Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.028850
Article

Tech Science Press

Secured Cyber Security Algorithm for Healthcare System Using Blockchain Technology

D. Doreen Hephzibah Miriam[1], Deepak Dahiya[2], Nitin[3] and C. R. Rene Robin[4,*]

[1]Computational Intelligence Research Foundation (CIRF), Chennai, 600 023, Tamilnadu, India
[2]College of Computer and Information Sciences, Majmaah University, Majmaah, 11952, Saudi Arabia
[3]Department of Electrical Engineering and Computer Science, College of Engineering and Applied Science, University of Cincinnati, Cincinnati, 45221, OH, United States
[4]Department of Computer Science and Engineering, Sri Sairam Engineering College, Chennai, 600 044, Tamilnadu, India
*Corresponding Author: C. R. Rene Robin. Email: crrenerobincirf@gmail.com
Received: 19 February 2022; Accepted: 29 March 2022

Abstract: Blockchain technology is critical in cyber security. The most recent cryptographic strategies may be hacked as efforts are made to build massive electronic circuits. Because of the ethical and legal implications of a patient's medical data, cyber security is a critical and challenging problem in healthcare. The image secrecy is highly vulnerable to various types of attacks. As a result, designing a cyber security model for healthcare applications necessitates extra caution in terms of data protection. To resolve this issue, this paper proposes a Lionized Golden Eagle based Homomorphic Elapid Security (LGE-HES) algorithm for the cybersecurity of blockchain in healthcare networks. The blockchain algorithm preserves the security of the medical image by performing hash function. The execution of this research is carried out by MATLAB software. The suggested framework was tested utilizing Computed Tumor (CT) pictures and MRI image datasets, and the simulation results revealed the proposed model's profound implications. During the simulation, 94.9% of malicious communications were recognized and identified effectively, according to the total outcomes statistics. The suggested model's performance is also compared to that of standard approaches in terms of Root Mean Square Error (RMSE), Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), time complexity, and other factors.

Keywords: Healthcare system; cybersecurity; security; data sharing; blockchain

1 Introduction

In recent times, due to the huge development of the bitcoin system, block chain technology usage is highly improved and gathered more attention [1]. Block chain technology is performed based on the cryptography linked techniques to create various linked information blocks and each block is enclosed with the significant data to verify its authority and to create the subsequent blocks [2]. Moreover, block chain is worked as a distributed database because of this condition; it attains important features such as privacy protection, non-tamperability, and decentralization that are helped to secure data sharing [3].

Also, it contributes data integrity and transparency to the information system thus it is applied in various significant applications such as identity management, game systems, industries, supply chains, tracing food, etc [4]. Furthermore, the extensive development of block chain technology is widely used in power industries, the internet of vehicles, and medical care [5]. Block chain in the health care system is carried out a supreme transformation is happened. Normally, the patient data is straightforward but sometimes this will be more complicated to manage the unstructured data of patients [6]. This medical data is gathered from various users and it is accessed or manipulated for significant usage via different users. Due to the critical importance, the data of patients should be carried out as secured, reliability and protected [7]. Thus, the recent blockchain technology execution is considered for the access of entire data regulation, transaction, and storage [8]. However, it has carried out transaction numbers, block or address numbers. Thus, secured data sharing is a major challenge because the security of medical images stored in digital media is important [9,10]. The medical images have been large in size as well as number. Cybersecurity encloses robbing patient data, electronic health records, medical components, Ransomware attacks, and hospital infrastructure [11,12]. Consequently, blockchain system has certain characteristic issues while it is utilized to support a huge amount of customers which are creating a huge size of data like from the Internet of Things (IoT) [13]. Because a huge amount of users can slow the processing speed of the system and this leads to an authentication and scalability problem in blockchain [14]. Different types of methods are used in the cybersecurity system such as deep belief network along with ResNet [15], Convolutional Neural Network (CNN) [16], Fuzzy computing [17], Ring verification method [18], Elliptic Curve Integrated Encryption Scheme (ECIES) [19], etc. Recently, meta-heuristic optimization plays an important role in cybersecurity improvement such as African Buffalo Optimization (ABO) [20], Whale optimization [21], Ant lion optimization (ALO) [22], Improved Particle Swarm Optimization (IPSO) [23], Genetic algorithm (GA) [24] and so on. The conventional healthcare systems demonstrate weak security and privacy protection subject to malicious attacks [25]. For this reason, high secured and improved encryption methods are essential in healthcare applications. Also, the conventional methods have achieved a high amount of latency and computational complexity is more. To overcome the issues of cybersecurity, this research introduces a novel security improvement method with blockchain-based data sharing in the healthcare system. Here, the Lionized Golden Eagle based Homomorphic Elapid Security (LGE-HES) algorithm is proposed for the cybersecurity of blockchain in healthcare networks. The experimental execution of the proposed framework takes place using the Computed Tumor (CT) images, MRI images datasets and the simulation results pointed out the significant consequences of the pro-posed model. The structure of this article is articulated as follows: The state of the works related to this work cybersecurity for blockchain technology is explained in Section 2. The system model with problem statement is detailed in Section 3. In Section 4, the proposed framework of security improvement in the blockchain model for the healthcare system is described. The results and comparative analysis are carried out in Section 5.

2 Literature Review

Several recent publications pertaining to this research are as follows: The Internet of Things-based medical system is critical for disease diagnosis, patient health monitoring, and drug prescribing in a real-time manner. However, maintaining the confidentiality of patient records is a significant concern. As a result, Ogundokun, Roseline Oluwaseun, and colleagues G. N. Nguyen and et al. [26] developed the Crypto-Stegno framework, a security paradigm for IoT-based medical environments. Patients' healthcare and pertinent medical data are validated in terms of security, severe data loss, and supreme embedding capability. However, due to the lack of learning parameters, this strategy is inapplicable to blockchain security systems. Additionally, Abdellatif, Alaa Awad, and colleagues G. Kalyani and et al. [27] developed a health strategy dubbed a smart and secure healthcare system built on blockchain-based

medical technology for rapid emergency response and remote monitoring of patients. This established methodology ensures the security of healthcare data transmission between indigenous healthcare providers and multinational providers. The proposed design of the blockchain system, in particular, improves data transfer for medical care and a variety of other types of Quality of services (QoS). Nonetheless, the application of blockchain technology in medical care has been confirmed across several sectors. Cybersecurity is a significant barrier to data transfer and remote monitoring in the healthcare system. Pandey et al. [28] addressed this issue by developing a blockchain-based security architecture based on the deep belief network (DBN) and residual network (ResNet) models. The presented approach collects data via sensor devices and uses a DBN model to detect intrusions. Additionally, the suggested methodology makes use of the MSC concept to generate many copies of the collected image, which ensures privacy and security. Additionally, blockchain technology is employed to ensure safe data transmission to the cloud server, which detects sickness presence using a residual network (ResNet)-based categorization algorithm. Veeramakali et al. [29] have created a novel cryptographic-based IoT security authentication approach for blockchain security. The crucial data associated with the Internet of Things is protected in this study through the use of high-reliability Optimal Homomorphic Encryption (OHE). To categorise sensitive data from the IoT dataset, the Deep Learning Neural Network (DNN) structure is used. After categorization, OHE encrypts and decrypts sensitive data. During encryption, the key is authenticated, and the optimal key is chosen using the Step size FireFly (SFF) optimization method. Healthcare data is critical for a variety of reasons, including policy formulation, clinical management, and diagnostic medicine. A blockchain is a decentralised and distributed system that makes use of trustworthy cryptography techniques. Thus, Abd El-Latif et al. [30] demonstrated a highly secure blockchain-based architecture optimised for e-healthcare applications. Serrano [31] proposed the optimal deep-learning-based secure blockchain-enabled intelligent IoT and healthcare diagnosis paradigm. The ODLSB technique employs the orthogonal particle swarm optimization (OPSO) algorithm for the covert exchange of medical photographs. Additionally, the hash value is encrypted using the neighbourhood indexing sequence (NIS) approach. Finally, the optimum deep neural network (ODNN) is employed as a classification model to identify illnesses. Blockchain technology is crucial for cybersecurity. The majority of current cryptography schemes could be cracked as a result of efforts to construct large-scale quantum computers. Quantum walks may be utilised as a quantum-inspired paradigm to develop novel cryptographic algorithms. As a result, Cao et al. [32] offer a novel authentication and encryption system based on quantum-inspired quantum walks (QIQW). The proposed protocol is being used to lay the groundwork for a blockchain-based infrastructure for secure data transit between IoT devices. Additionally, it can guard against message interception and impersonation attempts, enabling the secure transport of data between IoT devices. New Big Data-driven Smart City applications will leverage 5G as the mobile network operator, eliminating the need for additional commercial infrastructure or cellular services. Cyber attackers will be given new digital aims, and independent providers will share mobile network technology, particularly access channel technology. Shankar et al., Will [33] introduced the Blockchain Random Neural Network for Cybersecurity Activities to address these cybersecurity concerns as part of a full physical and digital cybersecurity client and route authentication method. Private Blockchains that feature decentralisation, adaptable protocols, and solid confidentiality can be utilised in industrial IoT to analyse massive volumes of data while resolving security concerns. However, the endurance of blockchain technology constrains the functionality of industrial IoT. As a result, Mathews et al. [34] proposed an improved optimization technique for Two Arch2 that maximises scalability and decentralisation while minimising blockchain time and cost. The experimental results indicate that the proposed strategy is capable of optimising four model indicators satisfactorily. The majority of papers featured theoretical research, such as an architecture, a framework, or a model for usage in EHR administration [35], as well as blockchain applications. Additionally, technical details concerning the blockchain fundamentals used are omitted, such as blockchain type, consent procedure, platform, and

smart contract development. Blockchain technology is still in its infancy, particularly in healthcare, according to the literature. Simultaneously, interest in blockchain technology and its application to data management in healthcare is increasing. It is still possible to discover and explore new and more efficient strategies for administering electronic health records with this basic technology.

2.1 System Model and Problem Statement

A healthcare system is composed of numerous organisations, individuals, and actions with the primary objective of monitoring [36], promoting, and sustaining people's health. Examples include private clinics, pharmaceutical firms, hospitals, healthcare companies, workplace health and safety standards, and the ministry of health. Efficient e-health networks must respond rapidly, while maintaining a high level of service and security for the entire community, while also supporting disease prevention and cost management. To accomplish this, critical problems must be appropriately addressed.

3 Proposed Framework

The primary objective of this research is to develop a peer-to-peer image data transmission system using block chain technology that protects the secrecy, security, and validity of medical images. Fig. 1 illustrates the proposed structure for a security-enhanced blockchain method in the healthcare system. To begin, typical medical images are evaluated for the security procedure, which includes encryption and decryption; a technique based on the LGE-HES algorithm is proposed here. The objective of optimal key selection in a security programme is to select the most appropriate private and public keys for transmission and reception. After the photographs are encrypted, they are uploaded to the cloud or another suitable location, and the image decryption process uses the best feasible private key. After encrypting the photographs, they are uploaded to the cloud or another suitable location, the eagle optimization objective function is used, and the resulting framework is executed in MATLAB Version 2021a.

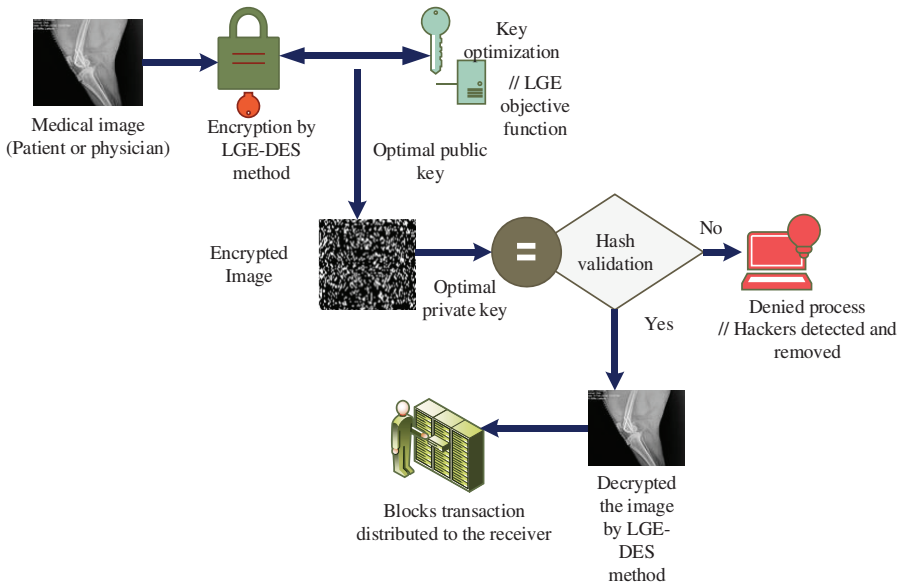


Figure 1: Proposed model of security improvement in blockchain technology for healthcare system

3.1 Optimal LGE-HES Method For Securing Healthcare Data

The proposed method is a hybrid of the LGE and HES techniques. In this case, the HES is used for both encryption and decryption; the LGE is used for optimal key selection and attack identification. The suggested methodology comprises several stages, including key generation and optimal key selection, encryption, verification, attack analysis, and decryption [37]. The suggested LGE-HES approach with the finest key selected provides a high level of security for transmitting medical messages containing previously encoded data. The block chain contains a hash function, transaction timestamps, iterations, and previous hashes.

3.1.1 Key Generation

While medical data re transferred via block chain it stores as each suitable blocks. Here, a novel security method is utilized to secure the events and storage of medical data. A key is the main component in the security purpose for encryption and decryption. In key generation functions takes place two kinds of key public and private key. The medical data are encrypted by public key (K_u) and decryption process is carried out by private key (K_u). The HES model is worked on different phases and each block size is 128 bits. Also, the proposed method can try to encrypt the plain image of 128 bits into acipher image of 128 bits under the control of 33 sub keys $(K_0 \ldots K_{32})$. The public key is expressed in Eq. (1)

$$K_u = (x, g) \tag{1}$$

where, $x = q.w$ for instance q and w are the two massive prime numbers and the integer modulus of the public key is articulated as G.C.D $[q.w(q-1) \times (w-1)] = 1 : h \in Y_{m^2}$. The private key is evaluated using Eq. (2) as,

$$K_r = (p, \beta) \tag{2}$$

where $p = L.C.M(q-1, w-1)$ and $\beta = (w^p \ modm^2)^{-1} \ modm$. The private key encloses on the data users or the customers particularly provided to them. This includes, the user defined key algorithm of 256 bit cipher. The private key is employed by the data user; every instant new medical data is to be provided thus the hash key verification is required. All users share with all another parameters of public key to works HES for connecting blocks of the chain. The generated key of private parameter is initialized using Eq. (3)

$$K_r = K_{r-8} \oplus (K_{r-7} <<< 1) \oplus (K_{r-6} <<< 2) \oplus (K_{r-5} <<< 3) \oplus (K_{r-1} <<< 4) \oplus H \tag{3}$$

where r is denoted as 0 to 131, $K_{r-8} \ldots K_{r-1}$ is the 256 user-defined key that is divided into 8 forms of 32-bit data to produce 132, the 32-bit data of pre-keys, and also the created pre-keys are combined and acquired as 128 bit. This procedure develops random key so optimal public and private keys are selected using the LGE optimization method. The income data contains missing values for categorical features such as work-class, occupation, country for which we use the imputed function and replace the missing value with the most frequently occurring value.

3.1.2 Authentication of Key by LGE Method

The proposed LGE algorithm is the combination of Lion optimization and Golden eagle optimization. The fitness of hunting and encircling behaviors are considered for the optimal key selection in proposed cybersecurity protocol.

Step 1: Key initialization

Initialize the keys in HES algorithm, prime number and parameters of algorithm. The randomly generated keys are articulated as in Eq. (4)

$$K_j = K_0, K_2 \ldots K_N \tag{4}$$

where $K_j = 1, 2, \ldots . N$ and the overall key quantity is denoted as N.

Step 2: Fitness calculation

The optimal fitness selection is the main concern in the proposed security algorithm. This cybersecurity function assumes the fitness as optimal key selection for each blockchain transaction with the finest solution. The fitness value of each key is estimated by evaluating the objective function using Eq. (5)

$$Fitnessvalueofkey(F_K) = f(optimalkey) = f(K_0, K_2 \ldots K_N) \tag{5}$$

where F_K is the fitness function that contributes optimal key as a finest solution. Each transaction must select a key for the transit and assault operations in the each iteration. The key is modeled as the best solution discovered yet by the flock of data users in the LGE algorithm. Every medical transaction has the ability to remember the greatest remedy it has identified up to this point. Each search agent chooses a target key from the entire flock's storage in the each iteration. After that, each transaction's offensive and transit vectors are determined in relation to the chosen key. The memory is updated if the current location (calculated using key selection procedure) is better than the prior position in the memory. In a medical transaction, the key selection method is crucial. A simple method of selection is for each transaction to choose the key in its own memory. A random one-to-one mapping mechanism is presented to help medical transactions better traverse the network, in which the key for the current iteration is randomly selected from the storage of any other group component. It's important to note that the chosen key is often not the public or private key. Each memory key is tied to a single medical transaction in this method. The strike and transit procedures are then carried out on the selected key by each medical transaction.

Step 3: Key Exploitation

A vector starting at the present position of the data transaction and terminating at the location of the key in the blocks memory may be used to model key exploitation. Then, the Eq. (6) may be used to determine the key exploitation vector for data transaction a as

$$\bar{K}_a \equiv \vec{Y}_{k_n} - \vec{Y}_a \tag{6}$$

where $\bar{K}_a$ is the key exploitation vector of data transaction a, $\vec{Y}_{k_n}$ is the best key stayed so far by block k_n, and $\vec{Y}_a$ is the present transaction position of block a. The exploitation phase of the proposed approach is highlighted by the key vector, which leads the population of data transactions in blocks toward the best frequented sites.

Step 4: Key Exploration : Based on the exploitation phase, the key exploration is computed. Within the tangent hyperplane to the round, the key exploration in n-dimensions is situated. Therefore, initially the tangent hyperplane is estimated for the exploration stage using Eq. (7),

$$h_1 k_1 + h_2 k_2 + \ldots h_m k_m = r \Rightarrow \sum_{i=1}^{m} h_i k_i = r \tag{7}$$

where $h_1, h_2 \ldots h_f$ are the ordinary vector and $k_1, k_2, \ldots k_f$ are the decision key vector of i^{th} node.

Step 4: Key updating: The sharing of the data transaction block comprises of key exploration and exploitation. Thus, the step vector for data transaction a in g^{th} iteration is expressed by Eq. (8),

$$\Delta K_i = r_1\left(c_{K_u}^0 + \frac{g}{G}\left|c_{K_u}^G - c_{K_u}^0\right|\right)\frac{\bar{K}_u}{\left\|\vec{K}_u\right\|} + r_2\left(c_{K_r}^0 - \frac{g}{G}\left|c_{K_r}^G - c_{K_r}^0\right|\right)\frac{\vec{K}_r}{\left\|\vec{K}_r\right\|} \tag{8}$$

where the random vector is in the limit of [0,1] is denoted as r_1 and r_2, $c_{K_u}^0$ and $c_{K_u}^G$ is the initial and final values for public key exploitation inclination in the g[th] iteration, $c_{K_r}^0$ and $c_{K_r}^G$ is the initial and final values for private key exploitation inclination in the g[th] iteration, $\left\|\vec{K}_u\right\|$ and $\left\|\vec{K}_r\right\|$ are the Euclidean distance of exploitation and exploration vector and g is the present iteration.

Step 5: Termination: The position of optimal key in each transaction in g + 1 iteration is estimated by the addition of g iteration step vector. The termination process is executed using Eq. (9) as,

$$k^{g+1} = f^g + \Delta K_i \tag{9}$$

New positions of features that are more fit are stored in memory, and old positions are discarded if the new positions are superior. Unless otherwise specified, the memory is left untouched, but the feature value is relocated to a different location inside the system. This iteration picks a random feature point from the population, calculates strike vector, cruise vector, and ultimately the step vector and new position for the following iteration to circle about its most-visited place. Any of the termination requirements must be met for this loop to continue.

3.1.3 Encryption Using LGE-HES Process

The HES method provides the encryption to the plain medical data to cipher data. The S-box components in the plain and cipher data enhance the uncertainty range. These S-box components are based on the Shannon property's confusion. The group of S-boxes includes with 4 times. Eight separate S-boxes are used in each of the 32 rounds, each mapping 4 input bits to 4 integer values. Each Sbox is utilized exactly 4 times in each round, and it is used 32 times in total. As a result of the bit variation from the input that can change more bits variation in the output, the direct transformation model is supplied to the function, which can improve the effect of an avalanche. The direct transformation input by 4 times of 32 bit words with Y_o, Y_1, Y_2, Y_3 and Y_3 is the most important input of 32 bits. The direct transformation is articulated as subsequently,

$$Y_o, Y_1, Y_2, Y_3 := P_j(x_j \oplus K_j)Y_o := Y_o <<< 13 Y_2 := Y_2 <<< 3 Y_1 := Y_1 \oplus Y_0 \oplus Y_2$$

where left rotation is represented as $<<<$ and left shift is signified as $<<$, x_{j+1} is the input value given to the following round and Y_o, Y_1, Y_2, Y_3 is the 4 times of 32 bit data that is the initial permutation EX-OR results via the optimal key from the user defined key function. The 32-round proposed encryption is explained by the Eq. (10),

$$x_{j+1} = P_j(x_j), j \in \{0, 1, \ldots..31\} \tag{10}$$

$$\begin{aligned} P_j(Y) &= DT(R_j(Y \oplus K_j), j \in \{0, 1, \ldots.31\} \\ P_{31}(Y) &= R_{31}(Y \oplus K_{31}) \oplus K_{31} \end{aligned} \tag{11}$$

DT is the direct transformation and R_j is the S-box application which is 32 times in parallel. Then the encrypted data is stored in the blocks of cloud storage.

3.1.4 Verification Analysis

The blockchain network alerts the destination node that a new transaction requires to be validated, and the recipient then uses the decryption algorithm to decryption using variables specific to the original source. The sender and receiver IDs, as well as the time stamp and encryption data, are the most important parameters

in each transaction. This phase's major goal is to verify a receiving transaction prior sending it over to the next phase (or deleting it), and to ensure that fraudulent activity in the server is quickly found. The hash function and key validation is considered for the security verification. Here, SHA-256 method is contributed for the hash function. The hash matching methods provides the improved security for data transaction in medical care system. Generally, hash operation and key matching is failed means the unauthorized person is try to download the document. Moreover, trust authority provided keys to the data owners and users. The public key is provided to the sender and private key is given to the receiver. The procedure of hash validation for transaction verification. The verification of hash function is validated by the homomorphic property. Consider the hash encrypted data from the data user is expressed as per in Eq. (12)

$$P(x1) = (h^{r1}, h^{x1} * K_j^{r1}) \tag{12}$$

Where, x is the hash data, h is the generator, r is the randomness and K_j is the optimal key. Also, the another hash data for the user is articulated in Eq. (13),

$$P(x2) = (h^{r2}, h^{x2} * K_j^{r2}) \tag{13}$$

In homomorphic validation the condition $P(x1) * P(x2) = P(x1 + x2)$ should be satisfied. Let us verify the hash validation in verification analysis as per subsequent equations.

$$\begin{aligned} P(x1) * P(x2) &= (h^{r1}, h^{x1} * K_j^{r1}) * (h^{r2}, h^{x2} * K_j^{r2}) \\ &= (h^{r1+r2}, h^{x1+x2} * K_j^{r1+r2}) \\ &= P(x1 + x2) \end{aligned} \tag{14}$$

Thus, the homomorphic property is validated and thus, the function is same then only the data transaction is occur in healthcare system.

3.1.5 Attack Avoidance by LGE-HES Method

In each block of transaction, the algorithm looks for an attack in a network to provide security for their information. These attack trackers have particular techniques to encircle the attack and found it. At the time of attack tracking, each block corrects its transaction location depends upon its own location and the location of data in the database. Also, during tracking, the trackers are chosen one after other arbitrarily and selected the attack. The position of attackers is expressed using Eq. (15),

$$\hat{H} = H + r(0, 1) \times k \times (H - T_a) \tag{15}$$

Where H is the present location of attackers, r is the random numbers, T_a is the new location of trackers for tracing attackers and the enhancement percentage of tracking fitness is denoted as k. The new tracking ability of the attack tracing for both left and right parts of the network are expressed using Eq.(16),

$$\hat{T}_a = \begin{cases} r((2 \times H - \hat{T}_a), H), & (2 \times H - \hat{T}_a) < H \\ r(H, (2 \times H - \hat{T}_a)), & (2 \times H - \hat{T}_a) > H \end{cases} \tag{16}$$

The center position of the network is analyzed using Eq. (17)

$$\hat{T}_a = \begin{cases} r(\hat{T}_a, H), & \hat{T}_a < H \\ r(H, \hat{T}_a), & \hat{T}_a) > H \end{cases} \tag{17}$$

Thus, this strategy contributes for optimal solution to track the attack in blockchain network. After tracking the attack the data transaction has been send to the optimal nodes. The success of attack

avoidance if it enhances the finest location of data transaction at the final iteration of the proposed algorithm. Moreover, in blockchain network (B) the success of attack (a) finding at d^{th} iteration is defined by Eq. (18)

$$S(a,d,B) = \begin{cases} 1 & f_{a,B}^{d} < f_{a,B}^{d-1} \\ 0 & f_{a,B}^{d} = f_{a,B}^{d-1} \end{cases} \tag{18}$$

The large amount of successive rate shows the proposed algorithm has converted to a fact that is distant from finest point.

3.1.6 Decryption

The decryption function is the inverse of the encryption function. The cipher data is converted to plain text data using the LGE-HES approach and optimal keys in the reverse order. Each completed transaction (*i.e.*, validated transaction) is considered in the present running block. The suggested approach is then used to link the present block to the preceding block in the chain using private key factors. After then, each system server uploads this new block towards their own blockchain.

4 Results and Discussion

The proposed cybersecurity framework in medical system is implemented using MATLAB 2019a software in windows platform with the 4 GB of RAM and i5 processor. This work is utilized to the compilation of optimization with the security algorithm to execute a sharing of medical image in a secured way. Moreover, certain parameters are validated for the performance analysis of proposed model over the conventional methods such as Root Mean Square Error (RMSE), Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), time complexity, and so on. For this analysis model, different medical images data are considered such as CT images and MRI images. To estimate the effectiveness of the proposed cybersecurity protocol in authentication function, the validation analysis is carried out for the DDoS attack and No-Message attack.

4.1 Case Study

Consider A is the transmit data from patient/physician to the node B (Specialist or health department). Thus, the person A encrypts the medical data using the proposed LGE-HES algorithm and exchanged the optimal key parameters with the receiver node B. Here, A is the data owner and B is the data user. Furthermore, the blockchain network indicates the B_{th} node that there has been a new data transaction that required to be established. Consequently, the data user runs the proposed decryption technique to decrypt the medical data with the key parameters and digital hash validation equivalent to the data owner and validates that the data owner is authenticated or not. If the optimal key is achieved but hash validation is failed then it indicates as the malicious attack and then removed the transmission node. Else if the transaction of data is successfully validated, then the medical transaction is included into the presently operating block.

4.1.1 Data Attack

When data owner sends a transaction of blockchain to data user via a communication network, hackers can interrupt. However, the medical image transaction has been accessed by the hackers by the exact estimation of nodes quality in the blockchain net-work. Also, extract the hash code from data owners and retrieve the cipher image from data users providing each initial key parameter. The initial key parameters of the data owner A and data user B are interchanges in a closed environment conditions. By considering the simulation estimation, the key space and hash value validation is provided and the key stream is 2851 that provides the additional security to the system. Thus, the proposed method of cybersecurity model is secured the blockchain technology in healthcare system against hackers/attacks.

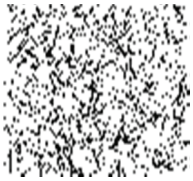
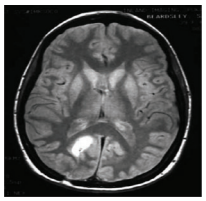
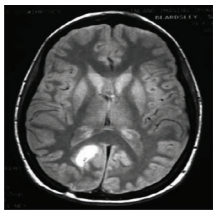
4.1.2 Data Attack Removal

Assume an attacker sends a fraudulent blockchain transaction to deceive a data user into believing it is a genuine transaction from the data owner. When a data user receives a transaction, he or she has no way of knowing if the transaction came from the data owner or the data user. To overcome this problem, the data user must first obtain the hash code 1 and private key from the data owner, as well as the cipher image based on the initial key parameters received with the data owner. He then receives the hash 2 and private key for the recovered plain image and compares it to hash 1 and hash 2, as described in the blockchain framework's verification process. Finally, because of the presence of assaults, this transaction is rejected. As a result, the suggested cybersecurity protocol for blockchain-based healthcare system utilities is safe from no-data attacks.

4.2 Performance Analysis

Consider five sample medical images for the performance analysis of proposed LGE-HES model in healthcare system. The sample medical images cybersecurity improved results are demonstrated in Tab. 1.

Table 1: Medical image cybersecurity results

Sample images	Encrypted	Decrypted	RMSE	PSNR	MSE
			0.99256	72	0.002
			0.982	68	0.009
			0.9813	65	0.001
			0.9725	64	0.004
			0.9621	63	0.003

The proposed model optimal security results are detailed in Tab. 2. This showed parameters including encryption time, key breaking time, encryption size, encryption memory, decryption memory, and decryption time. The encryption time rises as the file size increases, yet the suggested approach achieves the shortest encryption and decryption times. Consequently, in the suggested framework, encrypted and decrypted memory increases. Furthermore, the suggested approach is optimum when the key breaking time is the shortest possible given the file size.

Table 2: Proposed model optimal results

File size (kb)	Encryption memory	Encryption size	Encryption time (ms)	Key braking time	Decryption memory	Decryption time (ms)
50	1,246,468	62	49	99	656,258	51
100	1,289,169	89	52	98	665,568	62
150	1,314,894	93	58	96	678,896	74
200	1,327,952	102	64	94	681,347	73.6
250	1,346,962	189	69	93	690,354	76.09

4.2.1 Comparative Analysis

The performance of the proposed method has been compared with the different conventional methods such as Signcryption + (Adaptive Elephant Herd Optimization) AEHO [35], OHE [29] and ODLSB [31] in terms of PSNR, RMSE, MSE, Encryption time, Decryption time, key braking time, key size. The PSNR value obtained from the proposed method is compared with the conventional methods are demonstrated in Fig. 2. The integrity of a transmitter transmission is affected by the ratio between its highest achievable strength and the power of degrading noise is defined by PSNR. The comparisons of medical image security systems such as Signcryption +AEHO, OHE, and ODLSB are among the encryption methods are employed. The PSNR assessment in the suggested technique is improved more than the other existing methods. In a 250 kb picture, the PSNR in the suggested version is 63 dB, which is the highest among the different techniques. Although a greater PSNR value is typically suggests a higher-quality secured image reconstruction. MSE is a technique for determining how close estimations or projections are to actual values. The comparative analysis of proposed MSE value over the conventional methods is illustrated in Fig. 3.

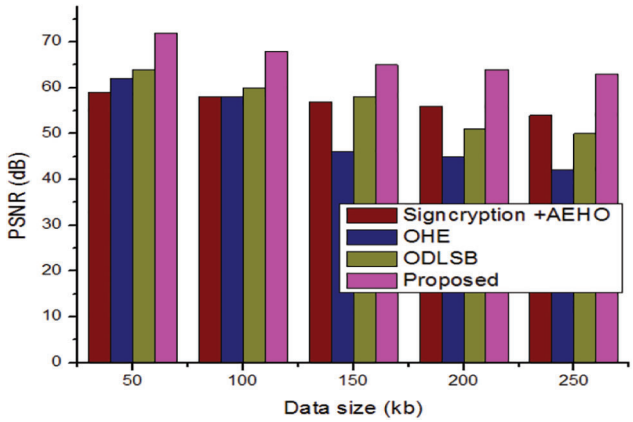


Figure 2: Comparison of PSNR value

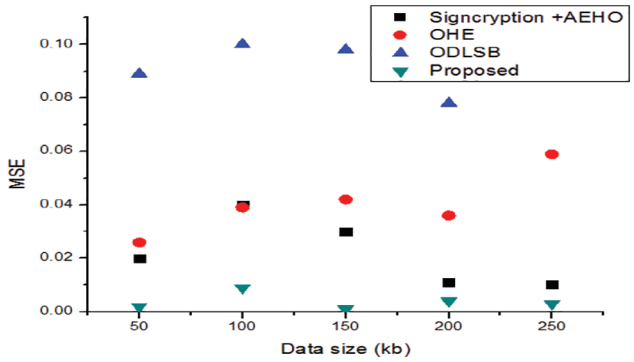


Figure 3: Comparison of MSE value

The observation demonstrates that the MSE value for the suggested system, which is lower when compared to the current system on a variety of image types and with a low error rate. Then, the RMSE value obtained from the proposed approach is compared with the conventional methods and the outcomes are demonstrated in Fig. 4. The Encryption time is defined as the time taken for encrypts the data from plain data to cipher data. The proposed time taken for the encryption is compared with the existing models is shown in Fig. 5. The demonstration shows that the proposed method has attained superior performance over the conventional methods for the different files sizes such as 50, 100, 150, 200 and 250kb. Because of the proposed model has attained very less time of encryption over the earlier models.

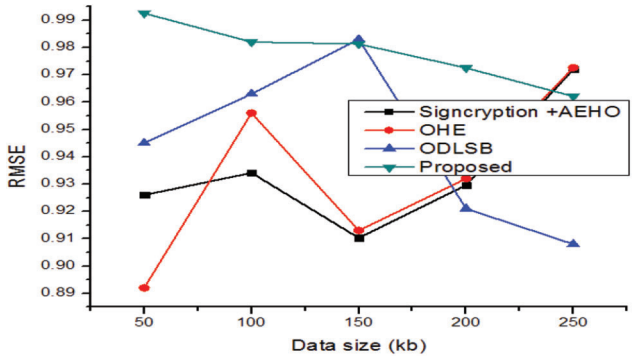


Figure 4: Comparative analysis RMSE value

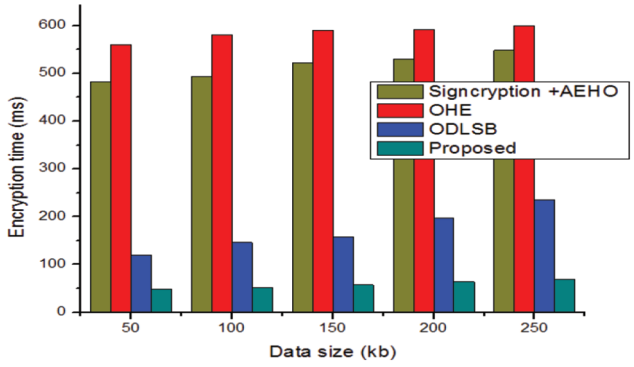


Figure 5: Comparative analysis Encryption time

The decryption time is defined as the time taken for decrypts the data from cipher data to original data. The proposed time taken for the decryption is compared with the existing models is shown in Fig. 6. The demonstration shows that the proposed method has attained superior performance over the conventional methods for the different files sizes such as 50, 100, 150, 200 and 250 kb. Because of the proposed model has attained very less time of decryption over the earlier models.

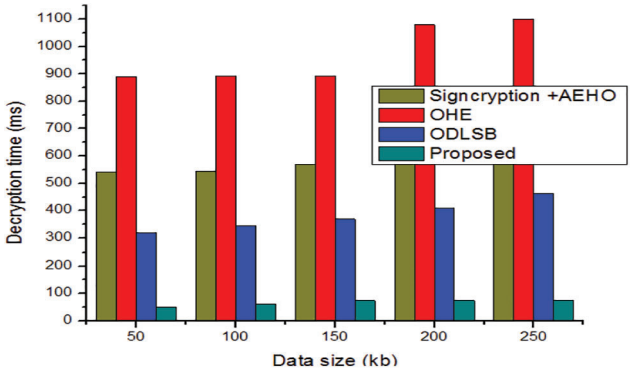


Figure 6: Comparative analysis Decryption time

The time taking for key braking in the proposed security system are compared with the different values from existing models are shown in Fig. 7. The key braking time is improved more than the conventional methods. Thus its shows the effective security improvement in healthcare system with blockchain technology. The functioning of a cipher is controlled by keys, and only the proper key can convert encrypted message to plain text. Many encryption techniques are based on publicly available techniques or are publicly available; therefore the system's security is entirely determined by the difficulty of getting the key, assuming no analytic attack. Thus, the estimation of key size is important and also this defines the number of bits in a key employed by security algorithm. The comparative analysis for key size is provided in Fig. 8. In comparison to previous strategies, the graphical observations depicted the optimal security attained by the suggested model.

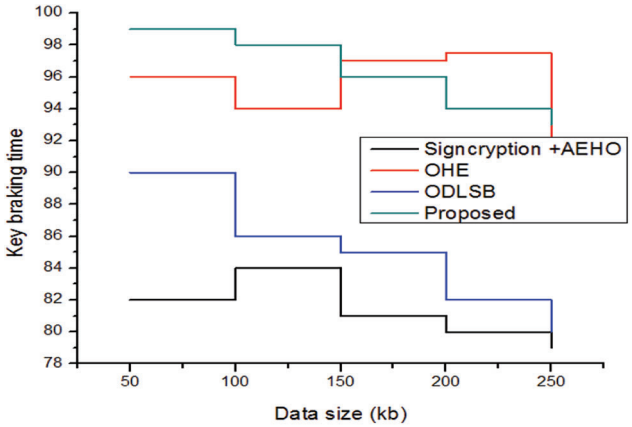


Figure 7: Comparative analysis of keybraking time

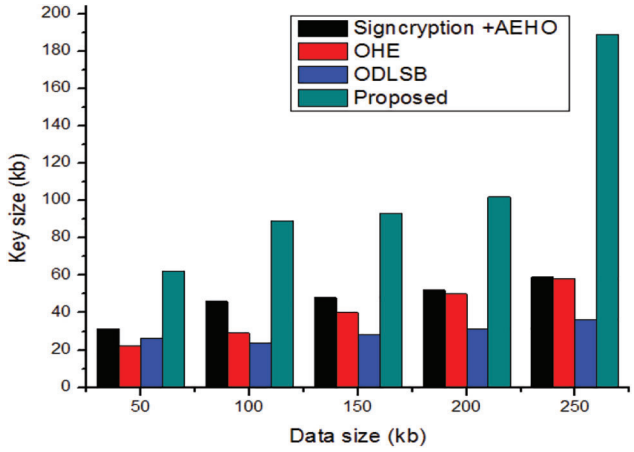


Figure 8: Comparative analysis key size

4.3 Analysis with Security Models

The analysis of proposed LGE-HES method over the conventional methods with respect to varied data size such as 50, 100, 150, 200 and 200 kb is described in Tabs. 3–7. When comparing the suggested LGE-HESmodel to the existing schemes, the proposed model exhibits greater performance values for all metrics.

Table 3: Performance analysis of proposed and conventional security model for 50 kb data size

Techniques	Signcryption +AEHO [35]	OHE [29]	ODLSB [31]	Proposed
PSNR (dB)	59	62	64	72
MSE	0.02	0.026	0.089	0.002
RMSE	0.926	0.892	0.945	0.99256
Encryption time (ms)	482	560	120	49
Decryption time (ms)	540	890	320	51
Key braking time	82	96	90	99
Key size	31	22	26	62

Table 4: Performance analysis of proposed and conventional security model for 100 kb data size

Techniques	Signcryption +AEHO [35]	OHE [29]	ODLSB [31]	Proposed
PSNR (dB)	59	62	64	72
MSE	0.02	0.026	0.089	0.002
RMSE	0.926	0.892	0.945	0.99256
Encryption time (ms)	482	560	120	49
Decryption time (ms)	540	890	320	51
Key braking time	82	96	90	99
Key size	31	22	26	62

Table 5: Performance analysis of proposed and conventional security model for 150 kb data size

Techniques	Signcryption +AEHO [35]	OHE [29]	ODLSB [31]	Proposed
PSNR (dB)	57	46	58	65
MSE	0.03	0.042	0.098	0.001
RMSE	0.9103	0.913	0.983	0.9813
Encryption time (ms)	521	590	158	58
Decryption time (ms)	569	893	369	74
Key braking time	81	97	85	96
Key size	48	40	28	93

Table 6: Performance analysis of proposed and conventional security model for 200 kb data size

Techniques	Signcryption +AEHO [35]	OHE [29]	ODLSB [31]	Proposed
PSNR (dB)	56	45	51	64
MSE	0.011	0.036	0.078	0.004
RMSE	0.9296	0.932	0.921	0.9725
Encryption time (ms)	530	592	197	64
Decryption time (ms)	579	1080	410	73.6
Key braking time	80	97.5	82	94
Key size	52	50	31	102

Table 7: Performance analysis of proposed and conventional security model for 250 kb data size

Techniques	Signcryption +AEHO [35]	OHE [29]	ODLSB [31]	Proposed
PSNR (dB)	54	42	50	63
MSE	0.01	0.059	0.102	0.003
RMSE	0.972	0.9726	0.908	0.9621
Encryption time (ms)	548	600	235	69
Decryption time (ms)	605	1100	463	76.09
Key braking time	59	58	36	189
Key size	79	92	80	93

Most particularly, the performance analysis from Tab. 7 for the large scale of 250 kb data size has adopted supreme consequences. The proposed LGE-HES method has attained high PSRN value, key braking time, RMSE, key size and very less encryption time, MSE, and decryption time over the conventional Signcryption +AEHO, OHE, and ODLSB methods. The proposed method has achieved higher PSNR value (63 dB) over the conventional methods such as 54, 42 and 50 dB. As a result, the overall evaluation demonstrates that the generated model performs better in cybersecurity when using the optimization-assisted encrypted approach.

5 Conclusion

In this research analyzed the cybersecurity of blockchain technology in healthcare system with the supreme encryption system, the non-public key, and the general public key are optimized using the LGE-HES methodology. Moreover, PSNR, MSE, RMSE, encryption time, decryption time, key size, and key braking time are used to assess the suggested approach's performance. The maximum PSNR is 63 dB, the minimum MSE is 0.003, and the encryption and decryption times are 69 and 76.09 ms, respectively, ac-cording to the implementation results. As a result, the image's secrecy is maintained in the end, and the recovered image is made available to the data user without compromising the image's quality. In addition, there are a number of other issues, such as the overall key size and the computation utilized in the prior technique being quite large. The hybrid optimization methodology will be considered in the future to account for the security of healthcare increasing level.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] K. M. Khan, J. Arshad and M. M. Khan, "Secure digital voting system based on blockchain technology," *International Journal of Electronic Government Research (IJEGR)*, vol. 14, no. 1, pp. 53–62, 2018.

[2] A. A. Monrat, O. Schelen and K. A. Andersson, "Survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, no. 4, pp. 117134–117151, 2019.

[3] T. A. Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem *et al.,* "A comparative analysis of blockchain architecture and its applications: Problems and recommendations," *IEEE Access*, vol. 7, pp. 176838–176869, 2019.

[4] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed and G. Soursou, "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives," *Cryptography*, vol. 3, no. 1, pp. 125–310, 2019.

[5] J. Chen, W. Wang, Y. Zhou, S. H. Ahmed and W. Wei, "Exploiting 5G and blockchain for medical applications of drones," *IEEE Network*, vol. 35, no. 1, pp. 30–36, 2021.

[6] S. Chakraborty, S. Aich and H. C. Kim, "A secure healthcare system design framework using blockchain technology," in *2019 21st Int. Conf. on Advanced Communication Technology (ICACT)*, PyeongChang, Korea (South), 12, pp. 260–264, 2019.

[7] G. Rathee, A. Sharma, H. Saini, R. Kumar and R. Iqbal, "A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology," *Multimedia Tools and Applications*, vol. 79, no. 15, pp. 9711–9733, 2020.

[8] A. Shahnaz, U. Qamar and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7, pp. 147782–147795, 2019.

[9] P. Zhang, D. C. Schmidt, J. White and L. Lenz, "Blockchain technology use cases in healthcare," *Advances in Computers*, vol. 111, no. 2, pp. 1–41, 2018.

[10] G. Nagasubramanian, R. K. Sakthivel, R. Patan, A. H. Gandomi, M. Sankayya *et al.,* "Securing e-health records using keyless signature infrastructure blockchain technology in the cloud," *Neural Computing and Applications*, vol. 32, no. 3, pp. 639–647, 2020.

[11] A. Banotra, J. S. Sharma, S. Gupta, S. K. Gupta and M. Rashid, "Use of blockchain and internet of things for securing data in healthcare systems," *Multimedia Security*, vol. 5, pp. 255–267, 2021.

[12] K. P. Satamraju, "Proof of concept of scalable integration of internet of things and blockchain in healthcare," *Sensors*, vol. 20, no. 5, pp. 1389–1395, 2020.

[13] G. N. Nguyen, N. H. Le Viet, M. Elhoseny, K. Shankar, B. B. Gupta *et al.,* "Secure blockchain enabled Cy-ber-physical systems in healthcare using deep belief network with ResNet model," *Journal of Parallel and Distributed Computing*, vol. 153, no. 2, pp. 150–160, 2021.

[14] Y. Li, Y. Zuo, H. Song and Z. Lv, "Deep learning in security of internet of things," *IEEE Internet of Things Journal*, vol. 23, no. 9, pp. 431–450, 2021.

[15] W. Yánez, R. Mahmud, R. Bahsoon, Y. Zhang and R. Buyya, "Data allocation mechanism for Internet-of-Things systems with blockchain," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3509–3522, 2020.

[16] H. Yi, "Secure social internet of things based on post-quantum blockchain," *IEEE transactions on Network Science and Engineering*, vol. 7, no. 21, pp. 554–568, 2021.

[17] S. Shukla, S. Thakur and J. G. Breslin, "Secure communication in smart meters using elliptic curve cryptography and digital signature algorithm," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, Rhodes, Greece, 2021, pp. 261–266, 2021. https://dx.doi.org/10.1109/CSR51186.2021.9527947.

[18] G. K. Chaitanya and K. R. Sekhar, "Knowledge-based gait behavioural authentication through a machine learning approach," *International Journal of Biomedical Engineering and Technology*, vol. 36, no. 1, pp. 25–42, 2021.

[19] N. Malik, P. Nanda, X. He and R. P. Liu, "Vehicular networks with security and trust management solutions: Proposed secured message exchange via blockchain technology," *Wireless Networks*, vol. 26, no. 6, pp. 4207–4226, 2020.

[20] T. Thilagam and R. Aruna, "Intrusion detection for network based cloud computing by custom RC-NN and optimization," *ICT Express*, vol. 17, no. 4, pp. 24–30, 2021.

[21] L. Feng, A. Ali, M. Iqbal, A. K. Bashir, S. A. Hussain *et al.,* "Optimal haptic communications over nanonetworks for E-health systems," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 5, pp. 3016–3027, 2019.

[22] F. Muheidat and L. A. Tawalbeh, "Artificial intelligence and blockchain for cybersecurity applications," *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*, vol. 4, no. 12, pp. 3–29, 2021.

[23] M. A. Almaiah, "A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology," *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*, vol. 4, no. 12, pp. 217–234, 2021.

[24] R. O. Ogundokun, J. B. Awotunde, E. A. Adeniyi and F. E. Ayo, "Crypto-Stegno based model for securing medical information on IOMT platform," *Multimedia Tools and Applications*, vol. 80, no. 21, pp. 31705–31727, 2021.

[25] A. A. ellatif, A. Z. Al-Marridi, A. Mohamed, A. Erbad, C. F. Chiasserini *et al.,* "Health: Toward secure, block-chain-enabled healthcare systems," *IEEE Network*, vol. 34, no. 4, pp. 312–319, 2020.

[26] G. N. Nguyen, N. H. Le Viet, M. Elhoseny, K. Shankar, B. B. Gupta *et al.,* "Secure blockchain enabled Cy-ber-physical systems in healthcare using deep belief network with ResNet model," *Journal of Parallel and Distributed Computing*, vol. 153, no. 9, pp. 150–160, 2021.

[27] G. Kalyani and S. Chaudhari, "An efficient approach for enhancing security in internet of things using the optimum authen-tication key," *International Journal of Computers and Applications*, vol. 42, no. 3, pp. 306–314, 2020.

[28] P. Pandey and R. Litoriya, "Securing and authenticating healthcare records through blockchain technology," *Cryptology*, vol. 44, no. 4, pp. 341–356, 2020.

[29] T. Veeramakali, R. Siva, B. Sivakumar, P. S. Mahesh and N. Krishnaraj, "An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model," *The Journal of Supercomputing*, vol. 4, no. 9, pp. 1–21, 2021.

[30] A. A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, V. Andraca *et al.,* "Quantum-inspired blockchain-based cybersecurity: Securing smart edge utilities in IoT-based smart cities," *Information Processing & Management*, vol. 58, no. 4, pp. 102549, 2021.

[31] W. Serrano, "The blockchain random neural network for cybersecure IoT and 5G infrastructure in smart cities," *Journal of Network and Computer Applications*, vol. 175, no. 3, pp. 102909, 2021.

[32] B. Cao, X. Wang, W. Zhang, H. Song and Z. Lv, "A many-objective optimization model of industrial internet of things based on private blockchain," *IEEE Network*, vol. 34, no. 5, pp. 78–83, 2020.

[33] K. Shankar, M. Elhoseny, E. Perumal, M. Ilayaraja and K. S. Kumar, "An efficient image encryption scheme based on signcryption technique with adaptive elephant herding optimization," *Cybersecurity and Secure Information Systems*, vol. 12, no. 4, pp. 31–42, 2019.

[34] R. S. Mathews, A. N. Maadhuree, R. R. Justus, K. Vishnu and C. R. Robin, "Fulcrum: Cognitive therapy system for stress relief by emotional perception using DNN," in *Int. Conf. on Emerging Current Trends in Computing and Expert Technology*, New Delhi, India, 35, pp. 1170–1178, 2019.

[35] P. Tare, S. Mishra, M. Lakhotia and K. Goyal, "Bias variance tradeoff in classification algo-rithms on the census income dataset," *International Journal of Computer Techniques*, vol. 6, no. 3, pp. 1–5, 2019.

[36] D. Prabakaran and S. Ramachandran, "Multi-Factor authentication for secured financial transactions in cloud environment," *Computers, Materials & Continua*, vol. 70, no. 1, pp. 1781–1798, 2022.

[37] K. S. Balaguru, C. R. Rachel Nallathamby and A. Rene Robin, "A novel approach for analyzing the social network," *Procedia Computer Science*, vol. 48, no. 12, pp. 686–691, 2015.