IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 17, 2021, accepted January 8, 2022, date of publication January 19, 2022, date of current version February 1, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3144681

CES Blocks–A Novel Chaotic Encryption Schemes-Based Blockchain System for an IoT Environment

R. DURGA[1], E. POOVAMMAL[1], (Member, IEEE), KADIYALA RAMANA[2], RUTVIJ H. JHAVERI[3], (Senior Member, IEEE), SAURABH SINGH[4], AND BYUNGUN YOON[4], (Senior Member, IEEE)

[1]Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, Tamil Nadu 603203, India
[2]Department of Computer Science and Engineering, Annamacharya Institute of Technology and Sciences, Rajampet 516126, India
[3]Department of Computer Science and Engineering, Pandit Deendayal Energy University, Gandhinagar 382007, India
[4]Department of Industrial and Systems Engineering, Dongguk University, Seoul 04620, South Korea

Corresponding author: Byungun Yoon (postman3@dongguk.edu)

This work was supported by the National Research Foundation of Korea under Grant NRF-2021R1I1A2045721.

ABSTRACT With the advent of the Internet of Things (IoT), smart devices have now changed their dimensions to provide applications in different domains such as medical, agriculture, and Industry 4.0. Although IoT provides more diversified applications, enhancing the security in IoT remains on the darker side of the research. Traditional IoT systems involve a third party to secure sensitive data during transmission in an IoT environment which can lead to complex and serious problems. To overcome security issues and eradicate third-party involvement, Blockchain technology is the modern-day solution in an IoT environment. In the context of a Secured IoT system, we proposed a novel chaotic encryption-based blockchain-IoT architecture to clinch the security and privacy of data. Since smart sensors and image sensors are used widely in an IoT environment, the proposed scheme was tested with different image sets to evaluate performance metrics such as Number of Pixel Change Rate (NPCR), Unified Averaged Changed Intensity (UACI), Correlation Coefficients, and entropy under different attack scenarios. We obtained an NPCR of 99.65%, a UACI of 34%, and an entropy value close to 8. These values incite that the novel chaotic encryption-based blockchain-IoT architecture will be safe from IoT attacks. Results showed that integrating chaotic encrypted blockchain architecture with IoT could be more effective in defending attacks.

INDEX TERMS Blockchain, Internet of Things, chaotic encryption, smart sensors, NPCR, UACI, entropy.

I. INTRODUCTION

Human medical care has been a cardinal part of our daily lives. Healthcare is getting preeminent focus in terms of revenue and data. Traditionally, healthcare data were written on paper, which might be prone to damage and modification. Thus, health care data need to preserved electronically. Digitalized health data such as medical images of patients could be shared, stored, and prolonged by various hospitals. As the era of technology grows, more data are being shared on a cloud-based model delineated by US National Institute Standard. Thus, the health care data obtained daily was limitless strikes into the cloud-based model for storing and scattered across the health care system.

The associate editor coordinating the review of this manuscript and approving it for publication was Hiram Ponce.

The enhancement of the Internet of Things has inflated the health care horizon by integrating prominent technologies for remote patient monitoring using wearable and connected devices. The digitally organized infrastructure to the new level with extensive centralization connects patient health monitoring, remote treatment transmitted the data in a single framework. The electronic health data market is highly powered with billions of dollars to meet an unshakeable infrastructure.

Internet of Things (IoT) allows interconnection of multiple devices without the need for human innervations [1]. It consists of sensors, central processing units (CPU), and transceivers. In today's scenario, image and video surveillance are playing an important role in IoT medical computing systems. It is being utilized for building board frameworks, performing logical exploration, gaining business knowledge,

and performing real-time analysis [2], [3]. With these applications, computer vision-based IoT systems play a major role in even building smart cities. With advancements in cameras, IoT has reached its new dimension with dark challenges due to the lack of inbuilt security. The huge privacy-sensitive health data stored on the centralized architecture can lead to disclosing and spilling of confidential data. Secondly, the current IoT architecture uses extensive centralization depending on a single party for the administration of health care data inclined with a single point of failure.

Medical images are highly sensitive. To avoid unauthorized access to medical data, encryption is needed before uploading to the decentralized network. Existing Image Encryption schemes cannot help effective implementation of smart cities where peers are decentralized [4]. Medical images are encrypted using a chaotic encryption technique that can withstand many attacks such as Denial-of-Service (DoS) attacks, bottleneck attacks, and Distributed denial of service (DDoS) attacks. Medical image data have unique features such as immense volume, redundancy, and heavy correlation with health care application. Thus, they need more cryptology techniques than Data Encryption Standard, Advanced Encryption Standard (AES), Rivest–Shamir–Adleman(RSA), and Secure Hash Algorithm (SHA). The encryption technique has drawn great fascinate on researches to be used in blockchain technology for health care applications. Depending on innate attributes of chaos such as high pseudorandom and sensitivity, cryptosystems with control parameters have evinced exemplary properties such as complexity, security, and computing power.

Blockchain has become a useful technique in cryptos and other sectors due to its immutable properties. Blockchain Cryptocurrency was developed by Satoshi [18] to track third parties' transactions and evade them. It is utilized in applications that include the Internet of Things (IoT), connected vehicles, industry 4.0, medical facilities, and so on. The blockchain resembles a peer-to-to-peer structure, which includes hashes (i.e., Blocks). Every block in the network is a digital ledger of the previous transaction. All data stay on the blockchain. All other features of a block are temporary alteration of each block timestamps the information is difficult Previous hashtags are the two important topographies for any transaction or data change in the block. This confirms each block as part of the network. It looks decentralized because it integrates all nodes and data.

Blockchain is a decentralized ledger that records all transactions from individuals. Blockchain is known to be a consensus-based system, implying that every hub checks each transaction and consensus about data before placing it into a blockchain-based ledger (BCL). It is the best solution ever for security-related issues [5], [6]. Its dynamic properties can be used to develop smart healthcare with the help of IoT. Blockchain has revolutionized IoT. It gives security and provides new functionalities of smart gadgets. This technology plays a vital role in industries to serve security. It also compliments the point of view [7].

Blockchain technology has five significant components: (i) Node, (ii) Transactions, (iii) Blocks, (iv) Miners, and (v) Consensus. Every component plays a vital role in blockchain operation. The node can be represented by computer, server, or individual users followed by the transaction as a building block of the network. Blocks are storage devices that contain a set of previous transaction data. Miners are a set of rules verified during block accumulation. Consensus algorithm is a major part used for blockchain execution. Fig.1. illustrates components of a blockchain.

This article explores the building mechanism of a secured private blockchain in a disintermediating peer-to-peer network that can be employed for smart healthcare. Although many blockchain-based image encryptions have been proposed for smart healthcare [8] improvisation is still needed in terms of the strength of security algorithm that can defend IoT attacks [19]. IoT networks are connected by a centralized based client server-based mechanism with very large cloud servers and a strengthened database through a high bandwidth internet. IoT networks have two hindrances.(i) single point of failure, and (ii) lack of confidence between units involved in the network. By adopting the blockchain mechanism for IoT-enabled networks [37], experimentation in scripts could be performed about the following issues: interoperability, confidentiality, patient-centric access, flexibility, and accountability. Therefore, scientists in the field of medical care can bring solutions for decentralized-based blockchain technology with unique attributes such as process automation, seamless data sharing, data monetization, advanced identity security, and preserved privacy. A chaotic-based image encryption venture has been implemented for blockchain-enabled IoT networks utilized in smart healthcare. The purposes of this paper are:

- To integrate Bi-Modal Multi Scroll Attractors for the image encryption process suitable for IoT -blockchain networks
- To implement private blockchain systems suitable for secured IoT medical networks.

This paper contributes a novel hybrid image encryption scheme for the IoT environment based on the blockchain system. The proposed work contributes a secured private own blockchain with the smart contract for automation, seamless data sharing, data monetization, advanced identity security and preserves privacy. Safe offloading of data from devices will be improved with the deployment of private blockchain systems appropriate for the protected IoT medical networks. The blockchain system is based on the dynamic behavior of a novel bi-scroller chaotic encryption scheme which is used to encrypt the images. Then the encrypted image is stored in the private blockchain system appropriate for secure IoT medical networks. During the transmission in an IoT environment, the proposed encryption scheme secures the sensitive data from attackers. The proposed scheme has experimented with the different image sets in which we evaluate the performance metrics such as Number of Pixel Change Rate (NPCR),

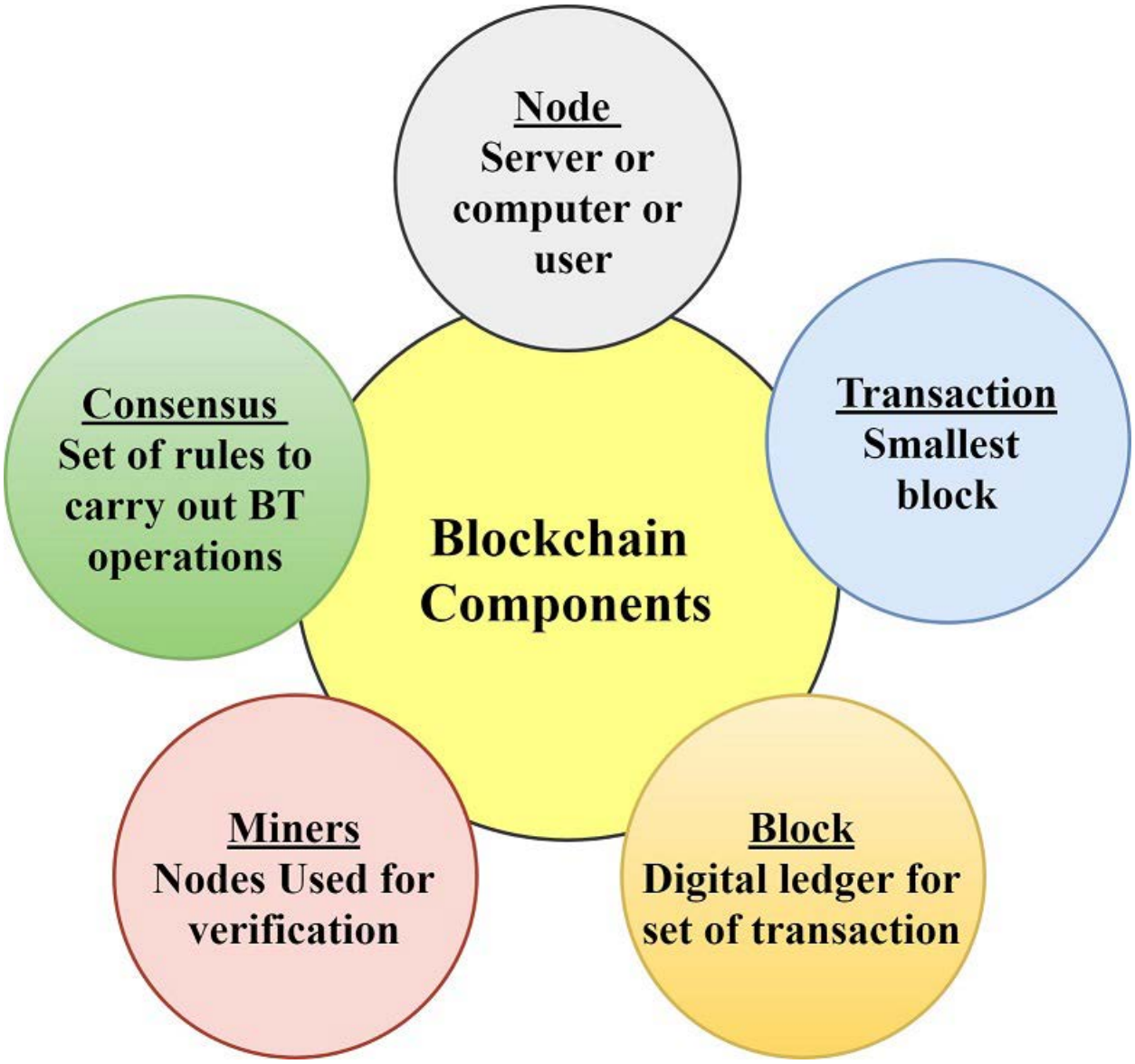

FIGURE 1. Major components of blockchain.

Unified Averaged Changed Intensity (UACI), Correlation Coefficients as well as entropy. Then the proposed work is compared with existing literature methods to ensure the safety and efficiency of the proposed algorithm.

This paper is arranged as follows. Related works are deliberated in Section 2. Section 3 illustrates system models with the propounded chaotic encryption framework in blockchain for IoT medical architecture. Section 4 details the implementation mechanism and experimental results with comparative analysis. All ideas discussed earlier as then summarized in Section 5.

II. RELATED WORKS

The decentralised based block chain technology employs several standard encryption techniques such as MD(5X) and SHA known to have some concerns about transferring medical data securely due to fixed key generation and the key dependency. To improve the security within the block, an efficacious hybrid chaotic encryption was proposed using 3D logistics based Sbox and 3D Lorenz code.

Prince Waqas Khan *et al.* [9] have propounded a scheme to encrypt image data by storing cryptographic pixels of an image on the blockchain. To evaluate the scheme against various attacks, three parameters, namely UACR, UACI, and Information Entropy, were taken. Encrypted results proved that this method could significantly secure the data from the leakage of information. The main upside of this work was that it could dispense IoT Security risks as this method could safely offload the data from different gadgets. Major limitation of this scheme are limited transaction speed and computing resources. In some cases, Web services can resolve this issue. However, this issue still needs to be addressed.

An innovative approach of chaotic image encryption venture is introduced. It was built on fingerprint. During resistance of CPA, enormous distribution of secret keys in a plaintext-related scheme could be overcome. Additionally, this method provides high tracking capabilities and authenticity by image distribution based on the blockchain. It prepares a high-rise security level. It is pertinent to a real-time network. The significant impediment of this method is that it devours more ability to keep a real-time ledger [10].

Mahalakshmi and Kuppusamy [11] have come up with a new encryption scheme to provide high security during image transmissions via cloud platforms. To enhance encryption algorithms, the proposed scheme utilizes the cipher blockchain. This scheme eliminates predicament key issues by crafting complex keys with a mathematical model. Hence, the encryption quality is significantly upgraded. To increase the execution time and storage space reduction, binary conversion is utilized. Information blocks are processed at the same time, which reduces time and computational intricacy. Processing speed can be increased by increasing basic matrix speed and utilizing logical operation between input images. Results demonstrate that this strategy works efficiently against various attacks and provides better results for RGB image encryption. The major limitation lies in the computational expense for critical trade among the consigner and proctor.

Nien *et al.* [12] have described a cipher block chaining technique for color images purely based on the rotation operation and random permutation. This is a hybrid technique where the scrambling activity is based on RGB planes in determined angles. Ciphered images can obscure dispersion qualities of RGB level matrices and guarantee to seal on crypt-analytic attacks. This can be accomplished in a spatial area itself without combining it so intricately by joining the transfer realm. This hybrid technique can be approached with a secret key. In addition, it is trouble-free.

Sultana *et al.* [13] have provided a framework that gives a short outline about how to decentralize a trust less model that can handle security issues of medical images in healthcare systems. This has been finished by the fussing blockchain with zero trust standards. A decentralized web application is utilized for the simulation. It can effectively store and share images among users. This method ensures role-based access that can improve the security of an image. The major disadvantage of this method is the network speed. Since every exchange expects distributed confirmation, it gets tedious particularly in a public blockchain with numerous hubs. Albeit Proof of Work guarantees all decentralization, it has an appeal for hub execution. In addition, it squanders energy.

Xiaoming *et al.* [14] have proposed a shared design that relies on the blockchain to provide a hypothetical premise to non-designing practice. The principle preferred position of this plan is it can ensure the proficiency of the framework and improve the application administration capacity of distant detecting pictures. A critical impediment of this framework is that assignments are intricate. Related information is recognizable. It cannot be messed with. In addition, the response time is moderate and the design is complex.

Indumathi *et al.* [15] have developed a layered architecture utilizing intermediate-based Internet of Medical Things (IoMT) especially for unlimited healthcare assistance. This architecture explores difficulties of cloud computing as well as IoMT. This framework supports fundamental capacities which are very basic to Patient-Centric Health Care. The principle preferred position of this system is it can deal with the most extreme illnesses progressively. However, this technique does not stand to ensure immutability.

Faragallah *et al.* [16] have introduced a color image cryptological version that utilizes RC6 for various operation vogues. A recreation model has been proposed to survey the presence of cryptological versions with various activity vogues utilizing different encryption calibers measurements. The reproduction exhibits that the usage of ''cipher block chaining'', ''cipher feedback'', ''output feedback'' is efficacious in hiding all information. Additionally, their results uncovered that using the ECB mode was not fitting as it could not effectively conceal the data in the analysed shading pictures without many subtleties. In addition, their outcomes guarantee the prevalence of output feedback activity mode from the commotion in-susceptibility viewpoint. Achieved results guarantee applicability and efficiency regarding security and encryption quality. This technique needs a spontaneous creation to ensure resistance to the commotion.

A novel picture encryption strategy based on the introduction of two new chaotic maps with large Lyapunov exponents and a new permutation scheme. The novel permutation strategy has a minimal computing cost due to its straightforward approach and achieves peak transformation in fewer stages than existing permutation algorithms. Additionally, our permutation technique has a satisfying speed of 18.6 ms, which is slightly faster than Arnold Cat map [40]. The challenge of encrypting pictures and movies broadcast via public channels utilising chaos-based cryptosystems and combined cryptocompression systems. These systems are developed and deployed with a high degree of security in mind for real-time applications [41].

With the advancement of mobile communication networks including 6G in the future, the security and privacy of digital pictures in network applications are critical. Facing these needs, an efficient and secure private blockchain system appropriate for secure IoT medical networks has been developed. The system is based on the dynamic behaviour of chaotic encryption. The author [39] proposed a chaotic dynamical map. It has been used to add one more security level to the proposed encryption scheme. The hybrid method scheme was evaluated with different statistical tests. When results were compared with those of already existing benchmarks, it was found that the hybrid algorithm had better security performance than existing image enciphering schemes.

Based on the above review, it can be consuded that the hybrid chaotic encryption is a dynamic process consisting of many unique inbuilt features such as high sensitivity and

high randomness behavior. The blockchain technology uses these features to do unshakable secure transmission as it is infeasible to find the time series generated by the high-rise dynamic hybrid chaotic system.

III. CES-BLOCKS—CHAOTIC ENCRYPTION SCHEMES FOR BLOCK CHAIN

The biggest challenge in the traditional generation of high random keys, encryption process, authentication, confidentiality, and integrity has been a highly complex issue concerning the level of security when sharing medical images. It takes a too long time to design and calculate with proportionally raise the time of execution. Figure 2 demonstrates the working architecture of the Proposed Chaotic Encryption Scheme (CES) Blockchain model. It starts with the input medical images which are uploaded by the people access system.

A. SYSTEM OVERVIEW

The image is encrypted using the proposed hybrid chaotic encryption algorithm before storing it in the disintermediated blockchain. Each node (h) possesses its key furnished by the authorized checker. Once validation is done by those nodes, it becomes part of the chain. Finally, images can be accessed and received with the transaction ID.

B. COMPONENTS OF CES-BLOCKCHAIN

In proposed CES blockchain framework, we used a chaotic-based encipher and decipher process. The goal of the proposed work is to achieve exorbitant security and performance. Specifically, this work has the following objectives:

1) To design a chaotic encryption scheme for medical images in blockchain to improve the entropy and to increase the randomness by raising the complexity.
2) To design a rapid and secure encryption/decryption-based architecture that supports permutation, substitution, diffusion properties to achieve a high level of performance, thereby enhancing the randomness behavior

The proposed architecture consists of three important layers: encryption, mechanism, and private blockchain methodology. The permutation process starts with the first column elements of RGB of the medical image been XOR mutually with attributes of initial column vector elements. The successive columns were made XOR with the nearby column like the first column with the second column. All the columns were done similarly. To obtain vectors, the procedure steps are given as:

1) Iterations are based on the generation of the logistic map using initial values to obtain the chaotic sequence. Iterations need to be set as 1 to improve the security.
2) Compute the in of image X and obtain the RGB matrix r[i], g[i], b[i].
3) Perform the modulo 2 of r[i], g[i], b[i].
4) Perform pixel row, column rotation of RGB based on the condition r modulus = g modulus = b modulus = 0 else 1.
5) If a condition is 0, then do the up circular shift; If the condition is 1, then do the up circular shift; If the condition is 1, then do the down circular shift. It results in a scrambled image.
6) Perform the pixel row, column rotation based on even or odd sequence according to the condition (i.j) = (0,0) or (1,1).
7) If the row (i) is 0, then multiply the r[i],g[i],b[i] with the random number K_c[i], else multiply r[i],g[i],b[i] with the 180 degree rotation of pixels of K_c[i].
8) If the column (j) is 0, then multiply the r[j],g[j],b[j] with the random number K_r[i], else multiply r[j],g[j],b[j] with the 180 degree rotation of pixels of K_c[j].
9) Thus the permutation of the scrambled pixel image of r[i][j],g[i][j],b[i][j] are obtained.

1) IMAGE ENCRYPTION MECHANISM

As indicated in [35], more complex elements can be introduced by dynamic progressive systems with a multi-scroll chaotic approach when compared to mono-scroll attractors. Generally, chaotic system imputes are inclined as follows:

$$x_1 = -ax_1 + bx_2x_3 \tag{1}$$
$$x_2 = -cx_2 + dx_1x_3 \tag{2}$$
$$x_3 = ex_3 - fx_1x_2 \tag{3}$$

the hyperbolic equations $p_1 sech(x_2+g)$ are added to the Eqns (1),(2),(3) which are presented as follows

$$x_1 = -ax_1 + bx_2x_3 \tag{4}$$
$$x_2 = -cx_2 + dx_1x_3 \tag{5}$$
$$x_3 = ex_3 - fx_1x_2 + p_1 sec_h(x_2 + g) \tag{6}$$

Chaotic attractor characteristics are acquired when a=2, b=6, c=6, d=3, e=3, f=1, $p_1 = 1$, g=2 with the original constraints of $[x_1(0), x_2(0), x_3(0)] = [0.1, 0.1, 0.6]$. For case 1, specification g=−3 with the original constraints of (0.1, − 0.1, − 0.6), it gives "twofold parchment attractor". For case 2, g=3 with original constraints of (0.1, − 0.1, − 0.6) it shows "four parchments". For case 3, g=3 with starting constraints of (0.1,0.1,0.6) it manifests a "solitary parchment". All cases (1-3) are delineated in Figure 3 accordingly. Hence it proves that the system holds multiscroll property. Equation 4 can be changed using derivative properties to procure Multi scroll 3D fractional integer-order chaotic systems as broached in [21]. Finally, the high rise dynamic chaotic system shows multi scroll properties as shown in Figure 6. The final mathematical expressions are given in Eqns (7),(8), (9).

$$\frac{d^q x_1}{dt^q} = -ax_1 + bx_2x_3 \tag{7}$$
$$\frac{d^q x_2}{dt^q} = -cx_2 + dx_1x_3 \tag{8}$$
$$\frac{d^q x_3}{dt^q} = ex_3 - fx_1x_2 + p_1 tan_h(x_2 + g) \tag{9}$$

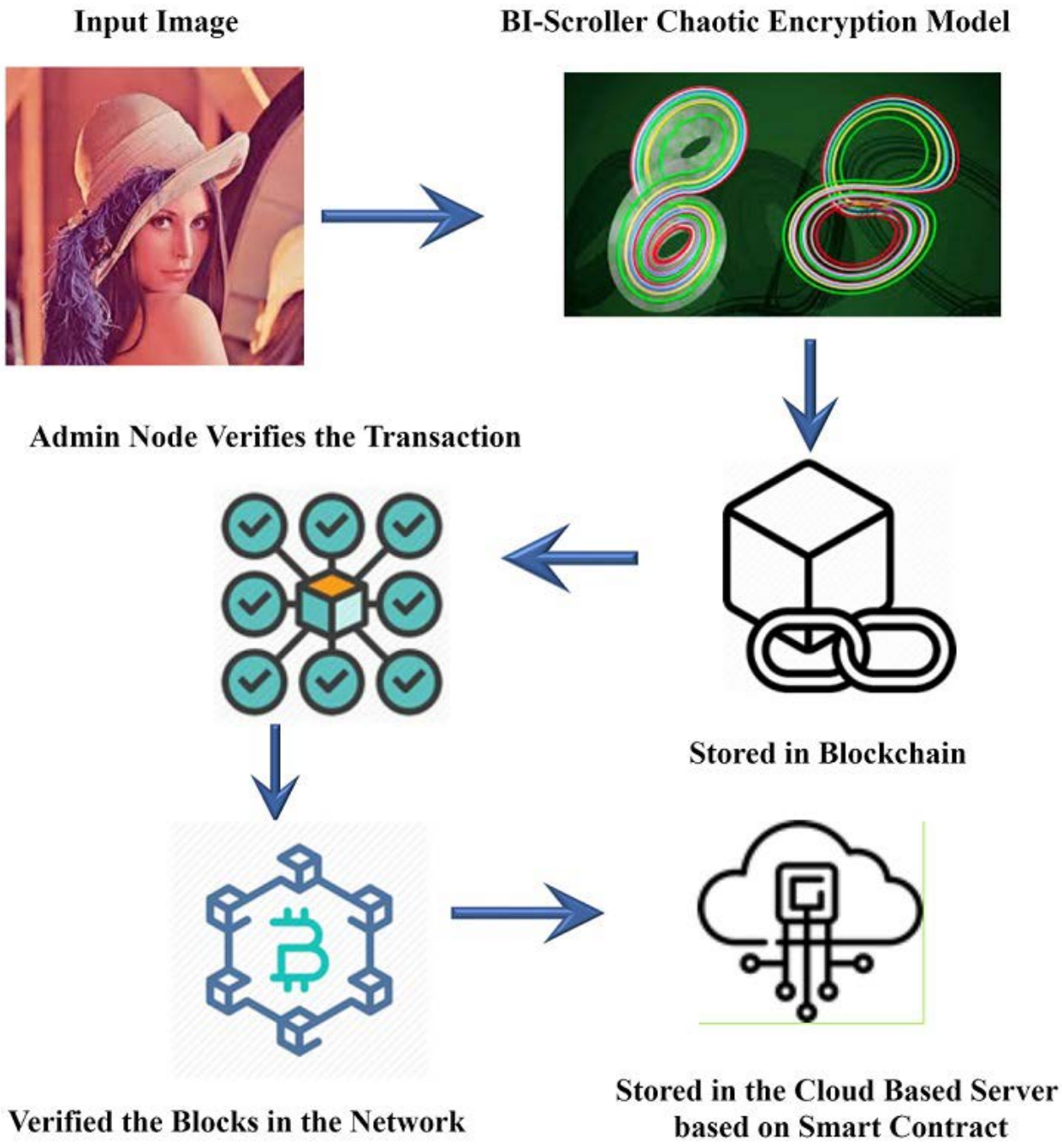

FIGURE 2. Proposed architecture for the chaotic encryption-based blockchain.

2) INITIAL CONDITIONS GENERATION

For the generation of initial conditions, the proposed system uses received signal strength (RSS) values of an IoT transceiver. The RSS can be calculated as mentioned in [22]. Chaotic behaviors obtained for different RSSI parameters are depicted in Figure 4.

These conditions make the proposed scroll algorithms exhibit more randomness which has proven to be strong and suitable for high-level encryption of image data. The complete working mechanism for the proposed encryption schemes is given below

Step 1: The first step is processing the basic medical_images / Plain image X utilize for transferral and conversion into grey scale images(bits) with M × N size

Step 2: Separate Image pixels as inter-bit pixels and intra-bit pixels.

Step 3: Generate 3D Multi scroll attractor system using RSS conditions.

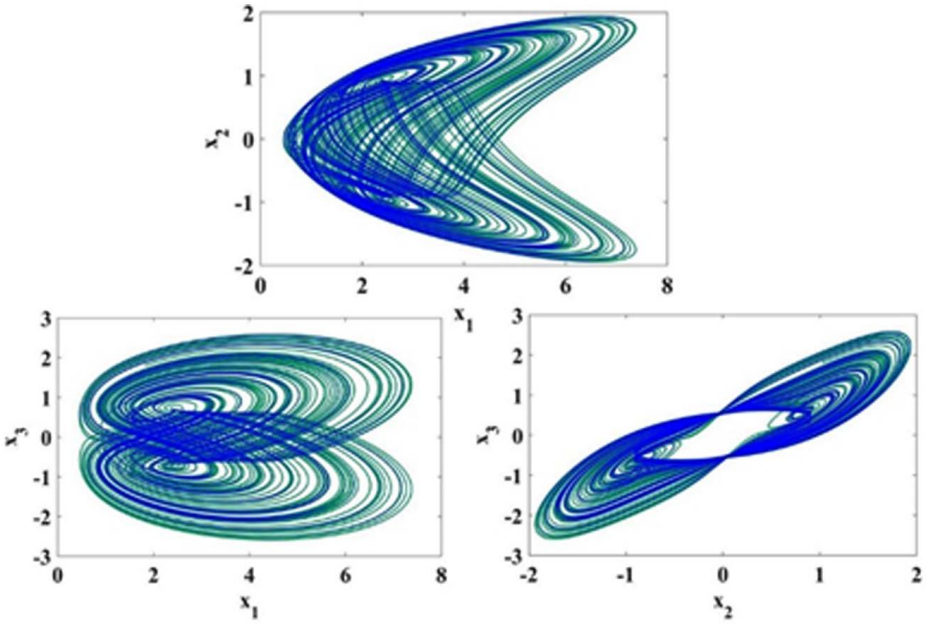

FIGURE 3. Phase representations -primary stage of CNS- cubic nonlinear system with $sechx_2 + g$.

Step 4: Generate 3D Multi scroll attractor system using initial conditions.

Step 5: Accomplish the first stage of encryption utilizing Inter-bit pixels with RSS based Multi scroll attractors using permutation and diffusion process to form intermediate image arrays which are given as I=(I1, I2. . . . . .In).

Step 6: Perform the second stage of encryption using the Intra-bit pixels with multi scroll attractors using permutation and diffusion process to form the intermediate key matrix which are given as F = f1, f2, f3. . . . . ..fl.

Step 7:: Permutated the matrix I and F again to obtain high randomness cipher keys which are expressed as

Cipher Key = IΘ F where data are scaled to 256

Step 8: Perform the permutation again among the Cipher Key and the Input Image to attain new encrypted image.

3) CES BLOCKS—BLOCKCHAIN METHODOLOGY

A private Blockchain system is proposed for an IoT System. A hub might be any server PC or client. Each hub can initiate a transaction, which is a very small structure block in the entire chain. All transactions join to construct a single block, which is appended to the chain on succeeding the confirmation from excavators or endorser hubs. Various adaptation rules are calibrated by the framework blockchain administrator to disintermediate tasks [24]–[26].

In this framework, the administrator can delineate the endorser and non-endorser peers. IoT gadgets are battery controlled. They require a bigger ability to run mining calculations. Inner IoT hubs go about as validator hubs. A hub or peer assumes a significant part in preparing exchange. It supports the imitation of a blockchain [39]. addresses the hawk perspective on the square chain hub joined in the IoT environment. The hub in the blockchain coordinates various squares, data set arrangements alongside shrewd agreement.

4) TRANSACTION LAYER

Figure 6 shows a simple transaction layer used for the proposed system. In our system, we designed a new structure to direct the encoded picture exchange between clients and servers. After acquiring accreditation from the excavator, a moral transaction is created. The contribution of the transaction in the data of turbulent encoded picture highlights that the yield is a determined IP address which is considered to be appropriate for downloading the images [27]–[29]. The proposed transaction structure consists of three layers: retrieval section, transaction section, and time stamps. Most importantly, the retrieval layer consists of User Number, Type of Images, Site of downloading, and Image label. The User Number cites a separate ID number of each user which is then used for uploading the encrypted images. The authentic original image URL is mentioned for better searching and downloading under the query result [30]–[32]. Finally, the image label is a narrative of the device type. It uses Chaotic hashes to trace the unique hash of the image.

The Input Fixed Address is characterized in the transaction data area. Therefore, the peak record esteems the record of an emergency clinic that transfers pictures in the information source's part. The Fixed Output Address is a fixed location of 32 bytes, which is accessible for clinical recovery administration to download the yield's part. The disorderly dynamic Hash Signature has a stretch of 16 bytes. It is utilized by the digger to check the legitimacy and trustworthiness of transferred pictures [20]. In the time data area, the Time Stamp fragment is utilized to demonstrate the aging season of

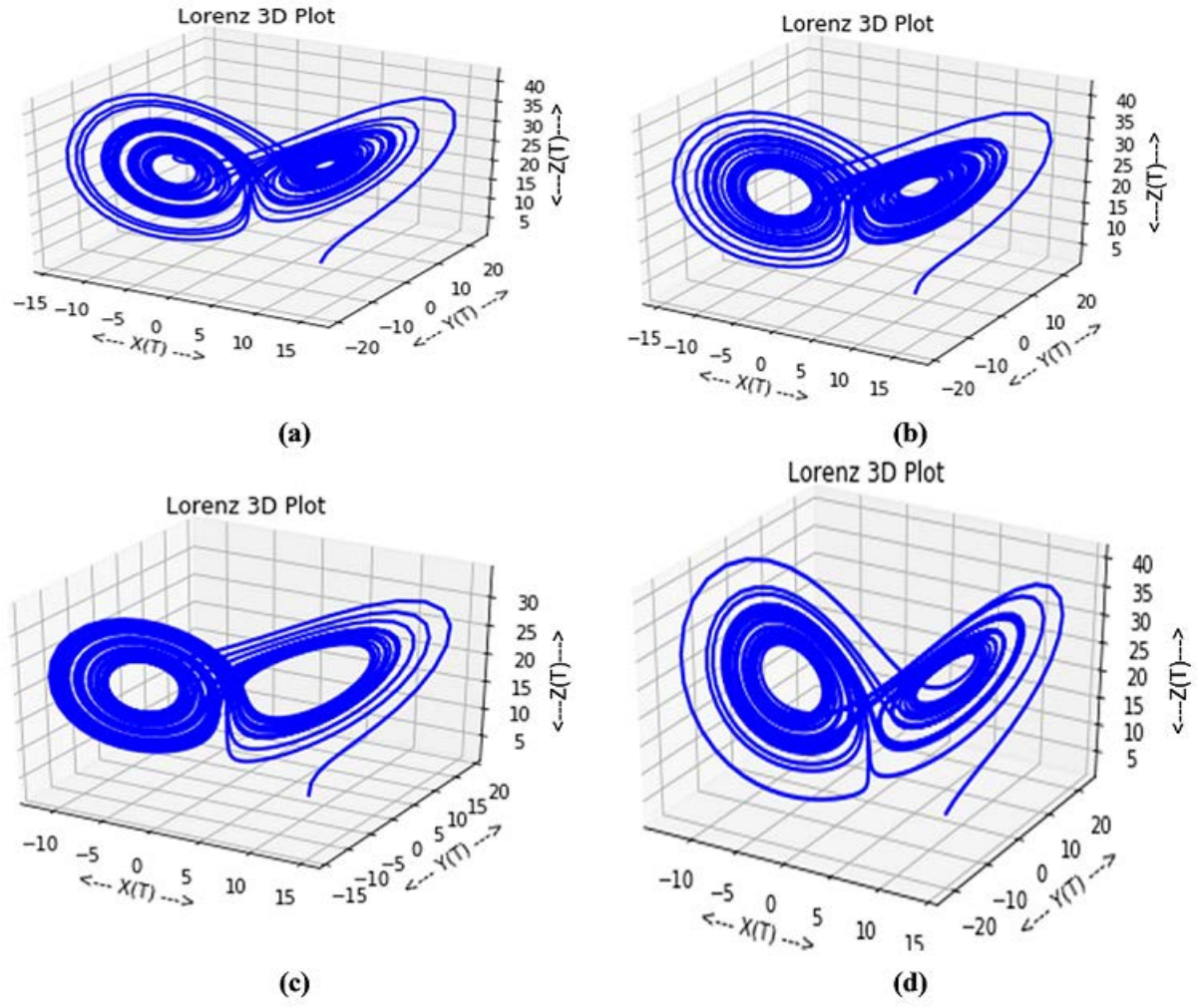

FIGURE 4. Chaotic behaviors for the proposed systems with the different RSSI values of α a) RSS = = 60. b) RSS=−75. c) RSS = −80. d) RSS=−85.

TABLE 1. Illustrates the number of bytes occupied by each frame in the transaction layer.

Sl. No.	Type of Frames	No of bytes Occupied
1	User ID Number	02
2	Image Identifier	02
3	Web for downloading	02
4	Image type	16
5	Hash Identity	16
6	Encrypted Image	256
7	Input /Output Address	32

the exchange, extraordinarily distinguishing the hour existing apart from everything else.

5) SMART CONTRACT

The smart contract is known as an electronic duplicate of the predetermined set of rules in the executable configuration. In the proposed system, the application invokes the smart contract before starting the transaction. These contracts contain all input parameters which determine the new state and responses depending on the successful validation of the transaction [34]. Figure 6 illustrates the system design used for the smart contract in the proposed system.

6) MINING

Since we have implemented a private blockchain, mining is not mandatory. Moreover, all processes are carried out in the built-in server or clouds.

IV. EXPERIMENTATION SETUP

We have developed a private blockchain which runs on IoT networks. We used our private servers /clouds for implementing the image encryption algorithms using Django Framework. The blockchain server runs on a PC workstation with a 2TB hard disk, 16GB RAM @3.00 GHz operating frequency. The blockchain servers were developed with Python 3.6.8 along with the integration of Angular JS

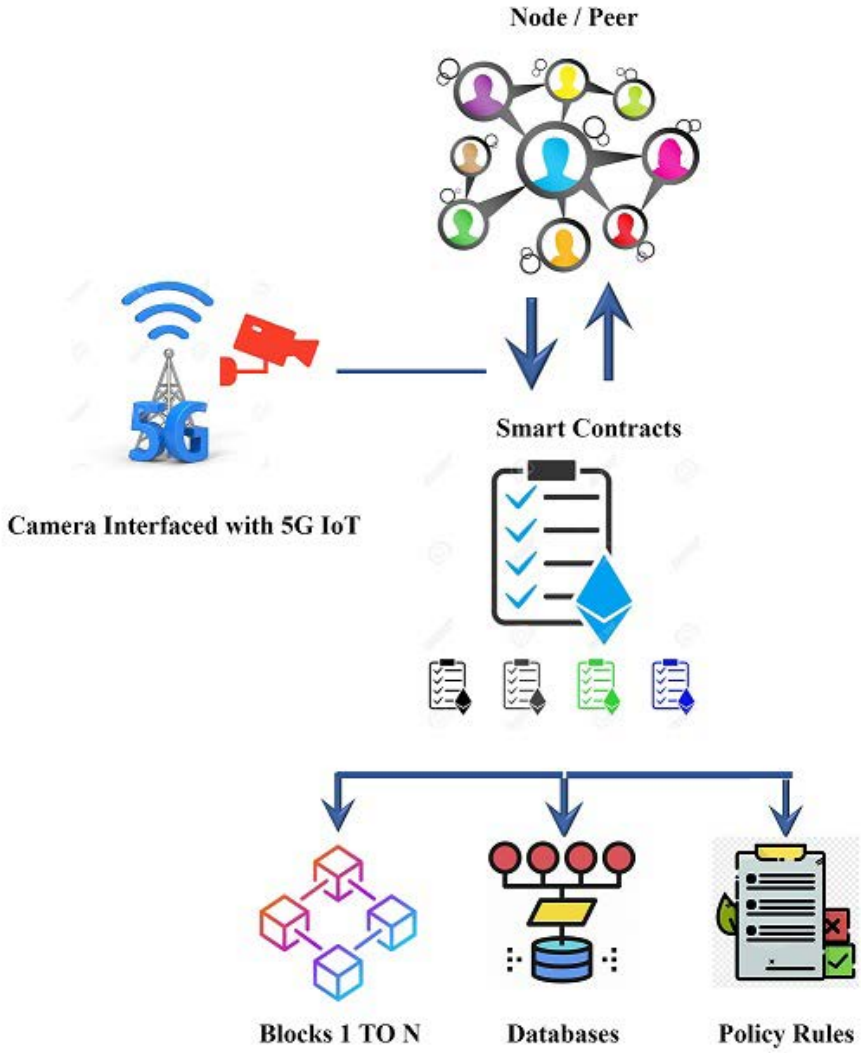

FIGURE 5. Block chain mode incorporated in the IoT network for image encryption.

A. PERFORMANCE EVALUATION

This section deals with proposed hybrid systems for encrypting various sets of medical images to analyze the security. We have used the 256 × 256 general LENA_Images, baboon_images, and vegetable_images. Figure 7 and Figure 8 depict input Images & encrypted images for analyzing the sensitivity of the encrypted images The Figure 8 (a), (b), (c) infers that the chaotic ciphered images are precisely unidentifiable.

B. SECRET KEY ANALYSIS

In the proposed approach, the secret key ought to be affectability delicate change for opposing ruthless power assaults. NPCR and UACI were determined for key sensitivity analysis to gauge the presentation of encryption calculation about code keys utilizing numerical articulations given beneath. The NPCR and UACI for distinctive scrambled pictures were determined. Results are shown in Figures 9-11.

NPCR and UACI values were conventionally appertained to explore the performance of repelling against differential attacks. It was appertained to probe that how modifying one bit of a pixel in the input influenced the respective output, supposing that p1 and p2 were two initial authentic images with a one-bit difference and that f1 and f2 were their corresponding ciphered images. Thus, the NPCR and UACI were computed as follows:

$$NPCR = \frac{\sum_{i,j} E(i,j)}{L} * 100 \tag{10}$$

$$UACI = \frac{1}{L} \sum_{i,j} \frac{|f_1(i,j) \neq f_2(i,j)|}{256} * 100 \tag{11}$$

where

$$\begin{aligned} E(i,j) &= 1, \quad f_1(i,j) \neq f_2(i.j) \\ &= 0, \quad f_1(i,j) = f_2(i,j) \end{aligned} \tag{12}$$

where L was the multiplication of width and height of respective images.

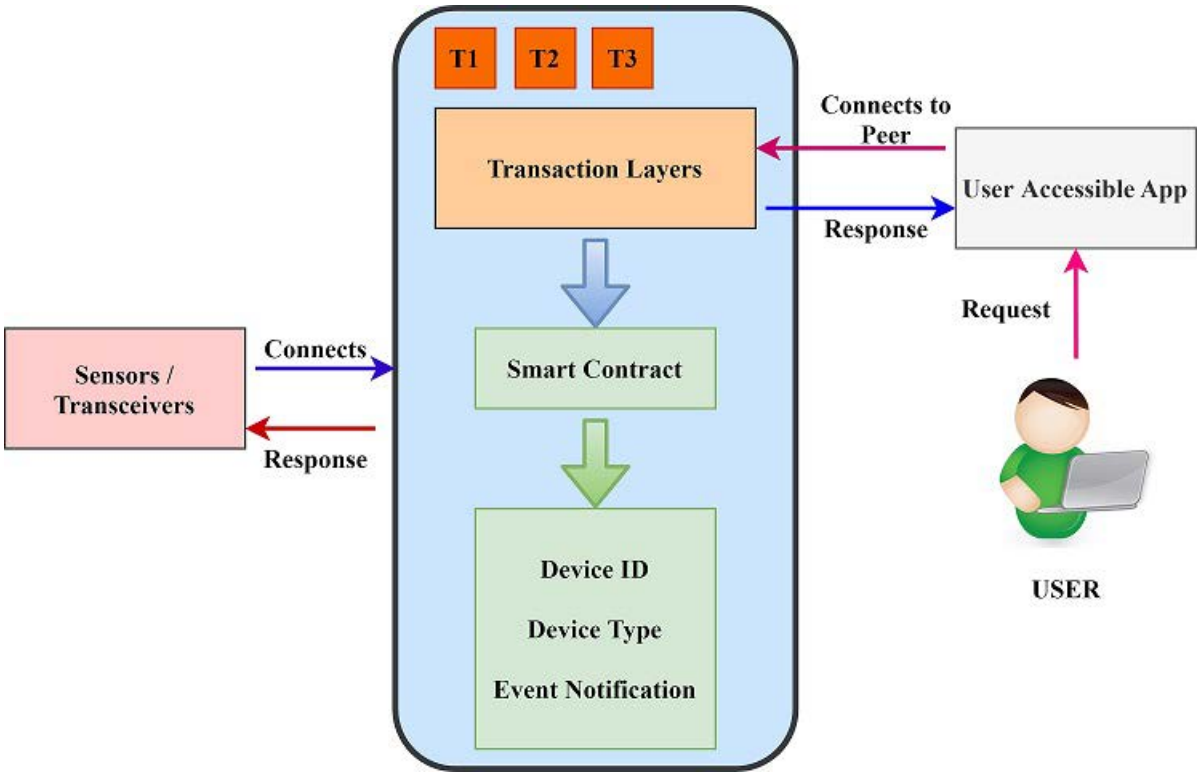

FIGURE 6. System design for smart contracts used in the proposed private blockchain.

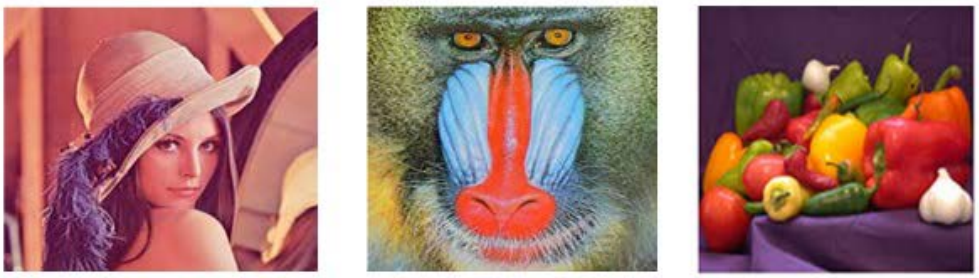

FIGURE 7. Input images for process (a) Lena. (b) Baboon. (c) Vegetable.

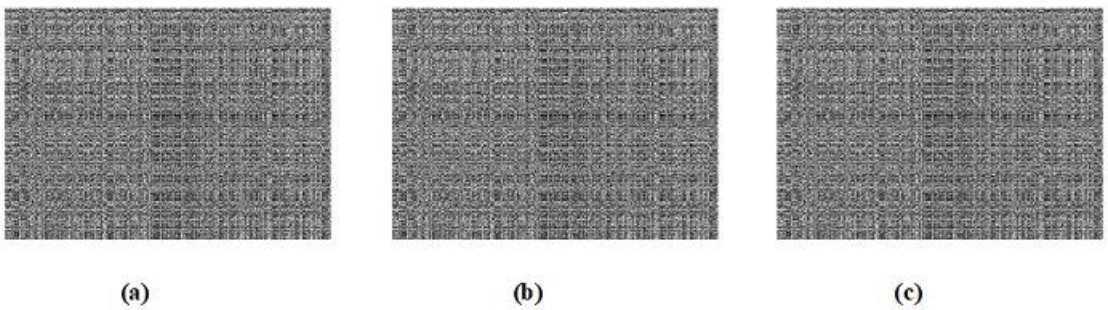

FIGURE 8. Chaotic ciphered_Images a) Lena cipered_images. b) Baboon_ciphered images. c) Vegetable_ciphered image.

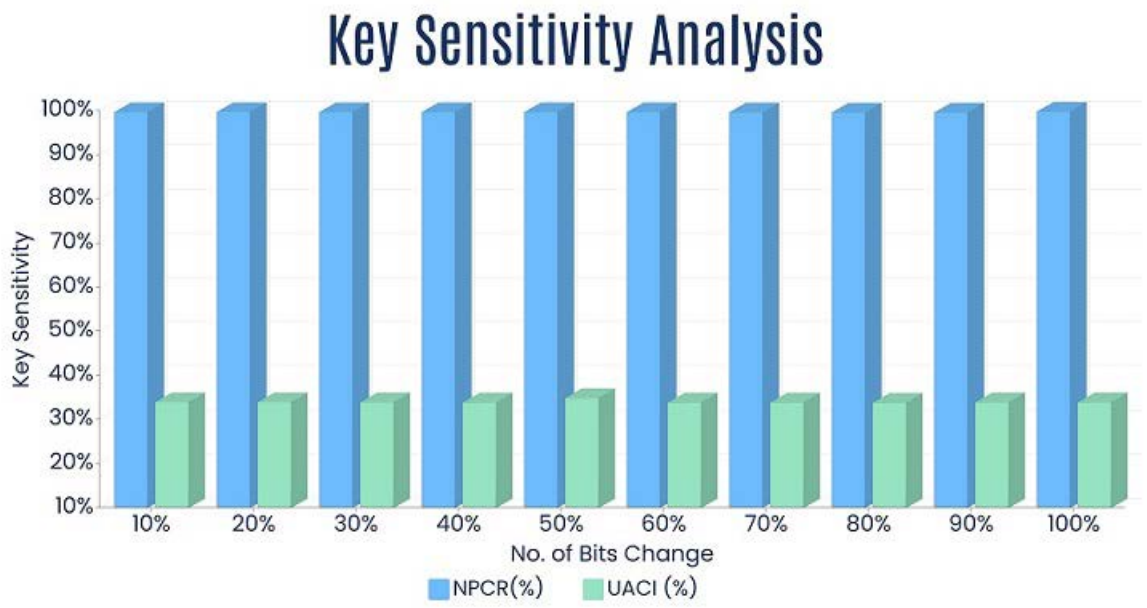

FIGURE 9. NPCR and UACI values for LENA images.

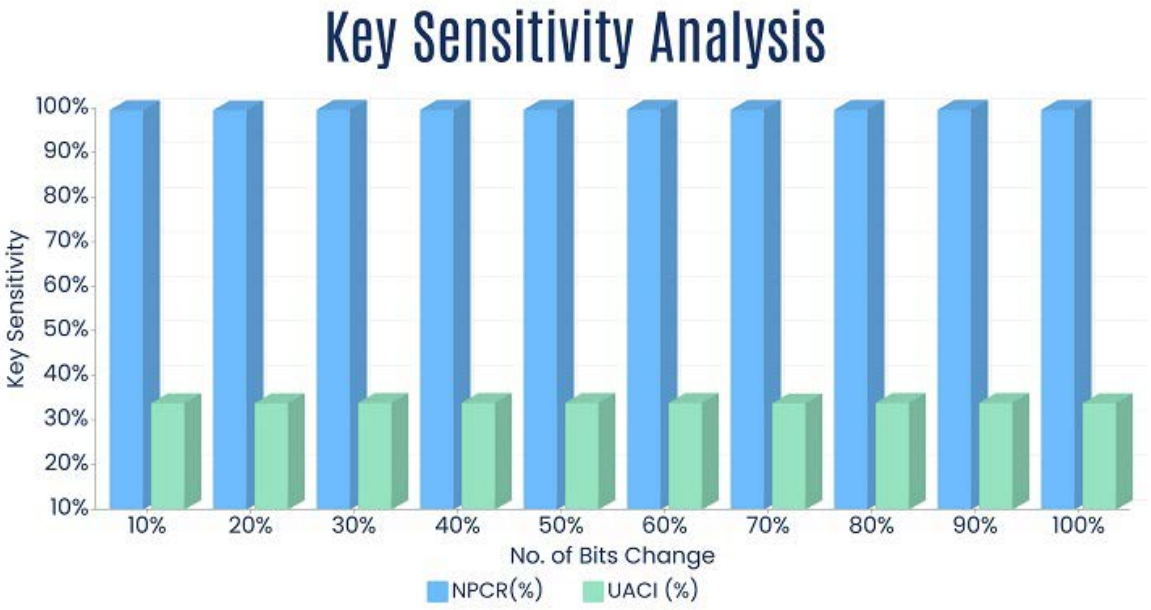

FIGURE 10. NPCR and UACI for baboon_images.

Figures 9 to 11 depict NPCR and UACI for distinct medical image datasets that have been calculated and analysed using equations (10) to (12). The changing interval of NPCR should be between 0 and 1. The encryption security will be very high by hitting the vicinity value of 1. Meanwhile, the UACI interval is the same as the NPCR interval of between 0 and 1. Higher scruples of NPCR and UACI certify the high security of encryption benefits from the propounded algorithm.

It is weigh-up with existing algorithms with the same inputs as medical images are shown in Table 2. The following results were found: NPCR = 99.65% and UACI = 33.90% for the encrypted Lena Images,

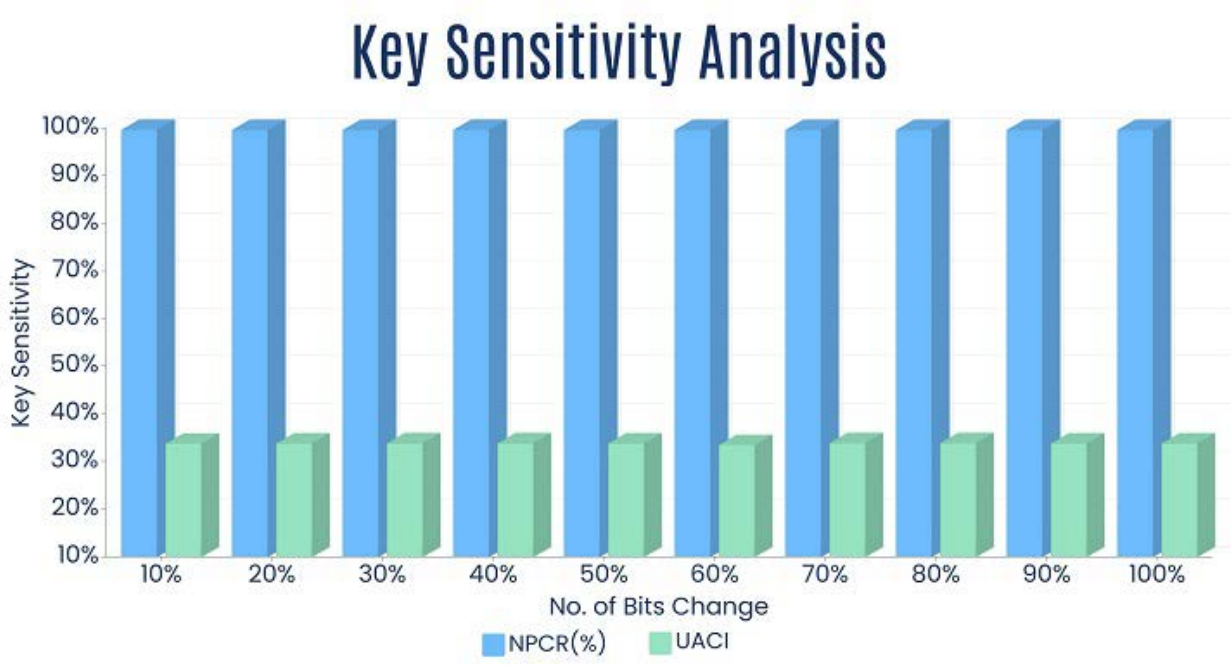

FIGURE 11. NPCR and UACI for vegetable_images.

TABLE 2. Comparative analysis - different encryption schemes.

Types of Image	Sensitivity Parameters	Mixed Chaotic Map	Hyper Chaotic Map	Chaotic Maps and Affine Transformation	Secret Key Algorithm	CES Blocks
LENA	NPCR	99.60	99.56	99.61	99.55	99.65
LENA	UACI	33.56	33.67	33.45	33.51	33.90
BABOON	NPCR	99.45	99.40	99.35	99.46	99.68
BABOON	UACI	33.26	33.45	33.30	33.70	33.90
VEGETABLE	NPCR	99.45	99.40	99.40	99.50	99.65
VEGETABLE	UACI	33.70	33.70	33.40	33.60	33.85

TABLE 3. Comparative analysis of variances of chaotic ciphered images.

Types of Image	Encrypted Image	Secret Key Algorithm	Substitution - Permutation Algorithm	Probabilistic Image Encryption	Mixed Chaotic Map
LENA	175.678	201.89	234.52	255.9	290.801
BABOON	193.78	215.9	229.78	278.23	300.42
VEGETABLE	221.867	245.9	278.34	265.89	289

NPCR=99.65%, UACI = 33.90% for encrypted baboon Images, NPCR=99.60%, UACI = 33.45% for encrypted vegetable images.

The correlated the scruples of NPCR and UACI values of the existing algorithms mixed chaotic map [26], hyperchaotic map [27], chaotic maps and affine transformation [29], and secret key algorithm [23] with those of the propounded encryption standard, can be culminated that CES blocks are more than that of the auxiliary algorithms mentioned in table 2. These simulations demonstrated that the proposed algorithm had a high strength of defending attacks in the network as shown in Figure 12.

C. CIPHERED CHAOTIC STATISTICAL PERFORMANCE ANALYSIS

The measurable exhibition of the chaotical encryption calculation is broken down by histogram examination. The histogram pictures uncover ordinary dispersion of pixels throughout the timeframe. If more unvaried peaks of pixels are present, it infers that very high is provided. Figure 14 explicitly shows the histogram circulation of scrambled pictures.

Figures 13 illustrates unvaried appropriation of scrambled pictures which equips that affectability is very high for tried pictures. Additionally, to discover histogram dissemination, variance is determined with the accompanying

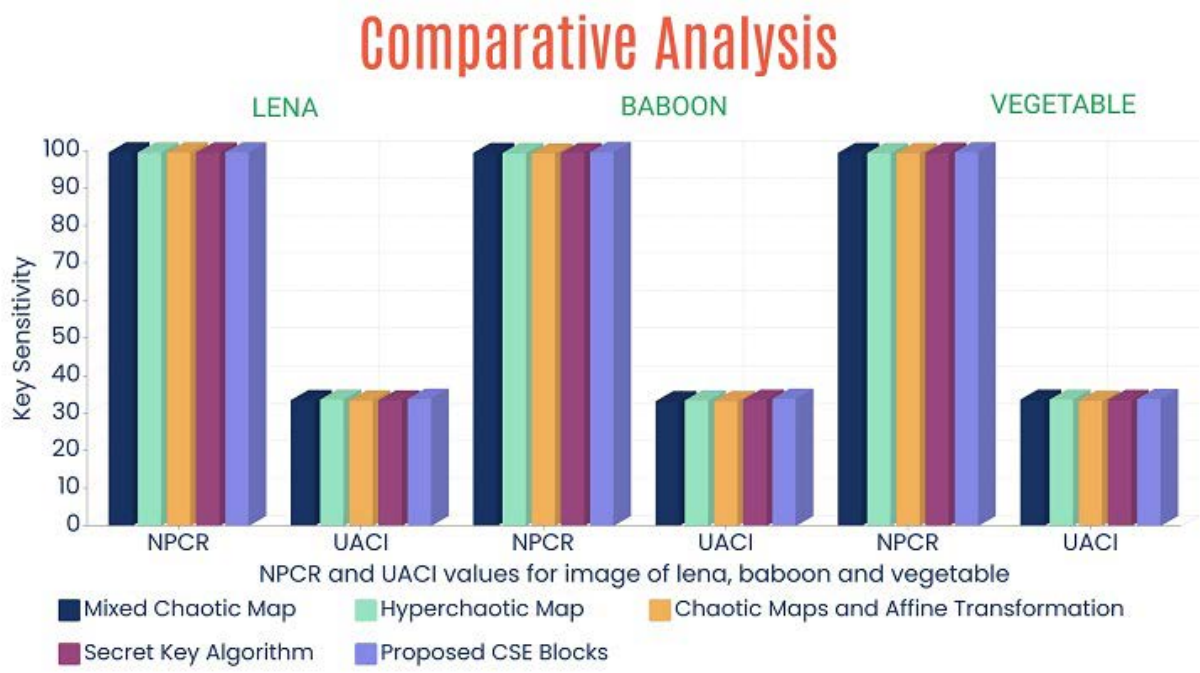

FIGURE 12. Comparative analysis - different encryption schemes.

TABLE 4. Plain and encrypted images correlation coefficient analysis.

-	Plain Images			Encrypted Images		
Image Details	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
LENA	348.9	356.9	392.89	0.00066	0.00022	0.00789
BABOON	367.9	335	400.23	0.00056	0.00004	0.00987
VEGETABLE	378.9	300.89	399.789	0.00079	0.00004	0.04789

TABLE 5. Analysis for computational time complexity.

Sl. No.	Image Dataset	Proposed Method	Discrete dynamical chaotic map [40]	Joint Crypto compression and encryption [41]
1	Lena Image	0.512	2.14	1.38
2	Baboon Images	0.520	2.17	1.45
3	Vegetable Images	0.519	2.17	NA

numerical articulation.

$$Var = \frac{1}{N} \sum \sum (\frac{1}{2}(S - H)^2) \tag{13}$$

where N is the No. of gray levels of images & assign N is 256. S is the vector for adjacent pixels of images and H is the vector for Neighbourhood pixels of images.

The level of uniformity is addressed by differences. Underneath these differences are elevated levels of uniformity. The fluctuation of distinctive scrambled pictures as shown in Figure 13 infers that it addresses the near examination of differences among the proposed calculations and existing s-enclose. The proposed system has preferable execution over current models. It employs the demonstration of the pixel intensity distribution in an image. Figure 13 depicts histogram analysis results of Lena, baboon, vegetable before and after the chaotic encryption. The histogram of the ciphered image is unvaried. It presents that equal distribution does not provide any kind of idea to do statistical attack by intruders to retrieve the original image.

In this CES block experimentation, variances of the histogram analysis of Lena, baboon, vegetable, and their ciphered images are computed using equation 13. The output determination as depicted in Table 3 infers that variances of these images of the propounded CES algorithm are 175.678, 193.78, and 221.867, which are much less than those of existing algorithms such as probabilistic image encryption [25], mixed chaotic map [26], secret key algorithm [23], and substitution-permutation [24]. Thus, our propounded CES algorithm for IoT networks has better execution in repelling statistical attacks.

D. APPC (ADJACENT PIXEL POINT CORRELATION) ANALYSIS

Typical pictures normally have immense correlation amidst pixels. Encoded pictures will possess decreased connections.

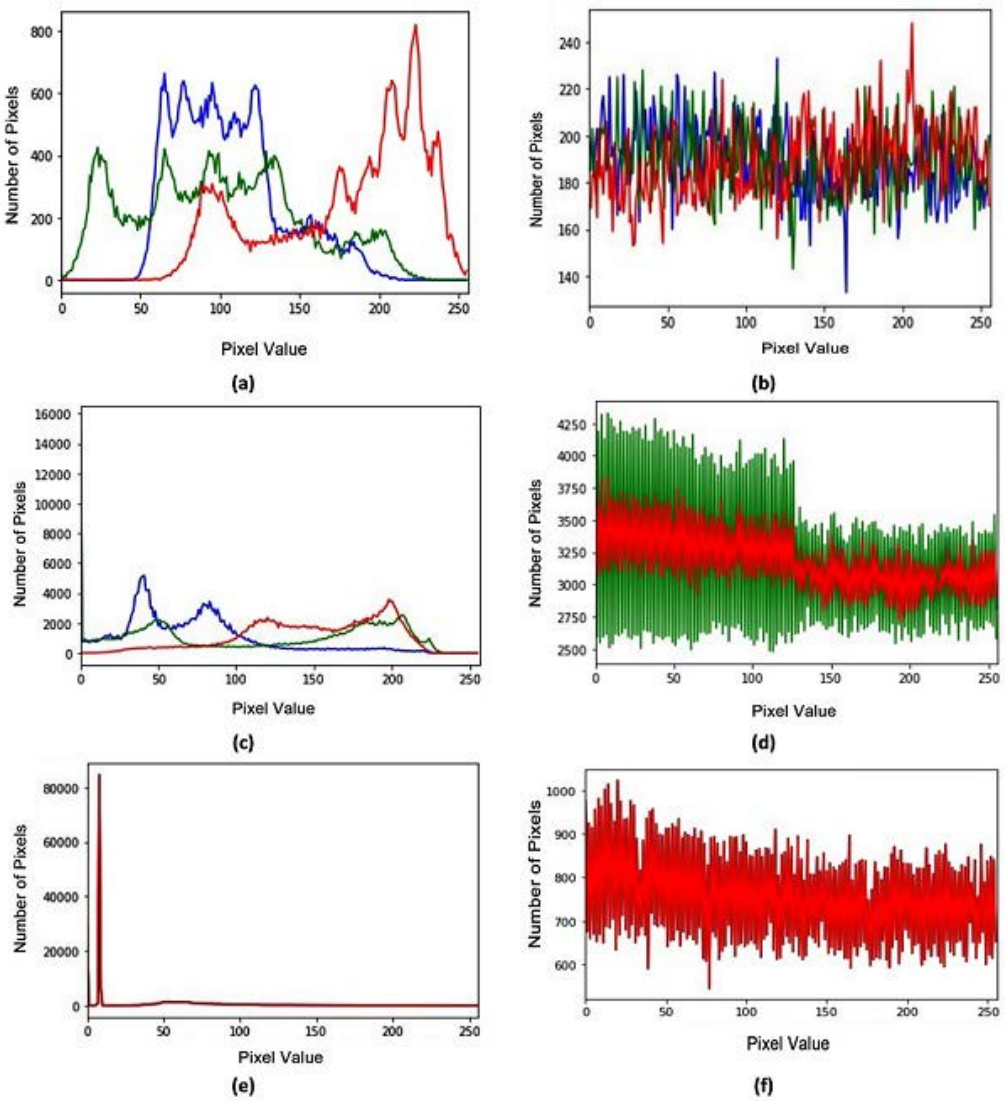

FIGURE 13. Distribution_Analysis of histogram of the scrambled images a) Lena_images. b) Chaotic ciphered_lena image. c) Normal baboon_images. d) Chaotic ciphered baboon_images. e) Normal vegetable_images. f) Chaotic ciphered vegetable_images.

TABLE 6. Disparate image datasets entropy values.

Types of Image	CES Blocks	Mixed Chaotic Map	Hyper Chaotic Map	Advanced Encryption Standard Algorithm	Chaotic Maps and Affine Transformation
LENA	7.999995	7.99967	7.99974	7.99966	7.9971
BABOON	7.999994	7.99945	7.99965	7.99965	7.99965
VEGETABLE	7.99992	7.99967	7.98965	7.99963	7.99961

In this experimentation, we allured correlation coefficient of divergent direction orders of adjacent pixels of the original image. We then correlated it with the correlation coefficient of divergent direction orders of adjacent pixels of the encrypted image. The correlation coefficient between devices was determined using mathematical expressions given by Equations. (14)(15)(16)(17):

$$R_{xy} = \frac{cov(a,b)}{\sqrt{E(x)E(y)}} \tag{14}$$

$$cov(a,b) = D\{[a - D(a)][b - D(b)]\} \tag{15}$$

$$e(a) = \frac{1}{n}\sum_{i=1}^{n} a_i \tag{16}$$

$$L(x) = \frac{1}{n}\sum_{i=1}^{n}[a_i - a(x)]^2 \tag{17}$$

where "e(a) is the expectation of the plain/ciphertext images datasets, L(x) is the variance of the plain/ciphertext images datasets."

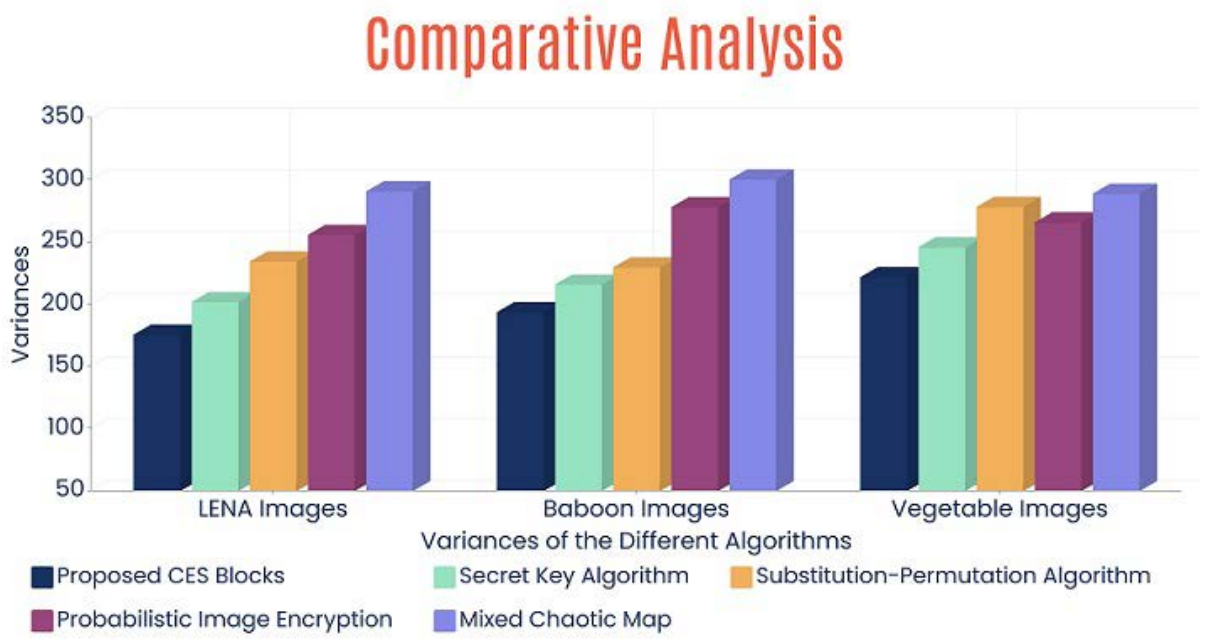

FIGURE 14. Comparative analysis of variances of chaotic ciphered images.

Table 4 depicts results of correlation coefficient analysis among plain images and ciphered images. Table 4 clearly shows that the correlation coefficient is high in the input image, whereas the correlation coefficient in ciphered images is almost zero. This manifests a close correlation among pixels in diagonal, horizontal, and vertical directions of the original image. However, in the ciphered images, this correlation becomes very weak.

E. COMPUTATIONAL TIME COMPLEXITY ANALYSIS

Any encryption plans ought to have a quicker reaction to encode the information. We possessed just the encryption energy for the picture and 256 × 256 info pictures for this investigation and the determined the time for distinctive picture sets given in Table 5.

F. INFORMATION ENTROPY ANALYSIS

Information entropy is the extent of promiscuity that reflects the most imperative degree of weakness of clinical information. A high entropy indicates a high inconsistency of pictures.

For an 8-bit gray image, the stretch of the bits is taken as 256. For a quality ciphered image, the entropy value should be 8 [36]. Divergent entropy values are acquired for disparate image sets listed in Table 5.

Table 6 presents various entropies of different picture stations. They were discovered to be near 8. Additionally, we have contrasted entropies from other subsisting calculations in Figure 15. Figure 15 revealed the examination of entropy esteems among various calculations in which the preferred hybrid chaotic encryption had a better contour of execution over other subsist calculations.

Extensive experimentations were accomplished to verify the security of the proposed parameterized algorithm. This was done using bimodal chaotic scroller methodology to overcome IoT attacks such as brute force attacks. At the same time, constraints, for example, limited computing resources, and lack of memory can forestall them from going about as hubs in a blockchain. Hence, the proposed system requires improvisation in terms of solving attacking problems.

V. DISCUSSION

In this paper, highly secured chaotic encryption is propounded to ensure that sensitive information collected cannot be accessed by attackers. The privacy preserving ability of the chaotic encryption scheme was calibrated in terms of performance, secret key analysis, histogram analysis, adjacent pixel points correlation, and information entropy analysis. The high Lyapunov exponent employed in the 3D hyperchaotic Lorenz attractor is highly sensitive to the initial condition. It promotes a non-corruption proof and no malicious change in the data of IoT network. Its performance was analyzed with 256 × 256 general benchmark images of lena, baboon, and vegetable. The secret key was analyzed using NPCR and UACI values of distinctive scrambled pictures to identify the strength of the proposed chaotic encryption. NPCR values of lena, baboon, and vegetable images of the propounded algorithm is 0.07%,0.27%,0.21% higher than those obtained with existing algorithms of mixed chaotic

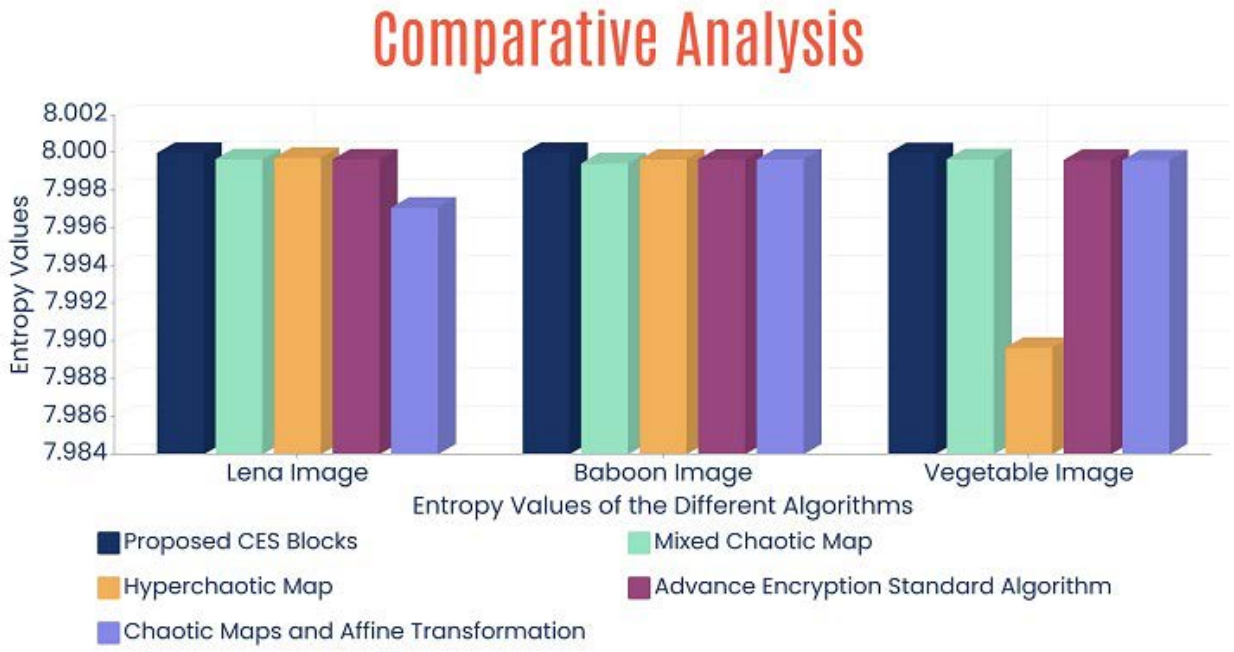

FIGURE 15. Comparative analysis - using entropy values among various algorithms.

map [26], hyperchaotic map [27], chaotic maps and affine transformation [29], and secret key algorithm [23].

UACI values of lena, baboon, and vegetable image of the propounded algorithm were 1.04%,1.39%,0.73% higher than those obtained with existing algorithms of mixed chaotic map [26], hyperchaotic map [27], chaotic maps and affine transformation [29], and secret key algorithm [23].Although results of the proposed algorithm showed significantly higher scruples of NPCR and UACI than existing algorithms, it ensured better privacy preservation of sensitive patient data

Histogram analysis of the proposed chaotic encryption produced low variances compared with conventional algorithms such as probabilistic image encryption [25], mixed chaotic map [26], secret key algorithm [23], and substitution-permutation [24]. Therefore, attackers are restricted to retrieve the sensitive image, revealing that the proposed chaotic encryption provides high level of security to the IoT environment during the transfer of sensitive data. The propounded chaotic encryption manifests a tight tension correlation among pixels in horizontal, vertical and diagonal directions of the adjacent pixel correlation analysis. The final analysis on information entropy exhibited randomness of the ciphered image. Values obtained by the propounded algorithm was closer to 8 than probabilistic image encryption [25], mixed chaotic map [26], secret key algorithm [23], and substitution-permutation [24] are shown in Table 6. Henceforth, the proposed chaotic image encryption generates a secured encrypted image with superiority randomness key and yields better security for the data collected.

Extensive experimentations were accomplished to verify the security of the proposed parameterized algorithm. This was done using bimodal chaotic scroller methodology to overcome IoMT attacks such as brute force attacks. Therefore, the blockchain that adopts this chaotic encryption can improve the security of the patient sensitive data collected from IoT and ensure protection to the privacy of users. However, constraints such as limited computing resources and lack of memory can forestall them from going about as hubs in a blockchain. Hence, the proposed system requires improvisation in terms of solving attacking problems.

VI. CONCLUSION

In this digital era, the fusion of divergent technology within one platform can resolve many technical, network, security-oriented issues. The Internet of Medical environment has distinct applications in our daily lives that need very high bandwidth and interconnection. IoT plays a unique role as a technical enabler in terms of speed and capacity for its new service delivery models. The motivation of blending the blockchain to the IoT medical environment tackles the storage through its secured disintermediate distributed ledger. This paper introduces a chaotic image encryption scheme based on private blockchain architecture for IoT medical environments. The proposed chaotic application in blockchain mechanism can defend IoT attacks such as brute force attacks.

We used standard image data for our extensive experimentation. The strength of the chaotic encryption was evaluated

based on calculations of parameters such as NPCR, UACI, Correlation Coefficients, and entropy. We obtained better results than outperforming the extant blockchain mechanisms is outrageous for the deterrence of data leakage and guaranteed data security in IoT. As a future enhancement, the CES-based blockchain architecture for 5G enabled network can be enhanced in terms of testing the security for images on the IoT network to make it more efficient and adaptable.

REFERENCES

[1] Y.-J. Choi, H.-J. Kang, and I.-G. Lee, "Scalable and secure Internet of Things connectivity," *Electronics*, vol. 8, no. 7, p. 752, Jul. 2019.
[2] K. Wang, Y. Wang, Y. Sun, S. Guo, and J. Wu, "Green industrial Internet of Things architecture: An energy-efficient perspective," *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 48–54, Dec. 2016.
[3] Z. Bi, L. Da Xu, and C. Wang, "Internet of Things for enterprise systems of modern manufacturing," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1537–1546, May 2014.
[4] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.
[5] G. Ateniese, B. Magri, D. Venturi, and E. Andrade, "Redactable blockchain—Or—Rewriting history in bitcoin and friends," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Apr. 2017, pp. 111–126.
[6] N. Teslya and I. Ryabchikov, "Blockchain-based platform architecture for industrial IoT," in *Proc. 21st Conf. Open Innov. Assoc. (FRUCT)*, Nov. 2017, pp. 321–329.
[7] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019.
[8] S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, and N. Guizani, "Securing smart cities through blockchain technology: Architecture, requirements, and challenges," *IEEE Netw.*, vol. 34, no. 1, pp. 8–14, Jan. 2020.
[9] P. W. Khan and Y. Byun, "A blockchain-based secure image encryption scheme for the industrial Internet of Things," *Entropy*, vol. 22, no. 2, p. 175, Feb. 2020.
[10] R. Li, "Fingerprint-related chaotic image encryption scheme based on blockchain framework," *Multimedia Tools Appl.*, vol. 80, no. 20, pp. 30583–30603, Aug. 2021.
[11] J. Mahalakshmi and K. Kuppusamy, "An efficient image encryption method based on improved cipher block chaining in cloud computing as a security service," *Austral. J. Basic Appl. Sci.*, vol. 10, no. 2, pp. 297–306, 2016.
[12] H. H. Nien, W. T. Huang, C. M. Hung, S. C. Chen, S. Y. Wu, C. K. Huang, and Y. H. Hsu, "Hybrid image encryption using multi-chaos-system," in *Proc. 7th Int. Conf. Inf., Commun. Signal Process. (ICICS)*, Dec. 2009, pp. 1–5.
[13] M. Sultana, A. Hossain, F. Laila, K. A. Taher, and M. N. Islam, "Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology," *BMC Med. Informat. Decis. Making*, vol. 20, no. 1, pp. 1–10, Dec. 2020.
[14] Z. Xiaoming, L. Caiping, T. Dejin, S. Yuchen, H. Zhen, and Z. Jisheng, "Design of remote sensing image sharing service system based on block chain technology," in *Proc. IEEE Int. Conf. Signal, Inf. Data Process. (ICSIDP)*, Dec. 2019, pp. 1–4.
[15] J. Indumathi, A. Shankar, M. R. Ghalib, J. Gitanjali, Q. Hua, Z. Wen, and X. Qi, "Block chain based Internet of Medical Things for uninterrupted, ubiquitous, user-friendly, unflappable, unblemished, unlimited health care services (BC IoMT u6 HCS)," *IEEE Access*, vol. 8, pp. 216856–216872, 2020.
[16] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-Sayed, M. A. Alzain, J. F. Al-Amri, and F. E. A. El-Samie, "Efficiently encrypting color images with few details based on RC6 and different operation modes for cybersecurity applications," *IEEE Access*, vol. 8, pp. 103200–103218, 2020.
[17] S. Zhai, Y. Yang, J. Li, C. Qiu, and J. Zhao, "Research on the application of cryptography on the blockchain," *J. Phys., Conf. Ser.*, vol. 1168, Feb. 2019, Art. no. 032077.
[18] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Decentralized Bus. Rev., White Paper 21260, Oct. 2008, pp. 1–9.
[19] H. N. Abdullah and H. A. Abdullah, "Image encryption using hybrid chaotic map," in *Proc. Int. Conf. Current Res. Comput. Sci. Inf. Technol. (ICCIT)*, Apr. 2017, pp. 121–125.
[20] X. Li, Q. Xue, and M. C. Chuah, "CASHEIRS: Cloud assisted scalable hierarchical encrypted based image retrieval system," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, May 2017, pp. 1–9.
[21] G. Gugapriya, P. Duraisamy, A. Karthikeyan, and B. Lakshmi, "Fractional-order chaotic system with hyperbolic function," *Adv. Mech. Eng.*, vol. 11, no. 8, Aug. 2019, Art. no. 168781401987258.
[22] S. Sridevi and R. Anandan, "RUDRA—A novel re-concurrent unified classifier for the detection of different attacks in wireless sensor networks," *Intell. Comput. Eng., Select Proc. RICE*, vol. 1125, p. 251, Apr. 2020.
[23] S. Zhou, Z. Wei, B. Wang, X. Zheng, C. Zhou, and Q. Zhang, "Encryption method based on a new secret key algorithm for color images," *AEU Int. J. Electron. Commun.*, vol. 70, no. 1, pp. 1–7, Jan. 2016.
[24] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016.
[25] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, and S. W. Baik, "Secure surveillance framework for IoT systems using probabilistic image encryption," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3679–3689, Aug. 2018.
[26] X. Wang, X. Zhu, and Y. Zhang, "An image encryption algorithm based on Josephus traversing and mixed chaotic map," *IEEE Access*, vol. 6, pp. 23733–23746, 2018.
[27] H. Natiq, N. M. G. Al-Saidi, M. R. M. Said, and A. Kilicman, "A new hyperchaotic map and its application for image encryption," *Eur. Phys. J. Plus*, vol. 133, no. 1, pp. 1–14, Jan. 2018.
[28] A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm," *J. Supercomput.*, vol. 75, no. 10, pp. 6663–6682, Oct. 2019.
[29] J. Ahmad and S. O. Hwang, "A secure image encryption scheme based on chaotic maps and affine transformation," *Multimedia Tools Appl.*, vol. 75, no. 21, pp. 13951–13976, Nov. 2016.
[30] R. H. Jhaveri, N. M. Patel, Y. Zhong, and A. K. Sangaiah, "Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile ad-hoc networks in industrial IoT," *IEEE Access*, vol. 6, pp. 20085–20103, 2018.
[31] M. H. Abidi, H. Alkhalefah, K. Moiduddin, M. Alazab, M. K. Mohammed, W. Ameen, and T. R. Gadekallu, "Optimal 5G network slicing using machine learning and deep learning concepts," *Comput. Standards Interface*, vol. 76, Jun. 2021, Art. no. 103518.
[32] C. Borrego, M. Amadeo, A. Molinaro, and R. H. Jhaveri, "Privacy-preserving forwarding using homomorphic encryption for information-centric wireless ad hoc networks," *IEEE Commun. Lett.*, vol. 23, no. 10, pp. 1708–1711, Oct. 2019.
[33] R. Kumar, R. Tripathi, N. Marchang, G. Srivastava, T. R. Gadekallu, and N. N. Xiong, "A secured distributed detection system based on IPFS and blockchain for industrial image and video data security," *J. Parallel Distrib. Comput.*, vol. 152, pp. 128–143, Jun. 2021.
[34] A. Khamparia, D. Gupta, V. H. C. de Albuquerque, A. K. Sangaiah, and R. H. Jhaveri, "Internet of Health Things-driven deep learning system for detection and classification of cervical cells using transfer learning," *J. Supercomput.*, vol. 76, no. 11, pp. 8590–8608, Nov. 2020.
[35] R. Ch, G. Srivastava, T. R. Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "Security and privacy of UAV data using blockchain technology," *J. Inf. Secur. Appl.*, vol. 55, Dec. 2020, Art. no. 102670.
[36] R. M. Haris and S. Al-Maadeed, "Integrating blockchain technology in 5G enabled IoT: A review," in *Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT)*, Feb. 2020, pp. 367–371.
[37] D. C. Nguyen, K. D. Nguyen, and P. N. Pathirana, "A mobile cloud based IoMT framework for automated health assessment and management," in *Proc. 41st Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Jul. 2019, pp. 6517–6520.
[38] N. Tsafack, S. Sankar, B. Abd-El-Atty, J. Kengne, K. C. Jithin, A. Belazi, I. Mehmood, A. K. Bashir, O.-Y. Song, and A. A. A. El-Latif, "A new chaotic map with dynamic analysis and encryption application in Internet of Health Things," *IEEE Access*, vol. 8, pp. 137731–137744, 2020.
[39] E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O.-Y. Song, A. K. Bashir, and A. A. A. El-Latif, "DITrust chain: Towards blockchain-based trust models for sustainable healthcare IoT systems," *IEEE Access*, vol. 8, pp. 111223–111238, 2020.

[40] M. Khan, F. Masood, A. Alghafis, M. Amin, and S. I. Batool Naqvi, "A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and Brownian motion," *PLoS ONE*, vol. 14, no. 12, Dec. 2019, Art. no. e0225031.
[41] M. Farajallah, "Chaos-based crypto and joint crypto-compression systems for images and videos," Eng. Sci. Phys., Universite De Nantes, Nantes, France, Tech. Rep. 01179610, 2015.
[42] M. Mollaeefar, A. Sharif, and M. Nazari, "A novel encryption scheme for colored image based on high level chaotic maps," *Multimedia Tools Appl.*, vol. 76, no. 1, pp. 607–629, Jan. 2017.

R. DURGA received the B.Tech. degree in information technology from the Kamaraj College of Engineering and Technology, Anna University, in 2008, and the M.Tech. degree in information technology from the SNS College of Technology, Anna University, in 2013. She has been a Research Scholar with the Department of Computer Science and Engineering, SRM Institute of Science and Technology, since 2019. Before joining the SRM Institute of Science and Technology, she served as a Teaching Faculty Member in engineering colleges for ten years. Her research interests include blockchain technology and machine learning. She is a Fellow Member of IE(I) and an active member of professional body of ISTE.

E. POOVAMMAL (Member, IEEE) received the B.E. degree in electrical and electronics engineering from Madurai Kamaraj University, in 1990, the M.E. degree in computer science and engineering from Madras University, and the Ph.D. degree in computer science and engineering from the SRM Institute of Science and Technology. She joined the SRM Institute of Science and Technology, in 1996, where she is currently a Professor with the Department of Computer Science and Engineering. Before joining the SRM Institute of Science and Technology, she worked in industry for five years. She is certified as an Adjunct Faculty by the Institute of software Research, Carnegie Mellon University, Pittsburgh, USA, and served for four years. She has published more than 40 referred journals and presented in various international and national conferences. Her research interests include big data analytics and machine learning. She is a Fellow Member of IE(I) and an active member of professional bodies, such as IET, ACM, ISCA, and ISTE.

KADIYALA RAMANA received the Bachelor of Technology degree in information technology from Jawaharlal Nehru Technological University Hyderabad (JNTUH), Hyderabad, India, the M.Tech. degree from the Sathyabama Institute of Science and Technology, Chennai, India, and the Ph.D. degree from the SRM Institute of Science and Technology, Chennai. He is currently working as an Associate Professor with the Department of Artificial Intelligence and Data Science, Annamacharya Institute of Technology and Sciences (AITS), Rajampet, India. He has 14 years of experience in teaching and research. He has authored more than 20 international publications. His research interests include wireless sensor networks, software-defined networking with machine learning, and data analytics. He is an Editorial Board Member and a reviewer of several journals of international repute.

RUTVIJ H. JHAVERI (Senior Member, IEEE) received the Bachelor of Technology degree in computer engineering from the Birla Vishvakarma Mahavidyalaya, Vallabh Vidyanagar, India, the M.Tech. (R) degree from SVNIT, Surat, India, and the Ph.D. degree from the Charotar University of Science and Technology, Changa, India. He pursued his postdoctoral research at Nanyang Technological University, Singapore. He is currently working as an Assistant Professor (Senior) with the Department of Computer Science and Engineering, Pandit Deendayal Energy University (PDEU), Gandhinagar, India. He has 18 years of experience in teaching and research. He has authored more than 70 international publications. His research interests include network security, software-defined networking with machine learning, and data analytics. He is an Editorial Board Member and a reviewer of several journals of international repute.

SAURABH SINGH received the Ph.D. degree from Jeonbuk National University, Jeonju-si, South Korea, carrying out his research in the field of ubiquitous security. He was a Postdoctoral Researcher with Kunsan National University, South Korea. He recently joined Dongguk University, Seoul, South Korea, as an Assistant Professor. He has published many SCI/SCIE journals and conference papers. His research interests include blockchain technology, cloud computing and security, the IoT, deep learning, and cryptography. He received the Best Paper Award from KIPS and CUTE Conference, in 2016.

BYUNGUN YOON (Senior Member, IEEE) is currently a Professor with the Department of Industrial and Systems Engineering, Dongguk University. His theme of study has involved blockchain technology, patent analysis, new technology development methodology, and visualization algorithms. His current research interests include enhancing technology road mapping, research and development quality, and product designing with data mining techniques.