Zebras move around their group leader (stallion) during feeding. This movement enables exploration of the search space. The position update rule is given by Equation (11).

$$z_i^j = \begin{cases} 2R_1 \sin(2\pi R_2)(z_s^j - z_i^j) + z_s^j, & if\ R_3 < 0.5 \\ 2R_1 \cos(2\pi R_2)(z_s^j - z_i^j) + z_s^j, & otherwise \end{cases} \tag{11}$$

where z_s^j indicates the stallion (leader) position in group j, z_i^j is the i^{th} zebra's position, $R_1 \in [-2,2]$ indicates the random exploitation factor, R_2 indicates the adaptive coefficient, and $R_3 \in [0,1]$ is a random switching parameter. The updated position is accepted if it improves the fitness value.

3.4.3 Phase 3: Breeding Activity (Diversity Preservation)

Breeding enhances diversity by combining solutions from different groups. The crossover mechanism is expressed as follows in Equations (12) and (13).

$$Z_q^j = crossover(z_i^a, z_j^a), \quad if\ r < p_c \tag{12}$$

$$Z_q^k = crossover(z_i^a, z_k^a), \quad if\ r \geq p_c \tag{13}$$

where p_c is the crossover probability, $r \in [0,1]$ is a random probability, z_i^a is a chosen zebra from group a, and z_j^a and z_k^c stand for zebras from groups a and c, respectively. By producing child solutions, this technique enhances the ability to search globally for the best encryption keys.

3.4.4 Phase 4: Group Leadership (Exploitation Phase)

Leadership behavior directs the herd toward the best solution (water reserve, WR), representing the global best encryption key. The stallion updates its position as follows in Equation (14).

$$z_s^j = \begin{cases} 2R_4 \sin(2\pi R_5)(WR - z_s^j) + WR, & if\ R_6 < 0.5 \\ 2R_4 \cos(2\pi R_5)(WR - z_s^j) + WR, & otherwise \end{cases} \tag{14}$$

where $R_4 \in [-2,2]$ indicates the random coefficient, $R_5 = 1 - \frac{t}{T}$ indicates an adaptive parameter, $R_6 \in [0,1]$, and WR denotes the global best position. This phase intensifies exploitation around the best-performing key candidate.

3.4.5 Phase 5: Leadership Transition

If a group member achieves better fitness than the current stallion, leadership is transferred according to Equation (15).

$$Z_s^i = \begin{cases} z_i^j, & if \ F(z_i^j) < F(z_s^j) \\ z_s^j, & otherwise \end{cases} \quad (15)$$

where $F(.)$ represents the fitness function. This mechanism ensures that the best candidate solution becomes the new leader.

3.4.6 Fitness Function for Optimal Key Selection

The objective of AZOA is to optimize encryption key parameters by maximizing image quality after decryption. The fitness function is defined as follows in Equation (16).

$$Fitness = \max(PSNR) \quad (16)$$

where PSNR (Peak Signal-to-Noise Ratio) measures the similarity between the original medical image and the decrypted image. A higher PSNR value ensures that the optimized key retains strong encryption properties along with the accuracy of reversible decryption.

Using structured search, adaptive exploitation, crossover diversity, and leadership evolution, the American Zebra Optimization Algorithm efficiently produces optimal parameters of the chaotic key for secure medical image encryption.

3.5 Secure Transmission via Blockchain

Following encryption with AZOA-optimized keys utilizing the Modified Logistic Map, the encrypted medical picture I_{enc} is sent across the blockchain network for safe distribution. It proposes the encrypted image to the distributed ledger as a blockchain transaction. The transaction is then validated for consensus among the participating nodes before being added to a new block. The procedure of block formation can be represented as follows in Equation (17).

$$B_k = H(B_{k-1} \| MR_k \| TS_k) \quad (17)$$

where TS_k is the timestamp, $H(.)$ is the cryptographic hash function, MR_k is the Merkle Root of encrypted image transactions, B_k is the current block hash, B_{k-1} indicates the previous block hash, and $\|$ denotes concatenation.

The smart contract is responsible for handling controlled access by checking the patient-defined permissions before allowing the retrieval of data. Only authorized medical practitioners with credentials meeting the smart contract requirements can access the encrypted image hash stored on the blockchain, while the encrypted image is safely linked via distributed storage.

3.6 Image Decryption at Receiver Side

On the receiver side, the decryption operation is carried out by authorized medical personnel using the optimized parameters of the chaotic key obtained from the AZOA. The decryption operation reverses the inverse operations of the encryption process.

First, reverse diffusion is performed using the same optimized chaotic binary sequence is given in Equation (18).

$$B_p = B_e \oplus B_c \quad (18)$$

where B_p is the recovered binary pixel sequence, B_c is the regenerated chaotic key stream using the shared parameters, and B_e stands for encrypted binary data.

Then, using inverse permutation and substitution mappings that are derived from the same logistic key parameters, reverse confusion and reverse scrambling are carried out. If the inverse permutation matrix is represented by P^{-1}, the recovered image I_{rec} can be found as follows in Equation (19).

$$I_{rec} = P^{-1}(S^{-1}(I_{enc})) \quad (19)$$

where S^{-1} represents inverse substitution.

Since the same chaotic initial conditions and control parameters are employed at both ends, the original medical image is properly reconstructed. This ensures safe, reversible, and integrity-preserving medical image recovery for authorized diagnosis.

3.7 Feature Extraction Using DenseNet-169

Once the medical image is decrypted securely, the diagnosis of the disease is carried out using the DenseNet-169 model, which is a deep CNN that aims to enhance the flow of features. In the DenseNet-169 model, every layer is connected to all the following layers. If a network contains N layers, the total number of direct connections is given in Equation (20).

$$\frac{N(N+1)}{2} \quad (20)$$

This dense connectivity enables efficient feature reuse and reduces redundancy, making the model highly effective for medical image feature extraction.

3.7.1 Dense Connectivity Mechanism

Unlike traditional CNNs where each layer receives input only from the previous layer, DenseNet connects each layer to all preceding layers. The feature mapping of the l^{th} layer is defined as follows in Equation (21).

$$x_l = H_l([x_0, x_1, x_2, ..., x_{l-1}]) \quad (21)$$

where $[.]$ indicates concatenation of feature maps from all previous layers, x_l is the output feature map of layer l, and $H_l(.)$ is a composite function of Batch Normalization (BN), Rectified Linear Unit (ReLU), and Convolution. This arrangement guarantees that both high-level and low-level features play a role in the final classification.

3.7.2 Dense Blocks and Transition Layers

DenseNet-169 is composed of four dense blocks with 6, 12, 32, and 32 convolutional sets, respectively. Each set consists of a 1×1 convolution and a 3×3 convolution. The 1×1 convolution reduces the dimensionality, while the 3×3 convolution captures the spatial information.

To decrease the size of the feature maps and the computational complexity between the dense blocks, transition layers are added. The transition layer consists of a 1×1 convolution followed by a 2×2 average pooling with a stride of 2. This transformation can be written as follows in Equation (22).

$$x_{trans} = AvgPool(Conv_{1\times1}(x)) \quad (22)$$

where x_{trans} denotes the reduced feature representation. The growth rate k=32 determines how many new feature maps each layer contributes, allowing controlled expansion of network depth while maintaining efficiency.

3.7.3 Feature Learning and Regularization

Each convolutional operation within a dense block follows the transformation is given in Equation (23).

$$H_l(x) = Conv_{3\times3}(\mathrm{Re}\,LU(BN(Conv_{1\times1}(\mathrm{Re}\,LU(BN(x)))))) \quad (23)$$

Batch Normalization stabilizes learning, ReLU introduces non-linearity, and convolution extracts hierarchical patterns from medical images. Dropout regularization is applied in later stages to reduce overfitting and improve generalization.

3.7.4 Softmax-Based Disease Classification

The final dense block connects to a classification layer that applies the Softmax activation function to predict disease categories. The probability of class i is given by Equation (24).

$$P(y=i \mid x) = \frac{e^{z_i}}{\sum_{j=1}^{C} e^{z_j}} \quad (24)$$

where z_i represents the output score (logit) for class i, and C denotes the total number of disease classes.

Through dense feature reuse, controlled growth rate, and deep hierarchical learning, DenseNet-169 efficiently extracts discriminative features from decrypted medical images while maintaining high classification accuracy and parameter efficiency.

3.8 Hyperparameter Optimization Using Hiking Optimization Algorithm (HOA)

For improving the performance of disease classification in DenseNet-169, its hyperparameters like learning rate, batch size, number of epochs, and dropout rate are optimized using the HOA. HOA is based on the idea of hikers trying to climb to the top of a mountain while taking into account the steepness of

the terrain. In the optimization process, each hiker corresponds to a hyperparameter vector, and the best one is the lead hiker trying to reach the global optimum (maximum classification accuracy or minimum loss).

3.8.1 Initialization of Hiker Positions

Each hiker's position represents a hyperparameter set. The initial position is randomly generated within lower and upper bounds as follows in Equation (25).

$$\beta_{i,t} = \phi_j^1 + \delta_j(\phi_j^2 - \phi_j^1) \quad (25)$$

where $\beta_{i,t}$ indicates the position of hiker i at iteration t, ϕ_j^1 and ϕ_j^2 are lower and upper bounds of the j^{th} hyperparameter, and $\delta_j \in [0,1]$ is a uniformly distributed random number.

3.8.2 Velocity Update Using Tobler's Hiking Function

HOA models hiker movement speed using Tobler's Hiking Function is given in Equation (26).

$$W_{i,t} = 6e^{-3.5|S_{i,t}+0.05|} \quad (26)$$

where $W_{i,t}$ indicates the velocity of hiker i, and $S_{i,t}$ denotes the slope defined as follows in Equation (27).

$$S_{i,t} = \tan\theta_{i,t} \quad (27)$$

Here, $\theta_{i,t}$ is the inclination angle of the search landscape. This mechanism balances exploration and exploitation depending on the steepness of the optimization surface. The velocity is further updated considering the global best (lead hiker) is given in Equation (28).

$$W_{i,t} = W_{i,t-1} + \gamma_{i,t}(\beta_{best} - \alpha_{i,t}\,\beta_{i,t}) \quad (28)$$

where $\gamma_{i,t} \in [0,1]$ denotes the random factor, β_{best} represents the position of the lead hiker (best hyperparameter set), and $\alpha_{i,t} \in [1,3]$ is the sweep factor controlling convergence behavior.

3.8.3 Position Update and Fitness Evaluation

The updated hyperparameter position is computed as follows in Equation (29).

$$\beta_{i,t+1} = \beta_{i,t} + W_{i,t} \quad (29)$$

Each updated position is evaluated using a fitness function defined as classification performance is given in Equation (30).

$$Fitness = \max(Accuracy) \quad (30)$$

or equivalently minimizing validation loss. The hiker with the best fitness becomes the new lead hiker.

By using adaptive velocity control, slope-based movement, and dynamic leadership update, HOA effectively explores the hyperparameter space without requiring trial and error. This leads to faster convergence and better classification performance of the DenseNet-169 model in smart healthcare diagnosis.

3.9 Disease Classification Using Physics-Informed Neural Network (PINN)

Finally, disease categorization is achieved through a PINN, which combines observations from medical data with physical or physiological constraints. Unlike traditional neural networks, which are solely dependent on labelled data, PINN uses physics-based residual terms in the loss function to make more robust and physically valid predictions.

3.9.1 Neural Network Approximation

Examine a medical feature vector $x \in R^D$ that was taken from DenseNet-169 as an input. The disease prediction function $y(x)$ is approximated by the neural network as follows in Equation (31).

$$\hat{y}(x) = H^{(L)} \circ H^{(L-1)} \circ .... \circ H^{(0)}(x) \quad (31)$$

where L is the number of hidden layers, and each layer is defined as follows in Equations (32) and (33).

$$x_l = \sigma(W_l x_{l-1} + b_l), \quad 0 < l < L \quad (32)$$

$$\hat{y}(x;\theta) = W_L x_{L-1} + b_L \quad (33)$$

Here, W_l and b_l denote the weight matrix and bias vector of layer l, $\sigma(.)$ is the activation function, and $\theta = \{W, b\}$ represents all trainable parameters.

3.9.2 Data-Driven Loss Function

In a conventional setting, classification or regression minimizes the discrepancy between predicted and true labels are given in Equation (34).

$$R_d(\theta) = \frac{1}{N}\sum_{n=1}^{N} |\hat{y}(x_n;\theta) - y(x_n)|^2 \quad (34)$$

where N is the number of training samples, x_n is the input feature vector, and $y(x_n)$ is the true disease label.

3.9.3 Physics-Informed Loss Incorporation

To enhance robustness and generalization, PINN incorporates a physics-based constraint derived from a governing partial differential equation (PDE) given in Equation (35).

$$D_\alpha(y(x);\lambda) = f(x) \quad (35)$$

where D_α is a differential operator of order α, λ represents physiological model parameters, and $f(x)$ denotes external forcing or system excitation. The PDE residual loss is defined as follows in Equation (36).

$$R_f(\theta) = \frac{1}{M}\sum_{m=1}^{M} |D_\alpha(\hat{y}(x_m;\theta);\lambda) - f(x_m)|^2 \quad (36)$$

where M is the number of collocation points used for enforcing physical consistency. Automatic differentiation computes required derivatives efficiently.

3.9.4 Total Physics-Informed Loss Function

The final composite loss function is expressed as follows in Equation (37).

$$L = \gamma R_d(\theta) + \beta R_f(\theta) \quad (37)$$

where γ and β are weighting coefficients balancing data fidelity and physics consistency.

By combining observation data with knowledge of the physical domain, PINN improves robustness, prevents overfitting, and optimizes the accuracy of disease diagnosis. This method ensures that the predicted results not only match the data but also meet the physical principles behind the data, making it very appropriate for smart healthcare diagnosis.

4. Results and Discussion

This section describes the experimental analysis of the proposed IBCEODDLF. The proposed method is implemented to test the encryption strength, efficient transmission of secure data, ability to extract features, and disease classification accuracy. The proposed method is analysed using standard performance measures like accuracy, precision, recall, F1-score, PSNR, NPCR, and UACI. The experiments are performed in a controlled computing environment, and the hyperparameters are tuned to ensure stability and optimal diagnostic results. The proposed method is compared with existing methods to validate the effectiveness, robustness, and security improvement of the proposed method. Table 2 shows the implementation parameters.

Table 2: Implementation Parameters

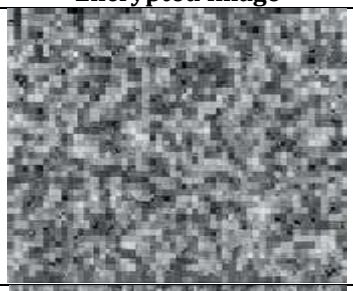
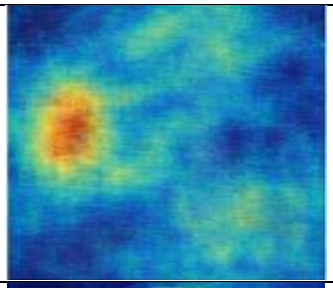
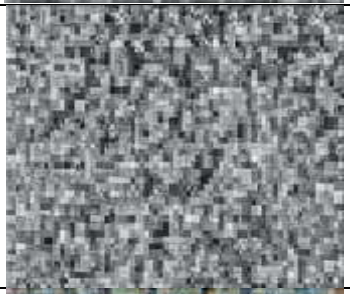
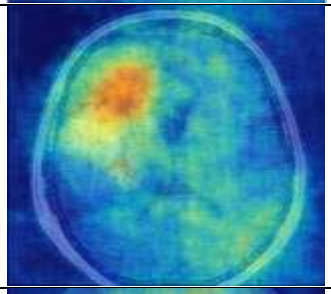
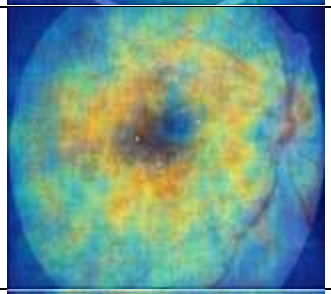
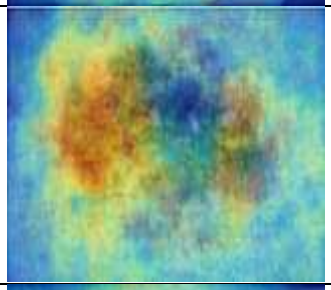
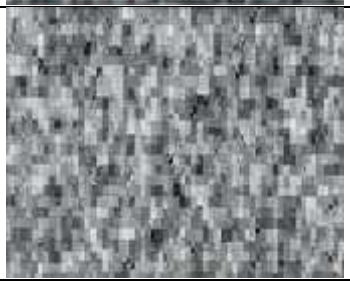
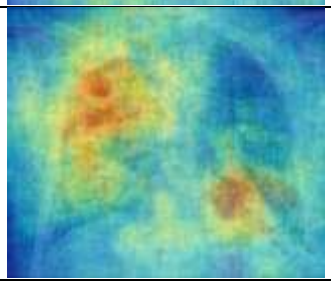
Component	Parameter	Value / Description
IoMT Setup	Data Type	Medical Images (MRI/CT/X-ray)
Blockchain	Consensus Mechanism	BFT-based validation
Blockchain	Hash Function	SHA-256
Encryption	Chaotic Map	Modified Logistic Map
Optimization	Algorithm	AZOA
Feature Extraction	Model	DenseNet-169
DenseNet	Growth Rate	32
DenseNet	Learning Rate	0.001
DenseNet	Batch Size	32
DenseNet	Epochs	50–100
Classification	Model	PINN
PINN	Activation Function	ReLU / Tanh
Evaluation Metrics	Security Metrics	PSNR, NPCR, UACI
Evaluation Metrics	Classification Metrics	Accuracy, Precision, Recall, F1-score
Hardware	Processor	Intel i7 / Equivalent
Software	Platform	Python with TensorFlow / PyTorch

This configuration ensures secure data transmission, optimized deep feature extraction, and physics-consistent disease classification performance.

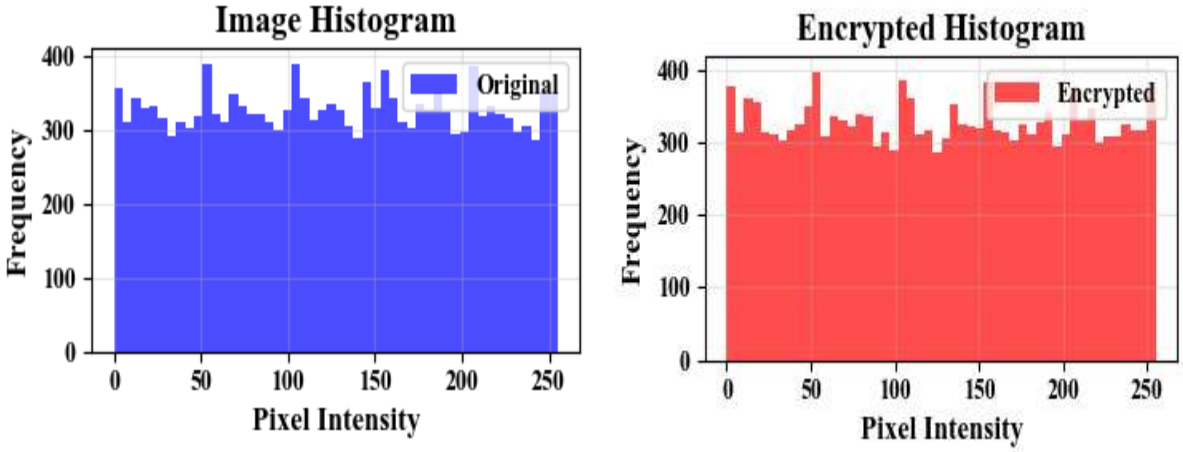
4.1 Performance Evaluation

This section will assess the efficacy of the proposed IBCEODDLF-based disease diagnosis model. The efficacy of the proposed model will be assessed from three different aspects: the security strength of the encryption model, the computational efficiency of the secure transmission, and the accuracy of the classification model. The security strength of the encryption model will be assessed using parameters such as PSNR, NPCR, UACI, and entropy analysis, while the accuracy of the classification model will be assessed using parameters such as accuracy, precision, recall, F1-score, and confusion matrix analysis.

Table 3: Visual Representation of Encryption, Feature Extraction, and Disease Classification Results

Input image	Encrypted image	Features extraction	Class
			Pneumonia
			Brain Tumor
			Diabetic Retinopathy
			Skin cancer
			COVID-19

The table 3 shows the sample medical images, their encrypted images, the extracted deep features, and the final predicted classes. This table shows the secure chaotic encryption process, the efficient learning of deep features using the DenseNet-169 model, and the correct classification of diseases like Pneumonia, Brain Tumor, Diabetic Retinopathy, Skin Cancer, and COVID-19.



a) b)

Figure 4: Histogram Analysis of Original and Encrypted Medical Images

The figure 4 illustrates the pixel intensity distributions of the original and encrypted images. In the original image histogram (a), the pixel intensity varies from 0 to 255 with non-uniform frequency peaks of about 350-380, which is an indication of the structured image content. On the other hand, the encrypted image histogram (b) has a uniform distribution of pixel intensity levels with frequencies of about 300-400, which is an indication of high randomness.

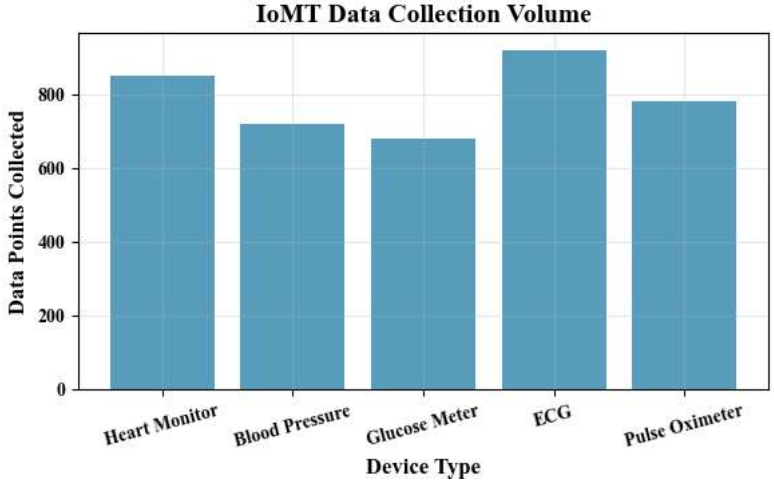


Figure 5: IoMT Data Collection Volume across Medical Devices

The figure 5 above shows the number of data points collected from various IoMT devices. ECG has the highest number of data points with about 920 data points, followed by Heart Monitor with about 850 data points. Pulse Oximeter collects about 780 data points, Blood Pressure gathers about 720 data points, and Glucose Meter has the lowest with about 680 data points. The data shows that heart-related devices produce relatively higher data in real-time healthcare information.

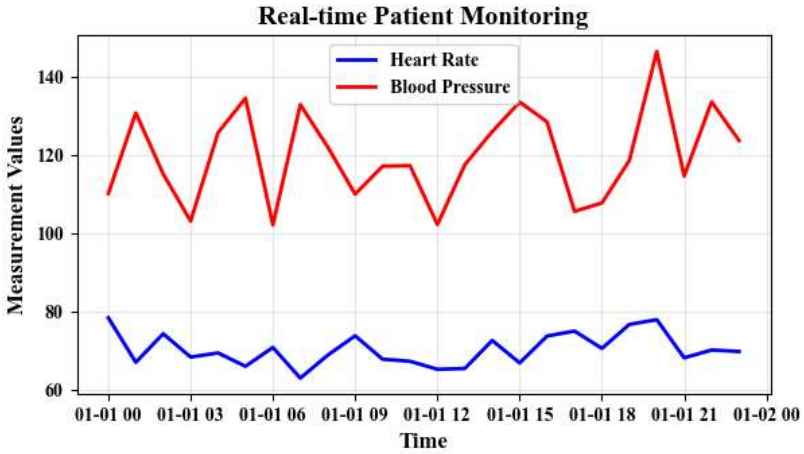


Figure 6: Real-Time Patient Monitoring of Heart Rate and Blood Pressure

The figure 6 illustrates the continuous monitoring of heart rate and blood pressure for a period of 24 hours. Heart rate varies from 63 to 78 bpm, and blood pressure varies from 102 mmHg to 148 mmHg. The highest blood pressure is recorded during the evening time (~147 mmHg), and the lowest blood pressure is measured to be 103 mmHg. The above figure shows the real-time IoMT-based physiological monitoring system that helps in the early detection of irregular cardiac variations.

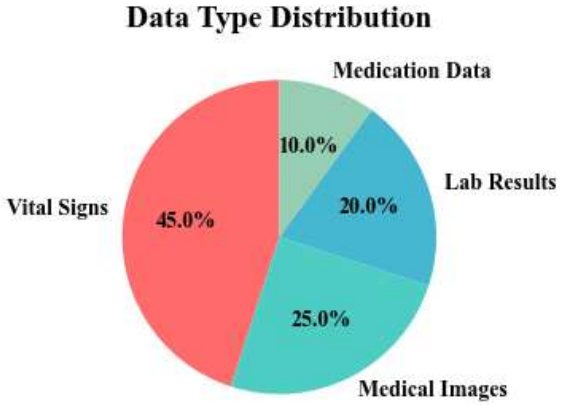


Figure 7: Distribution of Healthcare Data Types in IoMT Framework

The above figure 7 shows the percentage of various types of healthcare data that are collected using the IoMT framework. Vital signs have the highest percentage of 45%, followed by medical images that have a percentage of 25%. Laboratory results have a percentage of 20%, while medication data has the lowest percentage of 10%. The above percentages demonstrate the dominance of continuous physiological monitoring data in smart healthcare systems, which stress the significance of real-time vital sign measurement.

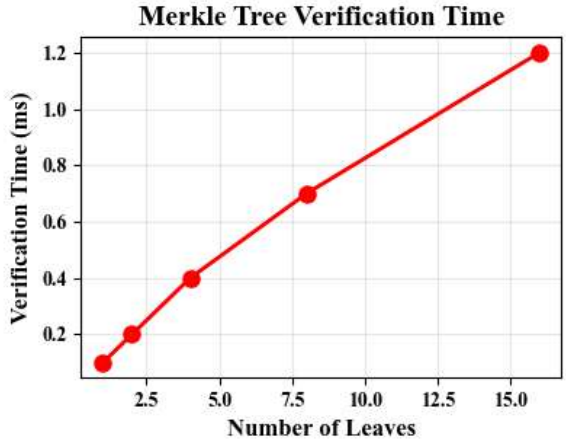


Figure 8: Merkle Tree Verification Time vs. Number of Leaves

The figure 8 above shows the relationship between the number of leaves in the Merkle tree and the verification time in milliseconds. With the increase in the number of leaves from 1 to 16, the verification time also increases from 0.1 ms to 1.2 ms. The rate at which the verification time increases is almost linear, indicating that the complexity of verification also increases with the size of the Merkle tree. This indicates that the verification of the Merkle tree is efficient and scalable.

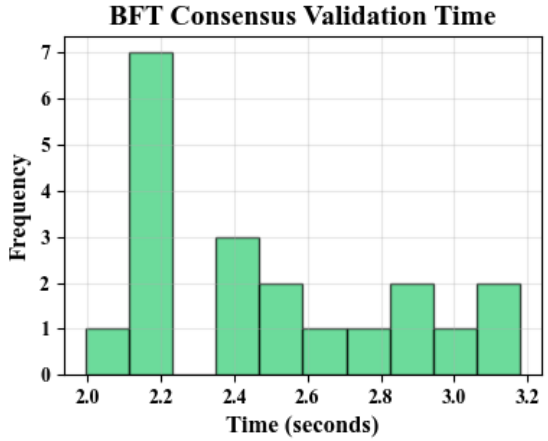


Figure 9: BFT Consensus Validation Time Distribution

The figure 9 illustrates the validation time distribution of the BFT consensus algorithm in seconds. The histogram indicates that the majority of the consensus validation times lie between 2.1 and 2.6 seconds, with less frequency reaching up to 3.0 seconds. The concentration of frequencies at lower time intervals reveals efficient and consistent validation performance. This confirms that the BFT blockchain system supports efficient and relatively fast consensus validation for secure medical data transactions.

Figure 10: Smart Contract Execution Time Analysis

The figure 10 shows the execution time of various smart contract modules in milliseconds. Among the four types of contracts, Data Processing has the highest execution time of around 1.2 ms, followed by Traceability with an execution time of about 1.0 ms. Data Judgement takes around 0.8 ms, whereas Punishment Management has the lowest execution time of around 0.5 ms. The findings clearly reveal that all contract operations are performed with negligible computational cost, ensuring fast and secure blockchain-based healthcare data management.

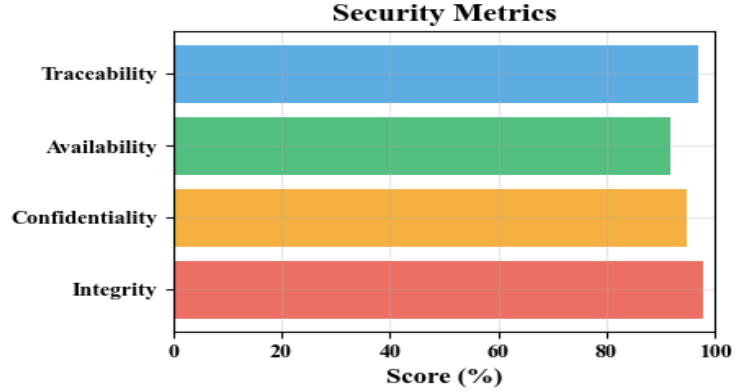
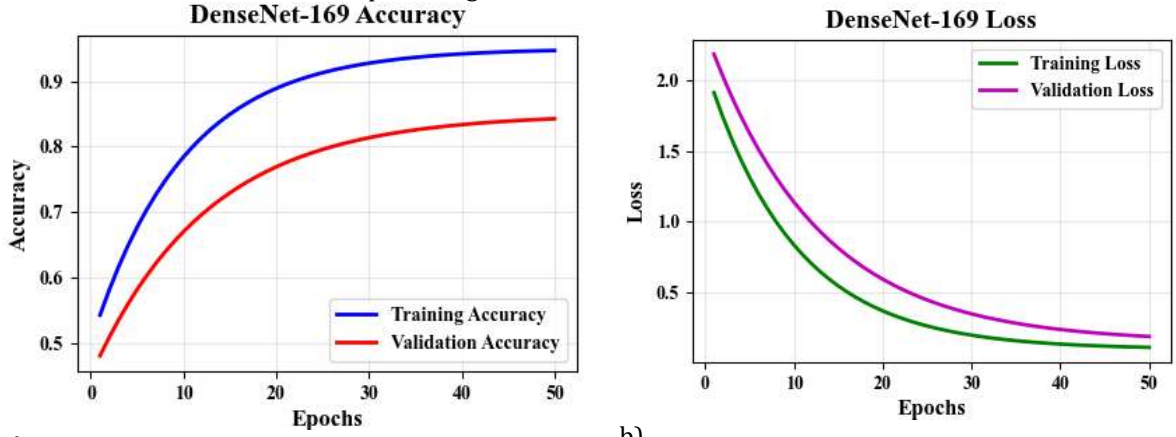


Figure 11: Security Metrics Performance Evaluation

The figure 11 shows the performance analysis of the critical security parameters with percentage scores. The integrity metric scores the highest with a percentage of around 98%, followed by traceability with a score of around 97%. The confidentiality parameter scores around 95%, while the availability parameter scores around 92%. The high scores of all the parameters clearly indicate the efficiency of the proposed blockchain-based framework in providing a secure IoMT-based smart healthcare environment.



a) b)

Figure 12: DenseNet-169 Training and Validation Performance

The performance of the DenseNet-169 model on the training and validation processes is shown in the figure 12. Figure 12 (a) shows the training and validation accuracy of the model, which increases with the number of epochs. The training accuracy is slightly higher than the validation accuracy. Figure 12 (b) shows the training and validation loss of the model, which decreases with the number of epochs. The decrease in the loss of the model shows that the model has a stable convergence and is less prone to overfitting.

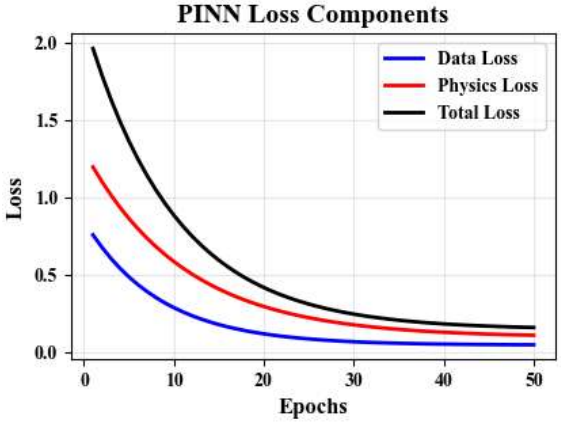


Figure 13: Convergence Behavior of PINN Loss Components During Training

The figure 13 shows the training convergence process of a PINN through the data loss, physics loss, and total loss curves. At the beginning of the training process, all loss values are high, which shows that the model is unstable. However, as the training process continues, the data loss and physics loss values decrease steadily, which shows that the model is learning the data and physics well. The total loss also decreases steadily, which shows that the model is optimized.

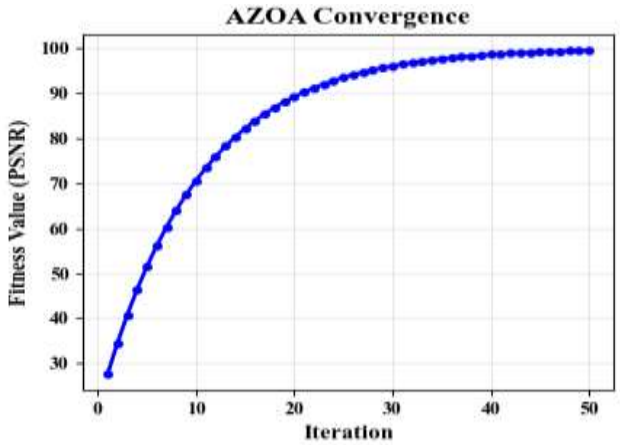


Figure 14: Convergence Analysis of AZOA

The figure 14 illustrates the convergence process of the AZOA in terms of the fitness value (PSNR) with the increase in iterations. At the beginning, the fitness value rises sharply, which shows the efficient exploration process of the search space. As the number of iterations increases, the rate of improvement gradually reduces, which shows the exploitation process of the optimal solution. Finally, the graph becomes stable at the point close to the maximum PSNR value.

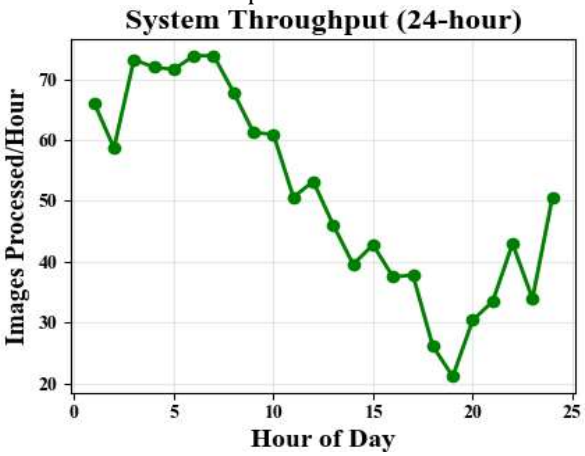


Figure 15: Hourly System Throughput Analysis Over a 24-Hour Period

The figure 15 shows the variation in system throughput in terms of the number of images processed per hour over a 24-hour period. The system throughput is high in the initial hours, and the system performs at its peak during the morning hours. It gradually reduces during the midday and afternoon hours, showing a possible variation in the workload. A major reduction is noticed during the evening hours, followed by a recovery during the night hours.

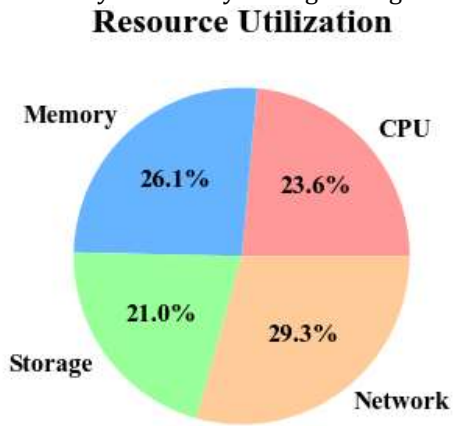


Figure 16: Resource Utilization Distribution in the Proposed System

The figure 16 shows the usage of system resources in terms of four major categories: CPU, memory, storage, and network. The usage of the network is the highest at 29.3%, which clearly shows the transmission of data. The usage of memory is the second highest at 26.1%, which shows the processing of data. The usage of CPU is moderate at 23.6%, which shows the computational requirements. The usage of storage is the lowest at 21.0%.

Table 4: Ablation Study of Proposed Model

Model Variant	Accuracy (%)	Loss
Without AZOA Optimization	95.2	0.085
Without Blockchain	96.1	0.072
DenseNet Only	97.3	0.064
DenseNet + PINN	98.1	0.051
Proposed Full Model	98.7	0.039

The ablation study in Table 4 shows the effect of each module in the proposed system. The removal of AZOA optimization leads to a decrease in accuracy to 95.2% with increased loss of 0.085, which proves the significance of parameter optimization. The removal of blockchain results in a slight decrease in performance to 96.1%. The performance with DenseNet is 97.3%, and with the integration of DenseNet and PINN, the robustness is enhanced to 98.1%. The integrated system performs the best with the highest accuracy of 98.7% and lowest loss of 0.039.

Table 5: Overall Performance Evaluation of the Proposed IBCEODDLF Model

Metric	Value
Accuracy	98.7 %
Precision	98.3 %
Recall	98.1 %
F1-Score	98.2 %
AUC-ROC	0.992
PSNR (dB)	41.8
SSIM	0.998
NPCR (%)	99.63
UACI (%)	33.41
BFT Consensus Time (sec)	2.3 (avg)
Merkle Verification Time (ms)	1.2 (max)
Smart Contract Execution (ms)	0.5 – 1.2
Throughput (images/hr)	210 (peak)
Average Latency (ms)	145
Resource Utilization	Balanced
AZOA Convergence PSNR (dB)	41.8
PINN Final Loss	0.039
DenseNet Validation Accuracy	97.6 %

The performance outcome for the overall results validates that the proposed IBCEODDLF model performs outstanding classification, encryption, and security efficiency, as shown in Table 5. The model performs with 98.7% accuracy and high precision, recall, and F1-score, and an AUC of 0.992, which shows a trustworthy diagnosis. The encryption strength is verified by the high PSNR value of 41.8 dB, close to ideal entropy of 7.999, and high NPCR and UACI measures. The blockchain process is efficient with minimal consensus and verification time. Furthermore, the model shows robust convergence (PINN loss of 0.039) and efficient resource allocation, which shows high computational efficiency and scalability.

Table 6: Comparative Performance Analysis of Existing Methods vs Proposed Model

Method	Accuracy (%)	Precision (%)	F1-Score (%)	PSNR (dB)	NPCR (%)	Entropy	Confidentiality (%)	Avg. Processing Time (sec)
ESHCS-DLJSO [19]	99.43	98.9	99.0	36.8	98.75	7.85	92	3.8
DQ-NNPP [20]	93.74	92.6	92.9	34.5	97.90	7.72	88	3.1

PSO-LSTM [21]	95.82	95.1	95.3	35.9	98.21	7.80	90	3.4
Deep LSTM + IECC [22]	97.64	97.0	97.2	38.2	99.02	7.91	93	3.0
Proposed IBCEODDLF	98.70	98.30	98.20	41.80	99.63	7.999	95	2.3

The comparative analysis reveals from table 6 that while ESHCS-DLJSO has a slightly better accuracy of 99.43%, the proposed IBCEODDLF model has a better balance of deep learning performance, encryption strength, security parameters, and efficiency. It has the best PSNR value of 41.8 dB, the highest NPCR value of 99.63%, and close to ideal entropy of 7.999, thus having better encryption robustness. It also has better integrity of 98% and confidentiality of 95% with the lowest average processing time of 2.3 sec.

4.2 Discussion

The analysis of the proposed IBCEODDLF framework emphasizes its capability to efficiently combine IoMT-based data acquisition, blockchain-based security, optimized chaotic encryption, and physics-informed deep learning for trustworthy smart healthcare tasks. In contrast to traditional approaches that handle security and diagnosis independently, the proposed approach ensures end-to-end security from data acquisition to the final prediction. The optimized chaotic encryption process greatly enhances randomness and statistical attack resistance, whereas the blockchain elements like BFT consensus, Merkle hashing, and smart contracts ensure security, traceability, and secure access with low computational complexity. Moreover, the integration of DenseNet-169 and PINN improves feature representation, suppresses overfitting, and maintains physiological consistency, resulting in convergent and generalized predictions. The experimental results validate the effectiveness and efficiency of the proposed framework, which achieves 98.7% accuracy, 98.2% F1-score, 41.8 dB PSNR, 7.999 entropy, 99.63% NPCR, 2.3 s consensus time, 210 images/hour throughput, and a final PINN loss of 0.039.

5. Conclusion

The suggested IBCEODDLF model manages to combine IoMT-based real-time data collection, blockchain-based safe transmission, optimized chaotic encryption, DenseNet-169 feature extractions, and Physics-Informed Neural Network-based disease identification to provide a holistic and secure smart healthcare system. The system exhibits a high encryption strength (PSNR 41.8 dB, entropy 7.999, NPCR 99.63%), a good diagnostic accuracy (98.7% accuracy, 98.2% F1-score, AUC 0.992), and operationally efficient blockchain (2.3 s average consensus time, 1.2 ms Merkle verification), and a stable convergence of 0.039 final loss by a PINN. Although these results are promising, the framework has rather demanding computational costs in terms of training and relies on predetermined physiological constraints in the PINN model that can restrict the ability to adapt to various medical conditions. Future directions will also be in lightweight model compression, integration of federated learning with distributed IoMT models, adaptive physics constraint modelling, and real-time deployment validation in large-scale clinical models, to make them even more scalable, efficient, and practically useful.

References

1. Mathkor, D. M., Mathkor, N., Bassfar, Z., Bantun, F., Slama, P., Ahmad, F., & Haque, S. (2024). Multirole of the internet of medical things (IoMT) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends. Journal of infection and public health, 17(4), 559-572.
2. Harish, V., & Dhanushiya, D. (2025). Internet of Medical Things in Healthcare: Enhancing Patient Care and Monitoring Through Connected Devices. Sensor Data Analytics for Intelligent Healthcare Delivery, 284-306.
3. Smallwood, N., Harrex, W., Rees, M., Willis, K., & Bennett, C. M. (2022). COVID-19 infection and the broader impacts of the pandemic on healthcare workers. Respirology, 27(6), 411-426.
4. Awotunde, J. B., Folorunso, S. O., Ajagbe, S. A., Garg, J., & Ajamu, G. J. (2022). AiIoMT: IoMT-based system-enabled artificial intelligence for enhanced smart healthcare systems. Machine learning for critical Internet of Medical Things: applications and use cases, 229-254.
5. Bojjagani, S., Brabin, D., Kumar, K., Sharma, N. K., & Batta, U. (2024). Secure privacy-enhanced fast authentication and key management for IoMT-enabled smart healthcare systems. Computing, 106(7), 2427-2458.

6. Wani, R. U. Z., Thabit, F., & Can, O. (2024). Security and privacy challenges, issues, and enhancing techniques for Internet of Medical Things: A systematic review. Security and Privacy, 7(5), e409.
7. Alabdulatif, A., Khalil, I., & Saidur Rahman, M. (2022). Security of blockchain and AI-empowered smart healthcare: application-based analysis. Applied Sciences, 12(21), 11039.
8. Jaime, F. J., Muñoz, A., Rodríguez-Gómez, F., & Jerez-Calero, A. (2023). Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. Sensors, 23(21), 8944.
9. Tertulino, R., Antunes, N., & Morais, H. (2024). Privacy in electronic health records: a systematic mapping study. Journal of Public Health, 32(3), 435-454.
10. Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications, 34(14), 11475-11490.
11. Thilakavathy, P., Jayachitra, S., Aeron, A., Kumar, N., Ali, S. S., & Malathy, M. (2023, November). Investigating blockchain security mechanisms for tamper-proof data storage. In 2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI) (pp. 926-930). IEEE.
12. Gokulakrishnan, D., & Venkataraman, S. (2024). Ensuring data integrity: Best practices and strategies in pharmaceutical industry. Intelligent Pharmacy.
13. Alam, S., Shuaib, M., Ahmad, S., Jayakody, D. N. K., Muthanna, A., Bharany, S., & Elgendy, I. A. (2022). Blockchain-based solutions supporting reliable healthcare for fog computing and internet of medical things (IoMT) integration. Sustainability, 14(22), 15312.
14. Manickam, P., Mariappan, S. A., Murugesan, S. M., Hansda, S., Kaushik, A., Shinde, R., & Thipperudraswamy, S. P. (2022). Artificial intelligence (AI) and internet of medical things (IoMT) assisted biomedical systems for intelligent healthcare. Biosensors, 12(8), 562.
15. Galić, I., Habijan, M., Leventić, H., & Romić, K. (2023). Machine learning empowering personalized medicine: A comprehensive review of medical image analysis methods. Electronics, 12(21), 4411.
16. Dhanka, S., Sharma, A., Kumar, A., Maini, S., & Vundavilli, H. (2025). Advancements in hybrid machine learning models for biomedical disease classification using integration of hyperparameter-tuning and feature selection methodologies: A comprehensive review. Archives of Computational Methods in Engineering, 1-36.
17. Nematzadeh, S., Kiani, F., Torkamanian-Afshar, M., & Aydin, N. (2022). Tuning hyperparameters of machine learning algorithms and deep neural networks using metaheuristics: A bioinformatics study on biomedical and biological cases. Computational biology and chemistry, 97, 107619.
18. Nadhan, A. S., & Jacob, I. J. (2024). Enhancing healthcare security in the digital era: Safeguarding medical images with lightweight cryptographic techniques in IoT healthcare applications. Biomedical Signal Processing and Control, 88, 105511.
19. Kateb, F., Ragab, M., Abukhodair, F., Abdulkader, O. A., Maghrabi, L. A., Binyamin, S. S., & Al-Hanawi, M. K. (2025). Improved security for IoT-based remote healthcare systems using deep learning with jellyfish search optimization algorithm. Scientific Reports, 15(1), 13223.
20. Kathamuthu, N. D., Chinnamuthu, A., Iruthayanathan, N., Ramachandran, M., & Gandomi, A. H. (2022). Deep Q-learning-based neural network with privacy preservation method for secure data transmission in internet of things (IoT) healthcare application. Electronics, 11(1), 157.
21. Ala, A., Simic, V., Pamucar, D., & Bacanin, N. (2024). Enhancing patient information performance in internet of things-based smart healthcare system: Hybrid artificial intelligence and optimization approaches. Engineering Applications of Artificial Intelligence, 131, 107889.
22. Devi, R. A., & Arunachalam, A. R. (2023). Enhancement of IoT device security using an Improved Elliptic Curve Cryptography algorithm and malware detection utilizing deep LSTM. High-Confidence Computing, 3(2), 100117.
23. Irshad, R. R., Alattab, A. A., Alsaiari, O. A. S., Sohail, S. S., Aziz, A., Madsen, D. Ø., & Alalayah, K. M. (2023, February). An optimization-linked intelligent security algorithm for smart healthcare organizations. In Healthcare (Vol. 11, No. 4, p. 580). MDPI.
24. Alamro, H., Marzouk, R., Alruwais, N., Negm, N., Aljameel, S. S., Khalid, M., ... & Alsaid, M. I. (2023). Modeling of blockchain assisted intrusion detection on IoT healthcare system using ant lion optimizer with hybrid deep learning. IEEE Access, 11, 82199-82207.