





## Research Article

## Improved Blockchain Technique based on Modified SLIM Algorithm for Cyber Security

Sarah Mohammed Shareef<sup>1,2,\*</sup> , Rehab Flaih Hassan<sup>2</sup> <sup>1</sup> *University of Technology- Iraq, Department of Production Engineering and Metallurgy, Department of Computer Science, 10066 Baghdad, Iraq*<sup>2</sup> *University of Technology- Iraq, Department of Computer Science, 10066 Baghdad, Iraq.*

## ARTICLE INFO

## Article history

Received 17 Dec 2024

Accepted 25 Jan 2025

Published 20 Feb 2025

## Keywords

Real Estate

SLIM Lightweight

Blockchain

S-Box

Chialvo Map



## ABSTRACT

The number of cybersecurity incidents is increasing, and the cost of a security breach has a catastrophic financial effect. The existing real estate information systems require more robust and resilient cybersecurity solutions to secure hardware, software, and databases. Cybersecurity often relies on user behavior. Phishing attacks and social engineering can bypass blockchain security, highlighting the need for robust user education and awareness. Many blockchain networks face challenges in handling a high volume of transactions. Solutions that work well on a small scale may not perform efficiently as the network grows, leading to delays and increased costs. A secure system is a significant area in cybersecurity that protects digital transactions from unauthorized access. This paper proposes a new real estate transaction encryption scheme using the modified SLIM cryptography algorithm in the context of blockchain based on a 2Dimension Chialvo map with high nonlinearity generation of the substitution box (S-Box) to make it robust against many linear attacks, which is a novel approach to enhancing transaction speed and security. Modifying lightweight SLIM cryptography is highly resistant to linear and differential cryptanalysis attacks, providing adequate protection. The modified lightweight SLIM cryptography applies to wireless networks, IoT applications, and real estate systems. The performance analysis of the blockchain shows that it completes transactions in a short time of approximately 29.368877 in milliseconds and satisfies the Bit Independence Criterion (BIC) and Hamming Distance (HD) tests above 50%, the new hash will be regarded as good and trustworthy. The performance analysis of the proposed S-Box shows that it has high nonlinearity and satisfies the Strict Avalanche Criteria (SAC), BIC, balanced, and low linearity/differential probability. In addition, the strength and randomness of the random number generators are analyzed via a set of tests and guidelines provided by the National Institute of Standards and Technology (NIST) tests (approximately 97%) to ensure that the generated random data are sufficiently unpredictable and suitable for cryptographic applications.

## 1. INTRODUCTION

Cybersecurity is one aspect of data security, but it has received the most attention because of its fast-changing and increasingly sophisticated cyber threats [1,2]. Blockchain technology has received tremendous interest in recent years, both in industry and academia. This basic technology underlying peer-to-peer electronic currency transactions has been accepted. It is of interest in many industries, such as business, finance, real estate, health care, privacy, government, and entertainment [3,4]. Organizations employ blockchain technology to handle cybersecurity, distributed databases, healthcare, and digital transactions for their consumers [5,6]. Blockchain technology requires significant investment in infrastructure, people, and system enhancements. For smaller real estate companies, transitioning to blockchain can be too expensive. This may limit their ability to benefit from blockchain technology. Blockchain networks, specifically those that are public, such as Ethereum, have scalability issues. This could hinder the wide adoption of blockchain technology in real estate transactions, which must be processed swiftly and efficiently. Encryption is one of the most significant approaches for protecting digital data. It is divided into asymmetric and symmetric ciphers. Symmetric-key cryptosystems are divided into two types: stream ciphers and block ciphers. Shannon's theory of diffusion and confusion serves as the foundation for block ciphers, which are implemented using mathematical processes (substitution-permutation networks) [7][26]. The S-box accepts a block of  $n$  bits as input and converts it into a new nonlinear block of  $m$  bits. In Galois field theory [8,9], the function mapping should be one-to-one, represented as  $GF(2^n) \rightarrow GF(2^m)$ . A permutation is a linear transformation that

\*Corresponding author. Email: [sarah.m.ali@uotechnology.edu.iq](mailto:sarah.m.ali@uotechnology.edu.iq)

flips the input bits. The outcomes of the first round of the S-box are permuted before moving on to the next round. The merging of the two approaches generates a cipher that is both resilient and secret [10]. The block cipher SLIM is a lightweight cryptographic method created by Aboushousha et al. SLIM is designed for radio frequency identification (RFID) systems, with a 32-bit block size, an 80-bit private key size, and a suggested number of rounds of 32. The security of a lightweight cryptographic method is determined by its computational difficulty. If an attacker conducts a brute-force search for a K-bit secret key, 2K repetitions of encryption are needed [11][32].

### 1.1. The Main Cof this Study are as Follows

1. The modified lightweight SLIM cryptography method suggested in this study is a new and effective approach for enhancing blockchain technology.
2. Reduced the number of rounds of lightweight SLIM cryptography and increased the number of input bits from 32 to 64 bits to avoid security flaws and speed up blockchain transactions.
3. The combination of modified lightweight SLIM cryptography with the Chialvo map in a blockchain context is a novel approach for enhancing transaction speed and security by reducing the number of rounds, reducing the time it takes to execute transactions in the blockchain, and avoiding potential security vulnerabilities.
4. To improve the performance of the proposed system, a  $[16 \times 16]$  S-box was generated by using a Chialvo map, which provides excellent protection and complexity.
5. The performance of the blockchain, key generation, and proposed S-box are calculated via the following performance metrics: time consumption, BIC, hamming distance, NIST, balanced, strict avalanche criteria, bit independence criteria, differential and linear approximation probabilities, and nonlinearity. The results revealed high-security performance for the proposed system.

As a result of the enormous development that is happening in digital transactions, real estate transactions are exposed from time to time to fraud or theft of sensitive data, and at the same time, it takes more time to complete transactions. Therefore, a powerful and secure system was created via lightweight SLIM cryptography by a 2D Chialvo map in the context of the blockchain to increase the transaction speed and prevent an unauthorized person from accessing it or sending it through the Internet. To provide more information protection, a suggested large S-box was generated using the 2D Chialvo map.

The literature review compares the types of lightweight block cipher cryptography in section 2; the description of the standard lightweight SLIM cryptography is covered in section 3; and the Chialvo map is displayed in section 4. This is the system proposed in part 5. The outcome analysis is in part 6, and the last part presents the conclusion.

## 2. LITERATURE REVIEW

Hatem et al. [12] proposed a lightweight cryptosystem to securely encrypt medical images via a 5-dimensional chaotic map with a current block cipher. The recommended approach was applied to a 256x256 medical DICOM image containing 25 images. The effectiveness of the suggested system is evaluated by neighbouring pixel correlation analysis, NIST assessment, mean square error, information entropy, uniform average change intensity, entropy, etc., which yields a structural similarity index picture. Alahdal et al. [13] presented NLBCIT, a lightweight and efficient algorithm that provides comprehensive data security while considering the limitations of IoT devices. The NLBCIT method is simulated in FELICS. This technique uses a wide range of data types, including text and graphics. Entropy, histogram, and avalanche tests were used to evaluate the resilience of the strategy. Compared with the other algorithms, the NLBCIT algorithm consumes less energy and memory during the encryption and decryption cycles. Altaay et al. [14] proposed an image encryption method that achieves high security by combining a light encryption method with the chaotic Peter De Jong map. The fundamental purpose of encrypting image data is to protect it during transmission, storage, and retrieval. Two approaches were used to evaluate a traditional picture collection including an encrypted image and a generated key. The image's entropy was determined after encoding, and the results were incredibly efficient. In addition, the degree of deviation from the original image was estimated, and the image quality was evaluated on the basis of preset standards. Teha et al. [15] investigated the protection of the BORON lightweight block cipher versus differential cryptanalysis in a single-key scenario. The linear layer of the BORON successfully initiates several S-boxes in smaller cycles. Using a SAT/SMT strategy, we look for differentials with various differential features and identical input and output variations. To test the performance of the proposed system, different rounds were used. While the attacks do not currently guarantee the safety of the BORON's entire 25 rounds, they provide a comprehensive examination of the cipher's security against unequal cryptanalysis. Mhaibes et al. [16] recommended altering the TEA by implementing a newly proposed key generation function that uses dual linear feedback shift registers (LFSRs) in tandem to solve the security problem caused by the use of unique keys for each round function. This improved method aims to improve the safety performance of the original TEA. The encryption and decryption performance of the updated TEA was evaluated by applying key sensitivity, avalanche effect, and completeness tests, and the results were compared with those of previous works on regular TEA and MTEA. The encryption achievements of the proposed improved TEA are superior to those of the original TEA. Nurwarsito and Yapputra [17] emphasized that datamust

be secure in terms of confidentiality, integrity and availability. Therefore, the SIMON encryption algorithm was introduced into the MQTT communication protocol to ensure that the transmitted data are secure. The encryption mechanism is applied to the publisher node, which encrypts the data before transmitting it to the broker node. The decryption mechanism is implemented on the subscriber node, which performs both the subscription and decryption functions to obtain the plaintext. Two active attack techniques are used during the attack test: “Ciphertext Only Attack” and “Known Plaintext Attack”. Fan et al. [18] addressed the design flaw by introducing a modified variant of ANU-II that is significantly more resistant to differential cryptanalysis while incurring no additional hardware or software implementation costs. The proposed MILP approach is applied to the altered version of ANU-II, where the ideal differential characteristic (ANU-II reduced for 5 rounds) has a significantly lower probability than one. Karode et al. [19] developed a compact hardware design for computing the CLEFIA block cipher algorithm, which can perform both the necessary expansion for all key sizes and data-time execution. This research shows how the power of FPGA innovation, such as addressable shift registers and slam blocks, can be leveraged to create the many branches of the Feistel organization. The diffusion switching mechanism in CLEFIA protects the system from significant threats. The recommended updated technique requires extremely low energy and power and requires minimal time for encryption and decoding. The work differences are shown in Table I.

TABLE I: COMPARISON OF PREVIOUS RESEARCH BASED ON LIGHTWEIGHT BLOCK CIPHER ALGORITHM IN THE SECURITY LEVEL

Ref.	Methodology	Cipher Algorithm	Type of Structure	Block Size	Key Size	Rounds	challenge	solution
[12]	Present block cipher and a five-dimensional chaotic map	Present	SPN	64 bits	80-bit or 128-bit	31	Images are vulnerable to unauthorized users who unlawfully use them for nondiagnostic reasons	Five-dimensional chaotic maps and the lightweight present block cipher are offered as a new method for improved image encryption.
[13]	NLBCIT with IoT devices	NLBCIT	SPN and Feistel	64 bits	64 bits	5	Traditional cryptographic algorithms, which involve complex mathematical operations and numerous computational cycles, result in high memory usage and energy consumption	The lightweight and efficient algorithm called NLBCIT has been proposed to provide robust data protection
[14]	Lilliput with key generation	Lilliput	Feistel	64 bits	80 bits	30	Protect image's data while it is being sent, stored, and retrieved	Combining a lightweight encryption algorithm with the chaotic Peter De Jong map
[15]	Differential cryptanalysis on BORON in the single-key model	Boron	SPN	64 bits	80 or 128	25	The cipher is under attack.	BORON with single-key model.
[16]	Key generation using two LFSRs with TEA	TEA	Feistel	64 bits	128 bits	32	The security vulnerability of the original TEA	Simple and a new modified method of key generation using two LFSRs
[17]	MQTT with SIMON algorithm	SIMON	Feistel	128 bits	128 bits	Depend on block and key size)	IoT there is a higher risk of security because the device can be used as a Botnet and can harm many parties	Addition of Simon encryption algorithm to the MQTT communication protocol so the data that moved remains safe
[18]	Applying our MILP model to the modified variant of ANU-II	ANU-II	Feistel	64 bits	80 or 128	25	The designers' security evaluation of ANU-II against differential cryptanalysis is incorrect	Provide an improved variant of ANU-II, which has much better resistance to differential cryptanalysis

[19]	FPGA with CLEFIA	CLEFIA	GFN (Generalized Feistel Network)	512	128	128 128, 192 or 256 18, 22 or 26	Very high in energy and power and requires more time for encryption and decryption,	Energy consumption, voltage, and time have been greatly enhanced.
Proposed System	Modified lightweight SLIM cryptography with Blockchain	Modified Slim	Feistel	64 bits	32 bits	16	Security potential vulnerabilities	Using MSLIM cryptography with the Chialvo map in a blockchain context

### 3. LIGHTWEIGHT SLIM CRYPTOGRAPHY

SLIM is a lightweight block encryption algorithm that employs a Feistel design and a block that is 32 bits. To avoid extensive key searches, SLIM utilizes a large key length of 80 bits. SLIM uses four-by-four robust substitution boxes to assess the relationship between ciphertext and plaintext data. SLIM has shown strong resistance to the most successful linear and differential cryptanalysis techniques; it has a significant protective effect against various types of assaults [20][41]. The standard approach is appropriate for wireless networks, particularly wireless sensor networks and Internet of Things applications, where data streams usually fall within a specific byte range. Equations (1) and (2) explain the entire process during each round, in which the right portion of the entered data  $R_i$  with the subkey is modified via an XOR technique [21][43].

$$L_i = R_i - 1 \tag{1}$$

$$R_i = L_i - 1 + P(S(K_i + R_i - 1)) \tag{2}$$

### 4. CHIALVO MAP

The key generation of the proposed method is based on a specific chaotic map known as the Chialvo map. The model is a reduplicate map, with the following Equations (3,4) at each time step:

$$x_{n+1} = x_n^2 e^{(y_n - x_n)} + k \tag{3}$$

$$y_{n+1} = ay_n + bx_n + c \tag{4}$$

where  $y$  is the recovery variable and  $x$  is referred to as the activation or action possibility variable. The four parameters of the sample are as follows:  $a$ , recovery time constant ( $a < 1$ );  $b$ , recovery activation dependency ( $b < 1$ ); and  $c$ , offset constant.  $k$  is a time-independent additive perturbation or constant bias. The sample exhibits rich dynamics, responding to small stochastic fluctuations and exhibiting oscillatory to chaotic behaviour [22,23].

### 5. PROPOSED METHOD

The proposed system provides a method of updating the activity occurring on properties for a particular area by updating a period of time, for example, a day, a week, a month or a year, and incorporating the constraints before and after the update in the blockchain process. This ensures that there is no fraud or subsequent manipulation process when these restrictions are changed. The dataset is an adapted version of the California Housing Data used in Pace and Barry's 1997 research article. The collection consists of 16 variables and 20,641 rows that provide information about residences in specific California counties as well as summary statistics. Figure1. View the suggested method.

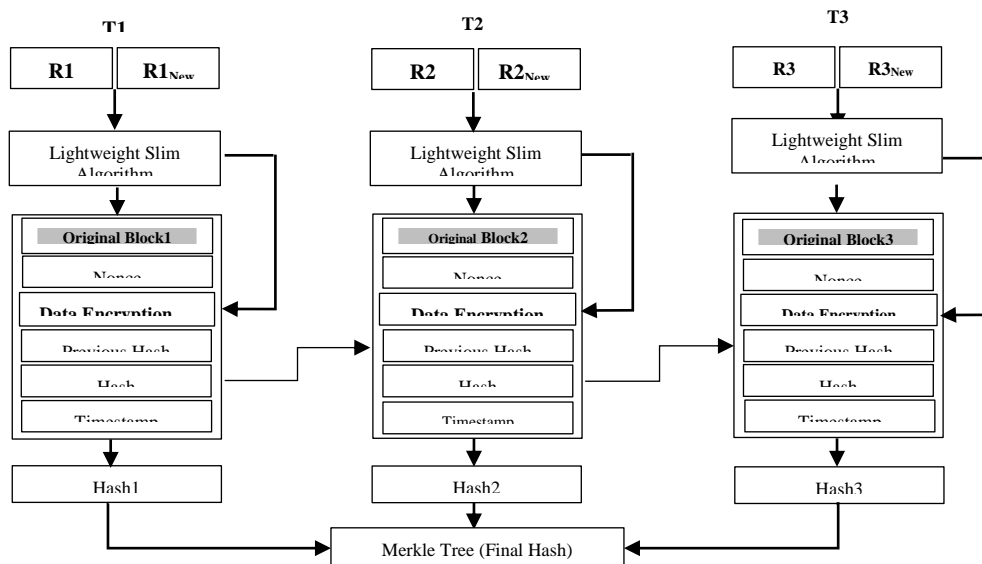


Fig 1. Proposed blockchain model

## 5.1 Blockchain Data

The data of the blockchain consists of the restrictions on which a change operation is carried out, such as selling or buying (changing the owner's name), for example, in the relevant department, in addition to all the details of the property, which are in the form of a single record. The set of restrictions that have been updated are converted into a string and connected to each other in a single string to be encrypted according to the proposed algorithm, the result of which will be entered into a hash function.

## 5.2 Modified Lightweight SLIM Cryptography (MLSLIMC)

In this algorithm, the block size was changed to 64 bits, divided into two parts. Each part is 32 bits and entered in steps close to thin, reducing the number of rounds to 16 or 8. The necessary keys are generated by the proposed Chialvo map, which gives us a series of numbers that appear random. The result of this stage enters the 2D S-box, which is generated by the Chialvo map under different conditions, and we obtain the round state. This process is repeated four times, and the stages of the algorithm are implemented as follows in Figure 2:

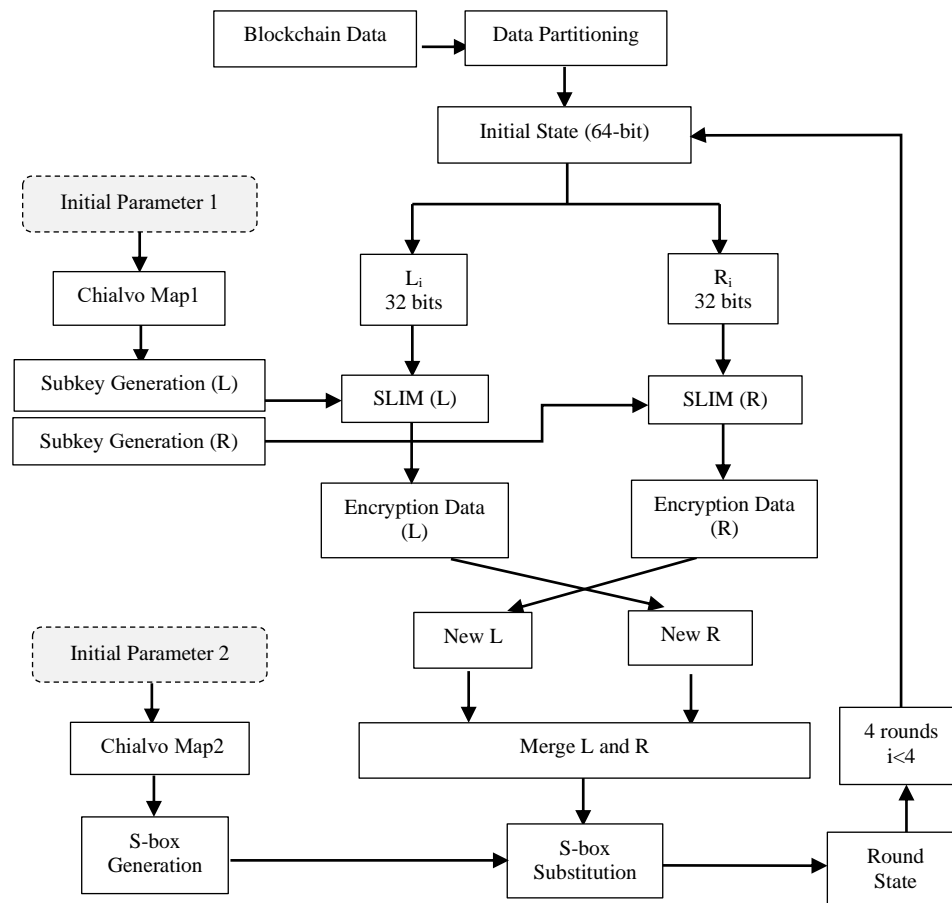


Fig. 2. The Proposed Method with Modified lightweight SLIM and 2D S-Box cryptography

### 5.2.1 Data partitioning

At this stage, the data are divided into a set of blocks, each block is 64 bits long, and a padding is added to the last block when needed, i.e., if the length of the last block is less than 64 bits, each block enters the encryption process and produces a corresponding encrypted block.

### 5.2.2 Split State (left and right)

Each block is in the initial state and separates into two equal portions, left and right, each of which is 32 bits in size. The right portion is the entrance to the lightweight SLIM cryptography but with fewer rounds. The same process is repeated for the left portion. After applying the encryption process, the left and right parts are merged in reverse to obtain the intermediate state. This is the intermediate state that will enter the substitution process through the proposed S-Box.

### 5.2.3 First Key Generation via a Chialvo Map

The Chialvo map is used in generating the required keys in the lightweight SLIM cryptography, which in turn generates a subkey for each round.

- The initial five keys ( $K_1, K_2, \dots, K_5$ ) are produced from the primary 80-bit key. Sixteen bits are taken from the least important key, and 16 bits of an 80-bit key are taken from the subsequent key.
- The original 80-bit key is split into two equal sections with 40 bits each and a labelled key (LSB) and a key (MSB).
- At each round, Key-LSB performs a two-bit circular left shift, and the output is then XORed by Key-MSB. The outcome of the XOR method is sent to a substitution level. The round subkey is created by combining the outcomes of the S-boxes and the flipped key-MSB (key-MSB  $\ll 3$ ) via a procedure known as XOR [20]. The generation is performed as shown in Figure 3:

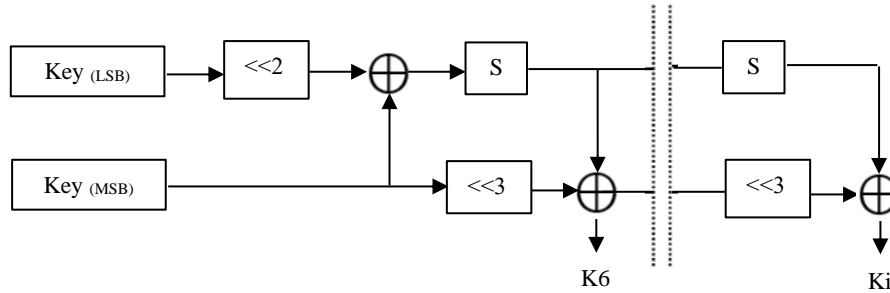


Fig. 3. Key generation for the lightweight SLIM cryptography

### 5.2.4 Applied modified lightweight SLIM cryptography

The modified lightweight SLIM cryptography architecture depends on the Feistel framework. The data that are input are separated into right and left parts, which are processed along with the created subkeys in 16 cycles. The input can be 64 bits long, with an 80-bit key. Examining the internal structure of only one round leads to a more comprehensive lightweight SLIM cryptography architecture. The first step is to divide the 64-bit input into two similar 32-bit parts,  $L_i$  and  $R_i$ . All operations in each cycle may be described by the right part of the input data  $R_i$  and the subkey  $K_i$ , which are modified via XOR. Figure 4. shows an iteration of the algorithm.

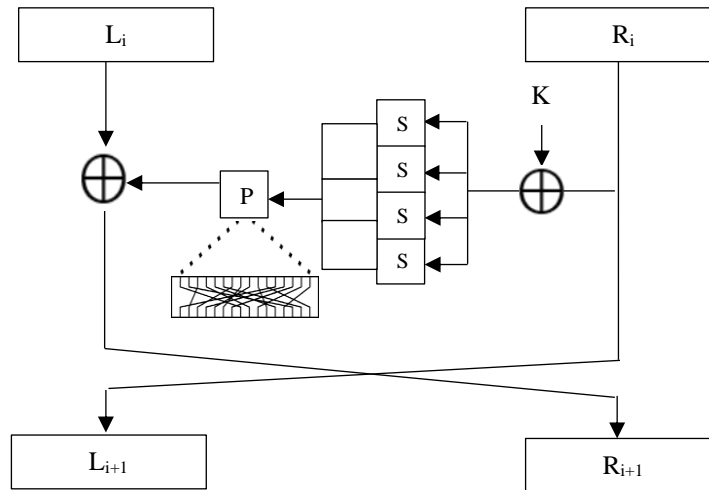


Fig. 4. One round algorithm

The output of the XOR procedure is sent to a substitution box, while the result of the S-boxes is fed into the permutation operation. Finally, the output is XORed with the left-hand component to obtain the right-hand component input for the following cycle. Figure 4 shows how the right portion of the given input data  $R_i$  forms the left-hand component of the following cycle.

### 5.2.5 Merge State

The results obtained from the right and left encryption, are merged in opposite directions. The S-Box outcome is XORed with the left part to obtain the right part input for the next cycle. As shown in Figure 5, the right part of the data entering Ri was transformed into the left part of the input for the following cycle.

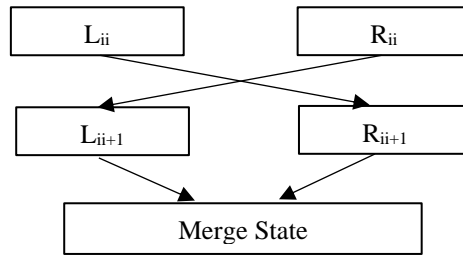


Fig. 5. Merge state

### 5.2.6 Second Key Generation via a Chialvo Map

At this stage, new keys are generated via the Chialvo map by giving different initial values to obtain numbers that differ from the previously generated numbers. These numbers are processed to obtain 256 values, and each value is 8 bits, i.e., two digits in the hexadecimal. They are placed in a table consisting of 16 × 16 bits. Each value in this table is used in the substitution process. To avoid ambiguity, these numbers range from [0--256] without repetition, as shown in Table II.

TABLE II. GENERATYION PROPOSED 16x16 S-BOX DESIGN

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1e	2c	48	64	80	9c	b8	d4	f0	fe	e2	c6	aa	8e	72	56
1	3a	1d	39	55	71	8d	a9	c5	e1	ef	fd	d3	b7	9b	7f	63
2	47	2b	10	22	3e	5a	76	92	ae	ca	e6	f4	d8	bc	a0	84
3	68	4c	30	17	25	41	5d	79	95	b1	cd	e9	f7	db	bf	a3
4	87	6b	4f	33	14	5	0f	23	3f	5b	77	93	af	cb	e7	f5
5	d9	bd	a1	85	69	4d	31	15	9	2	1b	29	45	61	7d	99
6	b5	d1	ed	fb	df	c3	a7	8b	6f	53	37	3	0d	1a	28	44
7	60	7c	98	b4	d0	ec	fa	de	c2	a6	8a	6e	52	36	8	0c
8	21	3d	59	75	91	ad	e9	e5	f3	d7	bb	9f	83	67	4b	2f
9	13	1f	3b	57	73	8f	ab	c7	e3	ff	f1	d5	b9	9d	81	65
10	49	2d	20	2e	4a	66	82	9e	ba	d6	f2	e4	c8	ac	90	74
11	58	3c	24	40	5c	78	94	b0	cc	e8	f6	da	be	a2	86	6a
12	4e	32	16	12	1	11	4	0	7	19	27	43	5f	7b	97	b3
13	Cf	eb	f9	dd	c1	a5	89	6d	51	35	1c	2a	46	62	7e	9a
14	b6	d2	ee	fc	e0	c4	a8	8c	70	54	38	0a	0e	26	42	5e
15	7a	96	b2	ce	ea	f8	dc	c0	a4	88	6c	50	34	18	6	0b

### 5.2.7 S-box Substitution

This work designs a new S-Box utilizing a 2D Chialvo map; this method provides more robust protection and complexity to create a new large S-Box [16 X 16] by employing a two-dimensional Chialvo map, first applying the initial value to the Chialvo map and then generating numbers with (0--255). To avoid repeating numbers in the S-Box matrix, it will create a word for it, then take its index and convert the numbers to hexes 2, which you will find in Table III.

TABLE III: S-BOX LAYER DESIGN

X	2A	3B	67	81	44	50	95	D6
S(X)	6e	E9	8b	3d	14	D9	8f	89

The Chialvo map starting values  $(x,y)$  can significantly affect the trajectory of the map and, consequently, the randomness of the generated S-box. In addition to the four parameters of the sample,  $a$ ,  $b$ ,  $c$ , and  $k$  are as follows:  $a$ ,  $b$ ,  $c$ , and  $k$ . These parameters control the dynamics of the Chialvo map and influence the map's behaviour, such as stability and chaotic regions. Additionally, the number of iterations affects the degree of chaos in the output. More iterations generally enhance the unpredictability of the S-box.

### 1. Configuration Effects on Cryptographic Properties

- **Nonlinearity:** The choice of parameters (particularly  $a$ ,  $b$ , and  $c$ ) influences the nonlinearity of the S-box. Higher nonlinearity is desirable for cryptography, as it enhances resistance against linear cryptanalysis.
- **Avalanche Effect:** The sensitivity of the output to initial conditions ensures that small changes in  $x$  or  $y$  lead to significant differences in the resulting S-box. A strong avalanche effect is crucial for security.
- **Uniformity:** The distribution of output values from the Chialvo map can affect the uniformity of the S-box. A uniform output distribution is critical to prevent biases from being exploited in attacks.

### 5.2.8 Round State

All the previous operations are repeated for each state, the sum of which is called the round function of the proposed method. These operations are repeated four times, so that each state resulting from the round is an input to the next round, and the final result is produced from the last round.

### 5.3 Merge blocks

After the rounds process with the obtained encrypted data, all the encrypted blocks are merged into one string to be added to the data, which will enter the hash function.

#### 5.3.1 Nonce

A block nonce is a value added to the block header during the mining process, also known as a pointer. This makes it harder to find correct hashes and improves blockchain security [24]. In this work, adding nonce will involve adding specific numbers to the encrypted data to control the numbers that will start the final hash function.

#### 5.3.2 Previous Hash

**Prior Block Hash:** This is the hash of the prior block in the blockchain, which connects the current block to the previous block and guarantees the sequential order of the blocks [25]. In this proposal, the previous hash is generated in the first block from the Chialvo map to control the results through the proposed model. The values of the other blocks are present in the previous blocks.

#### 5.3.3 Time Stamp

The timestamp indicates when the block was generated or added to the blockchain, allowing blocks to be arranged in chronological order.

### 5.4 Hash Value

The final and most important component of a block is the hash value itself. It is the output of the hash function that is applied to the block header. All previous values are summarized in a string: encrypted data, nonce, and timestamp. They are entered into a hash function, resulting in a fixed hexadecimal length.

### 5.5 Blockchain Technique

All real estate transactions are subject to the same previous operations and are linked via the previous hash to form the blockchain.

### 5.6 Merkle Tree

The Merkle root represents a cryptographic hash of all transactions in the block. It functions as a concise representation of the whole collection of transactions and contributes to the block's integrity [44].



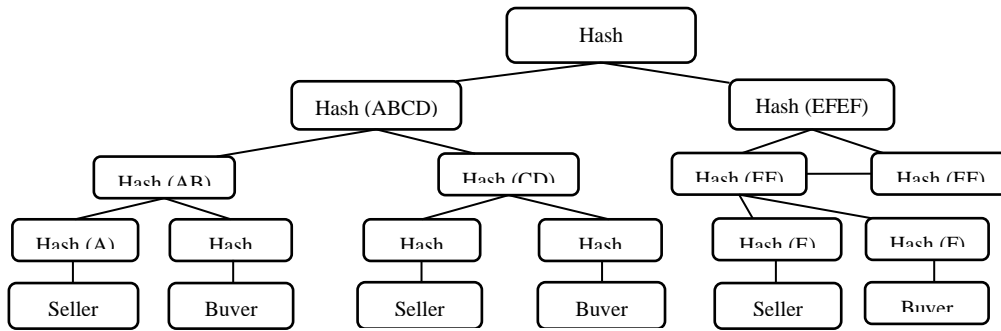


Fig. 6. Merkle Tree for and Hash Value

The Merkle tree is the final step in the suggested method for applying the block hash result; the final outcome is replicated if the number of nodes is odd. Five real estate agreements were completed for both the seller and buyer. Every two changed nodes are concatenated and put into the same hash algorithm, resulting in an intermediate hash that is then fed into the hash level above.

### 5.7 Data Retrieval in the Proposed Model

At this stage, the hash value is verified, which is created by the merkle tree, so that it is common to all existing transactions, and all the data that participated in generating the previous hash are prepared, so that any change in any part of the existing transaction leads to a difference in the final result. In the event that the final hash matches the stored hash, the original data are retrieved, as shown in Figure 7.

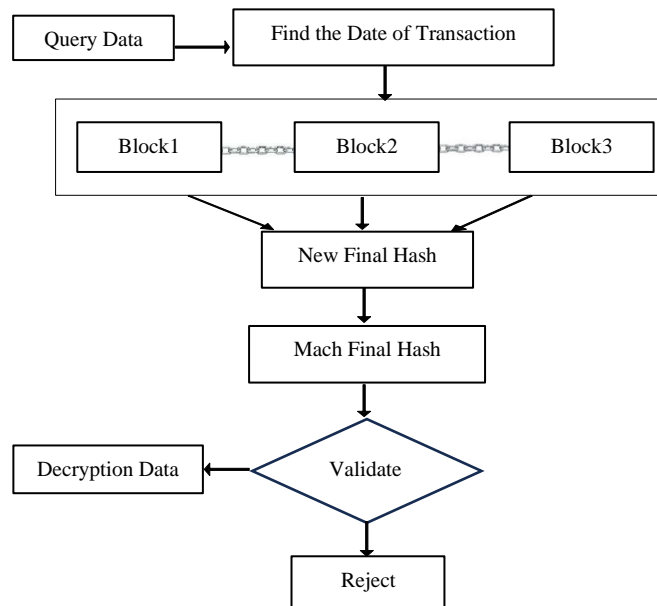


Fig. 7. Decryption of proposed

#### 5.7.1 Query Data with Hash

The required data obtained by providing all the data necessary for the information retrieval process, such as nonce and time to return the original data.

#### 5.7.2 Matching with existing hashes

To verify the existing hash, the entered data are relied upon to generate the same hash by bringing encrypted data, time, previous hash, nonce, and blocks from which the hash is formed at the specified time; the hash is taken for it, and the result is matched with the hash sent in the query. If the matching process is completed, the decryption is completed, but if this process is not completed, the request is rejected.

### 5.7.3 Generating the same Key

In the case of approval of the request and after confirming the correctness of the entered information, the keys are generated in the same way as the Chialvo map and use the same initial value that was used in the encryption stage.

### 5.7.4 Data Decryption via Modified Lightweight SLIM Cryptography

The decryption process of the encrypted data contained in the blockchain is carried out by using the same proposed algorithm, i.e., the first step with the decryption algorithm represents the last step with the encryption algorithm, which is the inverse s-box process, and then separates the result into two parts and applies the inverse lightweight SLIM cryptography to it, which uses the subkey in reverse

## 6. RESULTS AND ANALYSIS

The evaluation criteria are discussed in the following sections:

### 6.1 Dataset

Using a worldwide database, that is freely available online on Kaggle, this study tests the proposed strategy. The dataset contains 16 characteristics, 20,641 rows, and summary statistics about dwellings in certain California districts. Displayed column names and descriptions make columns and rows self-explanatory: Present Owner and buyers: Adding this column clarifies the property sale procedure between owners and purchasers [27].

### 6.2 Analysis of Blockchain Technology

In this section, the performance of the blockchain is tested in terms of time consumption, the bit independence criterion (BIC) and the Hamming distance (HD).

#### 6.2.1 Time consumption for the blockchain

Time execution in blockchain refers to the duration it takes to process and finalize various operations within the blockchain network after the data encryption process. The average time is 29.368877 milliseconds.

#### 6.2.2 BIC Blockchain

The evaluation metric bit independence criterion (BIC) is used to measure the strength and dependability of the blockchain hash function arising from real estate transactions, and is used to evaluate nonlinear transformation behaviour by changing the input bits that affect the output bits. If there is a difference of approximately 50%, the new hash is regarded as good and trustworthy. When five real estate transactions are taken, the results are shown in Table IV.

TABLE IV: THE RESULTS OF HD AND BIC METRIC TO EVALUATE NONLINEAR TRANSFORMATION

No. of Transaction	Hamming Distance	Bit Independence Criterion
1	258	0.493567
2	263	0.471262
3	255	0.504676
4	273	0.486314
5	250	0.510796

#### 6.2.3 Hamming distance blockchain

The Hamming distance between two equal-length characters or vectors is the number of sites where their associated symbols differ. In simpler terms, it determines the minimum number of substitutions required to convert one string to a different one, as well as the minimum number of errors that may have occurred during the transformation. In a larger sense, the hamming distance is one of several string statistics that calculates the edit distance between two strings. The HDs for five real estate transactions are shown in Table IV.

#### 6.2.4 Scalability challenges

When discussing the scalability of a proposed blockchain model, particularly in the context of handling large-scale real estate transactions, it is essential to address computational overhead and potential bottlenecks. A comprehensive analysis is as follows:

- **High Transaction Volume:**

Real estate transactions can involve numerous parties and documents, resulting in a high volume of transactions. Scaling the blockchain to handle thousands of transactions simultaneously can lead to congestion, increased latency, and potential failure.

- **Computational Overhead:**

Each transaction requires computational resources for validation, including cryptographic computations and consensus algorithm processes. As the transaction volume increases, the demand for computational power can lead to slower processing times and increased costs.

- **Data size and storage:**

Real estate transactions often require substantial data storage, including contracts, property details, and regulatory compliance documentation. Storing large amounts of data on-chain can lead to bloat, making it difficult for nodes to synchronize and increasing the time needed for data retrieval.

- **Network Latency:**

Owing to the geographical distribution of nodes in a decentralized network, latency can be introduced. Slow communication between nodes can result in delays in transaction validation and confirmation.

### 6.3 Time consuming encryption and decryption

By reducing the number of rounds of the modified SLIM algorithm to 16 and combining it with the Chialvo map, it reduces the time taken to encrypt and decrypt real estate transactions and avoids potential security vulnerabilities. As shown in Tables V and VI, the real estate transactions were encrypted and decrypted with lightweight SLIM cryptography and S-Box before entering the blockchain in six random attempts, starting from three transactions to ending with six real estate transactions. For the encryption time in Table V the average times for three, four, five, and six transactions were 186.482, 193.756, 202.964, and 214.610 milliseconds, respectively.

TABLE V: THE RESULTS OF ENCRYPTION TIMES IN M-SECOND

Encryption Time in M-sec				
#	6 Tran.	5 Tran.	4 Tran.	3 Tran.
1	202.488	197.706	191.608	176.848
2	219.217	208.127	195.286	192.624
3	216.944	202.261	190.125	188.386
4	221.357	213.199	209.539	206.874
5	221.796	205.765	195.086	186.694
6	205.862	190.726	180.893	167.471

For the decryption time in Table VI. the average times for three, four, five, and six transactions were 156.496, 163.206, 174.211, and 182.244 milliseconds, respectively. The resulting average encryption and decryption times prove that the lightweight encryption algorithm is excellent with the Chialvo map, which meets the speed, accuracy, and security requirements of transactions within the context of blockchain technology.

TABLE VI: THE RESULTS OF THE DECRYPTION TIMES IN M-SECOND

Decryption Time in M-sec				
#	6 Tran.	5 Tran.	4 Tran.	3 Tran.
1	163.819	162.711	166.750	154.502
2	185.525	182.908	157.400	161.429
3	193.386	178.628	164.011	155.539
4	192.605	174.323	174.835	168.052
5	183.146	175.979	156.783	158.842
6	174.987	170.717	159.459	140.617

The encryption and decryption times of the lightweight encryption algorithms were compared with those of lightweight SLIM cryptography, which revealed that by encrypting six real estate transactions, the average encryption time for the PRESENT algorithm was 215.310, the average encryption time for the BORON algorithm was 216.723, and the proposed lightweight SLIM cryptography was 214.610.

For decrypting the six transactions, the average decryption time for the PRESENT algorithm is 184.406, the average decryption time for the BORON algorithm is 182.325, and the proposed lightweight SLIM cryptography is 182.244, as shown in Table VII.

TABLE VII: COMPARISON OF ENCRYPTION AND DECRYPTION TIMES WITH OTHER LIGHTWEIGHT ALGORITHMS

Cipher Type	Encryption Time for 6 Trans. in M-sec	Decryption Time for 6 Trans. in M-sec
PRESENT	215.310	184.406
BORON	216.723	182.325
SLIM	214.610	182.244

#### 6.4 Entropy before and after encryption

The entropy of information is also important when calculating the randomness of the cipher file. The H (s) entropy is given by Equation (5) below [28]:

$$(S) = -\sum p(\text{si})\log_2 p(\text{si}) \quad (5)$$

Five real estate transactions were taken for the seller and the buyer, each transaction was merged separately, the entropy was measured before encryption, and it was also calculated after encryption, as shown in Table VIII. Below:

TABLE VIII. ENTROPY BEFORE AND AFTER ENCRYPTION DATA

No. of Transactions	Seller and Buyer Names	Entropy Before Encryption	Entropy After Encryption
1	Seller(A) and Buyer(B)	5.533343380268326	5.4007276488091005
2	Seller(C) and Buyer(D)	5.531156839114672	5.419315084740532
3	Seller(E) and Buyer(F)	5.545930197896672	5.42175772934887
4	Seller(G) and Buyer(H)	5.5405304516256475	5.394957807681793
5	Seller(I) and Buyer(J)	5.525694580521071	5.412294425011803

#### 6.5 NIST Test (key Generation)

A set of generated chains has been tested using the NIST global test.

TABLE IX. NIST TEST OF KEY GENERATION

#	Test	P Value	Status		Test	P Value	Status
1	“Random excursion test”	0.938822	“Pass”	6	“Non overlapping template matching”	0.967748	“Pass”
2	“Frequency test within a Block test”	0.876548	“Pass”	7	“Random excursion variant test”	0.802584	“Pass”
3	“The longest run of one”	0.912748	“Pass”	8	“Overlapping template matching test”	0.729638	“Pass”
4	“Frequency Monobit Test”	0.81589	“Pass”	9	“Cumulative Sums Test”	0.974789	“Pass”
5	“Run Test”	0.55856	“Pass”	10	“Serial Test”	0.94573	“Pass”

The recommended technique passed the tests, and the results are shown in Table IX. above and as shown below:

- *Frequency (monobit)*: This test determines whether the number of ones and zeroes in the sequence is roughly equal. A score of 0.81589 indicates that the sequence passes this test, implying that it contains nearly equal numbers of ones and zeros, indicating positive evidence of randomness.
- *Frequency Test Within a Block*: This test analyses the frequency of blocks in fixed-size blocks inside a sequence. A score of 0.876548 indicates a pass, indicating that the distribution of ones inside the blocks matches statistical expectations.
- *Runs Test*: This test measures the number of consecutive values and zeros in a sequence. The sequence passes the test with a value of 0.55856, indicating that its runs of ones and zeros are random.
- *Longest Run of Ones (LRO) Test*: This test measures the length of the longest continuous run of ones in the given sequence. The result of 0.912748, indicating a pass, indicates that the longest runs are not particularly long and align with randomness.
- *Serial Test*: This test examines pairs of neighbouring bits in the sequence to identify any deviations from randomness. A passing score of 0.94573 indicates that the sequence passes this test with few variations.

- *The cumulative sums (Cusum) test:* This test assesses the cumulative total discrepancy between the actual and predicted values. A pass rate of 0.974789 indicates that the variances are within permissible limits.
- *Random Excursion Test:* This test measures the number of deviations from zero in the cumulative sum of a sequence. The score of 0.938822, which represents a pass, indicates that the sequence does not include too many excursions.
- *Random Excursion Variant Test:* This test is a variation of the preceding test. A passing score of 0.802584 indicates that the variation test does not raise concerns about the sequence's unpredictability.
- *Nonoverlapping template matching test:* This test detects the existence of preset templates inside the sequence. A score of 0.967748, indicating a pass, shows that the templates are not present in a manner that would indicate nonrandomness.
- *Overlapping template matching test:* This test focuses on the number of instances of prespecified target strings. This indicates a pass score of 0.729638.

A suitable random measure is to continuously modify the derived insights. This update prevents hash number analysis and hash code breaking.

### 6.6 Algebraic Analysis of the S-Box

The security report of the created S-box is evaluated and reviewed in this section. The usual security criteria used to evaluate our S-box's cryptographic strength include balanced, strict avalanche, bit independence, nonlinearity, differential, and linear likelihood. S-boxes are considered more secure, stronger, and superior if they have higher NL and BIC ratings, a SAC ratio of 50%, and a smaller differential and linear likelihood. The next section delves deeper into these performance metrics.

#### 6.6.1 Balanced

An essential requirement that the S-box should fulfil is the balanced distribution of the 0 and 1 integers in the created output sequence through this evaluation of the recommended technique [29,30]. The produced S-boxes are balanced since they include equal numbers of 0 s and 1 s. For example, when the word (Computer) is taken and entered into 16 S-boxes, each letter is converted to hexadecimal, and then entered into each S-box, and the number of ones and zeros in the output is calculated, as shown in Table X.

TABLE X. S-BOX BALANCED

No. of S-Box	Balanced of word (Computer)		No. of S-Box	Balanced of word (Computer)	
	No. 1's	No. 0's		No. 1's	No. 0's
1	33	31	9	37	27
2	43	21	10	29	35
3	33	31	11	35	29
4	36	28	12	21	43
5	32	32	13	33	31
6	30	34	14	38	26
7	24	40	15	31	33
8	32	32	16	36	28

#### 6.6.2 Nonlinearity

A linear mapping between the output and input makes an S-box less immune and weak. If an S-box structure can translate an input to an output in a nonlinear form, it is considered a stronger S-box. Equation (6) may be used to calculate the nonlinearity (NL) of an 8-bit Boolean function G [31].

$$NL(G) = 128 \times (1 - 2^{-8}(WH_{max}(G))) \tag{6}$$

Where,  $WH_{max}(G)$  represents the Walsh–Hadamard transformation of an 8-bit Boolean function G. The S-box nonlinearity scores are 110, 107, 109, 108, 108, 106, and 107, with an average of 110.82. This clearly demonstrates that the suggested confusion component (S-box) has great nonlinearity performance and is very capable of resisting any linear attacks.

#### 6.6.3 Strict avalanche criterion (SAC)

The SAC effectively mandates that if only one bit is changed in the input, the entire output bit set should change by 50% [31]. That is, altering one input bit results in an avalanche of variants; an S-box with a SAC value close to 0.5 is deemed

robust, implying that the attacker will be unable to quickly anticipate a plaintext via statistical analysis. The rigorous avalanche criterion for the recommended S-box analysis is 0.5563 for the maximum value, 0.4256 for the minimum value, and 0.5157 for the average value.

**6.6.4 Bit Independence Criterion (BIC)**

The BIC indicates that altering one bit in the input affects the output bits independently of one another. Guarantees that the changes in output bits have no association, resulting in significant unpredictability and complexity in the output [42]. This unique property of S-boxes ensures that the two output bits vary independently of one another whenever one input bit changes. The suggested S-box for nonlinearity is estimated to have a minimum BIC of 102, maximum BIC of 110, and average BIC of 107.

**6.6.5 Cryptanalysis**

The most essential cryptanalytic methods are linear and differential cryptanalysis, which are utilized in block cipher systems. In both cryptanalysis approaches, the attacker seeks a linear or differential path across the many rounds of a cipher. However, implementing such a technique directly to any cipher necessitates considerable coding skills to alter the cipher in the needed format.

1) *Differential Probability*

Attackers identify encrypted text and use certain differentials to find any traces of plaintext. The study of these differentials helps attackers discover the whole or partial plaintext or key. To counteract differential cryptanalysis, S-box designers aim to minimize the difference between these two forms [33]. The low differential uniformity and differential probability scores, as seen in Equation (7), indicate that the predicted S-box has the potential to defy differential cryptoanalysis.

$$DP = \text{MAX}_{\Delta_u \neq 0, \Delta_v} [\#\{u \in K | S(u) \oplus S(u \oplus \Delta_u) = \Delta_v\}] / 256 \tag{7}$$

where  $\Delta_u$  is the input differential,  $\Delta_v$  is the result of the differential, and  $K = \{0,1,2,3,255\}$ . The proposed S-box represents a maximum DP=0.0425.

2) *Linear Approximation Probability*

A cryptosystem developer aims to jumble plaintext bits in the best feasible way to generate ciphertext that is more nonsensical to the invaders, rendering their attempts to break the ciphertext futile [34]. A suggested S-box was deliberately constructed to help achieve this goal by establishing a nonlinear mapping between plaintext bits and ciphertext bits, as shown in Equation (8).

$$LAP = \max_{\alpha_i, \beta_i \neq 0} |2^\alpha - 8 (\#\{i \in K | i.\alpha_i = S(i).\beta_i\}) - 0.5| \tag{8}$$

where  $\alpha_i$  is the input mask and  $\beta_i$  is the output mask. The suggested S-boxes have an optimal LAP of 0.1176, demonstrating their efficacy against linear assaults.

Table XI lists the proposed S-boxes, and compares the security performance of the recommended S-box to that of various other S-boxes. The comparison analysis is based on widely acknowledged S-box characteristics such as nonlinearity, SAC, the BIC-S-Box, differential probability, and linear approximation probability.

TABLE XI. COMPARISON EVALUATION OF SUGGESTED S-BOX WITH RELATED WORK S-BOXES

S-boxes	NL	SAC-S-Box	BIC-S-Box	DP-S-Box	LAP-S-Box
Suggested s-box	110.82	0.5157	107	0.0425	0.1176
Ref. [31]	110.5	0.5065	106.43	0.0391	0.1172
Ref. [35]	107.25	0.4982	104.78	0.0325	0.1103
Ref. [36]	107.25	0.5013	107	0.0234	0.1092
Ref. [37]	108	0.4975	105.286	0.0625	0.1253
Ref. [38]	107.25	0.5017	107	0.0234	0.1093
Ref. [39]	105.25	0.4991	104	0.0391	0.1325
Ref. [40]	105.87	0.4974	103.67	0.0392	0.1282

Figure 8 shows that the suggested S-box performs optimally; thus, the suggested S-box has sufficient power and resilience to survive linear assaults. Our S-box performs well on other metrics, which is consistent with previous S-box research.

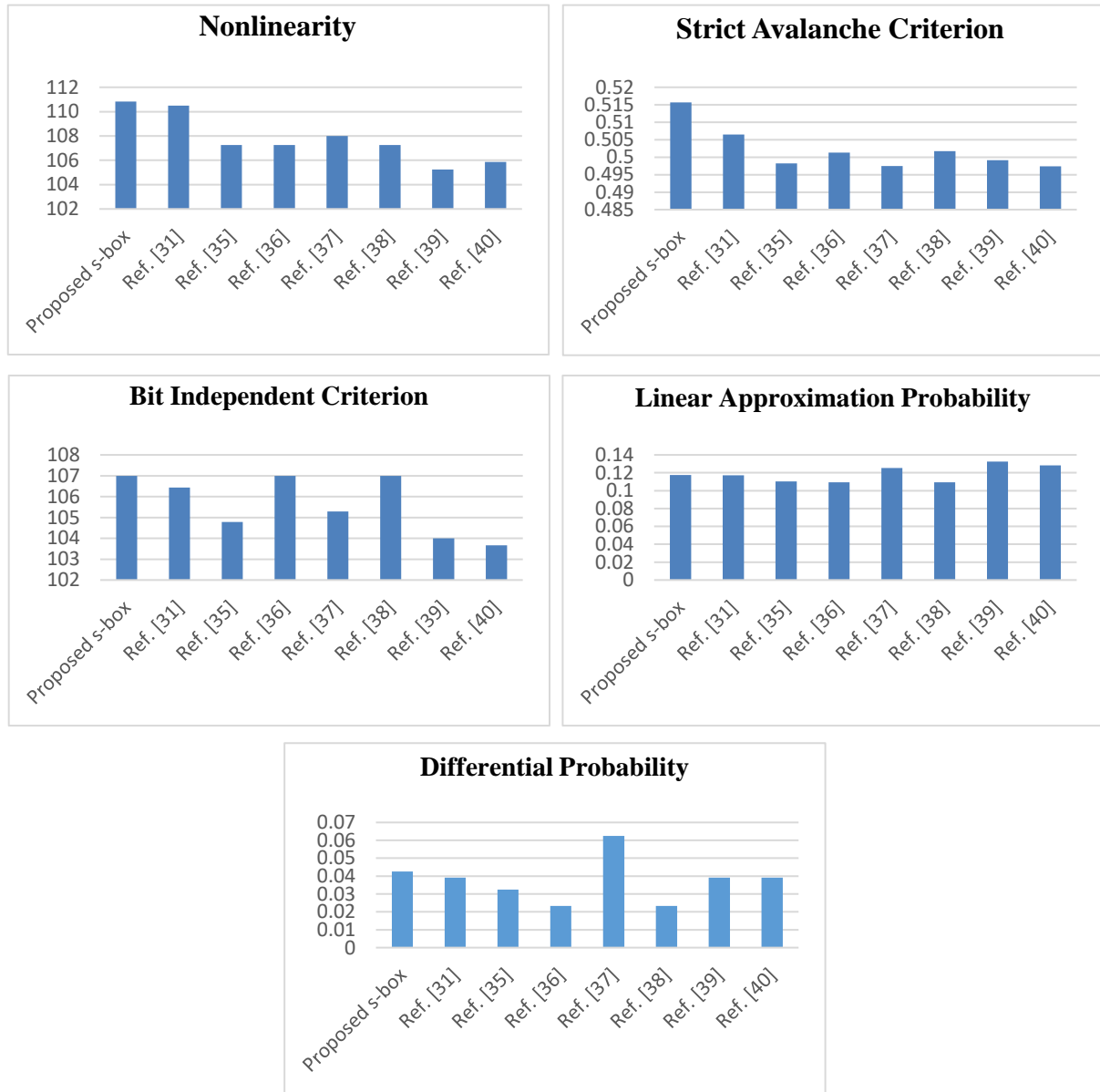


Fig. 8. Displays NL, SAC, BIC, DP, and LAP of the proposed S-box with different S-boxes.

### 7. LIMITATIONS OF THE STUDY

The proposed system focuses on protecting real estate transactions from damage, loss, and forgery; therefore, the first limitation of using a lightweight encryption algorithm with blockchain is resource constraints: while designed for environments with limited resources, the actual resource requirements can still be higher than expected in certain blockchain applications, affecting scalability. The second limitation is performance trade-offs: While lightweight algorithms are designed for efficiency, their performance in a blockchain context can vary. Factors such as network latency, block size, and transaction volume can affect how well these algorithms perform under real-world conditions, and the third limitation is implementation complexity: developing and integrating lightweight encryption into blockchain systems can be complex, requiring specialized knowledge and potentially resulting in implementation errors. The last limitation in security concerns is vulnerability to attacks. While lightweight algorithms aim to minimize resource usage, they may also be more susceptible to certain types of attacks, such as brute-force or side-channel attacks. Ensuring robust security while maintaining efficiency is a significant challenge. Key Management: Implementing secure key management practices is

critical. In a decentralized environment, ensuring that keys are distributed and managed securely can be complex and may introduce vulnerabilities.

## 8. CONCLUSION

Encryption is one of the most significant methods for verifying secret data. Real estate transaction encryption is a significant area in cybersecurity that protects digital transactions from unauthorized access. The originality of this research lies in the use of blockchain technology with modified lightweight SLIM cryptography. The 2D Chialvo map was used to generate two types of keys, the first type: to generate the master and subkeys of the modified encryption algorithm, and the second type: to produce the suggested 16x16 S-box, which is highly nonlinear to make it robust against many linear attacks and to enhance transaction speed and security. Real estate transactions are vulnerable to several malicious assaults and forgeries. The main problem is providing an effective defence against these threats. As a result, lightweight encryption methods are among the best options for safeguarding data in these situations. Lightweight SLIM cryptography outperforms other existing and applied lightweight algorithms because it employs an intensive key length of 80 bits to prevent exhaustive key searches. Lightweight SLIM cryptography employs a robust 4x4 substitution box to assess how cryptographic statistics are influenced by plaintext statistics, and it has demonstrated strong immunity to the most successful linear and differential cryptanalysis attacks and has a considerable protective margin against these types of assaults. We analyzed the strength of the suggested S-box with other S-boxes found in previous research and used algebraic tests that include (SAC, BIC, DP, and LAP). The results showed that the suggested S-box meets all the requirements of the analysis and was considered effective in secure communication. The results of the blockchain performance analysis show that it meets the requirements of the BIC, HD, and time through its ability to complete real estate transactions in a short time. The average blockchain data encryption time for five real estate transactions is 29.368877 milliseconds, and the average times for the encryption and decryption of five S-Box transactions before they enter the blockchain are 202.964 and 174.211 milliseconds, respectively. The strength of the random number generators is analyzed via a set of tests by NIST, which reaches 97%. For future work, exploring the integration of lightweight SLIM cryptography with the IoT: Given the resource constraints of IoT devices, we could focus on integrating lightweight SLIM cryptography with blockchain solutions designed for IoT applications, ensuring secure communication and data integrity. Incorporating the created technology into an easy-to-use mobile application would improve both accessibility and usability, helping users engage with the system effortlessly from their smartphones or tablets. produce two solutions to the scalability of the proposed blockchain: Sidechains, which utilize sidechains to offload some of the transaction loads from the main chain. This allows for specialized chains that can handle specific types of transactions, such as real estate. In addition, sharding is implemented to divide the blockchain into smaller, more manageable pieces (shards). Each shard can process transactions independently, increasing overall throughput and reducing latency.

### Conflicts of interest

The researchers have no conflicts of interest to report. The authors confirm that the material provided is original and has not been published in another publication for review.

### Funding

No government, corporate, or nonprofit entity provided a particular grant for this research.

### Authors' Contributions:

All the authors contributed equally to the composition of this research study.

### Acknowledgement

The author's is grateful to the institution for their collaboration and provision of necessary facilities that contributed to the successful completion of this research.

### References

- [1] K. P. S. Sherin, T. A. Amma, K. Sivakumar, and S. Divya, "Cyber Security in Blockchain Technology," *International Journal of Research in Engineering, Science and Management*, vol. 6, no. 2, pp. ISSN (Online): 2581-5792, Feb. 2023.
- [2] D. H. Tahayur and M. Al-Zubaidie, "Enhancing Electronic Agriculture Data Security with a Blockchain-Based Search Method and E-Signatures," *Mesopotamian journal of Cybersecurity*, vol. 4, no. 3, pp. 1–21, 2024. doi: <https://doi.org/10.58496/MJCS/2024/012>.



- [3] A. S. Jamil and A. M. S. Rahma, "Cyber Security for Medical Image Encryption using Circular Blockchain Technology Based on Modify DES Algorithm," *International Journal of Online and Biomedical Engineering (iJOE)* , vol. 19, no. 03, 2023.
- [4] S. S. Abdul-Jabbar, A. K. Farhan, and R. F. Ghani, "Data Analytics and Blockchain: A Review," *Iraqi Journal of Computers, Communications, Control & Systems Engineering (IJCCCE)* , vol. 23, no. 1, Mar. 2023.
- [5] H. S. Hassan, R. Hassan, and E. K. Gbashi, "E-voting System Based on Ethereum Blockchain Technology Using Ganache and Remix Environments," *Engineering and Technology Journal* , pp. 562-577, 2023.
- [6] Z. A. Kamal, R. F. Ghani, and A. K. Farhan, "Blockchain-based E-Government system using WebSocket protocol," *Engineering and Technology Journal* , pp. 421-429, 2024.
- [7] S. S. Dhanda, B. Singh, and P. Jindal, "Lightweight Cryptography: A Solution to Secure IoT," *Wireless Personal Communications* , part of Springer Nature 2020. doi: 10.1007/s11277-020-07134-3.
- [8] Q. Y. Zhang, T. Li, and G. R. Wu, "An Image Tamper-proof Encryption Scheme Based on Blockchain and Lorenz Hyperchaotic S-box," *International Journal of Network Security* , vol. 25, no. 2, pp. 252-266, Mar. 2023. doi: 10.6633/IJNS.202303 25(2).08.
- [9] S. Hussain, S. S. Jamal, T. Shah, and I. Hussain, "A Power Associative Loop Structure For The Construction Of Non-Linear Components Of Block Cipher," *IEEE Access* . doi: 10.1109/ACCESS.2020.3005087, 2020.
- [10] O. Kuznetsov, N. Poluyanenko, E. Frontoni, and S. Kandy, "Enhancing Smart Communication Security: A Novel Cost Function for Efficient S-Box Generation in Symmetric Key Cryptography," *MDPI journal, Cryptography* , 2024. doi: 10.3390/cryptography8020017.
- [11] N. M. Naser and J. R. Naif, "A systematic review of ultra-lightweight encryption algorithms," *International Journal Nonlinear Analysis and Applications* , ISSN: 2008-6822, 2022. doi: 10.22075/ijnaa.2022.6167.
- [12] M. A. Hatem, B. A. Hameedi, and J. N. Hasoon, "Lightweight digital imaging and communications in medicine image encryption for IoT system," *TELKOMNIKA Telecommunication Computing Electronics and Control* , vol. 21, no. 4, pp. 771-783, Aug. 2023. doi: 10.12928/TELKOMNIKA.v21i4.24766.
- [13] A. Alahdal et al., "NLBCIT: A Novel Approach for Securing data in IoT devices based on a Lightweight Block Cipher Design Algorithms," *African Journal of Biological Sciences* , ISSN: 2663-2187, 2024. doi: 10.48047/AFJBS.6.12.2024.6203-6221.
- [14] A. A. Altaay, J. N. Hasoon, and H. K. Albahadily, "Lightweight Image Encryption Based on A Hybrid Approach," *International Journal on Informatics Visualization* , vol. 8, no. 2, pp. 977-982, May 2024.
- [15] J. S. Teha, L. J. Thama, N. Jamilc, and W. Yapd, "New Differential Cryptanalysis Results for the Lightweight Block Cipher BORON," *Journal of Information Security and Applications* . doi: 10.1016/j.jisa.2022.103129, 2022.
- [16] H. I. Mhaibes, M. H. Abood, and A. K. Farhan, "Simple Lightweight Cryptographic Algorithm to Secure Imbedded IoT Devices," *International Journal of Interactive Mobile Technologies (iJIM)* , Oct. 2022. doi: 10.3991/ijim.v16i20.34505.
- [17] H. Nurwarsito and S. Yapputra, "Implementation of Simon's Algorithm in the Encryption Process of Publish-Subscribe Data Sending in the MQTT Protocol using the Raspberry," *The 1st International Conference on Engineering and Technology (ICoEngTech)* . doi: 10.1088/1742-6596/1962/1/012064, 2021.
- [18] T. Fan, L. Li, Y. Wei, and E. Pasalic, "Differential cryptanalysis of full-round ANU-II ultra-lightweight block cipher," *International Journal of Distributed Sensor Networks* , vol. 18, no. 9, 2022. doi: 10.1177/15501329221119398.
- [19] A. H. Karode, S. R. Suralkar, and V. B. Patil, "Performance Evaluation of Light Weight Cryptographic CLEFIA Algorithm," *International Journal of Electronics and Communication Engineering* , vol. 10, no. 8, pp. 48-58, Aug. 2023. doi: 10.14445/23488549/IJECE-V10I8P105.
- [20] B. Aboushousha, R. A. Ramadan, A. D. Dwivedi, A. El-Sayed, and M. M. Dessouky, "SLIM: A Lightweight Block Cipher for Internet of Health Things," *IEEE Access* . doi: 10.1109/ACCESS.2020.3036589, 2020.
- [21] N. Sugio, N. Shibayama, and Y. Igarashi, "Higher-order Differential Attack on Reduced-round SLIM," *Journal of Information Processing* , vol. 32, pp. 352–357, 2024. doi: 10.2197/ipsjip.32.352.
- [22] A. A. Salih, Z. A. Abdulrazaq, and H. G. Ayoub, "Design and Enhancing Security Performance of Image Cryptography System Based on Fixed Point Chaotic Maps Stream Ciphers in FPGA," *Baghdad Science Journal* . doi: 10.21123/bsj.2024.10521, P-ISSN: 2078-8665 - E-ISSN: 2411-7986, 2024.
- [23] P. Pilarczyk and G. Graff, "An absorbing set for the Chialvo Map," *Elsevier BV, Communications in Nonlinear Science and Numerical Simulation* , p. 107947, 2024.
- [24] Zainab A. Kamal and Rana.F. Ghani, "A Proposed Authentication Method for Document in Blockchain Based E-Government System," *Iraqi Journal of Computers, Communications, Control & Systems Engineering (IJCCCE)* , vol. 22, no. 4, Dec. 2022. doi: <https://doi.org/10.33103/uot.ijccce.22.4.10> .

- [25] K. K. Vaigandla, M. Siluveru, M. Kesoju, and R. Karne, "Review on blockchain technology: architecture, characteristics, benefits, algorithms, challenges and applications," *Mesopotamian journal of Cybersecurity* , vol. 2023, pp. 73–85, Mar. 2023. doi: 10.58496/MJCS/2023/012.
- [26] L. Hussain, "Fortifying AI Against Cyber Threats Advancing Resilient Systems to Combat Adversarial Attacks", *EDRAAK*, vol. 2024, pp. 26–31, Mar. 2024, doi: [10.70470/EDRAAK/2024/004](https://doi.org/10.70470/EDRAAK/2024/004).
- [27] [Online]. Available: <https://www.kaggle.com/datasets/abdallahsamman/california-housing-with-name-of-counties>
- [28] M. Lawnik, L. Moysis, and C. Volos, "Chaos-Based Cryptography: Text Encryption Using Image Algorithms," [Online]. Available: <https://www.mdpi.com/journal/electronics> . doi: 10.3390/electronics11193156, 2022.
- [29] Ala'a Talib Khudhair and Abeer Tariq Maolood, "A Novel Approach to Generate Dynamic S-Box for Lightweight Cryptography Based on the 3D Hindmarsh Rose Model," *Journal of Soft Computing and Computer Applications* , vol. 1, no. 1, 2024.
- [30] A. K. Farhan, R. S. Ali, H. R. Yassein, N. M. G. Al-Saidi, and G. H. Abdul-Majeed, "A new approach to generate multi S-boxes based on RNA computing," *International Journal of Innovative Computing, Information and Control (IJICIC)* , vol. 16, no. 1, pp. 331–348, 2020. doi: 10.24507/ijicic.16.01.331.
- [31] A. Alhudhaif, M. Ahmad, A. Alkhayyat, N. Tsafack, A. K. Farhan, and R. Ahmed, "Block Cipher Nonlinear Confusion Components Based on New 5-D Hyperchaotic System," *IEEE Access* . doi: 10.1109/ACCESS.2021.3090163, 2021.
- [32] A. Alsajri, A. Steiti, and H. A. Salman , Trans., "Enhancing IoT Security to Leveraging ML for DDoS Attack Prevention in Distributed Network Routing", *BJIoT*, vol. 2023, pp. 74–84, Oct. 2023, doi: [10.58496/BJIoT/2023/010](https://doi.org/10.58496/BJIoT/2023/010).
- [33] A. D. Dwivedi and G. Srivastava, "Differential Cryptanalysis of Round-Reduced LEA," *IEEE Access* . doi: 10.1109/ACCESS.2017, 2018.
- [34] E. O. Oraby and Salah A.K. Albermany, "Linear Cryptanalysis of S-Box BRADG," *International Journal of Engineering & Technology* , pp. 120-124, 2018.
- [35] S. A. Jassim and A. K. Farhan, "Designing a Novel Efficient Substitution-Box by Using a Flower Pollination Algorithm and Chaos System," *International Journal of Intelligent Engineering and Systems* , vol. 15, no. 1, 2022. doi: 10.22266/ijies2022.0228.17.
- [36] B. Arshad, N. Siddiqui, Z. Hussain, and M. Ehatisham ul Haq, "A Novel Scheme for Designing Secure Substitution Boxes (S Boxes) Based on Mobius Group and Finite Field," *Wireless Personal Communications* . doi: 10.1007/s11277-022-09524-1, 2022.
- [37] M. Sarfraz, I. Hussain, and Fateh Ali, "Construction of S-Box Based on Mobius Transformation and Increasing Its Confusion Creating Ability through Invertible Function," *International Journal of Computer Science and Information Security (IJCSIS)* , vol. 14, no. 2, 2016.
- [38] B. Arshad, N. Siddiqui, and Z. Hussain, "A Novel Method for Designing Substitution Boxes Based on Mobius Group," *Wireless Personal Communications* , vol. 124, pp. 3527–3548, 2022.
- [39] F. Riaz and N. Siddiqui, "Design of an Efficient Cryptographic Substitution Box by using Improved Chaotic Range with the Golden Ratio," *International Journal of Computer Science and Information Security (IJCSIS)* , vol. 18, no. 1, 2020.
- [40] W. Iftikhar and N. Siddiqui, "An Effective Technique of Substitution-box Construction using Recurrence Relation with Logistic Map," *International Journal of Computer Science and Information Security (IJCSIS)* , vol. 18, no. 3, 2022.
- [41] I. I. . Al Barazanchi and W. . Hashim, "Enhancing IoT Device Security through Blockchain Technology: A Decentralized Approach", *SHIFRA*, vol. 2023, pp. 10–16, Feb. 2023, doi: [10.70470/SHIFRA/2023/002](https://doi.org/10.70470/SHIFRA/2023/002).
- [42] Y. Aydin and F. Ozkaynak, "Automated Chaos-Driven S-Box Generation and Analysis Tool for Enhance Cryptographic Resilience," *IEEE Access* . doi: 10.1109/ACCESS.2023.3346319, 2023.
- [43] H. Alnabulsi, R. Islam, I. Alsmadi, and S. Bevinakoppa , Trans., "An Innovative Method of Malicious Code Injection Attacks on Websites", *Applied Data Science and Analysis*, vol. 2024, pp. 39–51, May 2024, doi: [10.58496/ADSA/2024/005](https://doi.org/10.58496/ADSA/2024/005).
- [44] T. Wang, H. Hua, Z. Wei, and J. Cao, "Challenges of blockchain in new generation energy systems and future outlooks," *International Journal of Electrical Power and Energy Systems* , vol. 135, Feb. 2022. Art. no. 107499. doi: 10.1016/j.ijepes.2021.107499, 2021.