Wireless Personal Communications (2023) 130:2959–2980
https://doi.org/10.1007/s11277-023-10411-6

An Adaptive Lightweight Hybrid Encryption Scheme for Securing the Healthcare Data in Cloud-Assisted Internet of Things

B. Padma Vijetha Dev[1] · K. Venkata Prasad[1]

Accepted: 22 March 2023 / Published online: 5 April 2023
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract

The revolution of IoT systems surpasses daily human facilities for providing financial, mechanical and social aspects. However, the secure transmission of health data over the Internet is a challenging task. Thus, to solve this issue, the proposed study presents the security of medical images in IOT through a new Lightweight Hybrid Encryption (LHE) method with optimization strategies. Initially, the input medical images are encrypted to access the data with higher security through an efficient substitution box (S-box) block cipher and elliptic curves. The proposed encryption scheme assists in minimizing the computational time to several extents by utilizing the Finite Elliptic Curves (FEC) of smaller sizes to generate the S-boxes. Then, a cover image is chosen to hide the information or the confidential images with different pixel sizes. The cover image is partitioned into several non-overlapping blocks. From this, an optimal block is selected by using an adaptive COOT optimization algorithm. After selecting the best block, the cipher image is decomposed and is concealed with the selected block through a Least Significant Bit (LSB) mechanism. Finally, the encrypted medical image data are securely stored in the cloud storage platform through the Internet. The simulation results show that the proposed model obtains better results in terms of security level (97.82%), encryption time (15.4 s), minimum energy consumption (1.33 pJ/bit) and better execution time (18.41 s) related to the data size (bits).

Keywords Substitution box · Internet of things · Image encryption · Security · Finite elliptic curve · Least significant bit

✉ B. Padma Vijetha Dev
padmavijetha@gmail.com

K. Venkata Prasad
prasad_kz@yahoo.co.in

[1] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur 522502, India

1 Introduction

The Internet of Things (IoT) links numerous devices around the globe which are presently linked to the Internet. Due to the advent of IoT applies to several fields, such as education, communication, transportation and business development, and the popularity of IoT concept has recently increased [1, 2]. Through IoT platforms, sensitive data can be shared without the intervention of humans [3]. Recently, cloud-assisted IoT has been enhancing rapidly because of its higher expansion and is widely utilized in the healthcare system for higher security [4]. The primary objective of IoT-based medical care services is to afford an increased user experience at a feasible cost while also enhancing the quality of life. In the medical sector, the IoT presents smart healthcare systems and comprises remote servers, smart sensors and a network [5].

The hyper-connectivity provided by the IoT to its users offered effortless communication from their remote locations. A recent study shows that about 26.66 billion devices are engaged in the IoT to obtain services and communication [6, 7]. The massive exploration of this IOT utility started in 2011 with wearable devices, smart energy meters, home automation, etc. [8]. Research studies and investigations on IOT helped to improve business strategies, market research, asset tracking, etc. Also, with the introduction of automated services, the lifestyle of individuals has changed tremendously [9]. Though the IoT offers several benefits to the users associated with it, there are problems with security issues and cyber-attacks due to the continuous and uncontrolled exploration of such technologies [10].

Security is one of the key factors that demonstrate the insecurity in the IoT, making it a critical issue restricting the growth of IoT. This insecurity was identified as one of the world's top five security threats in 2015, prompting researchers to find new ways to resolve those issues [11, 12] effectively. Common reasons for such vulnerabilities include unconscious use of device applications, lack of device updates, frequent changing of passwords, etc. [13]. Several security threats on the Internet breach secured information, causing privacy issues for users. Hackers intentionally develop malicious codes to breach the sensitive contents stored on cloud servers. To avoid this, traditional security mechanisms and cryptographic algorithms are applied. But the inappropriate use of these algorithms leads to an increased possibility of data breaches [14, 15].

Most security experts have identified that IoT devices are vulnerable to numerous forms of cyber-attacks due to the application of weak security protocols. Also, it is more important to gain thorough knowledge regarding the emerging security issues in the IoT to provide suitable security protocols [16, 17]. The traditional cryptosystems are identified to provide security for the IoT devices to a particular range. Still, the recent advancements in security issues are yet to be documented to guarantee better security. The sensitive information is mostly related to the patient's health records collected through the placement of sensors in the patient's body [18]. While transferring these data to the cloud server, security issues arise, leading to the requirement for effective security measures. Recently, lightweight cryptosystems have offered security to most of the recent vulnerabilities. Thus, this article follows an efficient, secure, lightweight block encryption method for protecting medical data in cloud IOT [19, 20].

1.1 Motivation

The cloud-based IoT environment is prone to several security issues, and complications arise when dealing with sensitive medical data. Medical data comprise sensitive personal information about the patients, and it becomes necessary to ensure privacy for these data to prevent them from being exposed. The research community utilizes several traditional cryptosystems to secure medical data stored in the cloud servers. But most of these algorithms are vulnerable to several attacks, such as replay attacks, impersonation, brute force attacks, etc. Apart from that, the computational complexity of the algorithms is higher, which restricts these algorithms from being followed for security purposes. Several lightweight security schemes have recently been introduced to improve the computational complexity and security in the cloud-assisted IoT platform. These algorithms are computationally inexpensive and can be followed to protect medical data from various cyber-attacks. Hence, lightweight cryptosystems are considered to provide medical data security while considering the IoT environment. Among the lightweight cryptosystems, block-based encryption methods are much more robust to security attacks while dealing with medical data. Due to the necessity of such an efficient and secure scheme, this paper introduces a lightweight hybrid encryption scheme for securing medical data in a cloud-based IoT platform.

1.2 Contributions

The major objectives of this proposal are as follows:

- Enhancing the security of patients' medical data stored in a cloud-assisted IoT platform through a novel hybrid lightweight encryption scheme using a substitution box and finite elliptic curves.
- Introducing an adaptive COOT-based optimal block selection scheme to select the optimal block from the image to enhance overall performance and security.
- Developing an LSB mechanism for hiding the patient's sensitive medical images to a selected optimal block.
- Conducting extensive evaluations for the proposed model to prove the effectiveness and efficiency of the proposed model compared to the existing models related to the security of medical data.

The rest of this paper is mentioned as follows: Sect. 2 represents several related works conducted in recent years. Section 3 mentions the proposed methodology based on a complete description of the S-Box generator with the FEC model, Adaptive coot optimization algorithm and LS bit substitution method. Section 4 represents the results and discussion using the python simulator. Finally, the conclusion and future work are mentioned in Sect. 5.

2 Related Work

Several research works have been done to secure the patient's data in the cloud. Some of the popular and effective methodologies are reviewed below:

Healthcare data is considered one of the most sensitive pieces of information, demanding a huge range of security. Data protection has been a major concern in ensuring patient privacy and other research areas in recent years. To ensure privacy and security for healthcare data, Akhbarifar et al. [21] introduced a health monitoring model that supported clinicians in diagnosing the disease early. Here, a lightweight encryption mechanism was introduced to afford security for patients' health data. In this, the confidentiality of input health data was enhanced by using a cloud-based IoT environment. That model determined the health status of the patients by gathering information from the sensor data collected by smart medical IoT devices. The data mining methodologies were applied to collect the information sensed by the devices. After decrypting the health data from the cloud, data pre-processing was performed to remove unwanted noises. The developed data mining approaches such as support vector machine (SVM), random forest (RF), K-star, and multilayer perceptron (MLP) helped to detect the diseases. Also, the model's experimentations achieved a higher accuracy rate (95%) with effective security enhancement. However, the developed encryption scheme consumes more time to convert plain text data into cipher text. Thus, it is considered the major drawback of this study.

Another methodology to offer security for the patient data stored in the cloud-IoT platform was formulated by Atiewi et al. [22]. The methodology was based on multifactor authentication with lightweight cryptography to offer big data system security. The system utilized a combination of private and public clouds to offer security to the sensitive and non-sensitive information collected from various sources. The sensitive data was partitioned into two, where one part was encrypted using the Feistel encryption algorithm, and the other was encrypted using the RC6. On the other hand, the non-sensitive data were encrypted using the advanced standard encryption (AES) algorithm. To provide more security to the provided input data, the developed methodology used the private cloud to store the sensitive data and the public cloud to store the non-sensitive data. Three levels of authentication were introduced in the methodology to provide access to the stored data. Different metrics such as encryption time, decryption time, security strength and computational time were utilized to evaluate the performance of the cloud-IoT architecture. Nevertheless, the system attained higher computational complexity because of the execution of three different encryption mechanisms.

The wireless body area networks (WBAN) or the telecare medical information system (TMIS) provide remote medical treatments to patients directly from the physicians via the Internet. Different authentication protocols were established in the literature to ensure privacy for the patients associated with the TMIS system. To resolve the research gap of the requirement for efficient and secured key agreement schemes, Alzahrani [23] introduced an authenticated key agreement scheme for cloud IoT. To afford higher security for medical data, Telecare Medical Information System (TMIS) was developed in this existing work. This approach utilized lightweight symmetric key operations to ensure patient privacy and security. Also, the approach was supported by rigorous formal security analysis and proved to withstand several security threats. The security properties were validated using the automated ProVerif tool. On average, the approach provided 38% more security features than the compared protocols. Also, the developed scheme troubles to managing replay and impersonation threats because of its inefficiency.

The sensitive information collected from the patients' bodies is stored in the cloud server that the user can access remotely anywhere and at any time. This creates several security issues in the case of remote user authentication. To avoid that, Sharma and Kalra [24] established a lightweight remote user authentication scheme for cloud-assisted IoT applications. The approach was resilient to multiple security threats in the cloud IoT due to lightweight cryptography. The scheme was initially verified using the random oracle model, which proved the robustness of the model in the login and authentication phases. Then, the mutual authentication of the scheme was verified using the BAN logic. The web-based AVISPA tool was utilized to simulate the scheme, proving the scheme's robustness against different known attacks. The security of the developed mechanism was proven by performing acute informal security analysis. Apart from that, the scheme's efficiency was proved through analysis regarding computational cost, security features and attack resistance. The analysis states that the overall computational cost of a developed model is not as much compromised.

One of the major issues arising in the cloud IoT platform is the security of patient data. It is also important to optimize the computational overheads as it requires high technical security mechanisms with complex computations. Vedaraj and Ezhumalai [25] developed a predictive security architecture for the cloud IoT to effectively predict patient disease from the sensed information. This existing study utilized an integrated algorithm combining homomorphic encryption with random diagonal elliptical curve cryptography and multi-nomial smoothing Naïve Bayes (HERDE-MSNB) to provide effective security while predicting the patient disease from the provided data. The developed cryptographic mechanism performs both encryption and decryption processes. Then, the medicinal person decrypted the ciphertext, and the prediction was carried out by using the Multi-nomial smoothing naïve bayes (MSNB) model. The model outperformed most of the existing state-of-the-art when evaluated with the UCI repository dataset.

Al-Zubaidie et al. [26] designed a lightweight mechanism to afford mutual user authentication. To ensure the security of patients' sensitive data, this existing study developed an authentication scheme which renders mutual authentication among clients and servers. Elliptic Curve Integrated Encryption Scheme (ECIES) and PHOTON were designed to attain effective security and the best system performance. The developed scheme was based on the physical address, multiple-pseudonym and one-time password schemes to authenticate actual users. The simulation analysis demonstrated that the developed scheme provides higher security over several attacks.

Similarly, Sarosh et al. [27] introduced an adaptive network to provide security for healthcare data. The developed network afforded higher confidentiality and security to the medical images via an e-health system. The developed mechanism uses the 3D-chaotic system to create a keystream employed to initiate eight and two-bit permutations of the given image. A pixel diffusion was enabled through a key image with a developed Piecewise Linear Chaotic Map (PWLCM). Here, the image parameter was evaluated with the support of image pixels and initiated criss-cross diffusion to improve security. The result analysis shows that the presented mechanism reduces several attacks and mentions that it can apply to the healthcare sector.

On the other hand, Das et al. [28] presented a new encryption method for preserving medical data in IoT-assisted medical care infrastructure. ECC and Advanced Encryption Standard (AES) were developed for converting plain text data into cipher text. Using the hybrid encryption schemes, the security measures of input medical care data were enhanced. In addition, the presented method also assures data integrity with the aid of an elliptic curve-based digital signature. The efficiency of a developed scheme is proved by performing a performance comparison and security analysis. However, the computational cost is the major concern of this existing work.

2.1 Problem Statement

The IoT is gathered from several devices that are linked through the Internet. Based on various needs, it can be interacted with different devices to achieve several operations over the Internet. The IoT system is related to the link between interrelated devices and various platforms for the evolution of a virtual and physical world. Security is a major concern for data transmission from the source (healthcare image) to the destination (servers). Therefore, an efficient method is required to guarantee the patient's healthcare data security for transmitting and receiving ends. To receive the Internet-based things (IoT) innovation, it is essential to make clients' data about its protection and security. In this model, the patient's data would not be at any risk of data secrecy or integrity in the medical field. The development of protection and security factors identifies IoT variables to improve the transmission of medical images. The main purpose of this paper is to achieve integrity and classification of data protection and network security. The cryptographic technique is used to input data into a cipher image using an advanced method.

3 Proposed Methodology

IoT offers the interconnection of devices through the Internet, thereby providing effective communication. With this innovation, the transmission of medical data to the cloud server has become an easy task. The medical data collected from the patient's body are highly sensitive as it consists of patients' health-related information. This data is required to be protected to ensure privacy for the patients. The lightweight block ciphers provide reliable results with efficiency even in resource-constrained IoT. Thus, a new lightweight block cipher is introduced in this article to facilitate security for the patient's health records. The structure of the hybrid encryption model of medical images is shown in Fig. 1.

Initially, the images are captured from the sensor devices placed on the patient's body. The collected images are required to be stored on cloud servers. For this, lightweight cryptography is applied over the input images. An efficient substitution box (S-box) block cipher with finite elliptic curves is applied to encrypt the collected input images in our proposed work. This algorithm reduces the computational time to several extents using the ordered elliptic curves of smaller sizes to generate the S-boxes.

The cipher images are then transferred to the home server, where those images are partitioned into several blocks. A cover image is chosen to hide the information or the confidential images with different pixel sizes. The cover image is then decomposed into non-overlapping blocks from which the best blocks are selected. The new model has proposed the adaptive

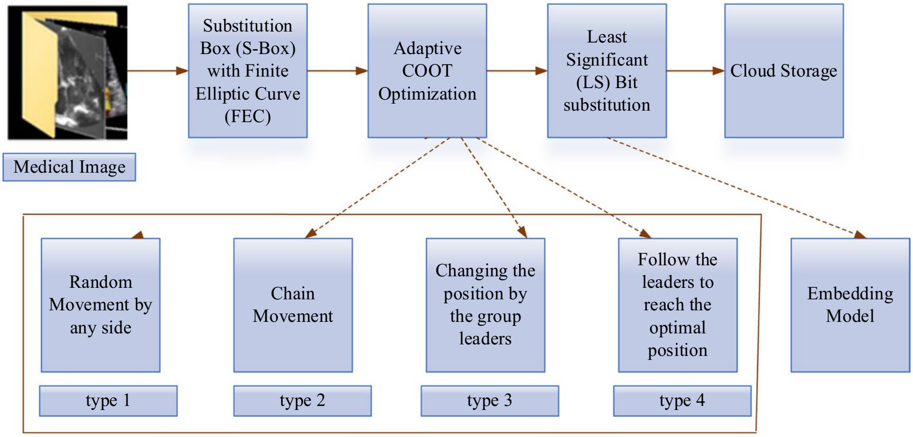

Medical Image
Substitution Box (S-Box) with Finite Elliptic Curve (FEC)
Adaptive COOT Optimization
Least Significant (LS) Bit substitution
Cloud Storage
Random Movement by any side
type 1
Chain Movement
type 2
Changing the position by the group leaders
type 3
Follow the leaders to reach the optimal position
type 4
Embedding Model

Fig. 1 Block diagram of hybrid encryption scheme of healthcare data

COOT-based optimal block selection scheme using the recently introduced meta-heuristic COOT optimization algorithm to select the blocks from the partitioned blocks. After selecting the best blocks, the embedding map is obtained. Then, the cipher image is decomposed and concealed with the selected block using the embedding map for encryption. Finally, the encrypted image is stored in the cloud server by transmitting it through the Internet.

This paper provides a hybrid encryption method based on the healthcare image data transmitted by IoT devices to the cloud database. It enhances web security and utilizes encryption of data from attacks by hackers. The data is secured using the elliptic cryptography method by the encryption process from the source to the destination. The proposed method involves various processes as follows:

- Substitution Box (S-Box) Generator based Finite Elliptic Curve (FEC)
- Adaptive Coot optimization model-based block selection
- Least Significant (LS) bit model

The input image is gathered from various IOT-based devices such as remote patient monitoring, glucose monitoring, heart-rate recognition, depression (or) mood analyzer, Ingestible sensors, robotic surgery and Parkinson's disease monitoring. It attains images of a patient's health-related problem that can be helpful for the doctors to analyze the exact disease. The health image data is transmitted from the IoT-based devices to the cloud storage with the help of the Internet through the network. Our aim is to transmit the data using an encryption process securely.

The adaptive coot optimization process is elaborated in the block diagram based on four types. The LS bit substitution is the embedding model for better data encryption to be securely stored in the cloud platform.

3.1 Image Encryption through Substitution Box (S-Box) Generator with Finite Elliptic Curve (FEC)

The S-Box generator can use to generate a dynamic S-Box along with better cryptography. The dynamic S-Box is more involved in enhancing the security of secret information against attacks than the static S-Box model. It is based on different mathematical factors to develop an S-box generator to generate highly dynamic and secure S-boxes. Based on the computing methods, the cryptographic strength of the S-box is tested against attacks such as linear, differential and algebraic threats.

The existing Elliptic Curve (EC) Cryptography-based S-box generators require a calculation based on large ECs to generate highly dynamic S-boxes. Because of large ECs, such S-box generators are unsuitable for lightweight cryptography due to limited computational power. The proposed method has involved a new S-box generator with a Finite Elliptic Curve (FEC) to generate highly dynamic and strong S-boxes using an EC combined with a small size. Here, this technique uses an ordered FEC to create random numbers in the integers in $[0,\ 2^x - 1]$. The binary sequence is used to generate a $x \times x$ S-box.

The prime field is denoted as F_a with a elements. Here, a represents prime value. Based on this paper, $p, q \in F_a$ shows any two integers. The EC can be denoted by $J_{a,p.q}$

$$J_{a,p.q} = \left\{ (n, o) \in F_a \times F_a \middle| o^2 \equiv n^3 + pn + q(\mathrm{mod}\, a) \middle| \right\} \cup \{Y\} \tag{1}$$

Here, Y denotes the point at infinity, $J_{a,p.q}$ is non-singular when $4p^{3} + 27\,q^{2} \neq 0 \,(\bmod\, a)$. The polynomial $n^{3} + pn + q\,(\bmod\, a)$ has unique root values. The equation $4p^{3} + 27\,q^{2}$ $^{3} + 27\,q^{2}$ is known as the discriminant of $J_{a,p.q}$. The FEC size is finite because of a finite field F_{a}. Over the FEC, the total number of points is shown as $\neq J_{a,p.q}$.

$$a + 1 - 2\sqrt{a} \leq \neq J_{a,p,q} \leq a + 1 + 2\sqrt{a} \tag{2}$$

If the values restrict $p = 0$ in Eq. (1) and $q \in F_{a}$, then the values become a new EC model called the Mordell elliptic (ME) curve. Based on this model, a ME curve is shown as $J_{a,0.q}$ and can be represented as:

$$J_{a,0.q} = \left\{ (n, o) \in F_{a} \times F_{a} \middle| o^{2} \equiv n^{3} + pn + q\,(\bmod\, a) \middle| \right\} \cup \{Y\} \tag{3}$$

The ME curve has a property with a prime $a \equiv 2\,(\bmod\, 3)_{,}$ and the number of points on an $J_{a,0.q}$ is exactly $a + 1$. For each integer number of o in $[0,\ a - 1]$, it contains only one integer value n in $[0,\ a - 1]_{,}$ and the point (n, o) lies on $J_{a,0.q}$.

To generate the S-boxes, the diffusion and natural ordering process can be denoted by L^{1} and L^{2}, respectively. For the arrangement of points on a ME curve, the ordering process is used. Let $(n_{1},\ o_{1}),\ (n_{2},\ o_{2}) \in J_{a,0,q}$

$$(n_{1},\ o_{1})L^{1}(n_{2},\ o_{2}) \Leftrightarrow \left\{ \frac{either\, n_{1} + o_{1} < n_{2} + o_{2},\ or}{n_{1} + o_{1} = n_{2} + o_{2}\, and\ n_{1} < n_{2}} \right. \tag{4}$$

$$(n_{1},\ o_{1})L^{2}(n_{2},\ o_{2}) \Leftrightarrow \left\{ \frac{either\, n_{1} < n_{2},\ or}{n_{1} = n_{2}\, and\ o_{1} < o_{2}} \right. \tag{5}$$

Here L^{1} and L^{2} are a total of two orderings such as diffusion L^{1} and natural L^{2} ordering.

The binary sequence can generate plaintext-dependent S-boxes. This model uses the secure hash algorithm (SHA)-256 hash function to obtain binary sequences based on the plaintext. It can be used for the S-box generator to attain the output plaintext-dependent S-boxes. The S-box generator consists of ten main steps for generating $x \times x$ S-boxes. Here, this method denotes $2^{x} - 1$ using t for notational convenience.

Step1 Choose two sequences $P^{s} = (p^{s}_{0}, p^{s}_{1}, p^{s}_{2}, \ldots, p^{s}_{t})$ over the set of non-negative integers $s = 1, 2$.

Step2 Choose an EC $J_{p,0,q}$ with $a \equiv 2\,(\bmod\, 3),\ a \geq 2^{x}$, and two ordering $\prec_{L^{s}},\ s = 1, 2$.

Step3 Choose two sets $Q^{s} = \left\{ q^{s}_{0}, q^{s}_{1}, \ldots, q^{s}_{t} \right\},\ s = 1, 2,$ such that $|Q^{s}| = 2^{x}$ and $Q^{s}\,(\bmod\, 2^{x}) = [0, t]$.

Step4 Calculate the sets $R^{s} = \left\{ r^{s}_{0}, r^{s}_{1}, r^{s}_{2}, \ldots, r^{s}_{t} \right\}$ such that $r^{s}_{e} = (n^{s}_{e},\ (q^{s}_{e} + p^{s}_{e})\,(\bmod a)) \in J_{a,0,q}$.

Step5 Now, to create randomness in Q^{s}, sort it to R^{s} such that q^{s}_{e} is smaller than $q^{s}_{e'}$ for the ordering $\prec_{L^{s}},\ s = 1, 2$.

Step6 Let $M^{s} = \left(m^{s}_{0}, m^{s}_{1}, \ldots, m^{s}_{t} \right),\ for\ s = 1, 2,$ represent the sequences attained from ordered Q^{s} after giving module 2^{x}, where $m^{s}_{e} \equiv (q^{s}_{e})\,(\bmod\, 2^{x})$.

Step7 Now, this method generates an S-box $\beta^{1,2}\ (P^{s}, L^{s}, Q^{s}, a, q, x) : [0, t] \rightarrow [0, t]$ such that

$$\beta^{1,2}\ (P^{s}, L^{s}, Q^{s}, a, q, x)\ (m^{1}_{e}) = m^{2}_{e},\ e \in [0,\ t] \tag{6}$$

Step8 Create a binary sequence T of size $x\,2^x$, divide it from left to right into sub-sequences (i_e) and the length of each sub-sequences is denoted as x. Now, the sub-sequences can be converted into decimal numbers $x_e\,, \quad e \in [0, t]$. Let $X = (x_0, x_1, ..., x_t)$ denote the integer sequence from the subsequent decimal form.

Step9 Total order $\prec_L$ denotes the integers in $[0, t]$ based on X such that, for $s, e \in [0, t]$, it holds that $s \prec_L e$ if "$x_s < x_e$" or "$x_s = x_e$"and $s < e$. Let $B = (b_0, b_1, ..., b_t)$ represent the sequence attained from the ordered set $[0, t]$, where the entries are registered from smallest to largest for $\prec_L$.

Step10 For $s = 1, 2$, the output of the S-box can be generated for $\beta^s\ (P^s, L^s, Q^s, T, a, q, x)$ such that

$$\beta^s\ (P^s, L^s, Q^s, T, a, q, x)\ (b_e) = m_e^s\,,\ e \in [0, t] \tag{7}$$

The parameters are given as P^s, L^s, Q^s, T, a, q and x, $s = 1, 2$, the proposed S-box generates to creates three S-boxes $\beta^s\ (P^s, L^s, Q^s, T, a, q, x)$, $s = 1, 2$, and $\beta^{1,2}\ (P^s, L^s, Q^s, a, q, x)$. Two different binary sequences T and T', and fixed P^s, L^s, Q^s, a, q, and x, the corresponding S-boxes are different; therefore, it holds that,

$$\beta^s\ (P^s, L^s, Q^s, T, a, q, x)\,(i) \neq \beta^s\ (P^s, L^s, Q^s, T', a, q, x)\,(i)\,,\ \forall_i \in [0, t] \tag{8}$$

The proposition can follow the sequences X and X' that is attained from T and T', respectively, in step (8) are different when $T \neq T'$. Figure 2 denotes the flow diagram of the S-box generator using the new approach.

The main purpose of an S-box generator is to create plaintext dependence, which can play an essential role against chosen-plaintext and known-plaintext threats in image encryption methods. In this model, the SHA-256 hash function generates a binary sequence based on the length 256. The hash function can be converted into a binary sequence with length $x\,2^x$ by commonly denoting the SHA-256 sequence. Therefore, each image can obtain a different binary sequence T. Using Eq. (8), this method can generate a different S-box based on each image. It also obtains high security against chosen plaintext and known plaintext threats.

3.2 Optimal Block Selection Using Adaptive Coot Algorithm

The Coots are members of the rail family, Rallidae. These small water birds constitute the genus Fulica, derived from the Latin for Coot. These birds have a vital frontal shield on the forehead along with coloured bills and red to dark red eyes. Some coot birds have white colour under the tail. The coots consist of several movements and behaviours on the water. They can travel at angles based on the direction of motion. This movement is related to a disordered movement of an activity, a synchronized movement, and a chain move on the water's surface. They also have several behaviours, but this paper represents the collective movements of the coots, like irregular and regular movements. These birds have few leaders to search for the prey, and the other whole group follows the leader coops that are considered the group leaders.

This paper considers four different kinds of movement based on the water's surface. They are:

(1) A random movement to any side
(2) Chain Movement

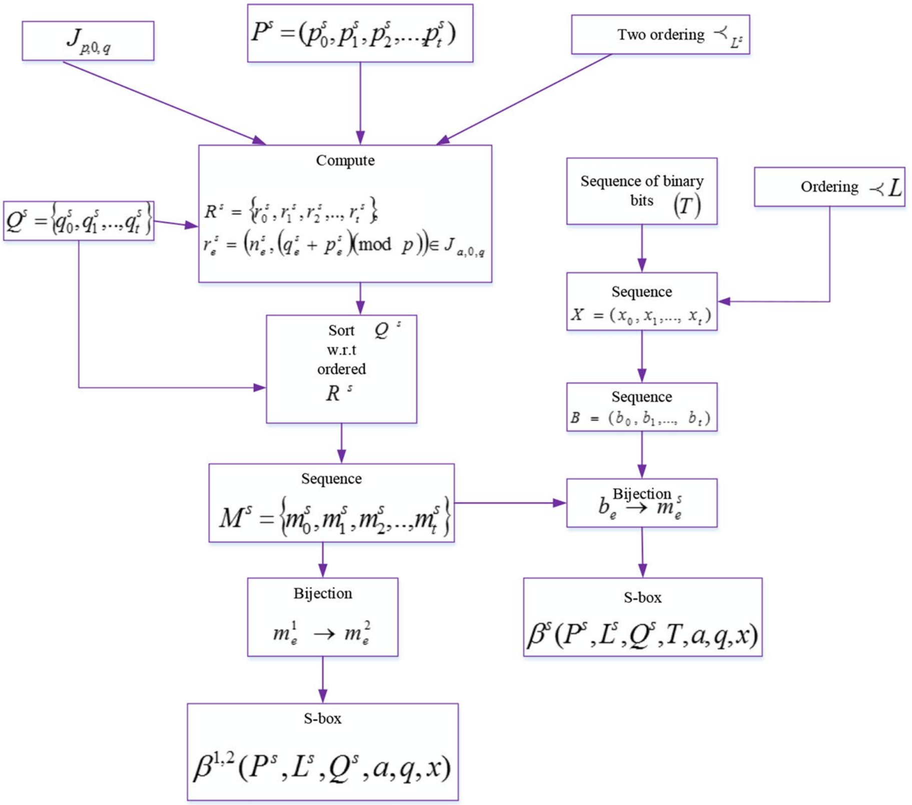

$J_{p,0,q}$
$P^s = (p_0^s, p_1^s, p_2^s, \dots p_t^s)$
Two ordering $\prec_{L^s}$
Compute
$R^s = \{r_0^s, r_1^s, r_2^s, \dots, r_t^s\}$
$r_e^s = (n_e^s, (q_e^s + p_e^s)(\mathrm{mod}\ p)) \in J_{a,0,q}$
$Q^s = \{q_0^s, q_1^s, \dots, q_t^s\}$
Sequence of binary bits (T)
Ordering $\prec L$
Sequence
$X = (x_0, x_1, \dots, x_t)$
Sort Q^s w.r.t ordered R^s
Sequence
$B = (b_0, b_1, \dots, b_t)$
Sequence
$M^s = \{m_0^s, m_1^s, m_2^s, \dots, m_t^s\}$
Bijection
$b_e \rightarrow m_e^s$
Bijection
$m_e^1 \rightarrow m_e^2$
S-box
$\beta^s(P^s, L^s, Q^s, T, a, q, x)$
S-box
$\beta^{1,2}(P^s, L^s, Q^s, a, q, x)$

Fig. 2 Flowchart of S-box generator

(3) Changing the position of the group leaders
(4) Leading the whole group using the leaders to reach the optimal location

3.2.1 Mathematical Algorithm and Model

The traditional structure of all optimization methods is the same. The model starts with $(\vec{n}) = \{\vec{n}_1, \vec{n}_2, \vec{n}_3, \dots, \vec{n}_x\}$ an initial random population that is repeatedly calculated using the target function. The target value is calculated $\left(\vec{T}\right) = \{T_1, T_2, T_3, \dots, T_x\}$. This method can be improved using a set of procedures to obtain the core value of an optimization model. It is not possible to attain the optimal solution using only one calculation. Because of this population-based optimization model, several random numbers and optimization steps are required to find the increased global optimal position. The population of this method is randomly created using the formula:

$$Cootposition(j) = rand(1,\ e)\ *\ (UB - LB) + LB \tag{9}$$

where $Cootposition(j)$ denotes the coot position, e represents the number of problems (or) variables dimensions, UB shows the upper bound search space and LB presents the lower bound search space. Each value contains a different upper bound and lower bound issue.

$$LB = [LB_1, LB_2, LB_3, ..., LB_e], \quad UB = [UB_1, UB_2, UB_3, ..., UB_e] \tag{10}$$

Based on the generation of the initial population and determination of each agent's position, the fitness function of each solution can be derived by $T_j = f(\vec{n})$ the objection function. In this method, the group leader is selected using NC number of coots. The choice for selection of leaders is random. The four movements of coots on the water's surface are derived as follows:

3.2.2 Random Movement by any Side

In this random method, a random position is considered using the search space and moving the Coot towards a random location. It can be denoted as Eq. (11):

$$P = rand(1, e) * (UB - LB) + LB \tag{11}$$

The movement of the Coot explores different search space parts. This random movement helps to escape from the optimal local position when the algorithm strikes the optimal location. The new position of a Coot is evaluated based on the formula (12),

$$Cootposition(j) = Cootposition(j) + M \times S2 \times (P - Cootposition(j)) \tag{12}$$

where $S2$ denotes the random number of the interval $[0, 1][0, 1]$, M is derived using the formula (13).

$$M = 1 - B \times \left(\frac{1}{Iteration} \right) \tag{13}$$

where B represents the current iteration, the maximum iteration is shown as *Iteration.*

3.2.3 Chain Movement

The implementation of chain movement can be derived using the average position of two coots. The other way is to evaluate a chain movement using two ways. Initially, the calculation is evaluated for the distance vector between the two coots. Afterwards, the Coot moves towards the other Coot about half the distance vector. Using this way, the Coot's initial position is obtained, and the new location using the formula (14),

$$Cootposition(j) = 0.5 \times (Cootposition(j - 1) + Cootposition(j)) \tag{14}$$

Here, the second Coot is represented as $Cootposition(j - 1)$.

3.2.4 Changing the position of the group leaders

Normally, the group of coots is led by a few coots that are moved in front of the location. The other coots must change their location related to the group's leaders and move according to them. One question that might be raised is whether every Coot will change its location based on which leader of the Coot. The leader's average location can be evaluated, and the other coots can update their location based on the Coot's leaders. For the implementation of a movement, a method is introduced to select the leader using the formula (15).

$$V = 1 + (j\,Mod\,NC) \tag{15}$$

where the current coot index number is denoted as j, the leader's number is represented as NC, and the index number of the leaders is shown as V.

Based on the leaders (v), the Coot (j) must update its position. The selected leader calculates the Coot's next position, which is evaluated in the following equation.

$$\begin{aligned} Cootposition(j) = & Leaderposition(v) + 2 \times S1 \times \cos(2S\pi) \\ & \times (Leaderposition(v) - Cootposition(j)) \end{aligned} \tag{16}$$

where, the Coot's current position is denoted as $Cootposition(j)$, the selected leader position is represented as $Leaderposition\,(v)$, the random number in the interval $[0, 1]$ is shown as $S1$, and the pi value π is denoted as 3.14. The random number in the interval $[-1, 1]$ is given as S.

3.2.5 Leading the Whole Group Using the Leaders to Reach the Optimal Location

The group's direction must move towards a goal (or) optimal position, so the leaders should update their correct position towards the goal. To update the leader's position, Eq. (17) shows as follow:

$$Leaderposition(j) = \left\{ \begin{matrix} L \times S3 \times \cos(2S\pi) \times & S4 < 0.5 \\ (gbest - Leaderposition(j)) + gbest & \\ L \times S3 \times \cos(2S\pi) \times & S4 \geq 0.5 \\ (gbest - Leaderposition(j)) - gbest & \end{matrix} \right\} \tag{17}$$

where $gbest$ denotes the best position ever obtained, $S3$ and $S4$ are random numbers based on the interval $[0, 1]$, π shows the pi value as 3.14, S represents a random number related to the interval $[-1, 1]$, and L is measured using the formula (18).

This model obtains a better position based on the current optimal point using this formula. Occasionally, the leaders are changed the current optimal location to find suitable locations. The above equation gives the best way to get closer to the exact optimal position and get away from the position.

$$L = 2 - B \times \left(\frac{1}{Iteration} \right) W_e \tag{18}$$

where the current iteration is denoted as B and the maximum iteration is shown as $Iteration$. The weight is represented as W_e. In the adaptive Coot-based optimization model, the weight's involvement helps to achieve the best optimal position based on the convergence.

$2 \times S3$ builds larger random variations that the algorithm does not strike in the local optimum. The new method also performs exploration during the exploitation process based on this method. To find a suitable position according to the search agent Cos $(2S\pi)$ searches to identify the best search agent. One question that may arise here is when these different variations are executed.

Using these four types of block selection, the adaptive coot optimization algorithm helps to attain a better path selection to identify the blocks. The weight function is introduced for a better iteration process than another traditional coot algorithm. Because of using the weight function in an adaptive COOT optimization method, the best optimal position is acheived.

Depending the preservation of the random nature of proposed optimization method, this new model randomly involves all these changes. For the execution of an optimization algorithm, the movement of a Coot is performed randomly, toward group leaders and in a chain form. The pseudo-code of the adaptive coot optimization method is shown in Table 1.

3.3 Concealing Cipher Image Using Least Significant Bit (LSB) Substitution Method

The LSB method is the most commonly used method to hide the data in the image without impacting the whole image. To embed the message, it uses the LSB based on each pixel in the image. The main purpose of LSB substitution is to embed the image in the LSB of a pixel image. This can be evaluated in the following Eq. (19):

$$N_j' = N_j - N_j \bmod 2^v + a_j \tag{19}$$

where the steganography image based on the jth pixel value is represented as *jth*, the cover image with *jth* pixel is denoted as N_j and the decimal value of the confidential data with *jth* block is shown as a_j. The number of LSBs denotes v. The image pixel can be copied to the LSB directly to extract the message. This operation is calculated using the following Eq. (20):

$$a_j = n_j' \bmod 2^v \tag{20}$$

This method is very fast and easy. The image places of the bits based on the pixel are shown in Fig. 3.

The usage of an LSB substitution process mainly focuses on making image steganography. Hidden data can be inserted randomly (or) sequentially.

After hiding the health care image data better, the image can be transmitted through the Internet to store it in the cloud platform. The proposed method is very efficient for storing health images with high security.

Cloud storage has emerged as an effective solution to provide convenient, on-demand access and ubiquitous to a huge amount of information through the Internet. After evaluating LSB to hide the data, the cloud-based storage is used to store the information gathered by the Internet of things (IoT) obtained from the health data daily. The images gathered from the patients in the hospital are effectively transmitted using IOT-based access to store them in the cloud platform securely. Using cloud storage, the data can be obtained at any point and gathered the data for any location.

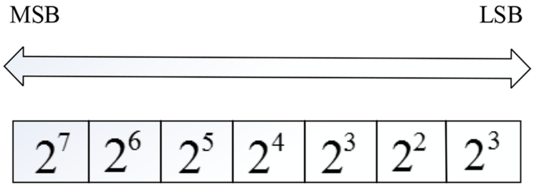
4 Results and Discussion

The results and discussion are mainly categorized into three parts. They are simulation environment, performance metrics and comparison analysis. For simulation purposes, the proposed study collects the input data from Brain MRI Images for Brain tumor Detection dataset, and its link is provided as follows, https://www.kaggle.com/navoneel/brain-mri-images-for-brain-tumor-detection.

Table 1 Pseudo-code of adaptive coot optimization method

```
Start
        Initialize the Coot's first population randomly using equation (9) and equation (10);
        Initialize the factors of $Q = 0.5$ , $NC$ (Number of leaders), $Xcoot$ (number of
coots);
                $Xcoot = Xpop - X1$;
            Random identification of leaders from the coots using,
                $P = rand\,(1, e) * (UB - LB) + LB$;
            Calculate the fitness value of leaders and coots ;
                Find the best leader (or) Coot based on the global optimum $(gbest)$ ;
            Update the new position of Coot by,
                $Cootposition(j) = Cootposition\,(j) + M \times S2 \times (P - Cootposition(j))$ ;
If the end measurement is not satisfied, then
                Compute the initial position of Coot by using
                    $Cootposition(j) = 0.5\times\ (Cootposition\,(j-1) + Cootposition(j))$;
              If $rand < Q$
                $S$, $S1$ and $S3$ are random numbers along with the dimensions of the problem;
 Else
    $S$, $S1$ and $S3$ are random vectors;
 End
    For $j = 1$ to the number of coots;
                Select the leader search agent by using $V = 1 + (j\,Mod\ NC)$;
            Calculate the Coot's next position by the selected leader using,
                $Cootposition(j) = Leaderposition\,(v) + 2 \times S1 \times \cos\,(2S\pi) \times$
                $(Leaderposition\,(v) - Cootposition(j))$
            If $rand < 0.5$  $j \sim= 1$
            Update the position of the Coot using equation (14)
Else
             Update the position of the Coot using equation (12)
End
End
    For the number of leaders
            If $rand < 0.5$
            Update the leader's position using,
                    $L \times S3 \times \cos\,(2S\pi) \times (gbest - Leaderposition(j)) + gbest$
Else
            Update the leader's position using,
                    $L \times S3 \times \cos(2S\pi) \times (gbest - Leaderposition(j)) - gbest$
End
            If the fitness of the leader $< gbest$
        $Temp = gbest$; $gbest = leader$; $leader = temp$; (update global
optimum)
        $Iteration = iteration + 1$;
Return;
Stop
```

Fig. 3 The location of the bits in the pixel



4.1 Simulation Environment

The open-source programming language python tool obtains the output graphs for the simulation process. The embedded system is combined with the following components:

- 1 GB RAM with Quad-core 1.2 GHz Broadcom BCM2837 bit Central processing unit (CPU)
- Micro SD card port for storing information and loading the Operating system (OS)

4.2 Performance Metrics

The performance metrics of this model involve a few parameters such as Security level, encryption time, execution time and energy consumption.

4.2.1 Security Level

The security level of a healthcare image is based on several factors, such as encryption, watermarking and steganography. The main purpose of these levels is to protect digital images from achieving security goals such as availability, integrity, and confidentiality.

4.2.2 Encryption Time

It is the ratio of a total encrypted plaintext in bits to the encryption time in milliseconds (ms). It is the process of encoding images (or) information gathered by IoT-based devices from hospitals. The plain images can be scrambled into ciphered images to protect data.

4.2.3 Execution Time

It is derived by the ratio of medical image data in bits to the total time taken for data transmission. The measured unit is denoted in seconds.

4.2.4 Energy Consumption

The power (or) energy consumption is derived based on the following formula:

$$E_C = P_U * \left(\frac{t_o}{1000}\right) \tag{21}$$

Here, E_C represents the energy measurements in kilowatt-hour (kwh) (or) Joules, t_o denotes the time taken for the energy (or) power consumption, P_U shows the power units in watts.

4.3 Comparison Analysis over other Existing Schemes

The proposed method is compared with other models using several measurements to evaluate the performances. Figure 4 represents the input image with other models like encryption, cover, steganography, and decrypted images.

The input healthcare image can be accessed using IOT-based devices and evaluated as an encrypted image in the next stage. The encrypted image is used to change the pixel size of the image to change the original values to prevent hackers and is placed to scramble original data. The encrypted image is applied to convert it into a cover image. Then, the cover image is changed into a steganography image to hide the image to secure the data from various attacks on the Internet. Finally, the steganography image is decrypted in the destination end for storing the output image in the cloud platform. Figure 5 denotes the security level approach for the lightweight cipher method.

Using the lightweight cipher model, an optimal level of security is obtained for the proposed technique in the range of 65 to 98% better than the other methods, such as the KATAN, SIMON, SIMECK and KLEIN models [7]. The existing methods only achieve the next level of security. Based on the security level for 350 blocks, the LHE method (97.82%) has obtained better security than other methods like KATAN (85.36%), SIMON (93.27%), SIMECK (84.67%) and KLEIN (85.64%) model. Figure 6 shows encryption time evaluation for security methods.

Based on the security formation of a new proposed LHE technique, the output graphs are obtained for execution time related to the data sizes. For the evaluation of high security with IoTs-based health data, the new LHE method (15.4 s for 256-bit data size) has achieved better encryption with the data size than the other existing KATAN (26.17 s), SIMON (22.26 s) and SIMON-Optimal share (20.35 s) creation models [7]. The graph clearly shows the output of the encryption time for data sizes 16, 32, 64, 128, and 256.

Figure 7 denotes the time process based on the data sizes. In the new LHE method, the execution time is minimized for each data size. The bar graph represents the output

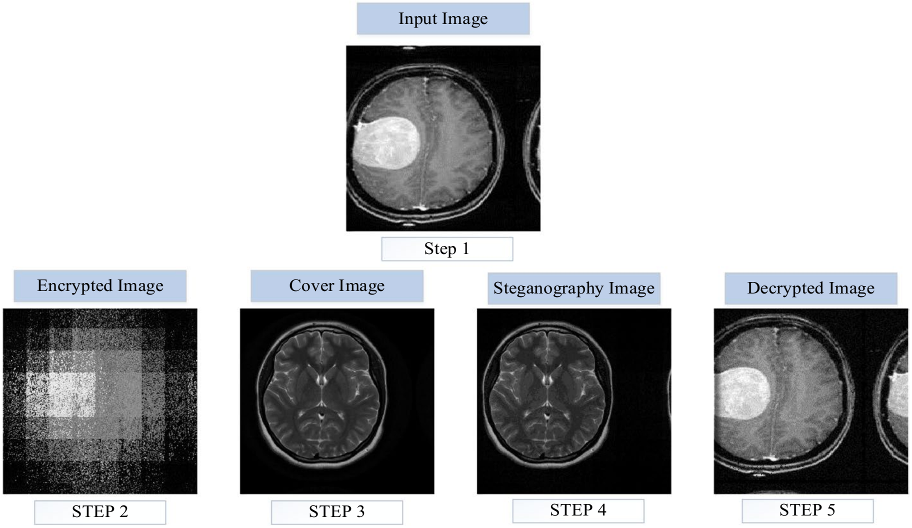


Fig. 4 Analysis of medical image data

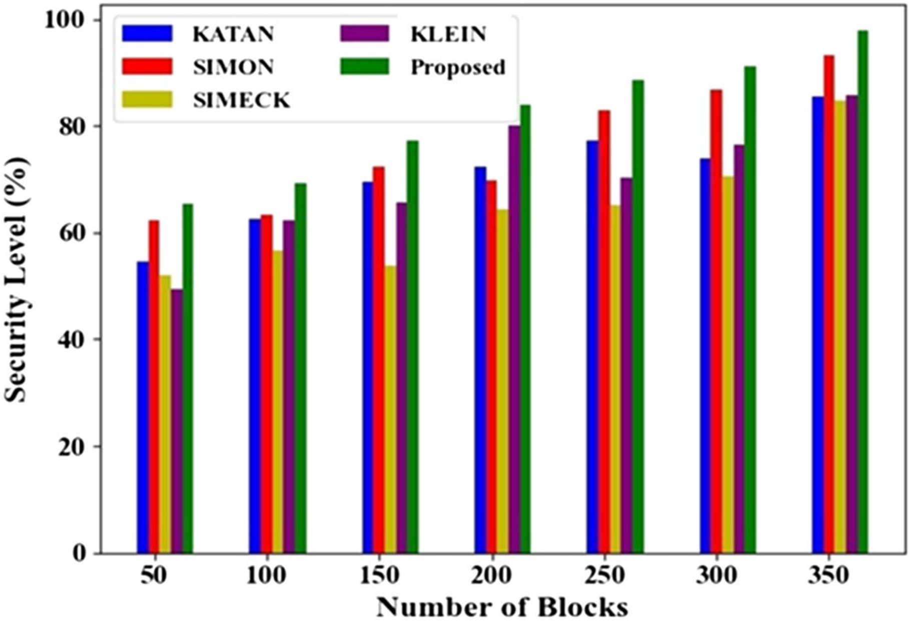


Fig. 5 Lightweight cipher

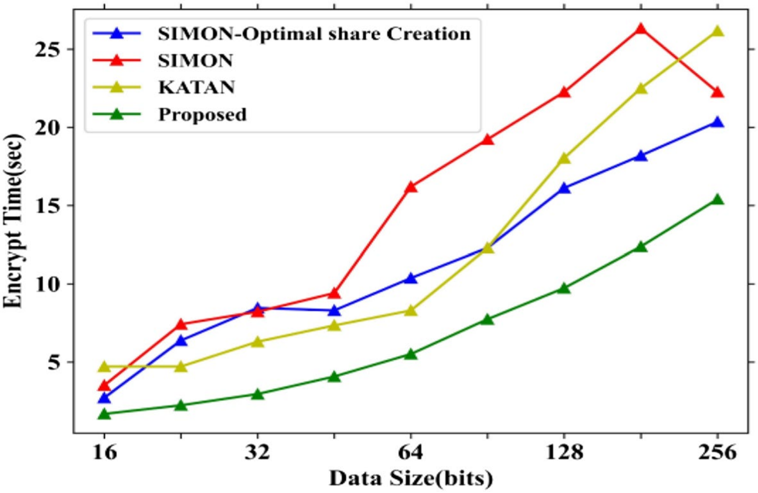


Fig. 6 Encryption time

of the execution time of the proposed LHE method (18.41 s for 256-bit data size) over other existing mechanisms such as KATAN (26.41 s), SIMON (32.61 s), and SIMON-Optimal share (22.5 s) [7]. The comparison analysis shows that the developed scheme attained reduced execution time compared to other existing schemes.

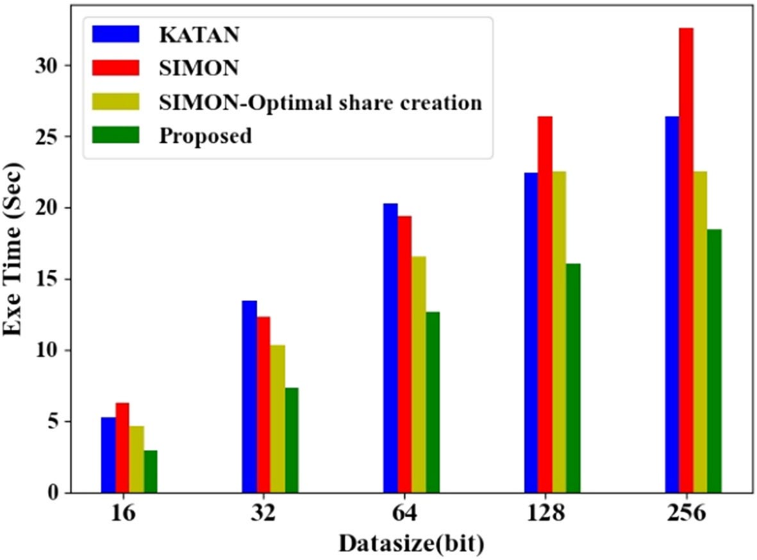


Fig. 7 Execution time

Figure 8 denotes the evaluation of an objective function. The fitness solution of this model for 100 iterations clearly shows the minimum energy level when compared to other techniques like Grey wolf optimization (GWO – 6.33), Cost safety optimization (CSO – 9.68) and Hybrid-teaching learning-based optimization (HTLBO – 3.16) [7].

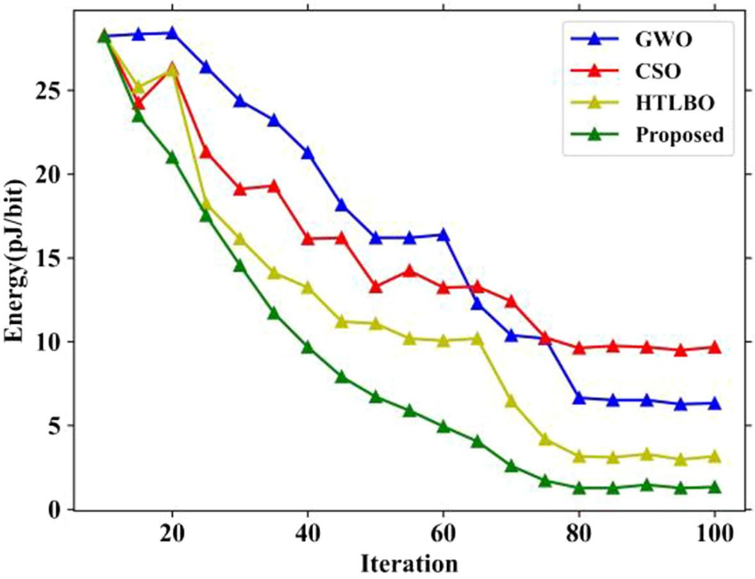


Fig. 8 Evaluation of the objective function

The new LHE technique (1.33) attains much less energy for every iteration. The iteration process continues until achieving an optimal solution.

5 Conclusion

IoT technology is widely used in the medical healthcare system to confer the best services, including the privacy and security of patients. This proposed method analyses the evaluation of security and privacy issues in terms of IoT-based smart healthcare systems. Because of recent advancements in cloud-based IoT platforms, this paper implemented an LHE method to encrypt the medical image for better data transmission in the cloud environment. The encryption process can be obtained using the S-box block chipper to increase the security level of the whole data. An adaptive Coot-based optimization algorithm was used to select the best optimal block. The outcomes showed that the new technique had enhanced data privacy in the cloud. Furthermore, execution time is better than the other SIMON optimal share creation, SIMON and KATAN models. The energy consumption in the iteration process has been reduced in the new model compared with other GWO, CSO and HTLBO methods. The security method confirmed that the new LHE model has higher security features than other medical image encryption processes. The proposed model obtained better results in terms of Security level (97.82%), encryption time (15.4 s), execution time (18.41 s) and energy consumption (1.33 pj/bit) compared to similar other models. The major shortcoming of this proposed work is that it utilized only brain MRI images to afford security in the cloud. Thus, it will be considered in the future by gathering different health information to extend the proposed work. In addition, the proposed study only uses four metrics to evaluate the proposed approach's efficiency. Thus, several metrics will be utilized in future studies to exhibit the proposed scheme's efficacy. Also, an optimal key selection process will be conducted in future work to make effective encryption. Furthermore, future work will study the evaluation of algorithms combined with different block selections using a new data encryption technique with a hybrid optimization model. This model will be relevant to several cloud-based medical image data security applications to prevent various attacks.

Author Contributions All authors read and approved the final manuscript.

Funding No funding is provided for the preparation of manuscript.

Data Availability Data sharing is not applicable to this article.

Declarations

Conflict of interest Authors declare that they have no conflict of interest.

Ethical Approval This article does not contain any studies with human participants or animals performed by any of the authors.

Consent to Participate All the authors involved have agreed to participate in this submitted article.

Consent to Publish All the authors involved in this manuscript give full consent for publication of this submitted article.

References

1. Arunkumar, S., Vairavasundaram, S., Ravichandran, K. S., & Ravi, L. (2019). RIWT and QR factorization based hybrid robust image steganography using block selection algorithm for IOT devices. *Journal of Intelligent and Fuzzy Systems, 36*(5), 4265–4276.
2. Hasan, M. K., Islam, S., Sulaiman, R., Khan, S., Hashim, A. H. A., Habib, S., & Hassan, M. A. (2021). Lightweight encryption technique to enhance medical image security on internet of medical things applications. *IEEE Access, 9*, 47731–47742.
3. Hassan, A. (2022). An effective lightweight cryptographic algorithm to secure internet of things devices. In *Proceedings of the future technologies conference (FTC) 2021* (vol. 1, pp. 403–419). Springer International Publishing.
4. Gaurav, A., Psannis, K., & Peraković, D. (2022). Security of cloud-based medical internet of things (miots): A survey. *International Journal of Software Science and Computational Intelligence (IJSSCI), 14*(1), 1–16.
5. Abounassar, E. M., El-Kafrawy, P., & Abd El-Latif, A. A. (2022). Security and interoperability issues with internet of things (IoT) in healthcare industry: A survey. *Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions, 95*, 159–189.
6. Hedayati, R., & Mostafavi, S. (2021). A lightweight image encryption algorithm for secure communications in multimedia internet of things. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-021-09173-w
7. Rani, S. S., Alzubi, J. A., Lakshmanaprabu, S. K., Gupta, D., & Manikandan, R. (2020). Optimal users based secure data transmission on the Internet of healthcare things (IoHT) with lightweight block ciphers. *Multimedia Tools and Applications, 79*(47), 35405–35424.
8. Lu, Q., Zhu, C., & Deng, X. (2020). An efficient image encryption scheme based on the LSS chaotic map and single S-box. *IEEE Access, 8*, 25664–25678.
9. Anuradha, M., Jayasankar, T., Prakash, N. B., Sikkandar, M. Y., Hemalakshmi, G. R., Bharatiraja, C., & Britto, A. S. F. (2021). IOT enabled cancer prediction system to enhance the authentication and security using cloud computing. *Microprocessors and Microsystems, 80*, 103301.
10. Ullah, A., Azeem, M., Ashraf, H., Alaboudi, A. A., Humayun, M., & Jhanjhi, N. Z. (2021). Secure healthcare data aggregation and transmission in IOT—A survey. *IEEE Access, 9*, 16849–16865.
11. Mohiyuddin, A., Javed, A. R., Chakraborty, C., Rizwan, M., Shabbir, M., & Nebhen, J. (2022). Secure cloud storage for medical IoT data using adaptive neuro-fuzzy inference system. *International Journal of Fuzzy Systems, 24*(2), 1203–1215.
12. Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. (2021). HealthBlock: A secure blockchain-based healthcare data management system. *Computer Networks, 200*, 108500.
13. Dutta, A., Misra, C., Barik, R. K., & Mishra, S. (2021). Enhancing mist assisted cloud computing toward secure and scalable architecture for smart healthcare. In G. S. Hura, A. K. Singh, & L. S. Hoe (Eds.), *Advances in communication and computational technology* (Vol. 668, pp. 1515–1526). Springer.
14. Selvaraj, S., & Sundaravaradhan, S. (2020). Challenges and opportunities in IOT healthcare systems: A systematic review. *SN Applied Sciences, 2*(1), 1–8.
15. Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in healthcare 4.0. *Computer Communications, 153*, 311–335.
16. Mubarakali, A. (2020). Healthcare services monitoring in cloud using secure and robust healthcare-based BLOCKCHAIN (SRHB) approach. *Mobile Networks and Applications, 25*(4), 1330–1337.
17. Rashid, M., Parah, S. A., Wani, A. R., & Gupta, S. K. (2020). Securing E-health IOT data on cloud systems using novel extended role based access control model. In M. Alam, K. A. Shakil, & S. Khan (Eds.), *Internet of things (IOT)* (pp. 473–489). Cham: Springer.
18. Sivan, R., & Zukarnain, Z. A. (2021). Security and privacy in cloud-based E-health system. *Symmetry, 13*(5), 742.
19. Ayub, M. F., Mahmood, K., Kumari, S., & Sangaiah, A. K. (2021). Lightweight authentication protocol for e-health clouds in IOT-based applications through 5G technology. *Digital Communications and Networks, 7*(2), 235–244.
20. Geetha, R., Suntheya, A. K., & Srikanth, G. U. (2020). Cloud integrated IOT enabled sensor network security: Research issues and solutions. *Wireless Personal Communications, 113*(2), 747–771.
21. Akhbarifar, S., Javadi, H. H. S., Rahmani, A. M., & Hosseinzadeh, M. (2020). A secure remote health monitoring model for early disease diagnosis in cloud-based IOT environment. *Personal and Ubiquitous Computing*. https://doi.org/10.1007/s00779-020-01475-3

22. Atiewi, S., Al-Rahayfeh, A., Almiani, M., Yussof, S., Alfandi, O., Abugabah, A., & Jararweh, Y. (2020). Scalable and secure big data IOT system based on multifactor authentication and lightweight cryptography. *IEEE Access, 8*, 113498–113511.
23. Alzahrani, B. A. (2021). Secure and efficient cloud-based IOT authenticated key agreement scheme for e-health wireless sensor networks. *Arabian Journal for Science and Engineering, 46*(4), 3017–3032.
24. Sharma, G., & Kalra, S. (2020). Advanced lightweight multifactor remote user authentication scheme for cloud-IOT applications. *Journal of Ambient Intelligence and Humanized Computing, 11*(4), 1771–1794.
25. Vedaraj, M., & Ezhumalai, P. (2021). HERDE-MSNB: A predictive security architecture for IOT health cloud system. *Journal of Ambient Intelligence and Humanized Computing, 12*(7), 7333–7342.
26. Al-Zubaidie, M., Zhang, Z., & Zhang, J. (2019). RAMHU: A new robust lightweight scheme for mutual users authentication in healthcare applications. *Security and Communication Networks, 2019*, 1–26.
27. Sarosh, P., Parah, S. A., & Bhat, G. M. (2022). An efficient image encryption scheme for healthcare applications. *Multimedia Tools and Applications, 81*(5), 7253–7270.
28. Das, S., & Namasudra, S. (2022). A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure. *Computers and Electrical Engineering, 101*(3), 107991.

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

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

B. Padma Vijetha Dev, Assistant Professor in Computer Science & Engineering, pursuing PhD from KL University, Guntur. Completed M.Tech in Computer Science Engineering from Acharya Nagarjuna University, Guntur and B.Tech in Computer Science Technology from Sathyabama Deemed University, Chennai having overall 11 years of academic and research experience and Presently working as Assistant Professor from a prestigious institution Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad. Her areas of Research are Internet of Things (IOT) and Computer Networks. She is Mentoring Coordinator, Technological & Innovation Cell Coordinator for CSE Department (GRIET). She is well skilled in communication and comprehension. She has delivered scheduled lecturers to sophomore and freshman students. She conveyed subject matter and lecture to the students in a creative way. She has conducted Moodle Courses effectively for handled subjects. She evaluated the students individually to identify areas of difficulties. She researched study materials per syllabus requirements. She performed experimental activities and drew out conclusions. She has thorough understanding of the subject. She is knowledgeable in internal administrative tasks. She guided mini and major projects under graduate level and one of her projects got shorlisted for 1st AICTE ChhatraVishwakarma Awards 2017. She has successfully completed an AICTE approved Faculty Development Programme (FDP201x) on Pedagogy for online and Blended Teaching-Learning Process conducted by IIT Bombay from September 14, 2017 to October 12, 2017 and stood top amongst 241 performers from a total of 5308 participants in the programme.

Dr. K. Venkata Prasad ME., Ph.D, He is currently an Associate Professor with Koneru Lakshmaiah Education Foundation. He received ME Degree in 2006 from Anna University. He received Ph.D from Bangalore University in 2016. He is having 17 Years of teaching experience. His research interests include Data Science, Deep Learning and Image processing. He published 17 research papers in International Journals and presented 5 research papers in international conferences. He has one patent.