International Journal of Safety and Security Engineering
Vol. 15, No. 6, June, 2025, pp. 1219-1228
Journal homepage: http://iieta.org/journals/ijsse

Blockchain Enabled Light Weight Encryption Scheme for IoT-Edge Devices Applied for Smart Medical Image Transmission

Goli Archana[1*], Rajeev Goyal[1], K.M.V. Madan Kumar[2]

[1] Department of Computer Science and Engineering, Amity School of Engineering and Technology, Amity University, Gwalior 474005, India
[2] Department of Computer Science and Engineering, Vignan Institute of Science and Technology, Hyderabad 508284, India

Corresponding Author Email: archanagoli44@gmail.com

https://doi.org/10.18280/ijsse.150612

Received: 30 January 2025
Revised: 10 March 2025
Accepted: 11 May 2025
Available online: 30 June 2025

Keywords:
Internet of Things, edge computing devices, blockchain, fractional order logistic maps, Hendon, tent chaotic maps

ABSTRACT

The Internet of Things (IoT) is an intelligent paradigm integrating users from the physical world to the cyber domain, enabling sensing, detection, communication, and decision-making processes. These systems enhance comfort, safety, reliability, and operational efficiency. To ensure secure, distributed storage and computation, IoT is now integrated with Edge Computing Devices (ECDs). However, internet-enabled communication networks expose these devices to increasing cyber threats, raising concerns about reliability and security breaches. Blockchain technology, a transparent and distributed database, offers high credibility, traceability, and versatility. Yet, deploying blockchain in IoT devices demands substantial computational resources, posing new challenges in combating data manipulation and unauthorized access. This research proposes a blockchain-driven lightweight encryption method using fractional-order logistic maps, Henon, and tent chaotic systems (BDLE-FOLHT). The integration of these chaotic maps generates highly random encryption keys to secure data transmitted via IoT devices. Encrypted data is securely stored in the blockchain, enhancing protection. Extensive experiments using benchmark medical image datasets demonstrate the proposed method's superiority over existing encryption frameworks. The BDLE-FOLHT scheme achieves strong security metrics with NPCR of 95.5%, UACI of 32.90, and entropy of 7.9. Furthermore, the randomness of the encrypted output is validated through the NIST randomness test, ensuring robustness and security.

1. INTRODUCTION

Rapid expansion of 5G and Wi-Fi, IoT, has shown the rapid development and exploded its growth in various domains like healthcare, automation, agriculture, and defense systems [1-3]. According to the Telecommunication Industry Association (TIA), nearly 18 billion devices were connected using IoT by the end of 2022 [4]. This paradigm of interconnected devices consists of different stages such as collection, processing, and communication [5, 6]. However, IoT still has many pitfalls such as insecure communication, energy consumption, centralized data storage, and privacy breaches [7-9].

Edge computing devices (ECDs) have emerged as a significant complement to IoT, designed to enhance both processing and data storage capacities at the network's edge. Within the ECD framework, IoT devices can access resources by assigning tasks to adjacent edge servers. These servers are positioned near IoT devices and data sources, effectively addressing challenges related to security, privacy breaches, and system vulnerabilities [10].

Moreover, edge node resources can be seamlessly incorporated and utilized to reduce the computational, storage, and bandwidth constraints typically associated with traditional IoT devices. As a result, ECD provides decentralized, low-latency computing services across various IoT applications, including smart cities, smart grids, and smart healthcare [11]. However, the constrained resources of IoT devices, diverse network infrastructure, and the rapidly changing environment pose challenges that prevent the full implementation of many existing data security techniques in the Edge-IoT architecture [12].

Recently, blockchain technology (BCT) has attracted the bright light of attraction to reduce the security risks in edge-IoT devices. Blockchain functions as a decentralized ledger that leverages technologies such as peer-to-peer (P2P) networking, cryptography, and distributed storage to attain key characteristics including decentralization, transparency, traceability, security, and immutability [13]. Fundamentally, blockchain enhances the reliability of edge nodes—comprising edge servers and devices in edge computing (EC)—by saving vital information within the blockchain [14]. Additionally, blockchain facilitates the implementation of security mechanisms in EC, such as access control, authentication, and privacy safeguarding through well-structured smart contracts [15, 16]. Moreover, blockchain enables edge computing devices (ECDs) to manage diverse edge resources via smart contract-driven techniques for resource allocation, task offloading, and resource pricing. In return, ECDs support blockchain by offering sufficient computational resources for mining tasks. For example, when edge devices contribute idle resources similar to edge servers, these facilities can be allocated through bidding and trading mechanisms for operations.

The incorporation of blockchain with ECD presents a promising approach, as the two technologies complement each other in constructing frameworks to address challenges across various fields [17]. However, despite its potential, the practical deployment of blockchain in edge environments introduces significant challenges. Blockchain protocols typically require considerable computational resources and storage capacity, which may exceed the capabilities of lightweight edge devices [18, 19]. The continuous synchronization of data, consensus validation, and encryption operations can strain device performance and lead to increased latency or power consumption. In resource-limited settings, this can compromise overall system reliability and even open up new vulnerabilities [20]. Thus, achieving a balance between the benefits of blockchain and the limitations of edge devices remains a critical research concern.

Motivated by the drawback, this research introduces the blockchain-driven light weight image encryption schemes which integrate the principles of fractional logistic maps, Henon and tent maps to produce the optimum cryptographic keys. The design of the integrated chaotic encryption in the blockchain is considered to be the novelty of the work. The major contribution of this study is as follows:

1) Proposed Blockchain driven Light weight Encryption Framework to be deployed for the IoT-Edge computing devices.
2) Proposed the Combination of the three lightweight chaotic maps like tent, fractional logistic maps and henon maps for achieving the high secured defence system against the unknown growing attacks.
3) Extensive experimentation is conducted and findings are analysed. To demonstrate the efficacy of the recommended approach, performance has been benchmarked against other cutting-edge frameworks in which the recommended model exceeded the varied procedures.

The structure of the paper is organised as pursues: Section 2 represents the related works designed by varied authors. The preliminary description about the Blockchain, types of chaotic maps are presented in the Section-3. The recommended encryption schemes with the detailed description and its deployment in blockchain is detailed in Section-4. The experimental implementation, performance validation and comparative outcomes are demonstrated in Section-5. Lastly, the paper wraps up with the discussion on future prospects in Section 6.

2. RELATED WORKS

Sammeta and Parthiban [21] proposed the Hyperledger Blockchain enabled multiple key–based homomorhic encryption to produce the optimal key generation that aids for the better security analysis. The hosted cuckoo optimization technique was adopted in the homomorphism encryption to achieve the better security mechanisms. The mechanism of this framework leads to high computational which Is not suitable for deploying the IoT-Edge devices.

Ali and Ali [22] presented an chaotic relied security system for clinical data. In this technique, a private encryption key is generated by the user with the medical center's public key. The recommended chaos-relied medical image encryption technique encrypts the image using the private key. Then, the medical institution creates a collective confidential data by merging the encrypted picture, private keys, and electronic seal. This mutual key is employed by the administrator to decipher the picture, authenticate it using a validation, and authorize it once confirmed.

Hosny et al. [23] proposed an encryption technique utilizing fractional-order chaotic systems to secure pictures. The process employs the 4D Hyperchaotic Chen System (HCS). The framework comprises a three-tier approach developed to generate highly random encrypted sequences, incorporating dual operations based on the 4D HCS. This method ensures optimal randomness, rendering this system exceptionally resilient to numerous types of threats.

Neelakandan et al. [24] introduced an innovative blockchain-based system integrated with deep learning (BDL-SMDTD) to ensure secured healthcare information transfer and diagnosis. Initially, the encryption process employed the Moth Flame Optimizer with Elliptic Curve Cryptography (MFO-ECC), which enhances key generation for ECC using the MFO system. Blockchain procedure is then utilized for preserving the encrypted images securely.

Bhaskaran et al. [25] proposed a unique blockchain-enabled lightweight cryptography-based image encryption system (BC-LWCIE) designed for Industry 4.0 setting. This framework generates cryptographic pixel values for image encryption from blockchain technology, assuring data privacy on Industrial Internet of Things (IoT) platforms.

Afzal et al. [26] developed a biplane and chaotic image encryption technique (BCE) for securing medical images. The chaotic key sequence is derived by combining two keys generated. Ultimately, following the retrieval of the ciphered image from the cryptographic system, the plain medical image is reconstructed. However, this procedure has a notably high computational cost.

Table 1 presents the summary of different existing techniques handled by the researches.

Table 1. Summary of related works

S. No	Reference	Technology	Results Obtained	Advantages	Disadvantages
1	Sammeta and Parthiban [21]	Hyperledger Blockchain with multiple key-based homomorphic encryption	Optimal key generation for better security analysis	Enhanced security mechanisms through hosted cuckoo optimization	High computational issue
2	Ali et al. [22]	Chaos-relied security system for clinical data	Secure encryption of medical images	Private key generation with public key of medical center	Requires significant processing for mutual key decryption
3	Hosny et al. [23]	Fractional-order chaotic systems using 4D	Highly random encrypted sequences	Three-tier approach ensuring optimal	Complex implementation of dual operations

		Hyperchaotic Chen System		randomness	
4	Neelakandan et al. [24]	Blockchain-based system with deep learning (BDL-SMDTD)	Secured healthcare information transfer and diagnosis	Enhanced key generation using Moth Flame Optimizer with ECC	Potentially resource-intensive due to blockchain and deep learning integration
5	Bhaskaran et al. [25]	Blockchain-enabled lightweight cryptography-based image encryption (BC-LWCIE)	Cryptographic pixel values for image encryption	Data privacy assurance for Industrial IoT platforms	Limited to Industry 4.0 settings
6	Afzal et al. [26]	Biplane and chaotic image encryption technique (BCE)	Secure encryption of medical images	Combined key generation for chaotic key sequence	High computational cost

3. PRELIMINARY BACKGROUND

This section discusses about the preliminary background of blockchain technology and different chaotic principles.

3.1 Blockchain technology

Blockchain has become a foundational technology in cryptosystems and various industrial domains because of its versatile structure and unique characteristics. Sammeta and Parthiban [21] originally introduced blockchain for cryptocurrency (digital currency) for monitoring transactions managed by third parties and eliminate their involvement. Today, this technology has been widely utilised in numerous real-world applications, including the IIoT, connected vehicles, energy trading systems, smart cities, Industry 4.0, healthcare, secure communications, cryptosystems, and more. The blockchain framework resembles a P2P network consisting of nodes (i.e., blocks) with unique hash values. Each block serves as a digital ledger, recording historical data from previous transactions conducted within the network. All information on the blockchain is permanent and immutable. Figure 1 depicts the blockchain framework, highlighting the blocks and their features.

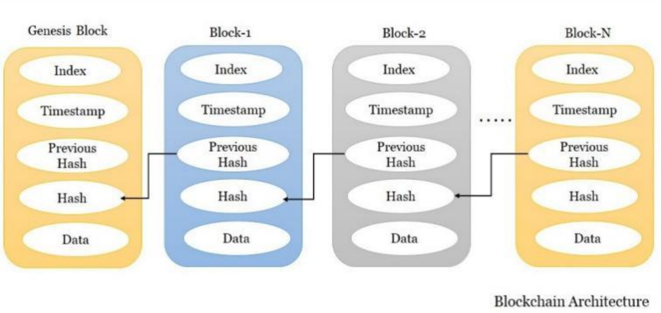


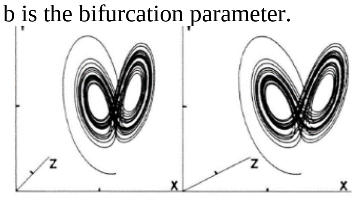
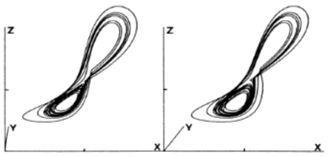
Figure 1. Basic structure of blockchain technology

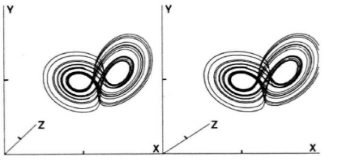
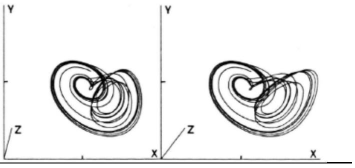
The genesis node represents the initial block in the blockchain structure, remaining constant throughout the system. Each block contains immutable attributes such as an index, timestamp, previous hash, hash, and data, with timestamping ensuring the integrity of stored data, making modification nearly impossible. The hash and previous hash are key components, updated with each transaction or data modification, establishing the chain-like structure by linking consecutive blocks. A blockchain framework operates as a decentralized system, where nodes are interconnected and share data, ensuring transparency and security. This integration allows for automated processes through smart contracts—self-executing scripts used to enforce rules and prevent fraudulent activities. Blockchain can be categorized into public and private networks, with public networks like Ethereum and Bitcoin supporting commercial applications, and private networks tailored to specific organizational needs. For secure transaction ledgers, the system uses a certificate authority to assign digital certificates to users and nodes, ensuring secure authentication and communication. Each node plays a role in validating and adding new blocks, maintaining data integrity and decentralization. Interaction between edge devices and the blockchain is facilitated by the REST API, allowing seamless communication between the distributed ledger and edge resources. They ensure blockchain's scalability and security when applied in edge computing environments.

3.2 Chaotic principles-A background theory

Chaos theory is focused on the behaviour of dynamic non-linear systems with high sensitivity to initial conditions. Therefore, a delta change in the initial conditions leads to a substantial change in outputs [27]. Lyapunov exponents are used to check the sensitivity of initial criteria. This crucial characteristic introduces additional randomness into the outputs, which drives numerous researchers to incorporate chaotic systems in cryptographic encryptions [28]. The Table 2 lists the chaotic maps commonly utilized for encryption.

Table 2. List of chaotic maps used for the different applications

Lorentz Equation	$\dot{x} = x - xy - z$ $\dot{y} = x^2 - ay$ z=b x—c z+d where, x and y represent the dual focus system, Z denotes constant, and b is the bifurcation parameter.
Lorenz-type chaos Axes: x: -1.8 to +1.8 y: 0 to +1.8 z: -0.18 to +0.18	
Sandwich chaos Axes: x: -1.2 to +1.2 y: 0 to +1.4 z: -0.1 to +0.1 t: 0 to 336.	

Double-horseshoe chaos Axes: x range from -1 to +1, y from 0 to 2, z from -0.1 to +0.1	
Screw type of chaos Axes: x and y range from -10 to +10, z from 0 to 10	

4. BDLE-FOHLT: PROPOSED SCHEME

This section discusses about the different categories of the chaotic employed and its application used for the encryption and its blockchain technology.

The recommended architecture is shown in Figure 2. As shown in Figure 2, the recommended BDLE-FOHLT framework consists of medical image collection unit from IoT devices, encryption process and finally the blockchain based edge storage mechanism. Each component is detailed in the preceding section.

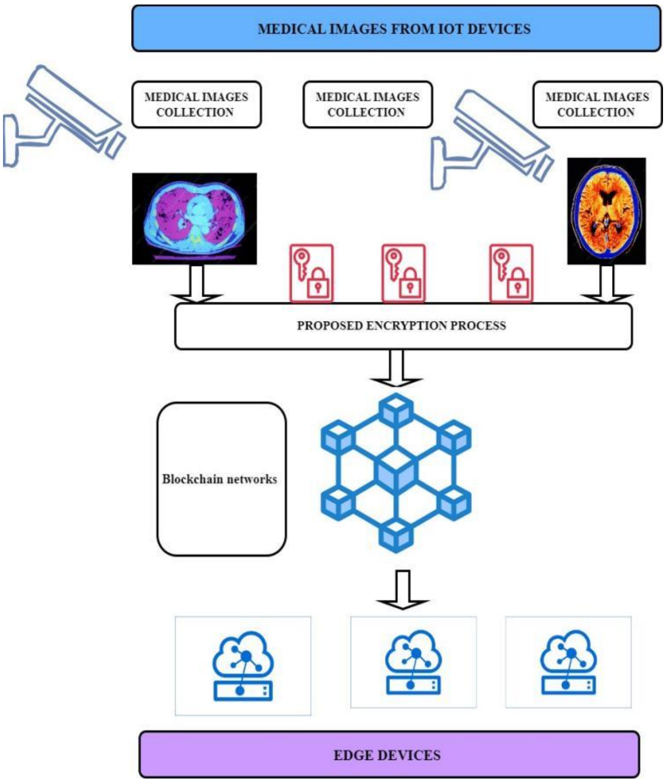

MEDICAL IMAGES FROM IOT DEVICES
MEDICAL IMAGES COLLECTION
MEDICAL IMAGES COLLECTION
MEDICAL IMAGES COLLECTION
PROPOSED ENCRYPTION PROCESS
Blockchain networks
EDGE DEVICES

Figure 2. BDLE-FOHLT-its frameworks and components

4.1 Medical image collection process

The suggested framework utilizes the medical imaging datasets in the form of CT and MRI format which is mentioned in references [29, 30]. Typically, IoT is used to collect the clinical information and transfers to the hospital cloud (HC) for the further processing.

4.2 Encryption process

In this encryption process, preliminary view of logistic maps and Henon maps are described in the first phase, followed by the encryption process in the proposed framework.

4.2.1 Fractional order logistic maps

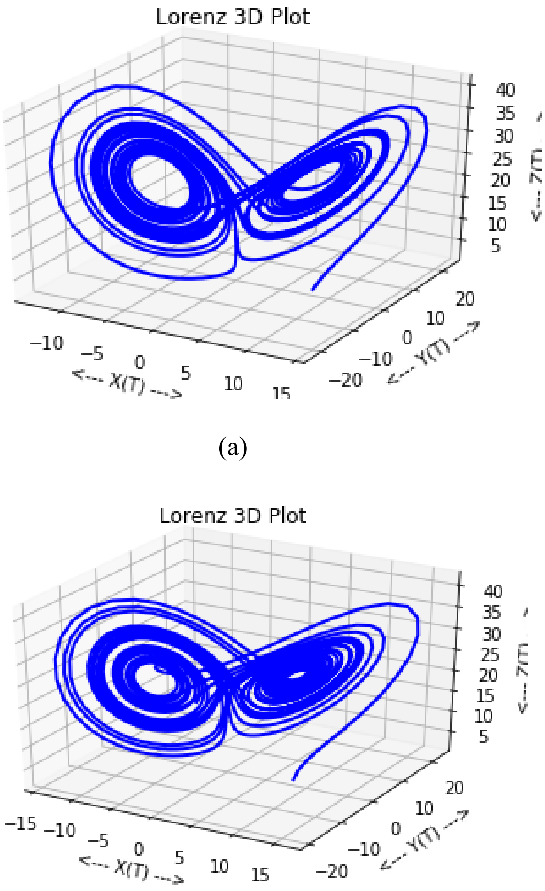
The fractional order LM, in the context of Caputo's fractional differences, is approached numerically. It is demonstrated that the required number of iterations to bypass transients should be on the order of thousands, rather than the hundreds often used in many studies. Additionally, an intriguing phenomenon is observed, where each initial condition corresponds to a distinct bifurcation diagram. This phenomenon appears to be present in other Fractional Order (FO) difference systems as well, which could pose a challenge for numerical analysis.

As discussed in reference [31], a 3D fractional logistic chaotic map exhibits more chaotic behavior compared to conventional chaotic maps. The Computational formulations for the proposed logistic maps (LM) are provided by:

$$X = \mu g\big(1 - g(i)\big) + Bh'X + \alpha Z \tag{1}$$

$$Y = \mu h\big(1 - h(i)\big) + Bg'Z + \alpha Y \tag{2}$$

$$Z = \mu s\big(1 - s(i)\big) + Bs'h + \alpha X \tag{3}$$



(a)

(b)

Figure 3. Lorentz plot for the proposed 3D fractional logistic maps for the different initial conditions

Here, the variable μ serves as the growth rate parameter that influences the system's nonlinearity. The functions g(i), h(i), and s(i) represent the fractional population values at a given iteration *i* for each respective dimension such as X, Y, and Z. The parameter B acts as a coupling coefficient, managing the interaction between these variables. The terms h′, g′, and h″ denote the fractional derivatives of the state variables, capturing the system’s memory-dependent behavior. α is a small constant that introduces cross-dimensional feedback among the variables, contributing to the chaotic characteristics of the system. Finally, X, Y, and Z are the state variables that dynamically evolve and collectively define the system's behavior over time.

When 0.35<μ<0.381, B<0.0022, and α=0.0015, the equations above demonstrate the 3D LM. Figure 3 illustrates the chaotic behavior for the specified values in the recommended 3D chaotic system.

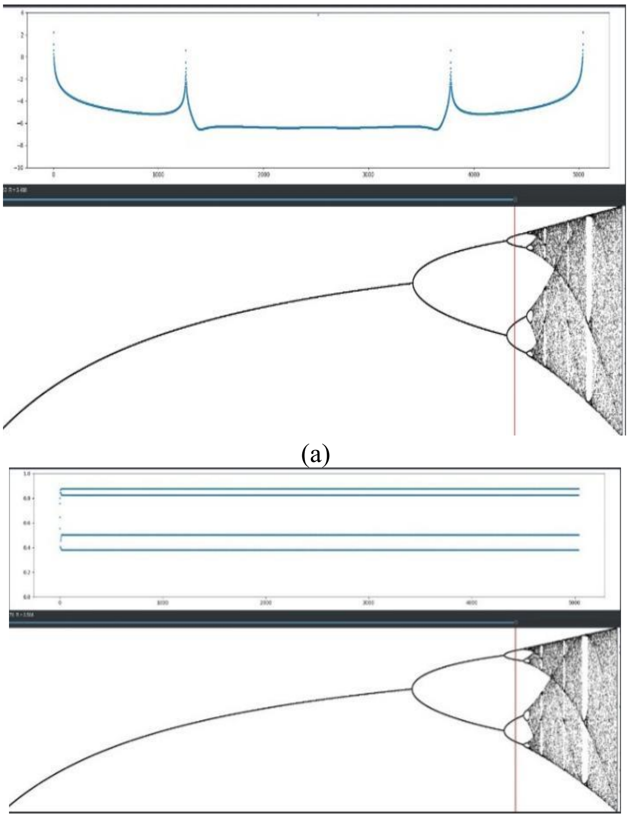
4.2.2 Henon maps-Its working principles

Henon Maps are the dynamic quadratic and non-linear mappings defined by their characteristic equation.

$$X_{n+1}=1-aX_n^2+Y_n \tag{4}$$

$$Y_{n+1}=1-bX_n \tag{5}$$

The classical maps depend on two parameters, *a* and *b*, with values set to *a=1.4* and *b=1.3.* At these classical values, the Henon map unveils chaotic behavior. For varied values of attributes, the map's dynamics vary and Henon maps may exhibit the chaotic behavior which can be identified with the several times of iteration. Figures 4 (a) and (b) represents the chaotic behavior of the Henon maps utilising conventional values.



(a)

(b)

Figure 4. Characteristics of Henon maps a) a=1.4 and b=1.3 b) a=2.0 and b=1.78

4.3 Proposed encryption process

As shown in Figure 5, encryption algorithm works in three different phases. In the first phase, inter-pixel of the images and fractional logistic maps are permutated and diffused to form the inter cryptographic pixels (J). In the second stage, intra-pixels of images are permuted and diffused with the Henon maps to form the intra-cryptographic pixels (K). The last level comprises unique sequence generated by diffusing the inter (J) and intra cryptographic pixels (K). The density of the recommended approach provides the strong resistance to the attackers. Figure 5 shows the proposed encryption schemes.

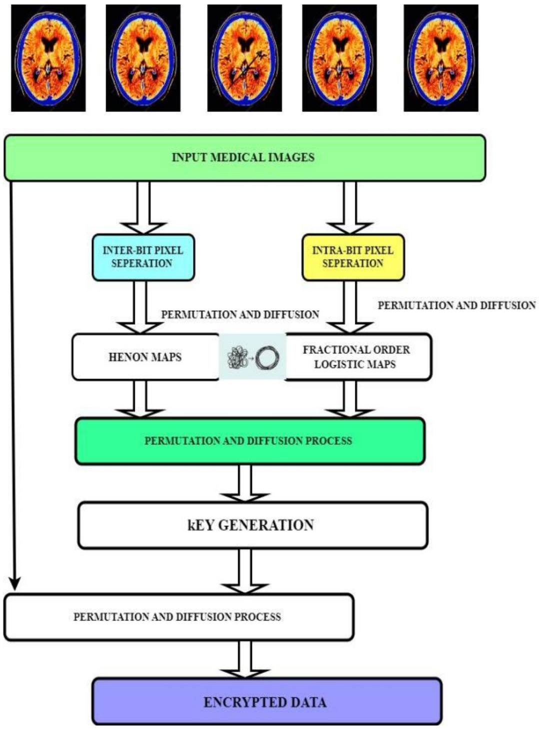

INPUT MEDICAL IMAGES
INTER-BIT PIXEL SEPERATION
INTRA-BIT PIXEL SEPERATION
PERMUTATION AND DIFFUSION
PERMUTATION AND DIFFUSION
HENON MAPS
FRACTIONAL ORDER LOGISTIC MAPS
PERMUTATION AND DIFFUSION PROCESS
kEY GENERATION
PERMUTATION AND DIFFUSION PROCESS
ENCRYPTED DATA

Figure 5. Proposed encryption process in the BDLE-FOHLT framework

4.4 Stage 1 of encryption

Recommended encryption framework consists of permuting the position of the inter-pixels in an Unaltered image. During the initial level of computation, chaotic sequence is generated using the fractional logistic maps(FLM) using the different fractional initial conditions. The chaotic sequence is generated repeatedly using FL maps. The inter-pixels of the images are permuted and diffused with the strong chaotic sequences. Mathematically the procedure is expressed as follows:

$$\text{E}= FOL\ maps(X,Y,Z)\ \text{For I=1,2…..L} \tag{6}$$

$$KEY1 = mod(byte\{\ (E)permutate(R)\}) \tag{7}$$

$$KEY2 = mod(byte\{\ (E)diffuse\ (KEY1)\}) \tag{8}$$

E=Chaotic Maps created by Fractional Order logistic maps.

4.5 Stage 2 of encryption

Recommended encryption framework consists of permuting the position of the intra-pixels in an Unaltered image. During the initial level of computation, chaotic sequence is constructed utilising the Henon Chaotic using the different f initial conditions. The chaotic sequence is constructed repeatedly utilising Henon maps. The inter-pixels of the images are permuted and diffused with the strong chaotic sequences. Mathematically the procedure is expressed as follows:

$$F = HENON\ maps(X, Y, Z) \text{ For I=1,2…..L} \quad (9)$$

$$KEY3 = mod(byte\{\ (F)permutate(S)\}) \quad (10)$$

$$KEY4 = mod(byte\{\ (F)diffuse\ (KEY1)\}) \quad (11)$$

F=Chaotic Maps created by Henon maps.

4.6 Stage 3 of encryption

Ultimately, the intermediates are combined to form the novel random sequence. After continuing the several times, inter and intra cryptographic pixels are then put through using diffusion process. Consequently, it generates robustly encrypted bytes that change independently with each instance. The entire encryption process is demonstrated in Algorithm-1. Mathematically, the final encrypted process is expressed as follows:

$$U = Concat(K2.K4) \quad (12)$$

$$\text{Final Encrypted Data} = \text{Diffusion (U, Input Data)} \quad (13)$$

Steps	Algorithm-1//Complete Encryption Procedure
1	Input : Medical images captured by the camera
2	Output : Encrypted data
3	Begin:
4	Divide the image into inter-pixels and intra-pixels
5	Create random sequences for Fractional logistic maps using Eq. (6)
6	Generate the Chaotic Sequence using Henon maps
7	Construct the Intermediate S1-box-S1-box
8	Formulate the intermediate sequence utilising inter-image pixels and FML maps using Eq. (13)
9	Generate the Intermediate S2-box utilising intra-pixels and Henon Maps
10	Key=J concatenates K
11	Encrypted Data=Key Diffused Input medical images.
12	End

4.7 Blockchain-edge deployment

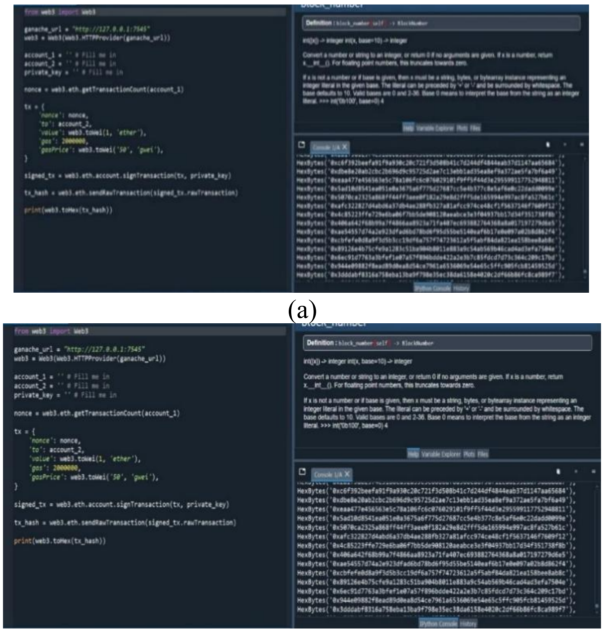
In the presented framework, the cryptographic pixels can be preserved on the Blockchain (BC) network, by ensuring the privacy and security of user's/patient's data. Moreover, BC offers amenability and resolves the security breaches. Additionally, blockchain supports the achievement of decentralization, privacy, and trust. It also facilitates seamless connections with multiple devices. In this study, the encrypted data is stored within the blockchain network that enables the secured communication with numerous nodes. The IoT devices act as the nodes and then commences making connections to the edge gateways. These nodes are exchanges the encrypted data with the edge gateways and may transfer to the cloud for the further processing.

The hash value represents each transaction that occurs within the block. Transactions are grouped to form a block, which is then added to the chain after receiving approval from the endorsed node. The process initiates when the client begins submitting a proposal. The transaction procedure involves dual categories of peers: committer peers and endorsers. The certificate authority (CA) issues credentials to the client, which are required for entity's applications to gain permission for submitting new communications. To initiate a new operation, the entity's application sends the transaction recommendations to an edge-based peer, which either updates or reads the ledger. Then the peer reads and verifies the authorization policy. At last, the committer peer asynchronously announces the transaction's status within the system.

5. RESULTS AND DISCUSSION

5.1 Implementation details

The recommended framework was designed utilising libraries from python that can be used to evaluate the effectiveness of the method in Etherum blockchain settings. The distributed applications (D-Apps) were created, and Influra APIs are utilized to interface with the Ethereum network which is shown in Figure 6.



```
from web3 import Web3

ganache_url = "http://127.0.0.1:7545"
web3 = Web3(Web3.HTTPProvider(ganache_url))

account_1 = '' # Fill me in
account_2 = '' # Fill me in
private_key = '' # Fill me in

nonce = web3.eth.getTransactionCount(account_1)

tx = {
    'nonce': nonce,
    'to': account_2,
    'value': web3.toWei(1, 'ether'),
    'gas': 2000000,
    'gasPrice': web3.toWei('50', 'gwei'),
}

signed_tx = web3.eth.account.signTransaction(tx, private_key)

tx_hash = web3.eth.sendRawTransaction(signed_tx.rawTransaction)

print(web3.toHex(tx_hash))
```

Definition : block_number(self) -> BlockNumber

int([x]) -> integer int(x, base=10) -> integer

Convert a number or string to an integer, or return 0 if no arguments are given. If x is a number, return x.__int__(). For floating point numbers, this truncates towards zero.

If x is not a number or if base is given, then x must be a string, bytes, or bytearray instance representing an integer literal in the given base. The literal can be preceded by '+' or '-' and be surrounded by whitespace. The base defaults to 10. Valid bases are 0 and 2-36. Base 0 means to interpret the base from the string as an integer literal. >>> int('0b100', base=0) 4

```
HexBytes('0xc6f392beefa91f9a930c20c721f3d508b41c7d244df4844eab37d1147aa65684'),
HexBytes('0xdbe8e20ab2cbc2b696d9c95725d2ae7c13ebb1ad35ea8ef9a372ae5fa7bf6a49'),
HexBytes('0xeaa477e456563e5c78a106fc6c076029101f9ff5f44d3e295599117752948811'),
HexBytes('0x5ad10d8541ea051e0a3675a6f775d27687cc5e4b377c8e5af6e0c22dadd0099e'),
HexBytes('0x5070ca2325a868ff44ff3aee0f182a29e8d2fff5de165994e997ac8fa527b61c'),
HexBytes('0xafc322827d4abd6a37db4ae288fb327a81afcc974ce48cf1f5637146f7609f12'),
HexBytes('0x4c85223ffe729e6ba06f7bb5de908120aeabce3e3f04937bb17d34f351738f8b'),
HexBytes('0x406a642f68b99a7f4866aa8923a71fa407ec693882764368a8a017197279d6e5'),
HexBytes('0xae54557d74a2e923dfad6bd78bd6f95d55be5140eaf6b17e0e097a02b8d862f4'),
HexBytes('0xcbfefe0d8a9f3d5b3cc19df6a757f74723612a5f5abf84da821ea158bee8ab8c'),
HexBytes('0x89126e4b75cfe9a1283c51ba904b8011e883a9c54ab569b46cad4ad3efa7504e'),
HexBytes('0x6ec91d7763a3bfef1e07a57f896bdde422a2e3b7c85fdcd7d73c364c209c17bd'),
HexBytes('0x944e09882f8ead89d0ea8d54ce7961a6536069e54e65c5ffc905fcb81459525d'),
HexBytes('0x3dddabf8316a758eba13ba9f798e35ec38da6158e4020c2df66b86fc8ca989f7'),
```

(a)

```
from web3 import Web3

ganache_url = "http://127.0.0.1:7545"
web3 = Web3(Web3.HTTPProvider(ganache_url))

account_1 = '' # Fill me in
account_2 = '' # Fill me in
private_key = '' # Fill me in

nonce = web3.eth.getTransactionCount(account_1)

tx = {
    'nonce': nonce,
    'to': account_2,
    'value': web3.toWei(1, 'ether'),
    'gas': 2000000,
    'gasPrice': web3.toWei('50', 'gwei'),
}

signed_tx = web3.eth.account.signTransaction(tx, private_key)

tx_hash = web3.eth.sendRawTransaction(signed_tx.rawTransaction)

print(web3.toHex(tx_hash))
```

Definition : block_number(self) -> BlockNumber

int([x]) -> integer int(x, base=10) -> integer

Convert a number or string to an integer, or return 0 if no arguments are given. If x is a number, return x.__int__(). For floating point numbers, this truncates towards zero.

If x is not a number or if base is given, then x must be a string, bytes, or bytearray instance representing an integer literal in the given base. The literal can be preceded by '+' or '-' and be surrounded by whitespace. The base defaults to 10. Valid bases are 0 and 2-36. Base 0 means to interpret the base from the string as an integer literal. >>> int('0b100', base=0) 4

```
HexBytes('0xc6f392beefa91f9a930c20c721f3d508b41c7d244df4844eab37d1147aa65684'),
HexBytes('0xdbe8e20ab2cbc2b696d9c95725d2ae7c13ebb1ad35ea8ef9a372ae5fa7bf6a49'),
HexBytes('0xeaa477e456563e5c78a106fc6c076029101f9ff5f44d3e295599117752948811'),
HexBytes('0x5ad10d8541ea051e0a3675a6f775d27687cc5e4b377c8e5af6e0c22dadd0099e'),
HexBytes('0x5070ca2325a868ff44ff3aee0f182a29e8d2fff5de165994e997ac8fa527b61c'),
HexBytes('0xafc322827d4abd6a37db4ae288fb327a81afcc974ce48cf1f5637146f7609f12'),
HexBytes('0x4c85223ffe729e6ba06f7bb5de908120aeabce3e3f04937bb17d34f351738f8b'),
HexBytes('0x406a642f68b99a7f4866aa8923a71fa407ec693882764368a8a017197279d6e5'),
HexBytes('0xae54557d74a2e923dfad6bd78bd6f95d55be5140eaf6b17e0e097a02b8d862f4'),
HexBytes('0xcbfefe0d8a9f3d5b3cc19df6a757f74723612a5f5abf84da821ea158bee8ab8c'),
HexBytes('0x89126e4b75cfe9a1283c51ba904b8011e883a9c54ab569b46cad4ad3efa7504e'),
HexBytes('0x6ec91d7763a3bfef1e07a57f896bdde422a2e3b7c85fdcd7d73c364c209c17bd'),
HexBytes('0x944e09882f8ead89d0ea8d54ce7961a6536069e54e65c5ffc905fcb81459525d'),
HexBytes('0x3dddabf8316a758eba13ba9f798e35ec38da6158e4020c2df66b86fc8ca989f7'),
```

(b)

Figure 6. (a), (b) Chaotic encrypted bits created in Etherum blockchain using the proposed architecture

5.2 Security assessment

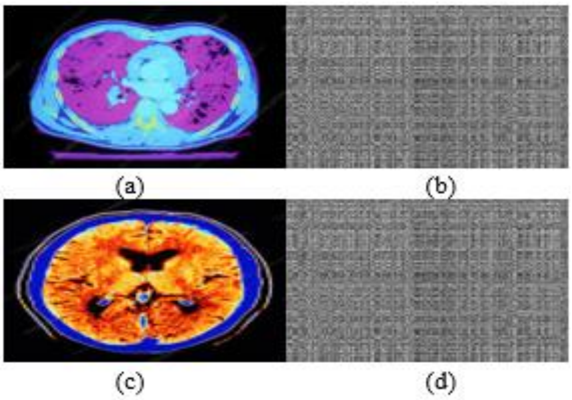


Figure 7. Encrypted Images a) CT input picture, b) Encrypted CT picture, c) MRI input picture, d) Encrypted MRI picture

This section focuses on the security assessment of the recommended hybrid systems used for encrypting several types of medical images. The experimentation validation involves 256×256 general CT images and MRI brain images. The algorithm has been tested on all image categories. Figure 7 illustrates the input images alongside their corresponding encrypted versions. As shown in the figures, it is evident that the encrypted images are completely unidentifiable.

5.3 Key sensitivity analysis

In this approach, the secret key must exhibit high sensitivity to minor changes in order to defend against brute-force attacks. To evaluate key sensitivity, NPCR and UACI were processed to examine the recommended encryption approach's efficacy concerning the cipher keys using the following mathematical formulas. The values from NPCR and UACI for the varied encrypted pictures are computed and represented in Tabular 2.

$$NPCR = \frac{\sum_{q,r} E(q,r)}{L} * 100 \tag{14}$$

$$UACI = \frac{1}{L}\sum_{q,r}\frac{|f(q,r) \neq f(q,r)|}{256} * 100 \tag{15}$$

where,

$$E(q,r) = \left[\begin{array}{l} 1, f(q,r) \neq f(q,r) \\ 0, f(q,r) = f(q,r) \end{array}\right. \tag{16}$$

Table 3. Proposed encryption frameworks with the values of NCPR and UACI

Image Type	NPCR	UACI
CT Images	91.7	32.90
MRI Images	90.89	32.80

From the Table 3, it is obvious that the above stated values for numerous clinical image datasets has been derived and evaluated. The findings show that the recommended encryption schemes deliver optimal performance, with NPCR=99.65% and UACI=33.90% for the tested input pictures, demonstrating their ability to withstand IoT attacks, including brute-force attacks.

5.4 Statistical adjacent pixel evaluation

Normal images typically exhibit high correlations between their pixels, while encrypted images show diminished correlations. To assess the correlations within the images, nearly 100 images were selected, and the interaction among adjacent pixel values in each image was calculated using the following mathematical expressions.

$$R_{xy} = \frac{cov(a,b)}{\sqrt{E(x)E(y)}} \tag{17}$$

$$cov(a,b) = D\{[a - D(a)][b - D(b)]\} \tag{18}$$

$$e(a) = \frac{1}{n}\sum_{i=1}^{n} a_i \tag{19}$$

$$L(x) = \frac{1}{n}\sum_{i=1}^{n}[a_i - a(x)]^2 \tag{20}$$

Here, e(a) and L(x) denote the expected values and diversity of the plaintext image and ciphertext datasets, respectively. The contrast of correlation values among distinct methods is presented in Table 4.

Table 4 clearly shows that the cipher images demonstrate minimal correlation, with a difference of less than 0.000001, which enables this approach more resilient against multiple attacks.

Table 4. Coefficient of correlation analysis among the plain and encrypted pictures

Image Types	Plain Images			Encrypted Images		
	Lateral	Upward	Crosswise	Lateral	Upward	Crosswise
CT Images	402.90	433.68	457.76	0.0005423	0.00019202	0.008945
MRI Images	428.90	435.91	468.91	0.0005690	0.00009202	0.008546

5.5 Information entropy evaluation

It depicts the degree of Irregularity that reflects the highest level of Variability in medical data. Higher Variability values may suggest increased unpredictability in encrypted images.

$$g(m) = \sum_{l}^{l-1} q(m)\log_2\frac{1}{q(m_i)} \tag{21}$$

where, *l* denotes the gray level, and q(m) is the probability of a specific gray value occurring in the image matrix. For an 8-bit grayscale picture, the bit length is considered to be 256. In a well-encrypted image, the Variability value could be 8. The Variability values acquired for varied picture sets are presented in Tabular 5.

Table 5 reports entropy values of 7.8964 for CT images and 7.87546 for MRI images. These values, though slightly below the ideal value, fall within an acceptable deviation range (typically ±0.1), which is common in practical encryption schemes due to data constraints and inherent image structures. This small deviation still reflects high randomness and strong unpredictability, implying the encryption algorithm is effective in key generation and resistant to entropy-based attacks.

Table 5. Entropy numerals for the different image datasets

Image Types	Entropy Values
CT Images	7.8964
MRI Images	7.87546

5.6 NIST test analysis

This experiment examined the security robustness of the encrypted bits. To assure the uncertainity of these bits—essential for confidentially transferring private schemes to central servers—National Institute of Standards and

Technology (NIST) tests were performed. The results of the 12 required NIST tests are synopsized in Table 6.

Based on the Table 6, it is clear that the ciphered bits demonstrate high uncertainty, making it more challenging for an attacker to alter the clinical information while transmutation.

5.7 Comparative analysis

To prove the superiority of the preferred encryption method, various chaotic encryption phases are examined, as detailed in references [32-37]. Table 7 presents a comparative valuation of the effectiveness of various encryption methods.

Tables 7 and 8 clearly show that the proposed method outperforms existing schemes in terms of NPCR, UACI, entropy, and encryption time. Specifically, the proposed method consistently achieves higher values in NPCR, UACI, and entropy, indicating enhanced sensitivity to pixel changes, stronger diffusion, and increased randomness, respectively. Furthermore, the encryption time of 24.79 seconds outperforms all other methods, highlighting its efficiency. This improvement stems from the integration of fractional order logistic and Henon maps, which provide higher complexity in chaotic behavior without significantly increasing computational load. Additionally, the proposed model successfully pass the NIST statistical test, further verifying its cryptographic strength. From this, it is very clear that adding the fractional logistic maps and henon maps has produced the considerable better performance against the growing attacks.

Table 6. NIST standard test results for the recommended framework

S.No.	NIST Test Specification	Status of Test
1	Linear Complexity Test	Authorized
2	Frequency MonoTest	Authorized
3	Frequency Test	Authorized
4	Long Run Test	Authorized
5	Matrix Rank Test	Authorized
6	RunTest	Authorized
7	Universal statistical Test	Authorized
8	DFT Test	Authorized
9	Overlapping Template of all One's Test	Authorized
10	Random Excursion Test	Authorized
11	Block Frequency Test	Authorized
12	Lempel-ZIV Compression Test	Authorized

Table 7. Performance comparision for various encryption schemes (CT images)

Algorithm	Performance Evaluation					
	NPCR	UACI	Entropy	Adjacent Pixel Analysis	NIST Test	Encryption Time(s)
Ref. [32]	86.4	29.90	7.342	Medium	Unavailable	45.90
Ref. [33]	85.4	28.78	7.23	Medium	Unavailable	35.90
Ref. [34]	90.45	29.78	7.12	Medium	Unavailable	33.89
Ref. [35]	91.23	20.89	7.56	Medium	Unavailable	34.90
Ref. [36]	90.56	29.9	7.34	High	Unavailable	32.90
Ref. [37]	92.8	29.45	7.4	High	Unavailable	31.90
Proposed Model	91.97	32.9	7.87	Very High	PASSED	24.79

Table 8. Comparative evaluation of various encryption techniques (MRI images)

Algorithm	Performance Evaluation					
	NPCR	UACI	Entropy	Adjacent Pixel Analysis	NIST Test	Encryption Time(s)
Ref. [32]	86.4	29.90	7.342	Medium	Unavailable	45.90
Ref. [33]	85.4	28.78	7.23	Medium	Unavailable	35.90
Ref. [34]	90.45	29.78	7.12	Medium	Unavailable	33.89
Ref. [35]	91.23	20.89	7.56	Medium	Unavailable	34.90
Ref. [36]	90.56	29.9	7.34	High	Unavailable	32.90
Ref. [37]	92.8	29.45	7.4	High	Unavailable	31.90
Proposed Model	91.97	32.9	7.87	Very High	PASSED	24.79

5.8 Blockchain transaction analyses

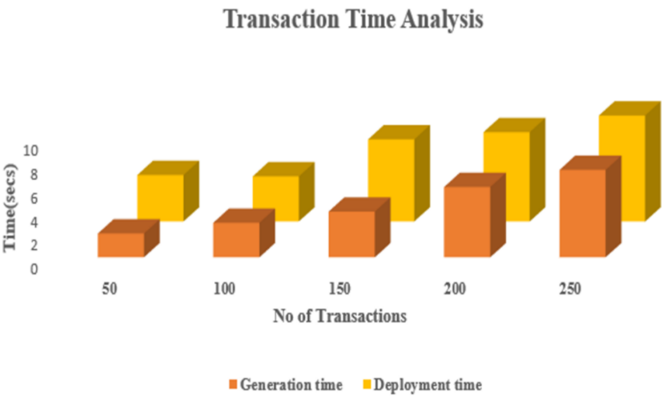


Figure 8. Transaction time analysis for the recommended approach

The performance evaluation of the proposed framework must consider the scenario where the number of transactions increases. To assess this, the computational cost for signing and verifying operations is examined in relation to the number of transactions, as shown in Figure 8. The outcomes reveal that both the generation and deployment times maximises progressively with the rising count of operations. Moreover, latency is estimated for per operation. Results shows that the latency linearly increases as the number of transaction maximises.

6. CONCLUSION AND FUTURE DIRECTION

This study article introduces a blockchain-driven medical image encryption scheme opt for an IoT-Edge computing setting. The encryption model incorporates fractional-order logistic maps and Henon maps to achieve a lightweight and highly cryptographic mechanism. Highly random keys and highly secure data are generated and preserved in the edge devices using the blockchain framework. The complete algorithm was developed using Python 3.9 and deployed in the Ethereum Blockchain environment. A comprehensive analysis was carried out, and results were compared with other existing frameworks. Results demonstrated that the recommended approach exceeds other models in terms of encryption time and security performance. Challenges such as compliance with healthcare data privacy regulations, interoperability across platforms, and latency in edge environments must be further evaluated. As a future direction, the framework could be enhanced by incorporating meta-optimization techniques that take into account the energy efficiency and operational lifetime of IoT and edge computing devices, while also ensuring alignment with legal and ethical standards in medical data processing.

REFERENCES

[1] Ravi, D., Ramachandran, S., Vignesh, R., Falmari, V.R., Brindha, M. (2022). Privacy preserving transparent supply chain management through Hyperledger Fabric. Blockchain: Research and Applications, 3(2): 100072. https://doi.org/10.1016/j.bcra.2022.100072

[2] Bokhari, M.U., Makki, Q., Tamandani, Y.K. (2018). A survey on cloud computing. In Big Data Analytics: Proceedings of CSI 2015, Hyderabad, India. pp. 149-164. https://doi.org/10.1007/978-981-10-6620-7_16

[3] Mishra, S., Sharma, S.K., Alowaidi, M.A. (2021). Retracted article: Analysis of security issues of cloud-based web applications. Journal of Ambient Intelligence and Humanized Computing, 12(7): 7051-7062. https://doi.org/10.1007/s12652-020-02370-8

[4] Altowaijri, S.M. (2020). An architecture to improve the security of cloud computing in the healthcare sector. Smart Infrastructure and Applications: Foundations for Smarter Cities and Societies, pp. 249-266. https://doi.org/10.1007/978-3-030-13705-2_10

[5] Dutta, A., Misra, C., Barik, R.K., Mishra, S. (2019). Enhancing mist assisted cloud computing toward secure and scalable architecture for smart healthcare. In International Conference on Advanced Communication and Computational Technology, Singapore. Springer Nature Singapore, pp. 1515-1526. https://doi.org/10.1007/978-981-15-5341-7_116

[6] Sri Vigna Hema, V., Kesavan, R. (2019). ECC based secure sharing of healthcare data in the health cloud environment. Wireless Personal Communications, 108: 1021-1035. https://doi.org/10.1007/s11277-019-06450-7

[7] Kamal, S.T., Hosny, K.M., Elgindy, T.M., Darwish, M.M., Fouda, M.M. (2021). A new image encryption algorithm for grey and color medical images. IEEE Access, 9: 37855-37865. https://doi.org/10.1109/ACCESS.2021.3063237

[8] Pustokhina, I.V., Pustokhin, D.A., Shankar, K. (2022). Blockchain-Based Secure Data Sharing Scheme Using Image Steganography and Encryption Techniques for Telemedicine Applications. Academic Press, Cambridge, MA, USA, pp. 97-108. https://doi.org/10.1016/B978-0-323-85854-0.00009-5

[9] Acharya, M., Sharma, R.S. (2021). A novel image encryption based on feedback carry shift register and blockchain for secure communication. International Journal of Applied Engineering Research, 16: 466-477.

[10] Khan, A.A., Laghari, A.A., Gadekallu, T.R., Shaikh, Z.A., Javed, A.R., Rashid, M., Estrela, V.V., Mikhaylov, A. (2022). A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment. Computers and Electrical Engineering, 102: 108234. https://doi.org/10.1016/j.compeleceng.2022.108234

[11] Shankar, K., Elhoseny, M., Perumal, E., Ilayaraja, M., Sathesh Kumar, K. (2019). An efficient image encryption scheme based on signcryption technique with adaptive elephant herding optimization. Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments, pp. 31-42. https://doi.org/10.1007/978-3-030-16837-7_3

[12] Kalpana, P., Kodati, S., Sreekanth, N., Ali, H.M., Ramachandra, A.C. (2024). Predictive analytics for crime prevention in smart cities using machine learning. In 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), Hassan, India, pp. 1-4. https://doi.org/10.1109/IACIS61494.2024.10721948

[13] Banik, A., Laiphrakpam, D.S., Agrawal, A., Patgiri, R. (2022). Secret image encryption based on chaotic system and elliptic curve cryptography. Digital Signal Processing, 129: 103639. https://doi.org/10.1016/j.dsp.2022.103639

[14] Kalpana, P., Anandan, R. (2023). A capsule attention network for plant disease classification. Traitement du Signal, 40(5): 2051-2062. https://doi.org/10.18280/ts.400523

[15] Kalpana, P., Almusawi, M., Chanti, Y., Kumar, V.S., Rao, M.V. (2024). A deep reinforcement learning-based task offloading framework for edge-cloud computing. In 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, pp. 1-5. https://doi.org/10.1109/ICICACS60521.2024.10498232

[16] Chen, Y., Chen, H., Han, M., Liu, B., Chen, Q., Ma, Z., Wang, Z. (2021). Miner revenue optimization algorithm based on Pareto artificial bee colony in blockchain network. EURASIP Journal on Wireless Communications and Networking, 2021: 1-28. https://doi.org/10.1186/s13638-021-02018-x

[17] Kalpana, P., Kodati, S., Smitha, L., Sreekanth, N., Smerat, A., Ahmad, M.A. (2025). Explainable AI-Driven gait analysis using wearable Internet of Things (WIoT) and human activity recognition. Journal of Intelligent Systems & Internet of Things, 15(2): 55-75. https://doi.org/10.54216/JISIoT.150205

[18] Kong, L., Tan, J., Huang, J., Chen, G., Wang, S., Jin, X., Zeng, P., Khan, M., Das, S.K. (2022). Edge-computing-driven Internet of Things: A survey. ACM Computing Surveys, 55(8): 1-41. https://doi.org/10.1145/3555308

[19] Lang, P., Tian, D., Duan, X., Zhou, J., Sheng, Z., Leung, V.C. (2022). Cooperative computation offloading in blockchain-based vehicular edge computing networks. IEEE Transactions on Intelligent Vehicles, 7(3): 783-798. https://doi.org/10.1109/TIV.2022.3190308

[20] Lee, C.K., Huo, Y.Z., Zhang, S.Z., Ng, K.K. (2020). Design of a smart manufacturing system with the application of multi-access edge computing and blockchain technology. IEEE Access, 8: 28659-28667.

https://doi.org/10.1109/ACCESS.2020.2972284

[21] Sammeta, N., Parthiban, L. (2023). Data ownership and secure medical data transmission using optimal multiple key-based homomorphic encryption with Hyperledger blockchain. International Journal of Image and Graphics, 23(03): 2240003. https://doi.org/10.1142/S0219467822400034

[22] Ali, T.S., Ali, R. (2020). A novel medical image signcryption scheme using TLTS and Henon chaotic map. IEEE Access, 8: 71974-71992. https://doi.org/10.1109/ACCESS.2020.2987615

[23] Hosny, K.M., Kamal, S.T., Darwish, M.M. (2022). Novel encryption for color images using fractional-order hyperchaotic system. Journal of Ambient Intelligence and Humanized Computing, 13(2): 973-988. https://doi.org/10.1007/s12652-021-03675-y

[24] Neelakandan, S., Beulah, J.R., Prathiba, L., Murthy, G.L.N., Irudaya Raj, E.F., Arulkumar, N. (2022). Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model. International Journal of Modeling, Simulation, and Scientific Computing, 13(04): 2241006. https://doi.org/10.1142/S1793962322410069

[25] Bhaskaran, R., Karuppathal, R., Karthick, M., Vijayalakshmi, J., Kadry, S. (2022). Blockchain enabled optimal lightweight cryptography based image encryption technique for IIoT. Intelligent Automation & Soft Computing, 33(3): 1593-1606. http://dx.doi.org/10.32604/iasc.2022.024902

[26] Afzal, I., Parah, S.A., Hurrah, N.N., Song, O.Y. (2020). Secure patient data transmission on resource constrained platform. Multimedia Tools and Applications, 83: 15001-15026.

[27] Kumar, M., Kumar, S., Budhiraja, R., Das, M.K., Singh, S. (2016). Lightweight data security model for IoT applications: A dynamic key approach. In 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, pp. 424-428. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.100

[28] Patil, J., Bansod, G., Kant, K.S. (2017). LiCi: A new ultra-lightweight block cipher. In 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI), Pune, India, pp. 40-45. https://doi.org/10.1109/ETIICT.2017.7977007

[29] Nickparvar, M. (n.d.). Brain tumor MRI dataset. Kaggle. https://www.kaggle.com/datasets/masoudnickparvar/brain-tumor-mri-dataset.

[30] Mader, K. (n.d.). SIIM medical images. Kaggle. https://www.kaggle.com/datasets/kmader/siim-medical-images.

[31] Rahman, A., Nasir, M.K., Rahman, Z., Mosavi, A., Minaei-Bidgoli, B. (2020). Distblockbuilding: A distributed blockchain-based SDN-IoT network for smart building management. IEEE Access, 8: 140008-140018. https://doi.org/10.1109/ACCESS.2020.3012435

[32] Gu, Z., Li, H., Khan, S., Deng, L., Du, X., Guizani, M., Tian, Z. (2021). IEPSBP: A cost-efficient image encryption algorithm based on parallel chaotic system for green IoT. IEEE Transactions on Green Communications and Networking, 6(1): 89-106. https://doi.org/10.1109/TGCN.2021.3095707

[33] Sun, Y., Chatterjee, P., Chen, Y., Zhang, Y. (2022). Efficient identity-based encryption with revocation for data privacy in Internet of Things. IEEE Internet of Things Journal, 9(4): 2734-2743. https://doi.org/10.1109/JIOT.2021.3109655

[34] Ramesh, S., Govindarasu, M. (2020). An efficient framework for privacy-preserving computations on encrypted IoT data. IEEE Internet of Things Journal, 7(9): 8700-8708. https://doi.org/10.1109/JIOT.2020.2998109

[35] Al-Moliki, Y.M., Alresheedi, M.T., Al-Harthi, Y., Alqahtani, A.H. (2021). Robust lightweight-channel-independent OFDM-based encryption method for VLC-IoT networks. IEEE Internet of Things Journal, 9(6): 4661-4676. https://doi.org/10.1109/JIOT.2021.3107395

[36] Kalpana, P., Narayana, P., Smitha, L., Madhavi, D., Keerthi, K., Smerat, A., Nazzal, M.A. (2025). Health-fots-a latency aware fog based IoT environment and efficient monitoring of body's vital parameters in smart health care environment. Journal of Intelligent Systems & Internet of Things, 15(1): 144-156. https://doi.org/10.54216/JISIoT.150112

[37] Sabir, S., Guleria, V. (2023). Multi-layer security based multiple image encryption technique. Computers and Electrical Engineering, 106: 108609. https://doi.org/10.1016/j.compeleceng.2023.108609