

Intelligent Tunicate Swarm-Optimization-Algorithm-Based Lightweight Security Mechanism in Internet of Health Things

Gia Nhu Nguyen^{1,2}, Nin Ho Le Viet^{1,2}, Gyanendra Prasad Joshi³ and Bhanu Shrestha^{4,*}

¹Faculty of Information Technology, Duy Tan University, Da Nang, 550000, Vietnam

²Graduate School, Duy Tan University, Da Nang, 550000, Vietnam

³Department of Computer Science and Engineering, Sejong University, Seoul, 05006, South Korea

⁴Department of Electronic Engineering, Kwangwoon University, Seoul, 01897, South Korea

*Corresponding Author: Bhanu Shrestha. Email: bnu@kw.ac.kr

Received: 01 July 2020; Accepted: 30 August 2020

Abstract: Fog computing in the Internet of Health Things (IoHT) is promising owing to the increasing need for energy- and latency-optimized health sector provisioning. Additionally, clinical data (particularly, medical image data) are a delicate, highly protected resource that should be utilized in an effective and responsible manner to fulfil consumer needs. Herein, we propose an energy-efficient fog-based IoHT with a tunicate swarm-optimization-(TSO)-based lightweight Simon cipher to enhance the energy efficiency at the fog layer and the security of data stored at the cloud server. The proposed Simon cipher uses the TSO algorithm to select the optimal keys that will minimize the deterioration of quality between the original and reconstructed (decrypted) images. In this study, the decrypted image quality is preserved by the peak signal-to-noise ratio (PSNR) such that consumers can generate precise medical reports from IoHT devices at the application level. Moreover, a lightweight encryption step is implemented in the fog to improve energy efficiency and reduce additional computations at the cloud server. Experimental results indicate that the TSO-Simon model achieved a high PSNR of 61.37 dB and a pixel change rate of 95.31.

Keywords: Internet of Health Things; healthcare; Simon cipher; tunicate swarm optimization

1 Introduction

The Internet of Things (IoT) provides different apparatuses and assets to build an incorporated healthcare framework for better treatment, cost-effective medical services, and positive treatment results [1]. The healthcare field, which is slow in embracing new advances, is expected to develop rapidly and will involve more than 50 million associated devices. Additionally, extraordinary application areas in health-related services have demonstrated different prospects of IoT application; according to the present pattern, smart healthcare services in the application space (e.g., smart pills, smart dispensing gadgets and syringes, smart observing gadgets, smart radio-frequency identification (RFID) cabinets, and electronic health records) are the latest development [2]. The Internet of Health Things (IoHT) pertains to the



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

exchange of data and processing of information to screen a patient's health status [3]. Numerous health-related institutions are now utilizing the IoHT for various purposes from monitoring infants to tracking inventory and resources. Two classes of operation cases exist: one for clinical administration and the other for support activities. In clinical settings, the IoHT enhances patient-centric exercises through remote patient monitoring. This pertains to clinical preliminaries, where the IoHT actively tracks important signs and other indicators essential to the examination, e.g., glucose levels and weight patterns. The IoHT facilitates support tasks by enabling the improved usage of portable clinical resources, which will reduce overall operational expenses [4]. Executing processes on the cloud may result in latencies that are inappropriate for certain application spaces, causing significant difficulties in providing real-time and conventional cloud computing (CC) [5]. CC provides a complete package, which benefits the clients; however, it has certain disadvantages. One of the advantages of the IoT is its rapid processing and computing of big data, which are generated and managed effectively in different applications. Smart healthcare frameworks are required, particularly to manage the rapidly changing pace of human life. Introducing fog computing and the IoT in machines relevant to clinical industry applications enables the productivity of tasks to be improved in such healthcare frameworks [6].

Fog computing enables on-time service delivery with consistency while addressing the problems related to CC, e.g., cost overheads, delays, and jitters while transferring data to the cloud. In addition, it involves a distributed design that enhances the computational capacity and networking assets in CC. It provides speedy access to assets, e.g., computing and storage for healthcare applications [7]. Furthermore, two fundamental concerns arise when transferring information to the cloud: (1) security and (2) access control. Therefore, information protection and access control should be guaranteed for approved clients of cloud-supported IoT. The conventional method for safeguarding private information is encryption; however, encryption schemes do not provide access control [8]. Moreover, it is difficult to structure a proficient security upgrading system that protects against unapproved access to the client's personal health information while simultaneously releasing an adequate amount of data to the cloud-based healthcare-related recommender administration to extract helpful suggestions [9]. Meanwhile, a secure IoT framework for in-home healthcare applications, including elderly patient information (e.g., big data, typically up to 23 GB/person/week generated from patient homes), should be established to guarantee information privacy and reliability, regardless of whether the information transfer speeds are affected by the security overhead of the communication protocols [10].

Herein, we propose an energy-efficient and minimal-delay fog based on the IoHT with a tunicate-swarm-optimization-(TSO)-based lightweight Simon cipher to enhance the cloud data security. In this section, we introduced some of the fog-based IoHT advantages and applications as well as the disadvantages of the cloud layer.

The remainder of this paper is organized as follows. Section 2 presents a review of relevant studies. Section 3 provides a detailed explanation of the proposed IoHT data security model. Section 4 presents the results of an experiment performed to prove the efficiency of the proposed method. Section 5 concludes the paper.

2 Literature Review

Mukherjee et al. [11] proposed a framework wherein the weighted majority game hypothesis was utilized to select fog gadgets in indoor and outdoor areas. The health information gathered using a body area network was stored and managed inside cloud servers. Clients could access their health information using their cell phones while simultaneously obtaining healthcare counsel. To decrease the energy utilization and delay over remote cloud servers, fog computing was used.

Mutlag et al. [12] presented a survey regarding innovations in fog computing in the healthcare IoT framework. Fog computing with no interruptions decreases latency compared with CC and is beneficial to healthcare-related IoT frameworks owing to its real-time prerequisites.

Santos et al. [13] conducted a review that introduced the advances of the most recent investigations based on clinical considerations and an assisted environment. They focused on articles pertaining to online observation, diagnosis, and support for the identification of cardiovascular ailments. They introduced a reference model based on the assessment of assets obtained from selected examinations. Further, their proposed method can assist future enthusiasts in discovering and specifying the necessary elements to establish a model for online heart monitoring purposes. Stergiou et al. [14] proposed a method for incorporating CC into the IoT as a fundamental state for big data. In addition, they attempted to build a structure that relies on the security of the system to enhance data security. Moreover, they proposed a solution by introducing a security “wall” between the cloud server and the Internet to eliminate confidentiality and security issues.

Manikandan et al. [15] proposed an IoT-based scheduling technique, called the hash polynomial two-factor decision tree (HP-TDT), to increase scheduling efficiency and reduce response time by categorizing patients as being normal or in a critical state within a short time. The HP-TDT planning strategy included three phases: the registration, data sorting, and scheduling stages. The registration step was performed using the open address hashing model to reduce the key generation response time. Subsequently, the data assortment stage was performed using the polynomial data collection algorithm.

3 Proposed Model

The IoHT has become a challenging application of the IoT and CC, where the exchange and processing of health information are performed to observe the health status of patients. The health-related information collected is stored and managed inside cloud servers. Users can obtain their health data using their cell phones and can obtain healthcare advice simultaneously. Medical information is a sensitive, highly protected asset that should be prepared in an effective and trustworthy manner. Moreover, sensitive personal information is subject to privacy leakage owing to unapproved access, accidental loss, or resale of IoHT devices. The structure of the proposed energy-efficient fog-based cloud IoHT security model is illustrated in Fig. 1.

In this study, we developed a high-security data storage approach using a Simon cipher-based encryption method to secure medical image data with less complexity in cloud servers. Moreover, to improve the efficiency of the encryption method, we included the optimal key selection method based on the TSO algorithm to improve the visual quality of the decrypted images. Healthcare systems using fog computing are emerging because of the increasing need for energy- and latency-optimized health service provisioning. Hence, to enhance reliability and reduce energy consumption over remote cloud servers, a data security scheme was implemented in a fog layer that was closer to the cloud layer. The proposed IoHT data security model encrypts data by obtaining the optimal key for which the quality of the decrypted image is similar to that of the original secret image. This is because medical image data are extremely sensitive and a slight change in them can result in incorrect medical report generation. Therefore, the quality of medical images must be prioritized when securing the images. Hence, the proposed data security model was designed to obtain the optimal key with the peak signal-to-noise ratio (PSNR) (i.e., the indicator used to determine the image quality) value of the decrypted image.

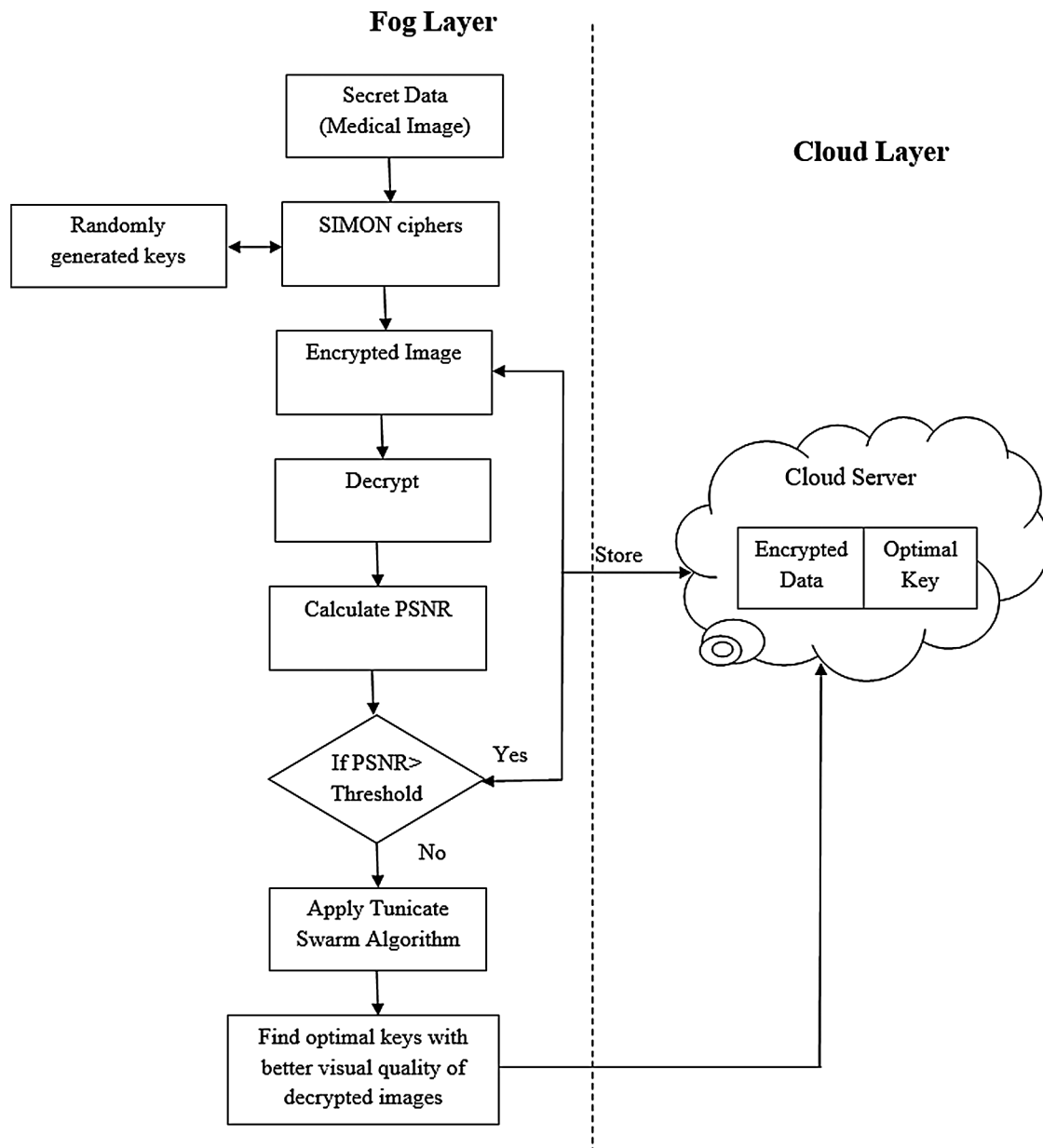


Figure 1: Structure of the proposed model

3.1 Design of IoHT Framework

The structural plan of an IoHT system should ensure an undisrupted data stream for precise and ideal dynamic decision making. The IoHT system in this study was designed to have five layers, i.e., the perception, mist, fog, cloud, and application layers. Each layer was designed using predefined functionalities applicable to the IoHT system's information transmission and processing pipeline [16–20].

- Perception layer: The perception layer is responsible for identifying physical objects and assembling appropriate healthcare information from gadgets including real-time and non-real-time information.
- Mist layer: The mist computing layer optimizes time-consuming data processing (i.e., through data preprocessing strategies) and contributes to ideal resource utilization.

- Fog layer: The fog layer can be used to process data “on the fly” to recognize anomalies, provide warning alarms in real time, and initiate important activities automatically. This demands a framework with high responsiveness and negligible latency, thereby limiting the load on the cloud.
- Cloud layer: The entire healthcare information from the fog layer is sent to the cloud layer for long-term storage and finer examination.
- Application layer: The uppermost application layer provides user interfaces between IoHT consumers and the system itself to directly access the produced healthcare status.

In the proposed IoHT data security model, medical image data are collected from the perception layer and secured at the fog layer to reduce the amount of computation required to secure the data at the cloud. For securing data, lightweight Simon block ciphers are used to enhance the energy efficiency of the fog layer. Next, the data are stored on cloud servers and sent to the application layer for user interfaces. Thus, cloud memory and time can be conserved.

3.2 Fog-Based IoHT Data Security Using Simon Ciphers

In this section, the proposed optimal and energy-efficient fog-based IoHT data security model using Simon ciphers is discussed. Simon ciphers are lightweight block ciphers that are primarily intended for resource-control strategies. However, because of the service necessities of large-scale IoHT systems, the requirement for proficient software implementation usage cannot be precluded. Therefore, we introduced TSO-based Simon ciphers in the proposed energy-efficient fog-based IoHT model to enhance the security level in the cloud platform. In the proposed TSO-based Simon ciphers, an optimal key is selected for the encryption of medical images. The proposed security model encrypts the clinical image data at the fog layer and stores the encrypted data along with its key in the cloud server. This enhances the data security and reduces the amount of computation required in the cloud server to safeguard the data from intruders [21–29].

3.2.1 Simon Ciphers

Simon ciphers are typically represented by $\text{Simon}^{\left(\frac{2r}{pr}\right)}$ with $2r$ -bit blocks and pr -bit keys, where $r = \{16, 24, 32, 48, 64\}$. The encryption and decryption operations are performed using bitwise AND, bitwise XOR, and a left circular shift on fixed-size blocks of plain data; subsequently, a block of cipher content is obtained for each input block.

The $\text{Simon}^{\left(\frac{2r}{pr}\right)}$ cipher performed to obtain the encrypted image $En(I)$ is expressed in Eq. (1).

$$En(I) = R(F)_1^k, R(F)_2^k, \dots, R(F)_t^k; t > 1$$

In Eq. (1), $R(F)_t^B$ represents the t^{th} round function of the k^{th} block. The Simon round function $R(F)_t^B$ used for encrypting the plain data is expressed as follows:

$$RF[b_L, b_R, S(\circ)] = (b_R \oplus [(B_1^s(b_L) \& B_2^s(b_L)) \oplus B_2^s(b_L)]) \oplus S(\circ), b_L,$$

where b_L and b_R denote the left-most and right-most words of a block, respectively; $S(\circ)$ represents the appropriate round key; $B_x^s(b_z)$ represents the bitwise shift function, with x being the number of rotation counts for the z^{th} bit, b_z .

Moreover, for 128-bit plain data with a 128-bit key, the round function is performed in 68 rounds to produce 128-bit cipher data. If the round functions are identical (or almost identical) for all rounds, then the cipher is termed as an iterated block cipher.

Finally, the decryption of the Simon cipher is performed using the inverse round function, as expressed in Eq. (3).

$$IRF(b_L, b_R, S(\circ)) = (b_R \oplus b_L \oplus [(S^1(b_R) \& S^8(b_R)) \oplus S^2(b_R)] \oplus S(\circ))$$

In the proposed Simon cipher, the keys are optimized using the TSO algorithm, i.e., they are selected for improving the decrypted image quality.

3.2.2 Key Optimization by TSO Algorithm

The TSO algorithm was developed by imitating the jet propulsion and swarm intelligence behaviors of tunicates in obtaining food sources, i.e., their optimum behaviors [30]. Hence, a tunicate must fulfil three criteria: avoid conflicts between search agents, move toward the position of the best search agent, and remain near the best search agent to model the jet propulsion behavior mathematically while the swarm behavior updates the positions of other search agents based on the best optimal solution.

By implementing TSO, we optimized the keys used for encrypting private medical images. Typically, optimization methods are implemented using an objective function (also known as the fitness function); toward that fitness value, the optimization problem is converged to produce the optimal solution. In this study, the objective function is the minimization function of the PSNR value calculated between the decrypted image and the original plain images. During every iteration, the PSNR value is verified, and the best keys that can maintain the decrypted image quality are selected. Therefore, the proposed Simon cipher can encrypt images without deteriorating the decrypted image quality as well as minimize the computation time required for the encryption. The steps involved in the proposed TSO algorithm are presented in the following section.

Step 1: Initialization

During initialization, the population (N_{mk} , where $m = 1, 2, \dots, c$ and $k = 1, 2, \dots, a$) of tunicates (i.e., set of key values) is determined randomly.

Step 2: Fitness Evaluation

Once the initial set of key values is generated, the fitness of the input solutions is assessed, and then the best one is selected during the fitness evaluation step. The fitness function can be defined as

$$fitness(N_{mk}) = \max(PSNR)$$

$$fitness(N_{mk}) = \max \left[10 \log_{10} \left(\frac{255^2}{\sum_{X,Y} (I(x,y) - I_{Dec}(x,y))^2 / X \times Y} \right) \right]$$

where $I(x,y)$ and $I_{Dec}(x,y)$ represent the plain and decrypted images, respectively; (x,y) represents the row and column of the image. If $PSNR \geq Threshold$, the current solutions are saved, and the algorithm further attempts to improve or maintain the maximal fitness value.

Step 3: Avoiding conflicts between search agents

The new search agent position (i.e., newer keys) is calculated using a vector \vec{K} to avoid conflicts between search agents (i.e., other tunicates) based on the following equation:

$$\vec{K} = \frac{\vec{G}}{\vec{S}}$$

Here, \vec{G} and \vec{S} denote the gravity force and social forces between search agents, which can be written as

$$\vec{G} = h_2 + h_{73} + \vec{W}$$

$$\vec{W} = 2 \cdot h_1$$

Moreover, \vec{W} denotes the water flow advection in the deep ocean, and h_1 , h_2 , and h_3 represent random numbers in the range $[0, 1]$.

In addition, the social forces between search agents \vec{S} are designed as

$$\vec{S} = \lfloor V_{\min} + h_1 \cdot V_{\max} - V_{\min} \rfloor$$

Here, V_{\min} and V_{\max} represent the initial and subordinate speeds for establishing a social interaction.

Step 4: Movement toward direction of best neighbor

The movement of search agents toward the direction of the best neighbor is obtained in this step. To find the best neighbor, the distance between the food source and search agent is established as follows:

$$\vec{D} = |\vec{N}_o - h \cdot \vec{N}(q)|,$$

where $\vec{N}(q)$ represents the tunicate position at the q^{th} current iteration, \vec{N}_o the optimality (i.e., position of the food source), and h an arbitrary number in the range $[0, 1]$.

Step 5: Converge toward best search agent

Once the best neighbor is obtained, the search agents converge toward the position of the best search agent (i.e., the food source). Consequently, the new position of the tunicate $\vec{N}'(q)$ is updated as

$$\vec{N}'(q) = \begin{cases} \vec{N}_b + \vec{K} \cdot \vec{D}, & \text{if } h \geq 0.5 \\ \vec{N}_b - \vec{K} \cdot \vec{D}, & \text{otherwise} \end{cases}$$

Step 6: Implement swarm behavior

The first two best optimal solutions are saved, and the positions of other search agents are updated according to the position of the best search agents to imitate the tunicate swarm behavior, which is expressed as

$$\vec{N}'(q+1) = \frac{\vec{N}(q) + \vec{N}'(q)}{2 + h_1}$$

Step 7: Termination

The above steps are repeated until the maximum iteration is accomplished. Moreover, at every iteration, the produced keys are evaluated for their fitness and updated based on the previous best keys.

Only the best keys obtained are employed to decrypt every private medical image. Once the optimal keys are obtained, then the private medical images are encrypted in the fog layer and then stored in the cloud server along with the optimal keys. Hence, the data are secured, and the amount of computation required in the cloud is reduced.

4 Results and Discussion

The results provided in this section were acquired from the proposed IoHT data security model implemented on a PC with the following parameters: CPU Intel® Pentium 1.9 GHz, 64-bit operating system, Microsoft® Windows 10, and 4 GB of RAM; furthermore, MathWorks MATLAB R2014b was used. All experiments were performed for a set of medical image data, of which a few examples are shown in Fig. 2.

Moreover, the encrypted and decrypted image results obtained for the proposed Simon-based IoHT data security model in the fog layer are provided in Tab. 1.

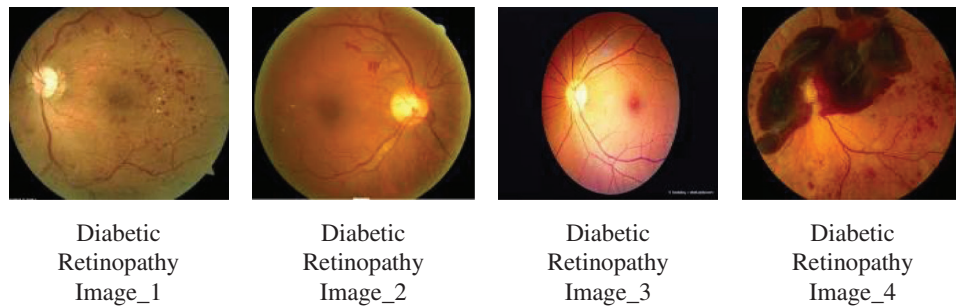

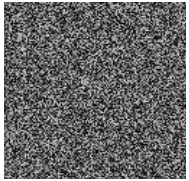

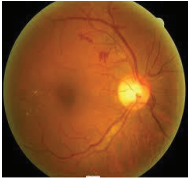










Figure 2: Medical images used in this study

Table 1: Experimental results of the proposed model

Image label	Plain image	Encrypted image	Decrypted image
DR Image_1			
DR Image_2			
DR Image_3			
DR Image_4			

4.1 Performance Analysis

To evaluate the performance of the proposed IoHT image data security model, certain indicators such as the number of pixel changing rate (NPCR) and PSNR were considered to determine the encrypted image quality. The NPCR is designed to test the number of changing pixels and the number of average changed intensities between encrypted images. During encryption, the NPCR pertains primarily to the absolute number of pixels that change in value, which can be written as

$$\text{npcr}(p_1, p_2) = \sum_{u,v} \frac{M(u,v)}{P} \times 100\%$$

Moreover, the PSNR representing the maximum possible power of the signal and the power of corrupted noise affecting the fidelity can be written as

$$\text{psnr} = 10 \log_{10} \left(\frac{255^2}{\sum_{X,Y} (I(x,y) - I_{\text{Dec}}(x,y))^2 / X \times Y} \right),$$

where $I(x,y)$ and $I_{\text{Dec}}(x,y)$ represent the plain and decrypted images, respectively, with (x,y) pixel locations.

4.2 Results Analysis

The results of encryption using the proposed TSO-based Simon (TSO_Simon), opposition-based particle swarm optimization with Simon (OPSO_Simon), and traditional Simon for a set of diabetic retinopathy (DR) images are shown in [Tab. 1](#). A comparison of the results was performed based on the PSNR and NPCR.

[Tab. 2](#) provides a detailed comparative analysis of the proposed model in terms of the PSNR and NPCR. The values listed in the table indicate that the proposed TSO_Simon model performed the best among the three methods. For DR Image_1, the TSO_Simon model achieved a maximum PSNR of 61.58 dB, whereas the OPSO_Simon and Simon models obtained minimum PSNR values of 54.52 and 45.92 dB, respectively. Similarly, for DR Image_2, the TSO_Simon model yielded a high PSNR of 63.21 dB, whereas the OPSO_Simon and Simon models yielded lower PSNR values of 56.15 and 47.81 dB, respectively. Likewise, on DR Image_3, the TSO_Simon model achieved a maximum PSNR of 60.74 dB, whereas the OPSO_Simon and Simon models obtained minimum PSNR values of 51.86 and 52.72 dB, respectively. Moreover, for DR Image_4, the TSO_Simon model achieved a high PSNR of 59.95 dB, whereas the OPSO_Simon and Simon models obtained lower PSNR values of 53.32 and 51.24 dB, respectively.

Table 2: Comparative analysis

Image	PSNR			NPCR		
	TSO_Simon	OPSO_Simon	Simon	TSO_Simon	OPSO_Simon	Simon
DR Image_1	61.58	54.52	45.92	97.25	82.43	80.89
DR Image_2	63.21	56.15	47.81	95.95	85.45	86.85
DR Image_3	60.74	51.86	52.72	97.62	93.56	88.85
DR Image_4	59.95	53.32	51.24	90.42	80.12	79.72

Additionally, the proposed TSO_Simon model was assessed based on the NPCR. On DR Image_1, the TSO_Simon model achieved a maximum NPCR of 97.25, whereas the OPSO_Simon and Simon models obtained minimum NPCR values of 82.43 and 80.89, respectively. Similarly, on DR Image_2, the TSO_Simon model achieved a high NPCR of 95.95, whereas the OPSO_Simon and Simon models obtained lower NPCR values of 85.45 and 86.85, respectively. Likewise, on DR Image_3, the TSO_Simon model achieved a high NPCR of 97.62, whereas the OPSO_Simon and Simon models obtained lower NPCR values of 93.56 and 88.85, respectively. Moreover, on DR Image_4, the

TSO_Simon model achieved a high NPCR of 90.42, whereas the OPSO_Simon and Simon models obtained lower NPCR values of 80.12 and 79.72, respectively.

Tab. 2 shows that the maximum PSNR of 63.21 was achieved for DR Image_2 using the proposed method, whereas it is lower for other existing methods. Likewise, the PSNR values of the other DR images were compared with those of existing methods. The obtained values show that the proposed TSO-based Simon method improved the image quality significantly compared to the other methods. In addition, the NPCRs of the proposed and existing methods were compared for the DR images. DR Image_1 and DR Image_3 yielded NPCR values greater than 97 using the proposed method, whereas the values were lower for existing methods. This demonstrates the better security attained while encrypting the medical image samples. It is clear from Tab. 2 that the proposed TSO_Simon outperformed the other existing methods.

Finally, graphical representations of the results obtained using the proposed and other Simon-based encryption techniques are shown in Figs. 3 and 4 to clearly depict the changes in values among the methods compared.

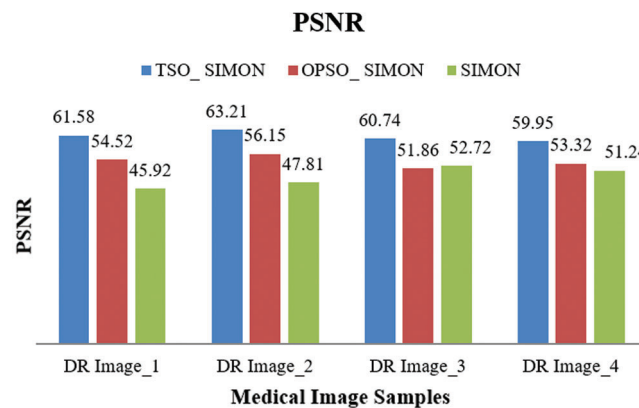


Figure 3: PSNR comparison among different Simon-based encryption techniques

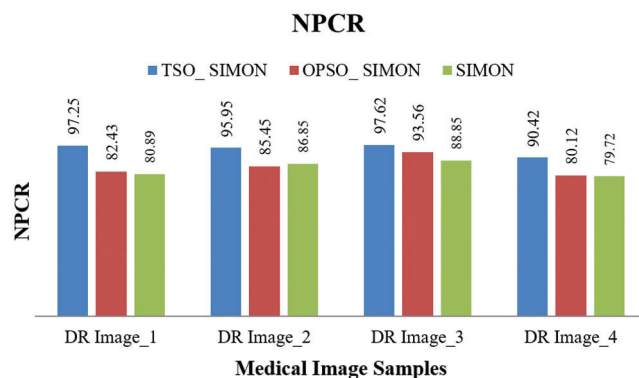


Figure 4: NPCR comparison among different Simon-based encryption techniques

5 Conclusion

In this study, we developed an energy-efficient fog-based IoHT data security model to secure medical image data in a cloud server. The various layers of the IoHT structure were discussed herein. The TSO-based Simon encryption method was implemented in the fog layer to improve the energy efficiency, and

encrypted private medical data were stored in the cloud. The performance of the proposed IoHT data security model was analyzed based on its PSNR and NPCR and compared with those of other Simon-based encryption methods. The results showed that the highest PSNR value of 63.21 was achieved using the proposed TSO_Simon method, whereas the value was low for the existing methods. In the future, the mist layer of the IoHT architecture will be implemented with optimal resource allocation using advanced optimization methods.

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

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

References

- [1] K. Tiwari, S. Kumar and R. K. Tiwari, "Fog assisted healthcare architecture for pre-operative support to reduce latency," *Procedia Computer Science*, vol. 167, pp. 1312–1324, 2020.
- [2] M. A. U. Rahman, F. Afsana, M. Mahmud, M. S. Kaiser, M. R. Ahmed *et al.*, "Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4049–4062, 2018.
- [3] D. Costa, C. André, C. F. Pasluosta, B. Eskofier, D. B. d. Silva *et al.*, "Internet of health things: Toward intelligent vital signs monitoring in hospital wards," *Artificial Intelligence in Medicine*, vol. 89, pp. 61–69, 2018.
- [4] A. Farouk, A. Alahmadi, S. Ghose and A. Mashatan, "Blockchain platform for industrial healthcare: Vision and future opportunities," *Computer Communications*, vol. 154, pp. 223–235, 2020.
- [5] M. G. Valls, C. C. Urrego and A. G. Fornes, "Accelerating smart eHealth services execution at the fog computing infrastructure," *Future Generation Computer Systems*, vol. 108, pp. 882–893, 2020.
- [6] N. Mani, A. Singh and S. L. Nimmagadda, "An IoT guided healthcare monitoring system for managing real-time notifications by fog computing services," *Procedia Computer Science*, vol. 167, pp. 850–859, 2020.
- [7] A. Kumari, S. Tanwar, S. Tyagi and N. Kumar, "Fog computing for healthcare 4.0 environment: Opportunities and challenges," *Computers & Electrical Engineering*, vol. 72, pp. 1–13, 2018.
- [8] S. K. Pasupuleti and D. Varma, "Lightweight ciphertext-policy attribute-based encryption scheme for data privacy and security in cloud-assisted IoT," *Real-Time Data Analytics for Large Scale Sensor Data*, vol. 6, pp. 97–114, 2020.
- [9] A. M. Elmisery, S. Rho and D. Botvich, "A fog based middleware for automated compliance with OECD privacy principles in internet of healthcare things," *IEEE Access*, vol. 4, pp. 8418–8441, 2016.
- [10] B. Mukherjee, S. Wang, W. Lu, R. L. Neupane, D. Dunn *et al.*, "Flexible IoT security middleware for end-to-end cloud-fog communication," *Future Generation Computer Systems*, vol. 87, pp. 688–703, 2018.
- [11] A. Mukherjee, D. De and S. K. Ghosh, "FogIoHT: A weighted majority game theory based energy-efficient delay-sensitive fog network for internet of health things," *Internet of Things*, vol. 11, pp. 1–41, 2020.
- [12] A. A. Mutlag, M. K. A. Ghani, N. Arunkumar, M. A. Mohammed and O. Mohd, "Enabling technologies for fog computing in healthcare IoT systems," *Future Generation Computer Systems*, vol. 90, pp. 62–78, 2019.
- [13] M. A. G. Santos, R. Munoz, R. Olivares, P. P. R. Filho, J. D. Ser *et al.*, "Online heart monitoring systems on the internet of health things environments: A survey, a reference model and an outlook," *Information Fusion*, vol. 53, pp. 222–239, 2020.
- [14] C. Stergiou, K. E. Psannis, B. B. Gupta and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & IoT," *Sustainable Computing: Informatics and Systems*, vol. 19, pp. 174–184, 2018.
- [15] R. Manikandan, R. Patan, A. H. Gandomi, P. Sivanesan and H. Kalyanaraman, "Hash polynomial two factor decision tree using IoT for smart health care scheduling," *Expert Systems with Applications*, vol. 141, pp. 1–14, 2020.
- [16] K. Shankar and M. Elhoseny, "Secure image transmission in wireless sensor network (WSN) applications," in *Lecture Notes in Electrical Engineering*, vol. 564. Springer, 2019. [Online]. Available: <https://www.springer.com/gp/book/9783030208158>.

- [17] K. Shankar, M. Elhoseny, E. D. Chelvi, S. K. Lakshmanaprabu and W. Wu, "An efficient optimal key based chaos function for medical image security," *IEEE Access*, vol. 6, pp. 77145–77154, 2018.
- [18] R. J. S. Raj, S. J. Shobana, I. V. Pustokhina, D. A. Pustokhin, D. Gupta *et al.*, "Optimal feature selection-based medical image classification using deep learning model in internet of medical things," *IEEE Access*, vol. 8, pp. 58006–58017, 2020.
- [19] K. Shankar, S. K. Lakshmanaprabu, D. Gupta, A. Khanna and V. H. C. de Albuquerque, "Adaptive optimal multi key based encryption for digital image security," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 4, pp. 1–11, 2020.
- [20] S. Kathiresan, A. R. W. Sait, D. Gupta, S. K. Lakshmanaprabu, A. Khanna *et al.*, "Automated detection and classification of fundus diabetic retinopathy images using synergic deep learning model," *Pattern Recognition Letters*, vol. 133, pp. 210–216, 2020.
- [21] S. R. Zhou and B. Tan, "Electrocardiogram soft computing using hybrid deep learning CNN-ELM," *Applied Soft Computing*, vol. 86, 2020.
- [22] F. J. Kuang, S. Y. Zhang, Z. Jin and W. H. Xu, "A novel SVM by combining kernel principal component analysis and improved chaotic particle swarm optimization for intrusion detection," *Soft Computing*, vol. 19, no. 5, pp. 1187–1199, 2015.
- [23] H. X. Li, W. J. Li, S. G. Zhang, H. D. Wang and Y. Pan, "Page-sharing-based virtual machine packing with multi-resource constraints to reduce network traffic in migration for clouds," *Future Generation Computer Systems-the International Journal of Esience*, vol. 96, pp. 462–471, 2019.
- [24] B. Yin and X. T. Wei, "Communication-efficient data aggregation tree construction for complex queries in IoT applications," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3352–3363, 2018.
- [25] X. M. Huang, R. Yu, J. W. Kang, Z. Q. Xia and Y. Zhang, "Software defined networking for energy harvesting Internet of Things," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1389–1399, 2018.
- [26] J. Wang, Y. N. Tang, S. M. He, C. Q. Zhao, P. K. Sharma *et al.*, "LogEvent-to-vector based anomaly detection for large-scale logs in Internet of things," *Sensors*, vol. 20, no. 9, pp. 1–19, 2020.
- [27] T. Wang, L. Qiu, A. K. Sangaiah, A. Liu, M. Z. A Bhuiyan *et al.*, "Edge-computing-based trustworthy data collection model in the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4218–4227, 2020.
- [28] T. Wang, Z. H. Cao, S. Wang, J. H. Wang, L. Y. Qi *et al.*, "Privacy-enhanced data collection based on deep learning for internet of vehicles," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6663–6672, 2020.
- [29] J. M. Zhang, W. Wang, C. Q. Lu, J. Wang and A. K. Sangaiah, "Lightweight deep network for traffic sign classification," *Annals of Telecommunications*, vol. 75, no. 7, pp. 369–379, 2019.
- [30] S. Kaur, L. K. Awasthi, A. L. Sangal and G. Dhiman, "Tunicate swarm algorithm: A new bio-inspired based metaheuristic paradigm for global optimization," *Engineering Applications of Artificial Intelligence*, vol. 90, pp. 1–29, 2020.