



# Securing healthcare big data in industry 4.0: cryptography encryption with hybrid optimization algorithm for IoT applications

Chandrashekhar Goswami<sup>1</sup> · P. Tamil Selvi<sup>2</sup> · Velagapudi Sreenivas<sup>3</sup> · J. Seetha<sup>4</sup> · Ajmeera Kiran<sup>5</sup> · Vamsidhar Talasila<sup>6</sup> · K. Maithili<sup>7</sup>

Received: 27 August 2023 / Accepted: 28 October 2023 / Published online: 30 December 2023  
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

## Abstract

In recent years, the Internet of Things (IoT) has grown at an exponential rate, transforming the healthcare business and perhaps leading to the creation of healthcare big data. As a result, there is a requirement to safeguard data from being attacked in order to ensure secure data transfer through the network. Cryptography has been discovered to be a simple and efficient method for safeguarding healthcare big data. At the same time, in cryptography, the best key generation process is viewed as an optimization issue that may be addressed with meta-heuristic algorithms. As a result, the main focus of this research is on the investigation of health care data security in IoT using the ASS-JFO-DHEA model, which combines an innovative hybrid Artificial Shuffle Shepherd Integrated Jellyfish optimization (ASS-JFO) algorithm with Digital Homomorphism Elgamal Algorithm (DHEA) encryption for data security. MATLAB software is used to carry out the execution and experiments for this research. On different benchmark images from a healthcare dataset, the ASS-JFO-DHEA model is experimentally validated. The peak signal to noise ratio, root mean square error, encryption time, mean square error, and other metrics are used to assess the findings. The findings are compared and contrasted as a consequence of this execution, and a variety of encryption algorithms with their optimization techniques from the literature are recognized as having the most intense PSNR values, i.e., 74 dB, generated by the suggested approach.

**Keywords** Security · Optimization · Cryptography · Healthcare · Internet of things and cloud

## 1 Introduction

The Internet of Things (IoT) is a collection of a massive multitude of devices (technologies) connected via the Internet (Mashal et al. 2020). Furthermore, the IoT is a realm where huge data is sent every second. In terms of IoT, a collection of smart devices, actuators and sensors collaborate to monitor and respond to the physical state and human frameworks (Lee et al. 2018). This system is linked to the communication across platforms as well as

interconnected devices in the appealing physical and virtual world (Ahmadi et al. 2019). The enormous amount of internet-enabled data transmission has generated huge information in real to satisfy diverse application specifications, like healthcare, social media platforms, e-commerce, banking industries, research community, and other manufacturing monitoring and security protocols, etc. (Perwej et al. 2019). IoT, as another phase in information systems, lets in telemedicine, an extra endeavor in which sensors and networks are used to traditional medicinal equipment, allowing them to attach knowledge to such gadgets and allowing patients to communicate and collaborate with remote professionals (Zhu et al. 2019). As a result, developing an effective way to ensure the confidentiality and reliability of the patient's diagnostics data transmitted and collected from the IoT background is critical (Kumar and Gandhi 2020).

E-health systems reduce healthcare costs while also improving quality of service, and these elements contributed to the optimization of the healthcare industry via the use of new equipment and solutions (Jasim et al. 2021). However, in order to assure dependable, smooth, and secure data transfer over uncertain networks, biomedical transmission of data has become one of the most pressing demands in the present health-care system (Ghazal 2021). IoT as well as cloud technology in healthcare systems have aided in the distribution of a large volume of healthcare data throughout the network. In an IoT and cloud environment, it is critical to protect the security and confidentiality of the patient's condition (Podder et al. 2101). Specific sensor devices, as well as the credibility of healthcare professionals, may be safeguarded in an IoT network. Patient data is often maintained on a cloud platform at the hospital, which necessitates a high level of security (Raghuvanshi et al. 2021). Regardless of networking and storage technologies, meanwhile, data security remains an issue. As a result, a new framework is necessary for the safe storage and transmission of medical data that are interfaced with patient data (Calvillo-Arbizu et al. 2021). This will find it difficult to use traditional IoT security solutions such as the widely used public key system and Internet protocol authentication.

Systems that are insecure, the information's privacy is maintained and ensured throughout the trading process (Luo et al. 2021). It retains its inventiveness, and the framework conceals no alteration. Confidentiality, authenticating, durability, and non-repudiation all play a part in the security methods used to safeguard the communication of multimodal outputs like data, images, video, audio, and so on (Zhan 2021). Several efforts have been made to protect of the kind incidences in the implementation of security structures, including the Rivest-Shamir-Adleman (RSA) (Rana et al. 2021), Digital signature algorithm (Zeadally et al. 2021), elliptic curve cryptography (Lara-Nino et al. 2020), Hybrid light weight encryption (Gyotheeswari and Jeyanthi 2020), intelligent cryptography algorithm (Pandey et al. 2020), Advanced Encryption Standard (AES) (Atiewi et al. 2020), diffie-Helman (Adat and Gupta 2018), and Quantum hash function (Shankar 2021). Considerable efforts are being made, meanwhile, either in developing shared data security mechanisms or security architecture, or in implementing a variety of data encryption techniques (Stergiou et al. 2020). Various meta-heuristic initiatives have been developed in recent years to increase data safety in the cloud, such as swarm optimization (Elhoseny et al. 2018), particle swarm optimization (Helmi et al. 2022), Genetic algorithm (Tripathi et al. 2022), and so on. Nevertheless, both security and computer performance have remained a major topic among researchers and healthcare professionals (Nagarajan and Minu 2018).

Furthermore, traditional approaches have a significant level of delay and high computational (Thyagarajan and Minu 2013; Dhanalakshmi and Nagarajan 2020). To address these concerns, the ASS-JFO-DHEA model combines the Artificial Shuffle Shepherd Integrated Jellyfish optimization (ASS-JFO) method with the Digital Homomorphism

ElGamal Algorithm (DHEA) encryption scheme for data security. The proposed model performs the encryption and decryption process using DHEA technique. In addition, the suggested model leverages a hybridization of the ASS-JFO method for optimum key selection to minimize the computation time required for the randomly chosen of secret keys. Typically, the IoT-based healthcare system produces large amount of data from different sources like medical equipment's, electronic health records, wearables, etc. This generated big data contains sensitive information; therefore ensuring security and privacy to this data is a challenge. In the proposed work, this challenge is resolved by using the integrated cryptographic algorithm. The utilization of cryptographic encryption protects this data from unauthorized access by performing data encryption process. In the proposed work, the homomorphic encryption approach named DHEA was applied to encrypt the sensitive information generated by IoT-based healthcare. The homomorphic encryption enables the system to perform computations on encrypted data before decryption, thus it provides privacy during data processing and confirms security and eliminates the risk of unauthorized access. In addition, the ASS-JFO approach was integrated in the developed model to optimize the encryption and decryption process. This algorithm has the capacity to handle optimal solution within a large solution space. It helps to select the optimal cryptographic keys for encryption process, thus, it enhances the data process and makes the system more scalable and reliable for handling large amount of data generated by IoT healthcare. Thus, the proposed hybrid cryptographic model provides greater level of security in big IoT-based healthcare. This article's contribution is summarized as follows:

- Propose a new ASS-JFO-DHEA model method for secure data exchange in healthcare systems based on IoT.
- For optimum key selection for the encryption and decryption of medical data, use the hybrid ASS-JFO optimization technique.
- Integrate the DHEA with IoT technology to allow for safe data sharing in healthcare systems.
- The efficiency of Secure Data is demonstrated through simulations of the proposed algorithms in terms of Root Mean Square Error (RMSE), Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), time complexity, and so on. The results show that Secure Data can be used to ensure security in IoT-based healthcare systems.

The following is the summary of the article's arrangement: Sect. 2 describes the current state of development on this task security for IoT applications. Section 3 describes the problem statement. The recommended framework for improving security in the IoT model for the healthcare sector is outlined in Sect. 4. Section 5 contains the results and a comparative analysis. Finally, Sect. 6 brings the research to a conclusion.

## 2 Related work

The following are some of the most recent papers linked to this research: The growth of the Internet of Medical Things (IoMT) is projected to revolutionize the healthcare business as the IoT develops. For this reason, Denis and Madhubala (2021) used a new hybrid of grasshopper optimization combined particle swarm optimization in elliptic curve cryptography, to explore the security of medical data in IoT. Medical images are safeguarded in the IoT architecture using this approach. Dhawan et al. (2021) offered an image steganography

approach that employs a Salp Swarm Optimization Algorithm (SSOA) based responsive encoding scheme to maximise payload capacity by adjusting various parameters. The fidelity of the stego pictures is then improved using a hybrid Fuzzy Neural Network with either a backpropagation learning technique. The stego pictures are then communicated to the destination using an IoT protocol that is very secure. Because of the nature of IoMT, some design issues arise, such as privacy and security, insufficient resources, and insufficient training data by Alqaralleh et al. (2021). This elliptic curve cryptography (ECC) is used, and the hybridization of grasshopper and fruit fly optimization (GO-FFO) technique is used to generate the best ECC keys. The hash values are then encrypted using the neighbourhood indexing sequence (NIS) combined burrow wheeler transform (BWT), known as NIS-BWT. Finally, to identify the presence of illness, a deep belief network (DBN) is used in the categorization process.

The healthcare data generated by the IoT network system is encrypted using the Lightweight SIMON based block cypher for safe transmission by Rani et al. (2020). Then, using the Chinese Remainder based Theorem (CRT), a duplicate of each ciphertext is generated depending on the number of users chosen, and the information is distributed one of the most appropriate number of customers. The Hybrid Teaching, as well as Learning Based Optimization (HTLBO) of meta-heuristic algorithm is used to choose users in the IoT. Then, proposed quality healthcare firms who can deliver a comprehensive number of healthcare treatments to IoT participants. Conventional cryptosystems are insufficient to address these difficulties, thus Elhoseny et al. (2020) proposed a model that combines 2D based Discrete Wavelet Transform 1 first or two Level steganography with a mix of the Advanced Encryption Standard (AES) as well as Rivest Shamir Adleman (RSA) techniques. The hybrid encryption approach is designed to keep diagnoses data safe while it is integrated in the RGB channels of a healthcare main picture. The employment of an Adaptive Genetic Algorithm based Optimal Pixel Adjustment Process (AGA-OPAP), which enriches data concealing ability and also steganography qualities, is one of the important innovations. Heterogeneous machine learning, as opposed to typical centralised learning algorithms, allows for the effective and beneficial application situations. Nevertheless, certain security needs may be incompatible with distributed learning. To overcome such obstacles, Ku et al. (2022) offered a privacy-preserving federated learning strategies focused on the cryptographic fundamental of homomorphic re-encryption that can either secure or learn over information using homomorphic re-encryption.

In recent times, privacy-preserving data analysis techniques have been studied in order to give accurate solutions for ensuring the privacy of information in the cloud. Therefore, Balashinnumaraja and Ganeshbabu (2022) presented a novel hybrid meta-heuristic paradigm for establishing a privacy protection strategy for cloud-based commercial data. The major goal of this study is to create a novel hybrid red deer-bird swarm method (RD-BSA) that ensures greater convergence while minimizing the use of control factors in solution creation. The security of the patient's records is a significant problem. As a result, Ogundokun et al. (2021) created the Crypto-Stegno framework, a security paradigm for IoT-based medical environments. The security, severe data loss, and supreme embedding ability of the patients' healthcare and vital medical data are all proven. Due to the lack of learning parameters, this approach is not usable in blockchain security systems. Kalyani and ShilpaChaudhari (2020) have created a novel cryptographic-based IoT security authentication technique for blockchain security. This work uses high-reliability Optimal Homomorphic Encryption (OHE) to secure IoT essential data. To categories sensitive data from the IoT dataset, the Deep Learning Neural Network (DNN) structure is utilized. Following classification, OHE encrypts and decrypts sensitive information. During encryption, the

key is authenticated, and the best key is selected using the Step size FireFly (SFF) optimization method.

### 3 Problem statement

An e-health IoT system manages the healthcare system, which includes multiple patient data. IoT technology solves serious security concerns connected to securing sensitive data that arise as a consequence of current conventional networks by connecting everything. As a result, effective access control is essential to transfer data in order to resolve difficulties. As a result, hostile attacks on healthcare systems are occurring, with the goal of hacking patient data at the transmission, data collecting, and storage stages. In any case, a third-party supplier would decrypt and calculate some secret data from customers using typical encryption technologies before processing it (Raghuvanshi et al. 2021). Encryption methods are commonly used to ensure the security of digital systems. A disadvantage of classical symmetric ciphering is the possibility of exposing the secret key. Encryption has become one of the options for keeping data confidential.

Encryption is a technique for turning an image into a cryptic image. A clever new encryption technology can help to reduce security threats significantly. In a vast and complicated setting, authentication process and validation are so complex that they threaten the logical effectiveness of the greatest cryptographic technique (Adat and Gupta 2018). Typically, the IoT-based healthcare functions by collecting the patient's medical records, treat history, etc., and store it in the cloud server for analysis and access by healthcare providers. However, this data storage and transmission poses several security challenges and risks. Some key challenges associated with big IoT healthcare systems includes data privacy and confidentiality, data integrity, secure data transmission, computational complexity, key management, etc. The storage of patient data in the cloud server concerns about unauthorized access, data breaches, and potential misuse of sensitive information. Therefore, ensuring data privacy and confidentiality during storage and transmission is important to prevent the unauthenticated access. Moreover, confirming stored information remains accurate and unaltered throughout its lifecycle is important to avoid incorrect medical decisions by health providers. Generally, the IoT devices such as medical wearables, monitoring sensors, etc., are vulnerable to cyber threats, providing an entry point for attackers to access the patient data. Furthermore, the transmission of healthcare data over unsecured communication networks or channels imposes risk of data interception. Therefore, providing a strong authentication mechanism is important to provide secure and authorized data access in IoT-based healthcare system. The proposed hybrid security framework combines the DHEA and ASS-JFO algorithms to address the security challenges in IoT-based healthcare systems comprehensively. To ensure data privacy and confidentiality, the DHEA algorithm encrypts patient data during storage and transmission, rendering it unreadable to unauthorized users. Additionally, DHEA's homomorphic encryption capabilities enable secure computation on encrypted data without decryption, ensuring data integrity throughout its lifecycle. The integration of the ASS-JFO model optimizes the encryption and decryption processes by selecting the optimal cryptographic keys, enhancing key security and reducing computational time. This robust key management process makes the system more scalable to handle the vast amount of data generated by IoT healthcare devices. Overall, the proposed methodology provides a strong security foundation, safeguarding patient data from

unauthorized access, data breaches, and potential cyber threats, thereby enabling secure and authorized data access in the IoT-based healthcare environment.

## 4 Proposed methodology

Securing data in the route of transmission has become a more critical and difficult undertaking in recent years. However, it is one of the most important models for securing patient data in the healthcare context. Healthcare services and infrastructure are improved to the smart level in the digitalized world through the internet. As a result, after using IoT technology to detect the body's condition, all of the data is saved on the cloud, resulting in a large amount of patient data. Because of the massive quantities of data in cloud environments, safeguarding the cloud, as well as the information in cloud services, is challenging (Fig. 1).

The main goal of this study is to develop an independently verified image data transfer system in IoT technology that assures medical image privacy, confidentiality, and authenticity. Figure 2 depicts the suggested framework for a secure IoT strategy in the healthcare sector. Firstly, standard healthcare data from IoT-based big data is evaluated for security method validation. For considerable data exchange, the size of the huge data is then compressed using the effective lossless compression technique known as Golomb coding. The suggested ASS-JFO-DHEA model also protects the shared data by combining a new hybrid Artificial Shuffle Shepherd Integrated Jellyfish optimization (ASS-JFO) method with Digital Homomorphism Elgamal Algorithm (DHEA) encryption. After the data has been encrypted, it is uploaded to the cloud server via internet, and the data decryption process uses the best feasible private key. The purpose of optimal key selection in a security programmer is to use hybrid optimization called ASS-JFO to find the best private and public keys for both transmitter and the receiver. and the built framework is run in MATLAB.

### 4.1 Data transmission in IoT

Gathering healthcare data from a number of sources facilitates effective interaction between patients and doctors, improving general patient care quality, and provides greater insight into individual illnesses. The data acquired by IoT nodes will be sent to a gateway server that will combine the information and send it to a cloud infrastructure for more analysis. Nevertheless, data security in healthcare research is critical because it necessitates the gathering, storage, and use of huge volumes of personal data, most of which is sensitive and possibly humiliating.

### 4.2 Golomb coding compression

Data compression is significant in the storage and transmission of big data because it decreases network bandwidth as well as resource capacity. Thus, the Golomb coding lossless compression method is provided in this work. For this execution, initially set up the parameter as  $G$  to a value of integer and the encoded number  $M$  is defined as

$$\begin{aligned} \text{Quotient} &= Q = \text{floor}(M/G) \\ \text{Remainder} &= R = M \text{ modulo } G \end{aligned} \quad (1)$$

Furthermore, the code word is generated for the processing as the format like  $\langle \text{Code of Quotient} \rangle \langle \text{Code of Remainder} \rangle$ . Where Unary coding is used to express the

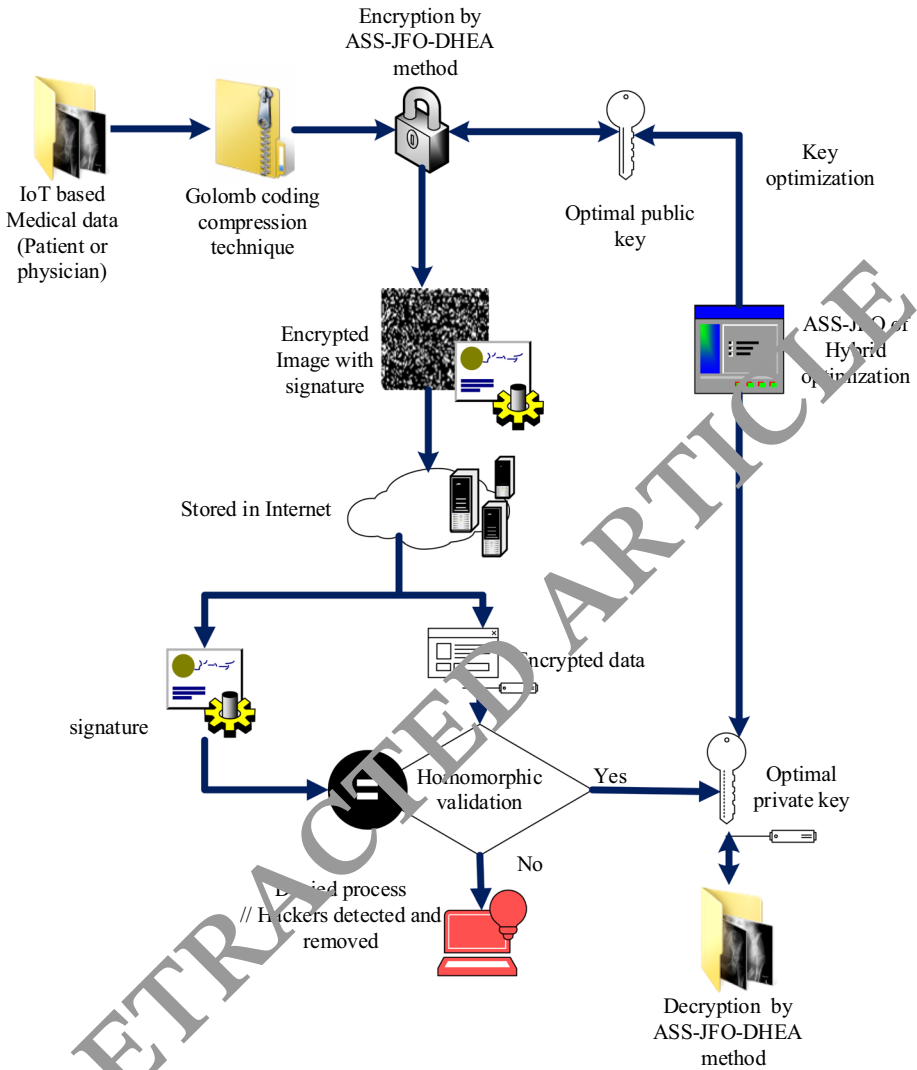


Fig. 1 Proposed framework of healthcare data security

quotient and truncated binary code is used to represent the remainder. In this way, the big amount of data is compressed for sharing to the users.

### 4.3 Proposed DHEA with ASS-JFO method

This section also summarizes the IOT health records in the healthcare portion, which includes DHEA. Key generation, key optimization, key distribution, encryption, signature, verification, and decryption are just a few of the necessary processes in this suggested DHEA cryptographic security system. For key generation, an ASS-JFO optimization model is being proposed to improve the level of security of IOT frameworks.



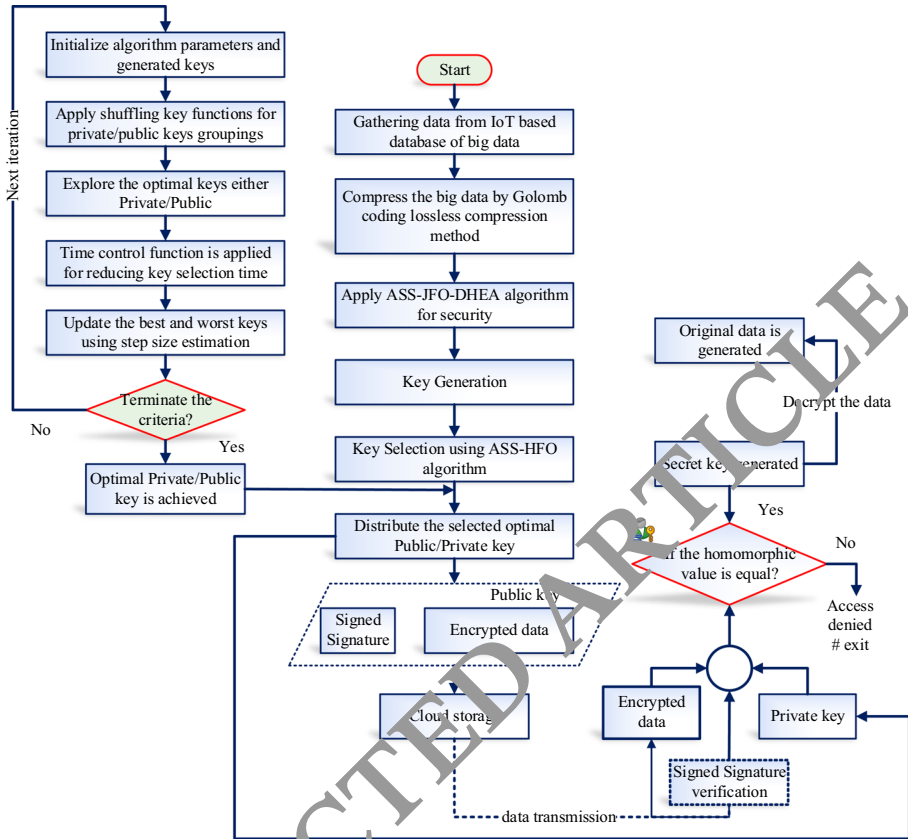


Fig. 2 The work flow of proposed security improvement in IoT based healthcare system

### 4.3.1 Key generation

The proposed DHEA algorithm has asymmetric key function. There are two stages to key generation. The first part involves selecting algorithm parameters that may be distributed across system users, while the second stage involves computing a unique pair of keys for a particular user. In parameter generation, the length of the key as  $L$  and prime number  $u$  of  $L$ -bit is selected. Furthermore, the cryptographic has function  $A$  is selected with the consequences of  $L$ -bits. While validation, if  $N > L$ , only leftover bits of  $L$  is used for the hash output. Then, the generator  $v < u$  is selected for the multiplication modulo  $u$ . Therefore, the parameter of DHEA is  $(u, v)$  and it is distributed between the users and data owners. The second stage evaluates the pair of keys for a specific user provided model parameters. The integer value of  $i$  is selected randomly from  $\{1, \dots, u - 2\}$ ,  $i$  is the private key and the public key  $j$  is estimated using Eq. (2),

$$j = v^i \text{ mod } u \tag{2}$$



### 4.3.2 Key selection optimization

To acquire the best public and private key for security, the ASS-JFO optimization approach have used. The conception of establishing the accumulation of specific ways of these approaches is described in the above parts, and the hybridization of shuffle shepherd with artificial jellyfish optimization is conducted in order to meet the needs of the ideal key of DHEA with the most extreme key.

#### Step 1: Initialization

When the key strategy is implemented, the integer values are considered to generate a new population size for the optimal key selection procedure. The following equation starts ASS-JFO with a randomly formed starting member of keys in the search process:

$$K_{x,y}^0 = K_{\min} + r \times (K_{\max} - K_{\min}); \quad x = 1, 2, \dots, i \quad \text{and} \quad y = 1, 2, \dots, j \quad (3)$$

where  $K_{\min}$  and  $K_{\max}$  are the minimum and maximum boundaries of  $x$  and  $y$  parameters, respectively;  $r$  is a random variable for each constituent created between 0 and 1;  $x$  is the number of individuals in key each group, and  $y$  is the number of key groups.

#### Step 2: Shuffling key

The first  $i$  parts of each key are randomly distributed in the first column of the multi-keys matrix (Eq. 4) as the first element of each key in this procedure, depending on their fitness values. The following  $i$  members are selected similarly to the previous stage and are randomly arranged in the column to form the second column of multi-keys. This technique is repeated  $j$  times till the multi-keys matrix are generated as follows:

$$M = \begin{bmatrix} K_{1,1} & K_{1,2} & \dots & K_{1,j} & \dots & K_{1,j} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ K_{x,1} & K_{x,2} & \dots & K_{x,y} & \dots & K_{x,j} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ K_{i,1} & K_{i,2} & \dots & K_{i,y} & \dots & K_{i,j} \end{bmatrix} \quad (4)$$

It's important to note that each row of multi-keys represents the users of each key, with the first column of multi-keys representing the best users in each key. In addition, the individuals in the last column are the lowest in each key.

#### Step 3: Key exploration

Here, the function of jellyfish optimization is applied for the optimal selection of keys. To replicate type selection, a key  $j$  different than the one of attention  $i$  is chosen at random, and the movement is determined by a vector from the key of focus  $j$  to the selected key  $i$ . When the quantity of data at the selected key's position  $i$  surpasses that at the key's position  $j$  the latter advances forward towards the earlier. If the quantity of data accessible to the selected key  $i$  is less than that provided to the key of attention  $j$  it goes aside from it. As a result, each key goes in a better direction to find food in a swarm. The vector of choice and the updated position of a key is estimated using Eq. (5). This movement is seen as a successful use of the search engine area.

$$K_i(t+1) = K_i(t) + r(0, 1) \times \begin{cases} K_j(t) - K_i(t) & \text{iff}(K_i) \geq f(K_j) \\ K_i(t) - K_j(t) & \text{iff}(K_i) < f(K_j) \end{cases} \quad (5)$$

where  $f$  is represented as the objective function of key selection  $K$ . The time control method is established for the optimal selection of keys because the typical elgamal encryption

method has consume more time to key selection. Thus, the proposed hybrid optimization method reduces the time consumption. The random value of the time control function varies from 0 to 1 over time. The time control function is executed using Eq. (6),

$$K(t) = \left| \left( 1 - \frac{t}{T_{\max}} \right) \times 2 \times r(0, 1) - 1 \right| \tag{6}$$

where,  $T_{\max}$  is denoted as the maximum count of iteration and the number of iteration for particular execution is denoted as  $t$ . As time passes,  $(1 - K(t))$  tactics one, and  $(1 - K(t)) > r(0, 1)$  of probability finally more than the  $r(0, 1) > (1 - K(t))$ . Thus, this kind of key selection is preferred.

**Step 4: Key updating**

Two vectors are used to determine a specific step size for each key member. The first vector  $S_{x,y}^w$  depicts the capacity to explore additional areas of the solution space. The second vector, on the other hand  $S_{x,y}^b$  denotes the ability to discover the vicinity of previously visited potential search space regions. The following is the mathematical expression for the iterations:

$$S_{x,y} = \gamma \times r_1 \times (K_{x,w} - K_{x,y}) + \phi \times r_2 \times (K_{x,b} - K_{x,y}) \quad x = 1, 2, \dots, i \text{ and } y = 1, 2, \dots, j \tag{7}$$

where,  $K_{x,b}$  and  $K_{x,w}$  are the best and worst parameters in terms of objective function value.  $K_{x,y}$ ,  $r_1$  and  $r_2$  are random parameters with each component created between 0 and 1; It's value observing that the  $x^{th}$  group's initial parameter  $K_{x,1}$  doesn't have an associate who is better than it, thus  $S_{x,y}^b = 0$ . Consequently,  $K_{x,j}$  does not have a worst parameter than itself due to the  $x$ th group final parameters, henceforth  $S_{x,y}^w = 0$ . Furthermore,  $\gamma$  and  $\phi$  are the variables that effect exploration as well as exploitation, correspondingly.

**Step 5: Termination**

The new parameter of the  $K_{x,y}$  is computed using Eq. (8) based on the previous step. Subsequently, if the  $K_{x,y}$  parameter is not lesser than its earlier objective function level, it will be updated using Eq. (8)

$$\text{New } K_{x,y} = K_{x,y} + S_{x,y} \tag{8}$$

This hybrid technique completes the task of learning the hybridization form with the greatest attention; the best solution is chosen from the algorithms. Until the ideal key for the health care data is obtained, the method is continued.

**4.3.3 Encryption stage**

Encryption is a method of encrypting images or data in a system that lets them to be authenticated. The data owner encrypts the data  $d$  to users under the  $j$  of public key. Record the data  $d$  to part  $D$  of  $j$  using reversible mapping strategy. The integer value of  $k$  is selected randomly from  $\{1, \dots, u - 2\}$ . Furthermore, estimate the shared secret using Eq. (9)

$$S := y^k \tag{9}$$

Also compute the cipher data  $x_1$  and  $x_2$  as follows

$$\begin{aligned} x_1 &:= v^k \\ x_2 &:= d \cdot S \end{aligned} \tag{10}$$

Consequently, the encrypted data of  $x_1$  and  $x_2$  sent to the users from data owners. Since  $x_2 \cdot d^{-1} = S$  is attained only if the encrypted  $(x_1, x_2)$  and original data is known by any one. As a result, a new  $S$  and  $k$  is generated for each data to enhance the security. Therefore,  $k$  is also known as an ephemeral key.

### 4.3.4 Signing stage

For powerful and secure connection, the authenticated data is transferred in encrypted form. Thus, the signing performance is applied for the encrypted data  $d$ . For this, the integer  $l$  is randomly selected as  $\{2, \dots, u - 2\}$  with the corresponding prime number  $q - 1$ . Computing the signature parameter  $q$  and  $z$  as follows:

$$\begin{aligned} q &:= v^k \pmod u \\ z &:= (A(d) - iq)l^{-1} \pmod{(u - 1)} \end{aligned} \tag{11}$$

If it is improbable function then  $z = 0$  and it repeats the function with different  $l$  value. Thus, the signed signature data is considered as  $(q, z)$ . After signing the data the information has been stored in the network storage.

### 4.3.5 Authentication analysis

If the cypher data has to be authenticated by transmitting a signature, the receiver must know the sender's optimal private keys, and the random values should be examined at that point. Finally, determine the homomorphism capability in order to improve the security level of healthcare data in IoT. For authentication analysis, the signature  $(q, z)$  is a valid signature for a data  $d$  as per the following states as validate that  $0 < q < u$  and  $0 < z < u - 1$ . The verification of the signature is validated as

$$v^{A(d)} = i^q q^z \pmod u \tag{12}$$

In the perspective that a signature issued using the signing method has always been recognized by the verifier, the algorithm is accurate. Thus, the homomorphic validation is performed for the encrypted data as  $x(d) = (v^q, d.y^r)$  for random of  $\{q, \dots, u - 2\}$ . Then, the homomorphic property is as follows

$$\begin{aligned} x(d_1) * x(d_2) &= (v^{q_1}, d_1.y^{r_1})(v^{q_2}, d_2.y^{r_2}) \\ &= (v^{q_1+q_2}, (d_1.d_2)y^{r_1+r_2}) \\ &= x(d_1 \cdot d_2) \end{aligned} \tag{13}$$

### 4.3.6 Decryption

Decryption is a diametrically opposed idea to encryption, and it is the process of converting an encrypted element into its own plain image. The encrypted data  $(x_1, x_2)$  is decrypted with the private key  $i$  as subsequently. Estimate  $S := x_1^i$ , meanwhile  $x_1 = v^k, x_1^i = v^{ik} = y^k$ . Thus, it is the identical shared secret that data owners used to encrypt his data. Evaluates  $S^{-1}$  in the group, this can be calculated in a variety of ways. If  $N$  is a subset of a multiplicative group of numbers modulo  $u$ , where  $u$  is a prime number, then compute

$$d := x_2 \cdot S^{-1} \quad (14)$$

The estimation generates the original data  $d$ , because  $x_2 = d \cdot S$ , thus, the evaluation is denoted as

$$x_2 \cdot S^{-1} = (d \cdot S) \cdot S^{-1} = d \cdot f = d \quad (15)$$

Therefore, the encrypted data is returns to the original data. The work flow of proposed security improvement in IoT based healthcare system is illustrated in Fig. 2.

## 5 Result and discussion

The suggested IoT security framework was designed using MATLAB 2019a on a Windows computer with an Intel (R) Core i5 processor running at 1.6 GHz and 4 GB RAM. Furthermore, the proposed algorithm is compared to many standard methods as well as a performance metric. Digital data are combined together in the Kaggle dataset. An imaging set, scans, genetic data, medical reports, and a CT scan are all included in the digital IoT based database. The following is the parameter configuration: The maximum number of fitness value evaluations for all parameters is  $4.25 \times 10^4$ , and the size of the population is 50.

### 5.1 Performance analysis

This section describes the data quality analysis of the planned task using several performance indicators. For security level analysis assessment measures such as Root Mean Square Error (RMSE), Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), time complexity, and so on are utilized. The proposed method is employed as the learning optimization algorithm. The square root of the average of the square of all errors is the root mean squared error (RMSE) over the each iteration using Eq. (16)

$$RMSE = \sqrt{\frac{\sum_{o=1}^n (t_o - a_o)^2}{n}} \quad (16)$$

where the actual output is denoted as  $a_o$  and the targeted output is denoted as  $t_o$ . Mean Square Error (MSE) can be used to determine the dependability of an image by quantifying its distortion and matching level.

$$MSE = \frac{1}{n} \sum_{a=I,E}^n (I - E)^2 \quad (17)$$

where  $n$  is the overall quantity of input data and  $I$  as well as  $E$  is the input and encrypted data respectively. The statistically significant difference between the expressive range of input data as well as data encryption invisibility is determined by the Peak Signal to Noise Ratio (PSNR). The PSNR is calculated by using the following:

$$PSNR = 10 \log_{10} \left( \frac{225^2}{MSE} \right) \quad (18)$$

The amount of received bits in a stream of data via a channel of communication that were changed due to distortion, noise, compression, or bit synchronization faults is known as the number of bit errors.

$$BER = \frac{1}{PSNR} \tag{19}$$

The compression ratio is calculated as the proportion between the uncompressed as well as compressed sizes of data, as expressed in Eq. (8)

$$CR = \frac{U_r}{C_s} \tag{20}$$

where  $U_r$  is the uncompressed data size, and  $C_s$  is the compressed data size. The encryption time is measured as the period it takes to convert plain data into encrypted data, which is calculated using Eq. (21) as follows:

$$\text{Encryption time} = \frac{\text{Overall encrypted plain data (bytes)}}{\text{Encryption time (ms)}} \tag{21}$$

The time it takes to decode encrypted data into plain data is measured in decryption time, which is computed as follows in Eq. (5):

$$\text{Decryption time} = \frac{\text{Overall decrypted cipher data (bytes)}}{\text{Decryption time (ms)}} \tag{22}$$

The data transfer rate is defined as the speed at which data is sent, which is calculated using Eq. (23) and is approximated based on data size and transfer time,

$$D_s = \frac{\text{Amount of data size (kb)}}{\text{transfer time}} \tag{23}$$

The volume of data accumulated at the receiver side is measured by the time it requires for data to be transferred through the procedure, which is referred to as throughput.

$$T = \frac{\text{Amount of data received to the users}}{\text{Delay of time}} \tag{24}$$

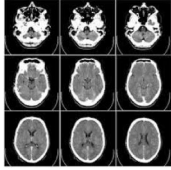
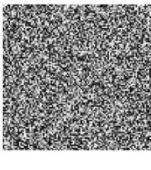
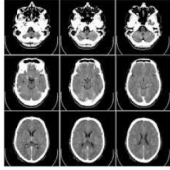
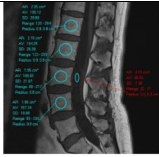
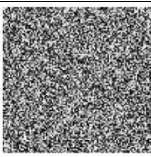

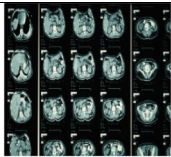
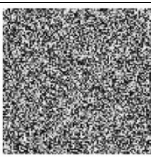
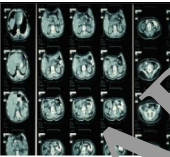

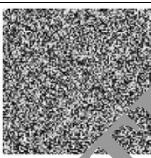
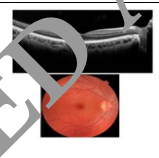
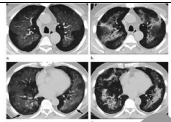
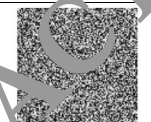
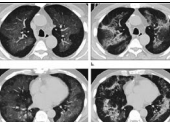
Data confidentiality is a fundamental data security service. The difference between the original and received data during data transfer determines the confidential rate.

### 5.2 Experimental analysis

For the performance study of the proposed ASS-JFO-DHEA model in the healthcare system, consider five sample healthcare images. Table 1 shows the enhanced information security outcomes for sample healthcare data. The five sample images are (a) MRI brain tumor, (b) Spinal cord, (c) CT scan images, (d) Retinal scan data and (e) CT lung disease data.

Consequently, Table 2 shows the suggested model’s optimal security outcomes. Encryption time, key breaking time, encryption size, encryption memory, decryption memory, compression ratio, and decryption time were all shown. Even if the encryption and decryption times increase as the file size grows, the recommended technique delivers the fastest

**Table 1** The outcomes of medical image security

Sample images	Encrypted	Decrypted	RMSE	PSNR	MSE	BER
a) 			0.6	80	0.002	0
b) 			0.7	79	0.0025	0
c) 			0.8	76	0.0026	0
d) 			0.85	76	0.003	0
e) 			0.87	74	0.008	0.01

encryption and decryption speeds. As a result, the amount of encrypted and decrypted memory in the proposed framework grows. Furthermore, when the key breaking time is the minimum possible given the file size, the recommended solution is optimal.

### 5.2.1 Comparative analysis

In terms of PSNR, RMSE, MSE, Encryption time, Decryption time, key braking time, confidential rate, BER, data transfer rate, compression ratio, throughput, and key size, the proposed method has been compared to various conventional methods such as GO-FFO-ECC (Alqaralleh et al. 2021), SIMON- HTLBO (Rani et al. 2020), AGA-OPAP (Elhoseny et al. 2020), RD-BSA (Balashunmugaraja and Ganeshbabu 2022), and OHE-SFF (Kalyani and ShilpaChaudhari 2020). The Comparative analyses in terms of (a) RMSE, (b) PSNR, (c) MSE and (d) BER are shown in Fig. 3a–d. The RMSE value obtained from the suggested methodology is then compared to that obtained from traditional approaches and the results are shown in Fig. 3a. The PSNR value derived from the suggested technique in comparison to the current methods are illustrated in Fig. 3b. PSNR is the ratio between

**Table 2** Proposed model of optimized results

Data size (kb)	Encryption size	Encryption memory	Encryption time (ms)	Decryption memory	Decryption time (ms)	Key breaking time	Compression ratio
500	74	1,257,345	36	668,758	38	98	16.71
1000	76	1,289,159	38	673,561	37.5	97	17.14
1500	150	1,304,884	39	680,873	40	97.6	17.40
2000	173	1,347,962	42	691,347	41	95	17.62
2500	248	1,345,969	45	699,354	44	92.6	17.67

RETRACTED ARTICLE



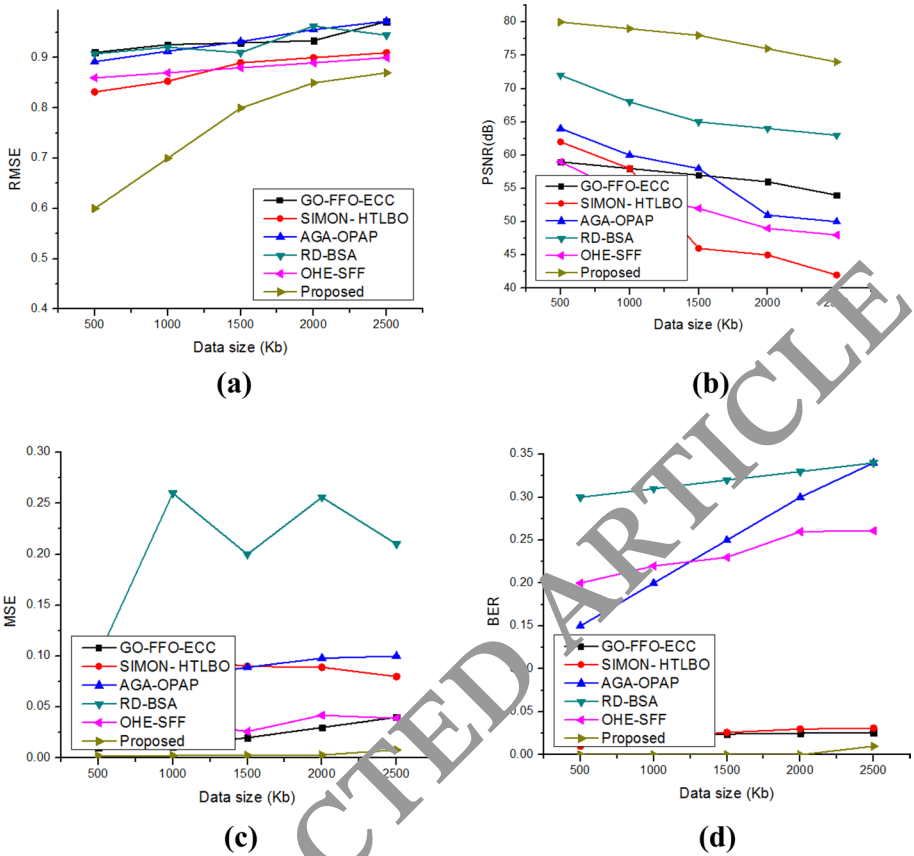
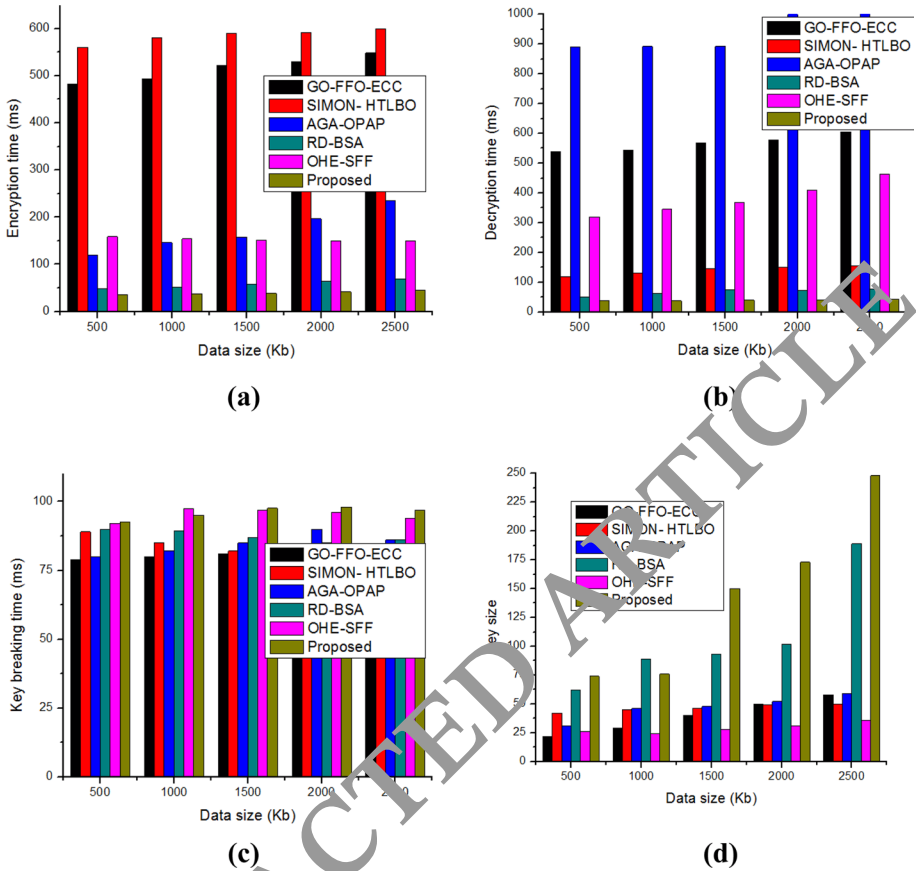


Fig. 3 Comparative analysis in terms of **a** RMSE, **b** PSNR, **c** MSE and **d** BER

the greatest attainable strength and the power of degrading noise that affects the integrity of a transmitter output. Comparing medical image security systems like GO-FFO-ECC, SIMON-HTLBO, AGA-OPAP, RD-BSA, and OHE-SFF is one of the encryption methods used. The recommended strategy improves the PSNR assessment more than the other current methods. The PSNR in the proposed version of a 2500 kb data is 74 dB, which is the greatest among the several ways. Thus, a higher PSNR value indicates a higher-quality guaranteed image restoration.

Figure 3c provides a comparative analysis of the suggested MSE value to traditional approaches. The observation shows that the MSE value for the proposed system is lower on a range of image categories and with a low error rate when compared to the existing system. The BER value derived from the suggested technique in comparison to the current methods are illustrated in Fig. 3d. Furthermore, the BER of the proposed method is highly reduced over the existing methods.

Figure 4a compares the suggested encryption time with the time taken by existing models. The presentation demonstrates that the suggested technique outperforms traditional methods for various file sizes, including 500 kb, 1000 kb, 1500 kb, 2000 kb, and 2500 kb. Because of the suggested approach, encryption time has been reduced



**Fig. 4** Comparative analysis **a** encryption time, **b** Decryption time, **c** key breaking time, and **d** key size

significantly compared to previous methods. The recommended decryption time in comparison to existing models are demonstrated in Fig. 4b. The presentation demonstrates that the suggested technique outperforms traditional methods for various file sizes, including 500 kb, 1000 kb, 1500 kb, 2000 kb, and 2500 kb. The suggested approach has achieved a much faster decryption time than previous models. In Fig. 4c, the time it takes to break a key in the proposed security system is compared to different values from previous models. When compared to traditional approaches, the key breaking time is improved significantly. As a result, it demonstrates how IoT technology would increase security in the healthcare sector.

Keys determine how a cypher works, and only the right key can convert an encrypted file to original message. Many encryption systems are based on publicly accessible techniques or are publicly available; hence, assuming no analytic assault, the system’s security is only defined by the difficulty of obtaining the key. Since a result, estimating key size is critical, as it determines the amount of bits in a key used by a security method. Figure 4d presents the comparative analysis for key size. The graphical findings demonstrated the optimal security reached by the recommended approach when compared to earlier solutions.

Furthermore, the comparison of the proposed ASS-JFO-DHEA model technique attained compression ratio over existing methods like GO-FFO-ECC, SIMON- HTLBO, AGA-OPAP, RD-BSA, and OHE-SFF for data sizes of 500 kb, 1000 kb, 1500 kb, 2000 kb, and 2500 kb are detailed in Fig. 5a. The graphical representation and its values show that the proposed method has achieved supreme compression ratio over the earlier techniques. Because the traditional GO-FFO-ECC, SIMON-HTLBO, AGA-OPAP, RD-BSA, and OHE-SFF has achieved very less throughput, the observation reveals that the suggested system ASS-JFO-DHEA has achieved excellent throughput efficiency over conventional methods are illustrated in Fig. 5b. However, the suggested system has a throughput efficiency of 98.96% for 2500 kb. The observed data transfer rates for 500 kb, 1000 kb, 1500 kb, 2000 kb, and 2500 kb are 11.76 kb/s, 12.03 kb/s, 13.64 kb/s, 18.52 kb/s, and 20.21 kb/s, respectively, using the suggested ASS-JFO-DHEA approach, which is very high while compared to the existing models are shown in Fig. 5c. The suggested system’s confidentiality rate validation is estimated for various file sizes. The suggested approach achieves a confidentiality rate of 100% for varied file sizes. The standard technique, on the other hand, has a much lower confidentiality rate for all data sizes (see Fig. 5d). As a result, the results suggest that the proposed ASS-JFO-DHEA model performs well.

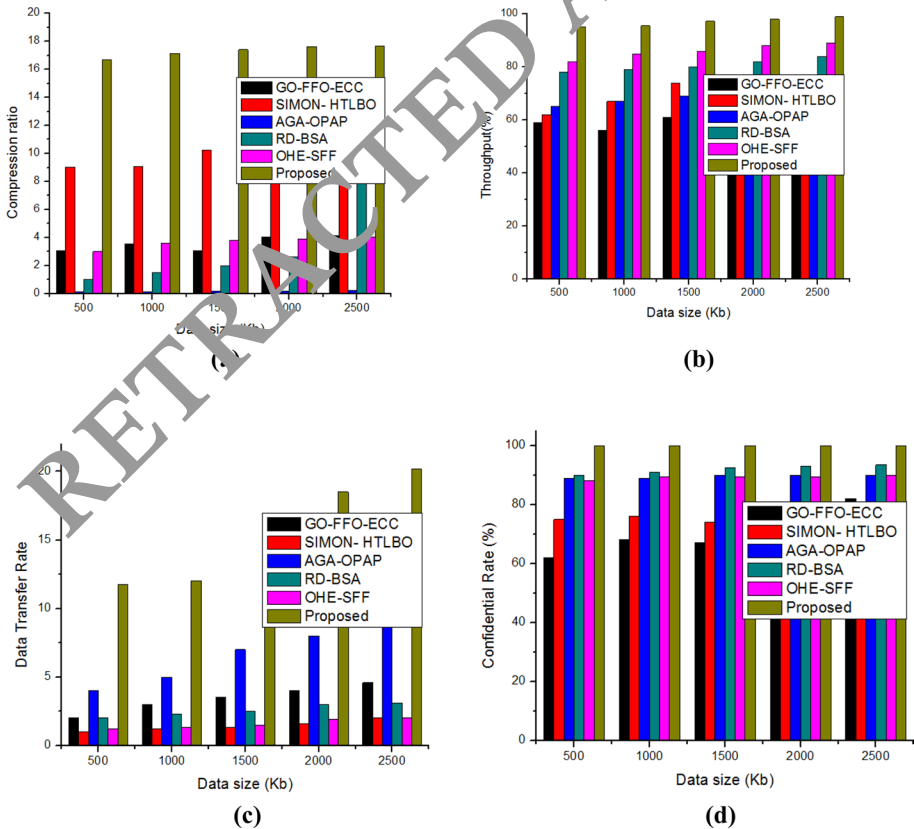


Fig. 5 Comparative analysis a compression ratio, b throughput, c data transfer rate, and d confidentiality rate

From the comparative analysis, it is observed that the traditional approaches like GO-FFO-ECC, SIMON-HTLBO, AGA-OPAP, RD-BSA, and OHE-SFF, the proposed model offers significant enhancements to the security of healthcare IoT. The developed ASS-JFO-DHEA framework confirms robust protection against unauthenticated data access and data breaches by encrypting the patient data at rest and during transmission. This process enables highly secure data processing and transmission in IoT healthcare system compared to the traditional models. Moreover, the optimization of encryption process using the ASS-JFO algorithm provides optimal cryptographic selection, and offers more scalability to the system. The strong encryption and optimal key management process helps to resist attacks and other susceptible events in the healthcare system and make challenge for attackers to break the encryption. Thus, the proposed algorithm provides greater data confidentiality and privacy than the traditional methods. Moreover, the data integrity is maintained in the system by preventing the data alteration through robust key management. This helps the healthcare management system to avoid incorrect medical decisions. The major challenge faced by the traditional techniques is the computational efficiency and scalability. The designed model mitigates these issues by enabling parallel data processing and optimization. The ASS-JFA integrated in the developed model allows parallel processing of data, enhancing the computational efficiency and scalability of the system. Furthermore, this model has the tendency to adapt to the dynamic and resource-constrained IoT network and provides a balance between the security and computational efficiency. These features of the presented cryptographic mechanism make it well-suited for large-scale IoT environment. Thus, the developed model provides improved security, data integrity, computational efficiency, scalability and resistance to attacks compared to the traditional models. Moreover, the ASS-JFO-DHEA approach complies with relevant privacy and security regulations, such as Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR), by offering strong encryption through DHEA, confirming data privacy and confidentiality during storage and transmission. Additionally, the optimization capabilities of ASS-JFO enhance key security and reduce vulnerabilities in key management, further aligning with HIPAA and GDPR requirements for safeguarding sensitive patient data. By encrypting patient data and enabling secure computations without decryption, the approach upholds data integrity and privacy principles set forth by these regulations, ensuring that healthcare IoT systems maintain the necessary privacy, security, and confidentiality standards to protect patient information.

### 5.3 Discussion

This module presents how the developed model outperforms the existing cryptographic approaches in terms of security, scalability, and computational efficiency in IoT-based healthcare system. Firstly, the combination of an optimization approach with the encryption algorithm provides a multi-layered security framework, preventing the unauthenticated access. This multi-layered security architecture potentially detects the cyber-attacks and safeguards the sensitive patient data in IoT healthcare. The utilization of ASS-JFO in the developed security mechanism ensures robustness against cyber threats by intelligently shuffling and guiding the optimization process. Moreover, the capacity of the ASS-JFO algorithm to determine the optimal solution in a large solution space provides parallel data analysis and processing, making the system more scalable to handle large IoT healthcare system. In addition, the parallel data analysis improves the computational efficiency by minimizing the computational overhead related with

key selection, and speed up the encryption and decryption process. The integration of optimization and encryption approaches reduces the data processing and transmission latency; thus, it can be more suitable for quick decision making in real-time healthcare scenarios. Furthermore, the employment of advanced DHEA encryption models in the developed framework ensures integrity of data transmitted and stored in IoT healthcare units. Thus, the developed model provides real-time data sharing and analysis in IoT healthcare units without compromising the data privacy and security.

The use of a unique ASS-JFO-DHEA approach in the healthcare system is examined in this study for IoT-based security enhancement. Although the usage of IoT has grown significantly in recent years, data security from other unauthenticated users remains a big issue. As a result, this paper proposed ASS-JFO-DHEA model technique used MATLAB software to create a unique security-enhanced method. The comparison of the proposed ASS-JFO-DHEA model technique to existing methods like GO-FFO-ECC, SIMON- HTLBO, AGA-OPAP, RD-BSA, and OHE-SFF for data size of 500 kb, 1000 kb, 1500 kb, 2000 kb, and 2500 kb are detailed in Tables 4, 5, 6 and 7. When comparing the new ASS-JFO-DHEA model to current schemes, the proposed model outperforms the existing schemes on all criteria.

The results of the analysis show that the suggested technique has a lower RMSE value as 0.6, 0.7, 0.8, 0.85, and 0.87, for 500 kb, 1000 kb, 1500 kb, 2000 kb, and 2500 kb, MSE value as 0.002, 0.0025, 0.0026, 0.003, and 0.008 for 500 kb, 1000 kb, 1500 kb, 2000 kb, and 2500 kb, and BER value is 0, 0, 0, 0 and 0.01 for 500 kb, 1000 kb, 1500 kb, 2000 kb, and 2500 kb, as well as 36 ms, 38 ms, 39 ms, 42 ms, and 45 ms of encryption time for 500 kb, 1000 kb, 1500 kb, 2000 kb, and 2500 kb and 38 ms, 37.5 ms, 40 ms, 41 ms, and 44 ms decryption time for 500 kb, 1000 kb, 1500 kb, 2000 kb, and 2500 kb data file while compared to the different existing GO-FFO-ECC, SIMON- HTLBO, AGA-OPAP, RD-BSA, and OHE-SFF models. Moreover, the higher PSNR value as 80 dB, 79 dB, 78 dB, 76 dB, and 74 dB, for 500 kb, 1000 kb, 1500 kb, 2000 kb, and 2500 kb, compression ratio as 16.71, 17.14, 17.4, 17.62, and 17.67 for 500 kb, 1000 kb, 1500 kb, 2000 kb, and 2500 kb, throughput value as 95.07%, 95.58%, 97.3%, 98.08%, and 98.96% for 500 kb, 1000 kb, 1500 kb, 2000 kb, and 2500 kb, data transfer rate as 11.76, 12.93, 13.64, 18.52, and 20.21 for 500 kb, 1000 kb, 1500 kb, 2000 kb, and 2500 kb, confidential rate as 100% for all 500 kb, 1000 kb, 1500 kb, 2000 kb, and 2500 kb, is attained while compared to the earlier methods. Similarly, the key breaking time and key size metrics from the proposed approach in highly enhanced over the existing GO-FFO-ECC, SIMON- HTLBO, AGA-OPAP, RD-BSA, and OHE-SFF models.

The performance analysis from Table 7, in particular, at the huge scale of 2500 kb data size, has yielded outstanding results. The suggested LGE-HES approach outperforms the traditional GO-FFO-ECC, SIMON- HTLBO, AGA-OPAP, RD-BSA, and OHE-SFF techniques in terms of high PSNR value, key breaking time, key size, confidential time, compression ratio, and data transfer rate, besides less encryption time, RMSE, MSE, BER and decryption time. The proposed ASS-JFO-DHEA method has achieved higher PSNR value (74 dB), higher key breaking time (97), higher key size (248), higher confidential time (100%), compression ratio (17.67), throughput (98.96%) higher data transfer rate (20.21), and less encryption time (45 ms), less RMSE (0.87), less MSE (0.008), less BER (0.01) and less decryption time (44 ms) over the existing GO-FFO-ECC, SIMON- HTLBO, AGA-OPAP, RD-BSA, and OHE-SFF techniques. As a consequence, the overall assessment shows that when employing the optimization-assisted encrypted technique, the resulting model performs better in terms of security.

**Table 3** Performance comparison of suggested and traditional security models for data sizes up to 500 kb

Methods and parameters	GO-FFO-ECC (Alqar- alleh et al. 2021)	SIMON-HEC- (Rani et al. 2020)	AGA-OPAP (Elho- seny et al. 2020)	RD-BSA (Balashunmugaraja and Ganeshababu 2022)	OHE-SFF (Kalyani and ShiipaChaudhari 2020)	Proposed
PSNR (dB)	59	62	64	72	59	80
MSE	0.01	0.1	0.10	0.1	0.059	0.002
RMSE	0.9103	0.832	0.92	0.908	0.86	0.6
BER	0.1	0.01	0.15	0.3	0.2	0
Encryption time (ms)	482	560	120	49	159	36
Decryption time (ms)	540	120	890	51	320	38
Key breaking time	79	89	80	90	92	92.6
Key size	22	42	31	92	26	74
Compression ratio	3.055	9.0255	0.1125	1	3	16.71
Confidential rate (%)	62	75	89	90	88	100
Data transfer rate	2	1	4	2	1.2	11.76
Throughput (%)	59	62	65	78	82	95.07

**Table 4** Performance comparison of suggested and traditional security models for data sizes up to 1000 kb

Methods and parameters	GO-FFO-ECC (Alqar-alleh et al. 2021)	SIMON-HEB (Rani et al. 2020)	AGA-OPAP (Elhoseny et al. 2020)	RD-BSA (Balashunmugaraja and Ganeshababu 2022)	OHE-SFF (Kalyani and ShripaChaudhari 2020)	Proposed
PSNR (dB)	58	58	60	68	54	79
MSE	0.098	0.078	0.26	0.036	0.0025	0.098
RMSE	0.926	0.85314	0.913	0.921	0.87	0.7
BER	0.02	0.02	0.2	0.31	0.22	0
Encryption time (ms)	493	580	146	52	154	38
Decryption time (ms)	543	130	892	62	345	37.5
Key breaking time	80	85	82	89.5	97.5	95
Key size	29	45	46	89	24	76
Compression ratio	3.546	9.0692	0.135	1	3.6	17.14
Confidential rate (%)	68	76	89	91	89.3	100
Data transfer rate	3	1.2	5	2.3	1.3	12.03
Throughput (%)	56	67	67	79	85	95.58



**Table 5** Performance comparison of suggested and traditional security models for data sizes up to 1500 kb

Methods and parameters	GO-FFO-ECC (Alqar- alleh et al. 2021)	SIMON-HEC- (Rani et al. 2020)	AGA-OPAP (Elho- seny et al. 2020)	RD-BSA (Balashunmugaraja and Ganesbabu 2022)	OHE-SFF (Kalyani and ShiipaChaudhari 2020)	Proposed
PSNR (dB)	57	46	56	65	52	78
MSE	0.02	0.09	0.08	0.2	0.026	0.0026
RMSE	0.9296	0.89	0.32	0.91	0.88	0.8
BER	0.0241	0.026	0.25	0.32	0.23	0
Encryption time (ms)	521	590	158	58	152	39
Decryption time (ms)	569	145	893	74	369	40
Key breaking time	81	82	85	87	97	97.6
Key size	40	46	48	53	28	150
Compression ratio	3.069	10.256	0.169	2	3.8	17.4
Confidential rate (%)	61	74	69	80	86	97.3
Data transfer rate	3.5	1.3	7	2.5	1.5	13.64
Throughput (%)	67	74	90	92.5	89.4	100

**Table 6** Performance comparison of suggested and traditional security models for data sizes up to 2000 kb

Methods and parameters	GO-FFO-ECC (Alqar-alleh et al. 2021)	SIMON-HEB (Rami et al. 2020)	AGA-OPAP (Elhoseny et al. 2020)	RD-BSA (Balashunmugaraja and Ganeshababu 2022)	OHE-SFF (Kalyani and ShripaChaudhari 2020)	Proposed
PSNR (dB)	56	45	51	64	49	76
MSE	0.03	0.089	0.09	0.256	0.042	0.003
RMSE	0.9341	0.9	0.956	0.963	0.89	0.85
BER	0.025	0.03	0.3	0.33	0.26	0
Encryption time (ms)	530	592	197	64	149	42
Decryption time (ms)	579	150	1080	73.6	410	41
Key breaking time	82	78	90	85	96	98
Key size	50	49	52	10	31	173
Compression ratio	4.05	11.055	0.16	2	3.9	17.62
Confidential rate (%)	80	71	90	93	89.5	100
Data transfer rate	4	1.6	8	3	1.9	18.52
Throughput (%)	65	75	75	82	88	98.08

**Table 7** Performance comparison of suggested and traditional security models for data sizes up to 2500 kb

Methods and parameters	GO-FFO-ECC (Alqar- alleh et al. 2021)	SIMON-HEB/ (Rami et al. 2020)	AGA-OPAP (Elho- seny et al. 2020)	RD-BSA (Balashunmugaraja and Ganesbabu 2022)	OHE-SFF (Kalyani and ShiipaChaudhari 2020)	Proposed
PSNR (dB)	54	42	50	63	48	74
MSE	0.04	0.08	0.1	0.21	0.039	0.008
RMSE	0.972	0.91	0.9726	0.945	0.9	0.87
BER	0.026	0.031	0.34	0.34	0.261	0.01
Encryption time (ms)	548	600	235	69	150	45
Decryption time (ms)	605	155	1100	76.09	463	44
Key breaking time	84	79	86	86	94	97
Key size	58	50	59	188	36	248
Compression ratio	4.12114	11.7807	0.24	9	4.05	17.67
Confidential rate (%)	82	76	90	93.5	89.9	100
Data transfer rate	4.6	2	9	3.1	2	20.21
Throughput (%)	62	75.04	76.1	84	89	98.96

In comparison to existing approaches, the suggested method has a greater confidential rate, and high throughput with less encryption time, and decryption time. This demonstrates the suggested security algorithm's effectiveness in an IoT application environment.

Furthermore, the acceptance and perception of the model is analyzed. It depends mainly on the transparency of the security framework that is the patients are concerned about how the proposed algorithm works and the impact of this approach on their healthy journey. The simple and easy integration of the developed model provides greater transparency in preserving privacy and security of medical data associated with the patients. Thus, the successful implementation of the developed novel security mechanism ensures the acceptance and perception among healthcare professionals and patients.

Although the developed model provides greater data security and privacy, it introduces some computational overhead during the key generation process and cryptographic processes. The ASS-JFO initialize its parameters to search for optimal cryptographic keys from a large population, this requires additional computational power compared to simple key generation process. The DHEA algorithm performs computation on encrypted data without performing decryption; this process ensures privacy and integrity of data in IoT healthcare. However, the mathematical process involved in this homomorphic encryption demands additional computational resources unlike symmetric encryption. This computational overhead induced by the proposed model leads to increased resource consumption, memory, and CPU usage. This increases the implementation cost of the proposed model and minimizes the battery lifetime of IoT devices. Moreover, the IoT devices have limited resources like battery life, memory, power, etc., therefore the optimizing the resource requirements of the proposed model is necessary to fit with these IoT devices in real-world healthcare environment. In addition, the designed model requires continuous updation on emerging attacks in IoT healthcare and it demands a potential risk management algorithm to mitigate the vulnerabilities in the system.

## 6 Conclusion

The issues with data gathering in IoT-based healthcare applications were investigated in this research article, and a novel healthcare data safe system was proposed to guarantee high big data security and ensure the confidentiality of patients' data. This work introduces a novel hybrid cryptographic encryption model based on the ASS-JFO-DHEA paradigm for data security. The encryption and decryption processes are carried out by the suggested model utilising the DHEA approach. In addition, the suggested model leverages a hybridization of the ASS-JFO method for optimum key selection to reduce the computation time required for the random choice of cryptographic keys. As a result, the ASS-JFO method is used to pick optimum keys, with PSNR serving as the fitness function. The ASS-JFO-DHEA model is experimentally validated using benchmark test data. The results are evaluated with respect to conventional methods and the proposed method has achieved shorter encryption time, RMSE, MSE, BER, and decryption time, high PSNR value, key breaking time, key size, confidential time, compression ratio, and data transfer rate. The security in IoT based healthcare system can be further strengthened in the future by employing image steganography as well as watermarking methods.

**Author contributions** Securing Healthcare Big Data in Industry 4.0: Cryptography Encryption with Hybrid Optimization Algorithm for IoT Applications Chandrashekhar Goswami<sup>1</sup>, P. Tamil Selvi<sup>2</sup>, Velagapudi

Sreenivas<sup>3</sup>, J.seetha<sup>4</sup>, Ajmeera Kiran<sup>5</sup>, Vamsidhar Talasila<sup>6</sup>, K.Maithili<sup>7</sup> Department of Computer Science and Engineering, Amity University, Gwalior, India. <sup>2</sup>School of Computing Science and Engineering, Rajalakshmi Engineering College, India. <sup>3</sup> Department of Computer Science and Engineering, Dhanekula Institute of Engineering and Technology Ganguru Vijjayawada, India. <sup>4</sup>Department of Computer Science & Engineering, Panimalar Engineering College, India. <sup>5</sup> Department of Computer Science & Engineering, MLR Institute of Technology, Dundigal, Hyderabad, Telangana., India <sup>6</sup>Dept.of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India. <sup>7</sup>Department of CSE, KG Reddy College of Engineering and Technology, Chilukuru village, Telangana, India. chandrashekhargoswami.cse@gmail.com \*1, tamilselvi.p@rajalakshmi.edu.in2, velagapudisreenivas@gmail.com3, jsvpec@gmail.com4, kiranphd.jntuh@gmail.com5, vamsi@kluniversity.in6, drmaithili@kgr.ac.in7 Chandrashekhkar Goswami : Idea conceptualization, correspondence P.Tamil Selvi : Algorithm specialization Velagapudi Sreenivas : Validation of the results, J.seetha : Writing original draft Ajmeera Kiran : Editing Vamsidhar Talasila : Data collection, validation K.Maithili : Big Data in Industry 4.0 related work & Reviewing .

**Funding** Not applicable.

**Data and material availability** Data sharing is not applicable to this article as no new data were created or analyzed in this study.

**Code availability** Not applicable.

## Declarations

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

**Human and animal rights** This article does not contain any studies with human or animal subjects performed by any of the authors.

**Informed consent** Informed consent does not apply as this was a retrospective review with no identifying patient information.

**Consent to participate** Not applicable.

**Consent for publication** Not applicable.

## References

- Adat, V., Gupta, L. B.: Security in internet of things: issues, challenges, taxonomy, and architecture. *Telecommun. Syst.: Syst.* **57**(3), 423–441 (2018)
- Ahmadi, J., et al.: The application of internet of things in healthcare: a systematic literature review and classification. *Univ. Access Inf. Soc.* **18**(4), 837–869 (2019)
- Almorad, B., Y., et al.: Blockchain-assisted secure image transmission and diagnosis model on internet of medical things environment. In: *Personal and Ubiquitous Computing*, pp. 1–11 (2021)
- Atiewi, S., et al.: Scalable and secure big data IoT system based on multifactor authentication and lightweight cryptography. *IEEE Access* **8**, 113498–113511 (2020)
- Balashunmugaraja, B., Ganeshbabu, T.R.: Privacy preservation of cloud data in business application enabled by multi-objective red deer-bird swarm algorithm. *Knowl. Based Syst.* **236**, 107748 (2022)
- Calvillo-Arbizu, J., Román-Martínez, I., Reina-Tosina, J.: Internet of things in health: requirements, issues, and gaps. *Comput. Methods Prog. Biomed.* **208**, 106231 (2021)
- Denis, R., Madhubala, P.: Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems. *Multimed. Tools Appl.* **80**(14), 21165–21202 (2021)
- Dhanalakshmi, A., Nagarajan, G.: Convolutional neural network-based deblocking filter for SHVC in H. 265. *Signal Image Video Proc.* **14**, 1635–1645 (2020)
- Dhawan, S., et al.: SSII: secured and high-quality steganography using intelligent hybrid optimization algorithms for IoT. *IEEE Access* **9**, 87563–87578 (2021)
- Elhoseny, M., et al.: A hybrid model of internet of things and cloud computing to manage big data in health services applications. *Futur. Gener. Comput. Syst.* **86**, 1383–1394 (2018)

- Elhoseny, M., et al.: Hybrid optimization with cryptography encryption for medical image security in internet of things. *Neural Comput. Appl. Comput. Appl.* **32**(15), 10979–10993 (2020)
- Ghazal, T.M.: Internet of things with artificial intelligence for health care security. *Arab. J. Sci. Eng.* 1–12 (2021)
- Helmi, A.M., ElsayedLotfy, M., Zamel, A.A.: Particle swarm optimization advances in internet of things industry. In: *Frontiers in Nature-Inspired Industrial Optimization*, pp. 93–110. Springer, Singapore (2022)
- Jasim, N.A., Haider, T.H., Rikabi, S.A.L.: Design and implementation of smart city applications based on the internet of things. *Int. J. Interact. Mobile Technol.* **15**(13), 4 (2021)
- Jyotheeswari, P., Jeyanthi, N.: Hybrid encryption model for managing the data security in medical internet of things. *Int. J. Internet Protoc. Technol.* **13**(1), 25–31 (2020)
- Kalyani, G., Chaudhari, S.: An efficient approach for enhancing security in internet of things using the optimum authentication key. *Int. J. Comput. Appl. Comput. Appl.* **42**(3), 306–314 (2020)
- Ku, H., et al.: Privacy-preserving federated learning in medical diagnosis with homomorphic re-encryption. *Comput. Stand. Interfaces* **80**, 103583 (2022)
- Kumar, Pr.M., Gandhi, U.D.: Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application. *J. Supercomput.* **76**(6), 3963–3983 (2020)
- Lara-Nino, C.A., Diaz-Perez, A., Morales-Sandoval, M.: Lightweight elliptic curve cryptography accelerator for internet of things applications. *Ad Hoc Netw.* **103**, 102159 (2020)
- Lee, C.K.M., et al.: Design and application of Internet of things-based warehouse management system for smart logistics. *Int. J. Prod. Res.* **56**(8), 2753–2768 (2018)
- Li, Y., et al.: Deep learning in security of internet of things. *IEEE Internet Things J.* 22133–22146 (2021)
- Mashal, I., et al.: A multi-criteria analysis for an internet of things application recommendation system. *Technol. Soc.* **60**, 101216 (2020)
- Nagarajan, G., Minu, R.I.: Wireless soil monitoring sensor for sprinkler irrigation automation system. *Wirel. Pers. Commun. Pers. Commun.* **98**, 1835–1851 (2018)
- Ogundokun, R.O., et al.: Crypto-stegno based model for securing medical information on IOMT platform. *Multimed. Tools Appl.* **80**(21), 31705–31727 (2021)
- Pandey, P., Pandey, S.C., Kumar, U.: Security issues of internet of things in health-care sector: an analytical approach. In: *Advancement of Machine Intelligence in Interactive Medical Image Analysis*, pp. 307–329. Springer, Singapore (2020)
- Perwej, Y., et al.: The internet of things (IoT) and its application domains. *Int. J. Comput. Appl. Comput. Appl.* **975**(8887), 182 (2019)
- Podder, P., et al.: Review on the security threats of internet of things. [arXiv:2101.05614](https://arxiv.org/abs/2101.05614) (2021)
- Raghuvanshi, A., et al.: An investigation of various applications and related security challenges of Internet of things. *Mater. Today Proc.* (2022)
- Rana, A., et al.: Internet of medical things-based secure and energy-efficient framework for health care. *Big Data* **10**, 18–33 (2021)
- Rani, S.S., et al.: Optimal servers based secure data transmission on the internet of healthcare things (IoHT) with lightweight blockchain. *Multimed. Tools Appl.* **79**(47), 35405–35424 (2020)
- Shankar, K.: Improving the security and authentication of the cloud with IoT using hybrid optimization based quantum hash function. *J. Intell. Syst. Internet Things* **1**(2), 61–71 (2021)
- Stergiou, C.L., et al.: Secure machine learning scenario from big data in cloud computing via internet of things network. In: *Handbook of Computer Networks and Cyber Security*, pp. 525–554. Springer, Cham (2020)
- Thyasharajan, K.K., Minu, R.I.: Prevalent color extraction and indexing. *Int. J. Eng. Technol.* **5**(6), 4841–4849 (2013)
- Tripa, M.M., et al.: Security in digital healthcare system. In: *Pervasive Healthcare*, pp. 217–231. Springer, Cham (2022)
- Zeadally, S., Das, A.K., Sklavos, N.: Cryptographic technologies and protocol standards for internet of things. *Internet Things* **14**, 100075 (2021)
- Zhan, K.: Sports and health big data system based on 5G network and internet of things system. *Microprocess. Microsyst. Microsyst.* **80**, 103363 (2021)
- Zhu, H., et al.: Smart healthcare in the era of internet-of-things. *IEEE Consum. Electron. Mag.* **8**(5), 26–30 (2019)

**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.

## Authors and Affiliations

Chandrashekhar Goswami<sup>1</sup> · P. Tamil Selvi<sup>2</sup> · Velagapudi Sreenivas<sup>3</sup> · J. Seetha<sup>4</sup> · Ajmeera Kiran<sup>5</sup> · Vamsidhar Talasila<sup>6</sup> · K. Maithili<sup>7</sup>

✉ Chandrashekhar Goswami  
shekhar.goswami358@gmail.com

P. Tamil Selvi  
tamilselvi.p@rajalakshmi.edu.in

Velagapudi Sreenivas  
velagapudisreenivas@gmail.com

J. Seetha  
jsvpec@gmail.com

Ajmeera Kiran  
kiranphd.jntuh@gmail.com

Vamsidhar Talasila  
talasila.vamsi@kluniversity.in

K. Maithili  
drmaithili@kgr.ac.in

<sup>1</sup> Department of Computer Science and Engineering, School of Computing, MIT ADT University, Pune, Maharashtra, India

<sup>2</sup> School of Computing Science and Engineering, Rajalakshmi Engineering College, Mevalurkuppam, India

<sup>3</sup> Department of Computer Science and Engineering, SRK Institute of Technology, Vijayawada (A.P), India

<sup>4</sup> Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, India

<sup>5</sup> Department of Computer Science and Engineering, MLR Institute of Technology, Dundigal, Hyderabad, Telangana, India

<sup>6</sup> Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur Dist(A.P), India

<sup>7</sup> Department of CSE, KG Reddy College of Engineering and Technology, Chilukuru Village, Telangana, India