SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I8P101

Volume 11 Issue 8, 1-10, August 2024
© 2024 Seventh Sense Research Group®

Original Article

Implementing a Multi-Way Distributed Blockchain Security System Using the RPBB-24-4 Algorithm

Md. Jaffar Sadiq[1], Abdul Ahad[2], Syed Mazharuddin[3], Mohd. Sirajuddin[4], Sayyada Hajera Begum[5]

[1,3]Department of CSE (Data Science), Sreenidhi Institute of Science and Technology, Telangana, India.
[2]Department of Artificial Intelligence, Anurag University, Telangana, India.
[4]Department of Information Technology, Vidya Jyothi Institute of Technology, Telangana, India.
[5]Department of Information Technology, Muffakham Jah College of Engineering & Technology, Telangana.India.

[1]Corresponding Author : dr.jaffarsadiqmd@gmail.com

Received: 25 May 2024 Revised: 08 July 2024 Accepted: 02 August 2024 Published: 31 August 2024

***Abstract** - There are a lot of technologies that are becoming more prominent in the world that we live in today, and one of these technologies is the Blockchain. The technology in question offers an exceptionally high level of protection, and it is also quite robust. Users are not privy to a great deal of information about Blockchain; nonetheless, the functionality of its security is used to safeguard the data that is sent in a number of different ways. After that, this specific user went on to make use of the "ChaCha" and RBJ25 algorithms, both of which are considered to be versions that are both compact and secure. The new security mechanism that we have decided to refer to as RPBB24-4 will be presented to the reader within the confines of this article. The RPBB-24-4 method is made up of two parts: encryption and decoding. The encryption process is made up of four steps. The first step in the process is to use the square root of the secret prime key in the matrix. The second step in the process is to use the "lattin letter" and multiply the value by four using Equation (1). In the third step, protected data is used to change the cell numbers, but the process fourth step in the process is to use the "SalSa" method in the grid. Finally, the plain text is changed into protected text. Instead of working in the same way as the encryption process, the decryption method operates in the opposite direction. There is a greater degree of security offered by the strategy that has been presented in comparison to the one that is presently being used.*

***Keywords** - Decryption, Encryption, Performance, RBJ25, RPBB-24-4, Salsa.*

1. Introduction

Blockchain is a sort of shared database that stores information in a manner that is distinct from that of a conventional database. Rather than keeping information in tables, blockchains store data in blocks that are cryptographically linked together with their hash values. Blockchains are a type of distributed database. A distributed database or ledger that is shared across the nodes of a computer network is referred to as a blockchain. In a nutshell, a blockchain is a distributed ledger or database. Many other types of data may be stored on a blockchain; however, the ledger function has proved to be the most beneficial use of blockchain technology for managing transactions, namely Bitcoin. Blockchain is decentralized, which implies that no one person or organization has control over it; rather, the whole user base maintains power collectively. No one person or group has authority over blockchain. The data that is added to a decentralized blockchain cannot be changed, which implies that it cannot be removed from the blockchain. When utilizing Bitcoin, every transaction is recorded permanently and may be read by anybody interested.

By using cryptography, one may transform the original data, which is known as plain text, into some information that has been jumbled. This information is referred to as the encrypted message or ciphertext. Because of this alteration of data, the only person who is able to decode the message is a user who has the correct key, also known as the secret key. The information may also be encrypted using quantum cryptography, which is an extension of the previous method. Utilizing the laws of quantum physics it ensures that the data is sent safely and securely. What makes quantum cryptography so difficult to understand and implement is the fact that it is based on the laws of quantum physics. It is possible to conceive of the idea of a quantum blockchain as a database that is decentralized, encrypted, and distributed. This database is supported by quantum computing and the concept of quantum information. Following the moment at which the information is uploaded to the quantum blockchain, it is not possible to make any illegal changes to the data subsequent to that point. In addition to being protected against classical assaults, it is also protected against quantum attacks.

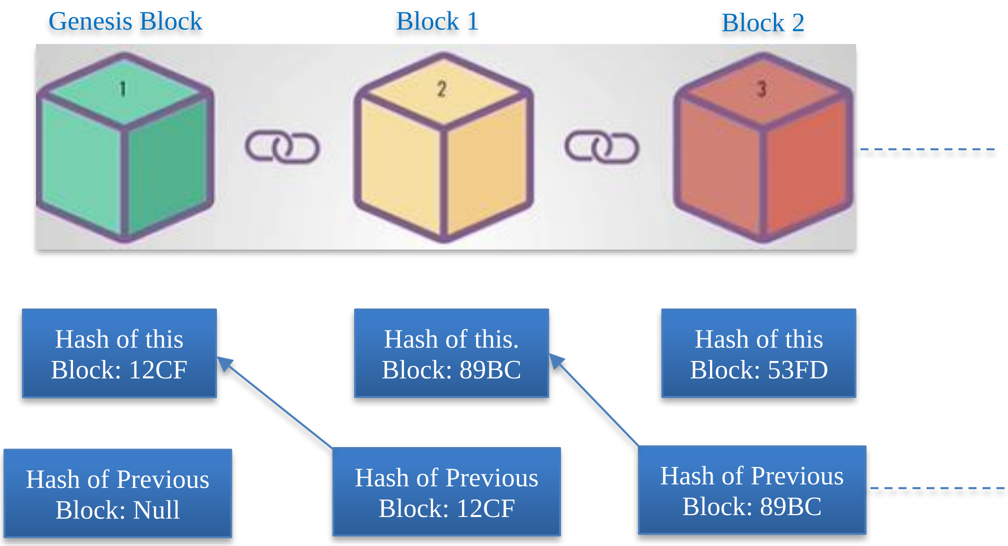
Genesis Block
Block 1
Block 2
1
2
3
Hash of this Block: 12CF
Hash of this. Block: 89BC
Hash of this Block: 53FD
Hash of Previous Block: Null
Hash of Previous Block: 12CF
Hash of Previous Block: 89BC

Fig. 1 The structure of blockchain

Today, the majority of firms are driven primarily by information as their main motivation. Both the fact that data may be obtained without any delay and the fact that it is accurate is desirable. Blockchain is the most effective technology for providing information because it stores data on an immutable ledger and can only be accessed by members of a network that has been permitted to do so.

This makes blockchain the best technology for delivering information because it offers data in real time that is shared and entirely transparent. Information is the engine that powers the bulk of businesses in today's world. It would be wonderful if it were received in a timely way and with the correct information included.

Due to the fact that it delivers data in real time that is completely shareable and transparent, data that is recorded on an immutable ledger, and data that is only available to members of a network who have been permitted to view it, blockchain technology is a perfect choice for the transmission of data which is of this kind. If a blockchain network is used, it is possible to keep track of production, as well as orders, payments, and accounts. As an additional benefit, you are able to see each and every stage of a transaction, beginning with its beginning and ending with its completion, due to the fact that everyone is able to read the same version of the ledger at the same time.

The term blockchain comes from the essential structure that it has within itself. The organizational structure of the blockchain is formed by the blocks when they are linked to one another. When it comes to understanding blockchain security, it is vital to have a solid understanding of the blockchain's design. In a blockchain, the distributed ledger is made up of blocks, which are storage units for the data that is being recorded.

The many transactions that are included in each block of the blockchain contribute to the expansion of the shared state that exists inside the blockchain network. The two components that comprise each block are referred to as the header and the body. Among the information that is included in the blockchain header is the following: the identification number of the block, the value of the timestamp, the value of the random nonce, the hash of the current block, the hash of the block that came before it, the Merkle tree root value, the owner's public key, the owner's identification number, and the block's signature.

At the same time, transactions are included in the body component (whether they are in plaintext or encrypted language). It is usual practice to refer to the structure of the blockchain as a collection of blocks that are securely connected to one another in a manner that prohibits the blocks from being altered. The values of the hash function are what link the blocks together. Figure 1 illustrates the structure of the blockchain that is being used.

2. Literature Survey

Saurabh Singh and his coworkers discussed several "Blockchain security issues such as transactions, network security, and privacy" [1] at their 2021 brainstorming session. Blockchain technology has several uses in the cryptocurrency "Bitcoin," and in 2021, Bhutta and colleagues studied these uses and the problems associated with blockchain security risks [2]. In 2021, Iqbal and colleagues investigated how to handle potential dangers posed by blockchain technology. The two main concerns that prompted their investigation were called "Sybil" and "double-spending" [3].

Rathore and others have put up the idea that blockchain technology with Deep Learning (DL) might provide security. We will use the DL method to analyze the data, and then we will use that analysis to make predictions. The information will then be used to implement security measures via the use of blockchain technology [4].

Researchers R. A. Mallah and colleagues have looked at the many mobility risks associated with blockchain technology [5]. They have also looked at blockchain technology's potential security issues. E. A. Shammar et al. sift through the mountain of literature on blockchain technology in search of relevant studies to investigate its safety [6]. Among the many writers who put out the idea of the blockchain were Junyu Ren and coworkers. At one point in time, this program was able to lessen the amount of delay [7].

The algorithm of cryptography was the main topic of debate when A. J. Cabrera-Gutiérrez and his colleagues met together in 2022. An algorithm was developed to strengthen the Internet of Things company's security measures [8]. The TDCB D3P technique was developed in 2022 by Y. Goh and colleagues, among other writers. By using this technique, the harmful activity might be reduced, and the network's security may be improved [9].

Blockchain security, V2X, storage, 5G, and the Internet of Things were the primary areas of study for P. M. Rao and colleagues in 2023. In order to concentrate mostly on the survey of technologies that lie somewhere in the center, it is needed to employ these technologies [10].

G. Thakur and his associates are the subjects of the author's investigation inside the "Digital Twin (DT)" environment. [11]. We employed this environment in order to conduct a thorough evaluation of blockchain technology's security. What we call "Sec-health" is really a strategy put out by L. D. Costa and coworkers. The principles of blockchain technology form the basis of this approach. The goal of this approach is to help clients save time by minimizing the amount of effort they have to put into remembering their health records [12].

The author, together with L. Li and D. Jin, among others, zeroed emphasis on blockchain technology's storage capabilities. As stated in [13], this storage approach is used to enhance fault support and provide a high level of security. In order to increase safety, the author proposed the "RBJ25" technique [14].

This method was developed from the research conducted by S. Rajaprakash and colleagues. C. Bagath Basha et al. suggested SRB18 as a solution, and the authors zeroed in on encryption security. Using this strategy, we were able to implement highly secure encryption while keeping the transfer rate manageable [15]. Working with colleagues from several research organizations, the author (Batcha, B.B.C.) researched the seven-stage security approach of RPBB31 [16].

Several authors have looked at potential ways to improve performance and security. Following a review of the relevant literature, we will provide the RajaprakashBagathbasha-24 (RPBB-24-4) method.

3. Methodology

The RPBB-24-4 method is made up of two parts: encryption and decoding. The encryption process is made up of four steps. The first step in the process is to use the square root of the secret prime key in the matrix. The second step in the process is to use the "lattin letter" and multiply the value by four using Equation (1).

In the third step, protected data is used to change the cell numbers, but the process fourth step in the process is to use the "SalSa" method in the grid. Finally, the plain text is changed into protected text, as shown in Figure 2. The decryption process works the other way around from the encryption process.

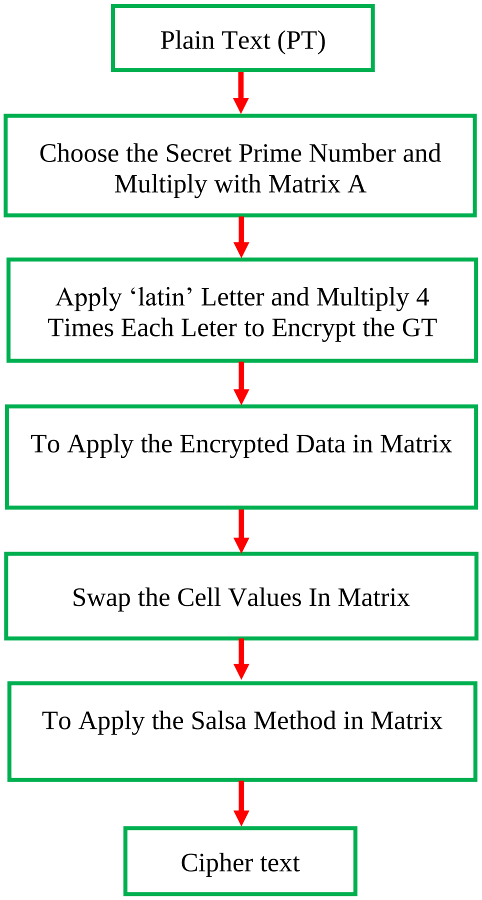
Plain Text (PT)
Choose the Secret Prime Number and Multiply with Matrix A
Apply ‘latin’ Letter and Multiply 4 Times Each Leter to Encrypt the GT
To Apply the Encrypted Data in Matrix
Swap the Cell Values In Matrix
To Apply the Salsa Method in Matrix
Cipher text

Fig. 2 RPBB-24-4 methodology

3.1. Encryption Algorithm

1. Apply the secret key prime for multiply in a given matrix
2. Then, we have to choose a private message as GT.
3. To convert to numbers from the “Latin alphabet” for GT.

4. In every letter, the number must be multiplied 4 times to encrypt the GT.

$$\begin{array}{l}
\text{if } a < n \text{ Then} \\
T_a \text{ - } GT_n \\
T_{a\,b} = T_{a\,b} * \; T_{a\,b} = R_a * \qquad\qquad \text{- (1)} \\
T_{a\,b} = (R_a *) * T_{a\,b} = R_a * \\
T_{a\,b} = (R_a *) * T_{a\,b} = R_a * \\
T_{a\,b} = (R_i *) * T_{i\,j} = R_i * \\
\text{Where T is Character and R is Remainder} \\
\qquad a = 0, a = a + 1 \text{ to } n, b = b + 1, b = 0 \\
\qquad \text{and } n = \text{number of charaters} \\
\text{else} \\
\; a > n \text{ then Stop } a
\end{array}$$

5. To apply the encrypted values in matrix A to swap the values.
6. To apply the Salsa method in matrix A.

3.2. Decryption Algorithm

1. First, we have to receive a Cipher Text message from the user as SE.
2. Apply the Salsa Method in matrix SE.
3. Apply the “Latin alphabet” for the DT message and convert it to numbers.
4. Each letter number is multiplied 4 times to decrypt the DT.

$$\begin{array}{l}
\text{if } a < n \text{ Then} \\
T_a \text{ - } GT_n \\
T_{a\,b} = T_{a\,b} * \; T_{a\,b} = R_a * \qquad\qquad \text{- (2)} \\
T_{a\,b} = (R_a *) * T_{a\,b} = R_a * \\
T_{a\,b} = (R_a *) * T_{a\,b} = R_a * \\
T_{a\,b} = (R_i *) * T_{i\,j} = R_i * \\
\text{Where T is Character and R is Remainder} \\
\qquad a = 0, a = a + 1 \text{ to } n, b = b + 1, b = 0 \\
\qquad \text{and } n = \text{number of charaters} \\
\text{else} \\
\; a > n \text{ then Stop } a
\end{array}$$

5. To apply the decrypted values in matrix DT for swap the values.
6. Finally, apply the secret prime key division in the DT matrix.

4. Result and Discussion

$$A=\begin{bmatrix} RT_{11} & RT_{12} & RT_{13} & RT_{14} \\ RT_{21} & RT_{22} & RT_{23} & RT_{24} \\ RT_{31} & RT_{32} & RT_{33} & RT_{34} \\ RT_{41} & RT_{42} & RT_{43} & RT_{44} \end{bmatrix}$$

4.1. Working for Encryption

Step 1 - To multiply the secret prime key 17 in matrix A

$$A=\begin{bmatrix} 17RT_{11} & 17RT_{12} & 17RT_{13} & 17RT_{14} \\ 17RT_{21} & 17RT_{22} & 17RT_{23} & 17RT_{24} \\ 17RT_{31} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$

Step 2 - To convert the number from the given text as RT

- RT = SOFTMICRO
- S-83, O-79, F-70, T-84, M-77, I-73, C-67, R-82, O-79 RT=837970847773678279
- Apply Equation (1) to encrypt the PT.

First Character -S= 83

- $$\begin{array}{l} a = 1, b = 1 \\ T_{11} = RT_9 \\ S = 83, b = 1 \\ T_{11} = 83*83 \\ T_{11} = 6889/91 \Rightarrow 64 \end{array} \qquad \begin{array}{l} b = 2 \\ T_{12} = 64*83 \\ T_{12} = 5312/91 \Rightarrow 34 \\ b = 3 \\ T_{13} = 34*83 \\ T_{13} = 2822/91 \Rightarrow 1 \\ a = 4 \\ T_{14} = 1*83 \\ T_{14} = 83/91 \Rightarrow 83 \\ T_{14} = 83 \end{array}$$

Second Character - O= 79

- $$\begin{array}{l} a = a + 1, \\ a = 1 + 1 = 2 \\ a = 2, b = 1 \\ T_{21} = RT_9 \\ O = 79, b = 1 \\ T_{21} = 79*79 \\ T_{21} = 6241/91 \Rightarrow 53 \end{array} \qquad \begin{array}{l} b = 2 \\ T_{22} = 53*79 \\ T_{22} = 4187/91 \Rightarrow 1 \\ b = 3 \\ T_{23} = 1*79 \\ T_{23} = 79/91 \Rightarrow 79 \\ b = 4 \\ T_{24} = 79*79 \\ T_{24} = 6241/91 \Rightarrow 53 \\ T_{24} = 53 \end{array}$$

Third Character - F= 70

- $$\begin{array}{l} a = a + 1, \\ a = 2 + 1 = 3 \\ a = 3, b = 1 \\ T_{31} = RT_9 \\ F = 70, b = 1 \\ T_{31} = 70*70 \\ T_{31} = 4900/91 \Rightarrow 77 \end{array} \qquad \begin{array}{l} b = 2 \\ T_{32} = 77*70 \\ T_{32} = 5390/91 \Rightarrow 21 \\ b = 3 \\ T_{33} = 21*70 \\ T_{33} = 1470/91 \Rightarrow 14 \\ b = 4 \\ T_{34} = 14*70 \\ T_{34} = 980/91 \Rightarrow 70 \\ T_{34} = 70 \end{array}$$

Fourth Character - T= 84

- $$\begin{gathered} a = a + 1, \\ a = 3 + 1 = 4 \\ a = 4, b = 1 \\ T_{41} = RT_9 \\ T = 84, b = 1 \\ T_{41} = 84 * 84 \\ T_{41} = 7056/91 \Rightarrow 49 \end{gathered}$$
  $$\begin{gathered} b = 2 \\ T_{42} = 49 * 84 \\ T_{42} = 4116/91 \Rightarrow 21 \\ b = 3 \\ T_{43} = 21 * 84 \\ T_{43} = 1764/91 \Rightarrow 35 \\ b = 4 \\ T_{44} = 35 * 84 \\ T_{44} = 2940/91 \Rightarrow 28 \\ T_{44} = 28 \end{gathered}$$

Fifth Character - M=77

- $$\begin{gathered} a = a + 1 \\ a = 4 + 1 = 5 \\ a = 5, b = 1 \\ T_{51} = RT_9 \\ M = 77 \\ T_{51} = 77 * 77 \\ T_{51} = 5929/91 \Rightarrow 14 \end{gathered}$$
  $$\begin{gathered} b = 2 \\ T_{52} = 14 * 77 \\ T_{52} = 1078/91 \Rightarrow 77 \\ b = 3 \\ T_{53} = 77 * 77 \\ T_{53} = 5929/91 \Rightarrow 14 \\ a = 4 \\ T_{54} = 14 * 77 \\ T_{54} = 1078/91 \Rightarrow 77 \\ T_{54} = 77 \end{gathered}$$

Sixth Character - I= 73

- $$\begin{gathered} a = a + 1, \\ a = 5 + 1 = 6 \\ a = 6, b = 1 \\ T_{61} = RT_9 \\ I = 73, b = 1 \\ T_{61} = 73 * 73 \\ T_{61} = 5329/91 \Rightarrow 51 \end{gathered}$$
  $$\begin{gathered} b = 2 \\ T_{62} = 51 * 73 \\ T_{62} = 3723/91 \Rightarrow 83 \\ b = 3 \\ T_{63} = 83 * 73 \\ T_{63} = 6059/91 \Rightarrow 53 \\ b = 4 \\ T_{64} = 53 * 73 \\ T_{64} = 3869/91 \Rightarrow 47 \\ T_{64} = 47 \end{gathered}$$

Seventh Character - C= 67

- $$\begin{gathered} a = a + 1, \\ a = 6 + 1 = 7 \\ a = 7,\ b = 1 \\ T_{71} = RT_9 \\ T = 67, b = 1 \\ T_{71} = 67 * 67 \\ T_{71} = 4489/91 \Rightarrow 30 \end{gathered}$$
  $$\begin{gathered} b = 2 \\ T_{72} = 30 * 67 \\ T_{72} = 2010/91 \Rightarrow 8 \\ b = 3 \\ T_{73} = 8 * 67 \\ T_{73} = 536/91 \Rightarrow 81 \\ b = 4 \\ T_{74} = 81 * 67 \\ T_{74} = 5427/91 \Rightarrow 58 \\ T_{74} = 58 \end{gathered}$$

Eight Character - R= 82

- $$\begin{gathered} a = a + 1, \\ a = 7 + 1 = 8 \\ a = 8,\ b = 1 \\ T_{81} = RT_9 \\ T = 82, b = 1 \\ T_{81} = 82 * 82 \\ T_{81} = 6724/91 \Rightarrow 81 \end{gathered}$$
  $$\begin{gathered} b = 2 \\ T_{82} = 81 * 82 \\ T_{82} = 6642/91 \Rightarrow 90 \\ b = 3 \\ T_{83} = 90 * 82 \\ T_{83} = 7380/91 \Rightarrow 9 \\ b = 4 \\ T_{84} = 9 * 82 \\ T_{84} = 738/91 \Rightarrow 10 \\ T_{84} = 10 \end{gathered}$$

Ninth Character - O= 79

- $$\begin{gathered} a = a + 1, \\ a = 8 + 1 = 9 \\ a = 9, b = 1 \\ T_{91} = RT_9 \\ O = 79, b = 1 \\ T_{91} = 79 * 79 \\ T_{91} = 6241/91 \Rightarrow 53 \end{gathered}$$
  $$\begin{gathered} b = 2 \\ T_{92} = 53 * 79 \\ T_{92} = 4187/91 \Rightarrow 1 \\ b = 3 \\ T_{93} = 1 * 79 \\ T_{93} = 79/91 \Rightarrow 79 \\ b = 4 \\ T_{94} = 79 * 79 \\ T_{94} = 6241/91 \Rightarrow 53 \\ T_{94} = 53 \end{gathered}$$
- ET=835370287747581053
- To make a pair and apply the encrypted code in Matrix.

  $$A = \begin{bmatrix} 17RT_{11} & 17RT_{12} & 17RT_{13} & 17RT_{14} \\ 17RT_{21} & 17RT_{22} & 17RT_{23} & 17RT_{24} \\ 17RT_{31} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$
- ET pair is (8,3), (5,3), (7,0), (2,8), (7,7), (4,7), (5,8), (1,0), (5,3)
- The 1st swap values (8,3)

  $$ET = \begin{bmatrix} 17RT_{11} & 17RT_{12} & 17RT_{13} & 17RT_{31} \\ 17RT_{21} & 17RT_{22} & 17RT_{23} & 17RT_{24} \\ 17RT_{14} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$
- The 2nd swap values (5,3)

  $$ET = \begin{bmatrix} 17RT_{11} & 17RT_{12} & 17RT_{13} & 17RT_{22} \\ 17RT_{21} & 17RT_{31} & 17RT_{23} & 17RT_{24} \\ 17RT_{14} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$
- The 3rd swap values (7,0)

  $$ET = \begin{bmatrix} 17RT_{24} & 17RT_{12} & 17RT_{13} & 17RT_{22} \\ 17RT_{21} & 17RT_{31} & 17RT_{23} & 17RT_{11} \\ 17RT_{14} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$

- The 4th swap values (2,8)

$$\text{ET}=\begin{bmatrix} 17RT_{24} & 17RT_{12} & 17RT_{14} & 17RT_{22} \\ 17RT_{21} & 17RT_{31} & 17RT_{23} & 17RT_{11} \\ 17RT_{13} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$

- The 5th swap values (7,7)

$$\text{ET}=\begin{bmatrix} 17RT_{24} & 17RT_{12} & 17RT_{14} & 17RT_{22} \\ 17RT_{21} & 17RT_{31} & 17RT_{23} & 17RT_{11} \\ 17RT_{13} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$

- The 6th swap values (4,7)

$$\text{ET}=\begin{bmatrix} 17RT_{24} & 17RT_{12} & 17RT_{14} & 17RT_{22} \\ 17RT_{11} & 17RT_{31} & 17RT_{23} & 17RT_{21} \\ 17RT_{13} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$

- The 7th swap values (5,8)

$$\text{ET}=\begin{bmatrix} 17RT_{24} & 17RT_{12} & 17RT_{14} & 17RT_{22} \\ 17RT_{11} & 17RT_{13} & 17RT_{23} & 17RT_{21} \\ 17RT_{31} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$

- The 8th swap values (1,0)

$$\text{ET}=\begin{bmatrix} 17RT_{12} & 17RT_{24} & 17RT_{14} & 17RT_{22} \\ 17RT_{11} & 17RT_{13} & 17RT_{23} & 17RT_{21} \\ 17RT_{31} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$

- The 9th swap values (5,3)

$$\text{ET}=\begin{bmatrix} 17RT_{12} & 17RT_{24} & 17RT_{14} & 17RT_{13} \\ 17RT_{11} & 17RT_{22} & 17RT_{23} & 17RT_{21} \\ 17RT_{31} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$

Step 3 - Now apply the “Salsa” method in the ETP matrix.

$$\text{SE}=\begin{bmatrix} 17RT_{12} & 17RT_{22} & 17RT_{33} & 17RT_{44} \\ 17RT_{11} & 17RT_{32} & 17RT_{43} & 17RT_{13} \\ 17RT_{31} & 17RT_{42} & 17RT_{14} & 17RT_{21} \\ 17RT_{41} & 17RT_{24} & 17RT_{23} & 17RT_{34} \end{bmatrix}$$

4.2. Working for Decryption

$$\text{SE}=\begin{bmatrix} 17RT_{12} & 17RT_{22} & 17RT_{33} & 17RT_{44} \\ 17RT_{11} & 17RT_{32} & 17RT_{43} & 17RT_{13} \\ 17RT_{31} & 17RT_{42} & 17RT_{14} & 17RT_{21} \\ 17RT_{41} & 17RT_{24} & 17RT_{23} & 17RT_{34} \end{bmatrix}$$

Step 1 - Now apply the “Salsa” method in the SE matrix.

$$\text{SD}=\begin{bmatrix} 17RT_{12} & 17RT_{24} & 17RT_{14} & 17RT_{13} \\ 17RT_{11} & 17RT_{22} & 17RT_{23} & 17RT_{21} \\ 17RT_{31} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$

Step 2 - To convert the number from the given text as DT

- DT =ORCIMTFOS
- O-79, R-82, C-67, I-73, M-77, T-84,F-70,O-79,S-83, DT = 798267737784707983
- Apply Equation (2) to decrypt the DT.

First Character - O= 79

- $$\begin{aligned} &a=1, b=1 \\ &T_{11}=RT_9 \\ &O=79, b=1 \\ &T_{11}=79*79 \\ &T_{11}=6241/91 \Rightarrow 53 \end{aligned} \qquad \begin{aligned} &b=2 \\ &T_{12}=53*79 \\ &T_{12}=4187/91 \Rightarrow 1 \\ &b=3 \\ &T_{13}=1*79 \\ &T_{13}=79/91 \Rightarrow 79 \\ &b=4 \\ &T_{14}=79*79 \\ &T_{14}=6241/91 \Rightarrow 53 \\ &T_{14}=53 \end{aligned}$$

Second Character - R= 82

- $$\begin{aligned} &a=a+1, \\ &a=1+1=2 \\ &a=2,\ b=1 \\ &T_{21}=RT_9 \\ &T=82, b=1 \\ &T_{21}=82*82 \\ &T_{21}=6724/91 \Rightarrow 81 \end{aligned} \qquad \begin{aligned} &b=2 \\ &T_{22}=81*82 \\ &T_{22}=6642/91 \Rightarrow 90 \\ &b=3 \\ &T_{23}=90*82 \\ &T_{23}=7380/91 \Rightarrow 9 \\ &b=4 \\ &T_{24}=9*82 \\ &T_{24}=738/91 \Rightarrow 10 \\ &T_{24}=10 \end{aligned}$$

Third Character - C= 67

- $$\begin{aligned} &a=a+1, \\ &a=2+1=3 \\ &a=3,\ b=1 \\ &T_{31}=RT_9 \\ &T=67, b=1 \\ &T_{31}=67*67 \\ &T_{31}=4489/91 \Rightarrow 30 \end{aligned} \qquad \begin{aligned} &b=2 \\ &T_{32}=30*67 \\ &T_{32}=2010/91 \Rightarrow 8 \\ &b=3 \\ &T_{33}=8*67 \\ &T_{33}=536/91 \Rightarrow 81 \\ &b=4 \\ &T_{34}=81*67 \\ &T_{34}=5427/91 \Rightarrow 58 \\ &T_{34}=58 \end{aligned}$$

Fourth Character - I= 73

- $$\begin{aligned}&a=a+1,\\&a=3+1=4\\&a=4,b=1\\&T_{41}=RT_9\\&I=73,b=1\\&T_{41}=73*73\\&T_{41}=5329/91\Rightarrow 51\end{aligned}$$
  $$\begin{aligned}&b=2\\&T_{42}=51*73\\&T_{42}=3723/91\Rightarrow 83\\&b=3\\&T_{43}=83*73\\&T_{43}=6059/91\Rightarrow 53\\&b=4\\&T_{44}=53*73\\&T_{44}=3869/91\Rightarrow 47\\&T_{44}=47\end{aligned}$$

Fifth Character - M=77

- $$\begin{aligned}&a=a+1\\&a=4+1=5\\&a=5,b=1\\&T_{51}=RT_9\\&M=77\\&T_{51}=77*77\\&T_{51}=5929/91\Rightarrow 14\end{aligned}$$
  $$\begin{aligned}&b=2\\&T_{52}=14*77\\&T_{52}=1078/91\Rightarrow 77\\&b=3\\&T_{53}=77*77\\&T_{53}=5929/91\Rightarrow 14\\&a=4\\&T_{54}=14*77\\&T_{54}=1078/91\Rightarrow 77\\&T_{54}=77\end{aligned}$$

Sixth Character - T= 84

- $$\begin{aligned}&a=a+1\\&a=5+1=6\\&a=6,b=1\\&T_{61}=RT_9\\&T=84,b=1\\&T_{61}=84*84\\&T_{61}=7056/91\Rightarrow 49\end{aligned}$$
  $$\begin{aligned}&b=2\\&T_{62}=49*84\\&T_{62}=4116/91\Rightarrow 21\\&b=3\\&T_{63}=21*84\\&T_{63}=1764/91\Rightarrow 35\\&b=4\\&T_{64}=35*84\\&T_{64}=2940/91\Rightarrow 28\\&T_{64}=28\end{aligned}$$

Seventh Character - F= 70

- $$\begin{aligned}&a=a+1,\\&a=6+1=7\\&a=7,b=1\\&T_{71}=GT_9\\&F=70,b=1\\&T_{71}=70*70\\&T_{71}=4900/91\Rightarrow 77\end{aligned}$$
  $$\begin{aligned}&b=2\\&T_{72}=77*70\\&T_{72}=5390/91\Rightarrow 21\\&b=3\\&T_{73}=21*70\\&T_{73}=1470/91\Rightarrow 14\\&b=4\\&T_{74}=14*70\\&T_{74}=980/91\Rightarrow 70\\&T_{74}=70\end{aligned}$$

Eight Character - O= 79

- $$\begin{aligned}&a=a+1,\\&a=7+1=8\\&a=8,b=1\\&T_{81}=RT_9\\&O=79,b=1\\&T_{81}=79*79\\&T_{81}=6241/91\Rightarrow 53\end{aligned}$$
  $$\begin{aligned}&b=2\\&T_{82}=53*79\\&T_{82}=4187/91\Rightarrow 1\\&b=3\\&T_{83}=1*79\\&T_{83}=79/91\Rightarrow 79\\&b=4\\&T_{84}=79*79\\&T_{84}=6241/91\Rightarrow 53\\&T_{84}=53\end{aligned}$$

Ninth Character -S= 83

- $$\begin{aligned}&a=a+1,\\&a=8+1=9\\&a=9,b=1\\&T_{91}=RT_9\\&S=83,b=1\\&T_{91}=83*83\\&T_{91}=6889/91\Rightarrow 64\end{aligned}$$
  $$\begin{aligned}&b=2\\&T_{92}=64*83\\&T_{92}=5312/91\Rightarrow 34\\&b=3\\&T_{93}=34*83\\&T_{93}=2822/91\Rightarrow 1\\&a=4\\&T_{94}=1*83\\&T_{94}=83/91\Rightarrow 83\\&T_{94}=83\end{aligned}$$

- DT=531058477728705383
- To make a pair and apply the encrypted code in Matrix.
  $$\text{SDP=}\begin{bmatrix}17RT_{12} & 17RT_{24} & 17RT_{14} & 17RT_{13}\\17RT_{11} & 17RT_{22} & 17RT_{23} & 17RT_{21}\\17RT_{31} & 17RT_{32} & 17RT_{33} & 17RT_{34}\\17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44}\end{bmatrix}$$
- DT pair is (5,3), (1,0), (5,8), (4,7), (7,7), (2,8), (7,0), (5,3), (8,3)
- The 1st swap values (5,3)
  $$\text{DT=}\begin{bmatrix}17RT_{12} & 17RT_{24} & 17RT_{14} & 17RT_{22}\\17RT_{11} & 17RT_{13} & 17RT_{23} & 17RT_{21}\\17RT_{31} & 17RT_{32} & 17RT_{33} & 17RT_{34}\\17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44}\end{bmatrix}$$
- The 2nd swap values (1,0)
  $$\text{DT=}\begin{bmatrix}17RT_{24} & 17RT_{12} & 17RT_{14} & 17RT_{22}\\17RT_{11} & 17RT_{13} & 17RT_{23} & 17RT_{21}\\17RT_{31} & 17RT_{32} & 17RT_{33} & 17RT_{34}\\17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44}\end{bmatrix}$$

- The 3rd swap values (5,8)

$$DT=\begin{bmatrix} 17RT_{24} & 17RT_{12} & 17RT_{14} & 17RT_{22} \\ 17RT_{11} & 17RT_{31} & 17RT_{23} & 17RT_{21} \\ 17RT_{13} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$

- The 4th swap values (4,7)

$$DT=\begin{bmatrix} 17RT_{24} & 17RT_{12} & 17RT_{14} & 17RT_{22} \\ 17RT_{21} & 17RT_{31} & 17RT_{23} & 17RT_{11} \\ 17RT_{13} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$

- The 5th swap values (7,7)

$$DT=\begin{bmatrix} 17RT_{24} & 17RT_{12} & 17RT_{14} & 17RT_{22} \\ 17RT_{21} & 17RT_{31} & 17RT_{23} & 17RT_{11} \\ 17RT_{13} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$

- The 6th swap values (2,8)

$$DT=\begin{bmatrix} 17RT_{24} & 17RT_{12} & 17RT_{13} & 17RT_{22} \\ 17RT_{21} & 17RT_{31} & 17RT_{23} & 17RT_{11} \\ 17RT_{14} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$

- The 7th swap values (7,0)

$$DT=\begin{bmatrix} 17RT_{11} & 17RT_{12} & 17RT_{13} & 17RT_{22} \\ 17RT_{21} & 17RT_{31} & 17RT_{23} & 17RT_{24} \\ 17RT_{14} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$

- The 8th swap values (5,3)

$$DT=\begin{bmatrix} 17RT_{11} & 17RT_{12} & 17RT_{13} & 17RT_{31} \\ 17RT_{21} & 17RT_{22} & 17RT_{23} & 17RT_{24} \\ 17RT_{14} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$

- The 9th swap values (8,3)

$$DT=\begin{bmatrix} 17RT_{11} & 17RT_{12} & 17RT_{13} & 17RT_{14} \\ 17RT_{21} & 17RT_{22} & 17RT_{23} & 17RT_{24} \\ 17RT_{31} & 17RT_{32} & 17RT_{33} & 17RT_{34} \\ 17RT_{41} & 17RT_{42} & 17RT_{43} & 17RT_{44} \end{bmatrix}$$

Step 3 - Divide the secret prime key in matrix DT as A

$$A=\begin{bmatrix} RT_{11} & RT_{12} & RT_{13} & RT_{14} \\ RT_{21} & RT_{22} & RT_{23} & RT_{24} \\ RT_{31} & RT_{32} & RT_{33} & RT_{34} \\ RT_{41} & RT_{42} & RT_{43} & RT_{44} \end{bmatrix}$$

Table 1. RPBB-24-4 encryption performance

File Size (Bytes)	Salsa	RBJ25	RPBB-24-4
25	1.62	2.2	2.7
77	1.19	2.6	3.1
110	1.39	3.4	3.7
311	2.43	4.5	4.8
811	2.24	5.3	5.4
1521	3.44	5.5	6.1
6580	2.97	6.8	7.3

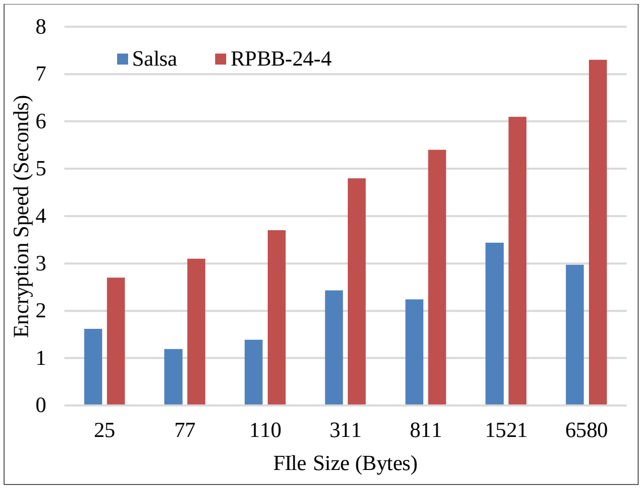

Fig. 3 Salsa vs RPBB-24-4 encryption speed

These three encryption speeds are compared in Table 1, which may be found here. When compared to other methods, the RPBB-24-4 approach that was suggested demonstrates performance that is satisfactory in terms of speed. When compared to the techniques that are already in use, which are "Salsa" in Figure 3, "RBJ25" in Figure 4, and RPBB-24-4 in Figure 5, the performance of the speed of the suggested method RPBB-24-4 is 2.7, 3.1, 3.7, 4.8 5.4, 6.1, 7.3 in various file sizes. This is an excellent result.

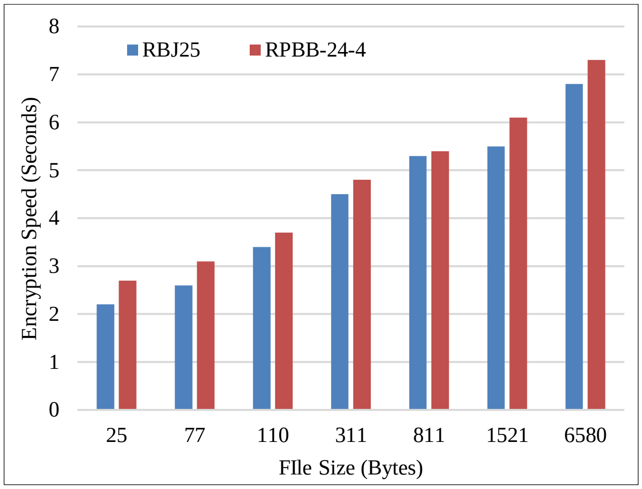

Fig. 4 RBJ25 vs RPBB-24-4 encryption speed

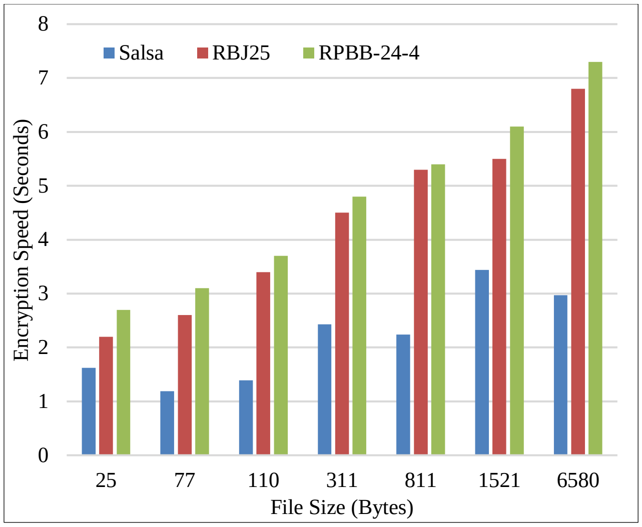

Fig. 5 RPBB-24-4 encryption speed

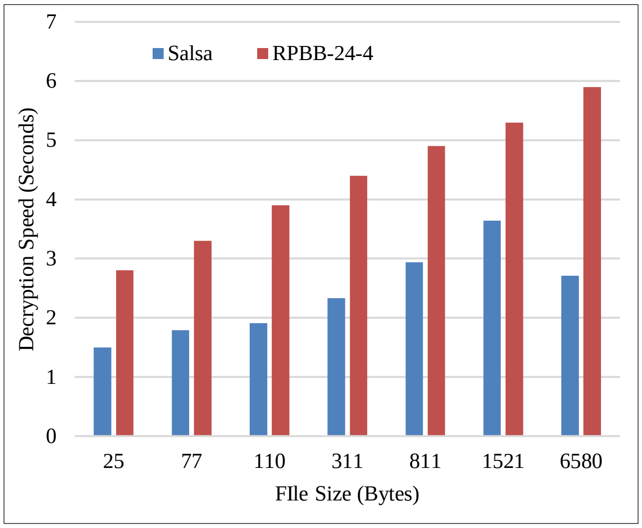

Fig. 6 Salsa vs RPBB-24-4 decryption speed

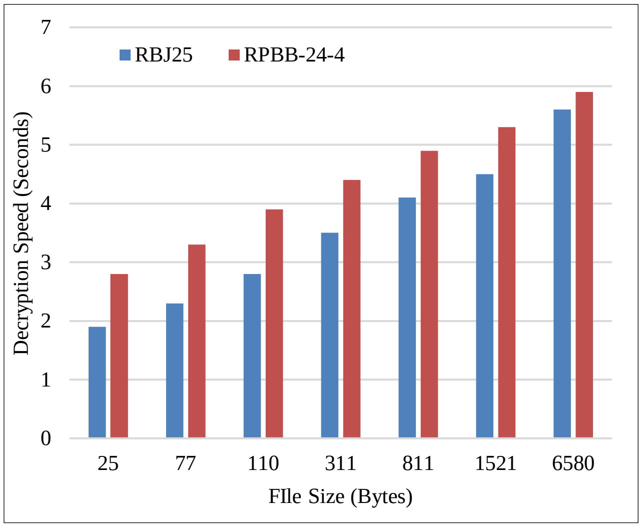

Fig. 7 RBJ25 Vs RPBB-24-4 decryption speed

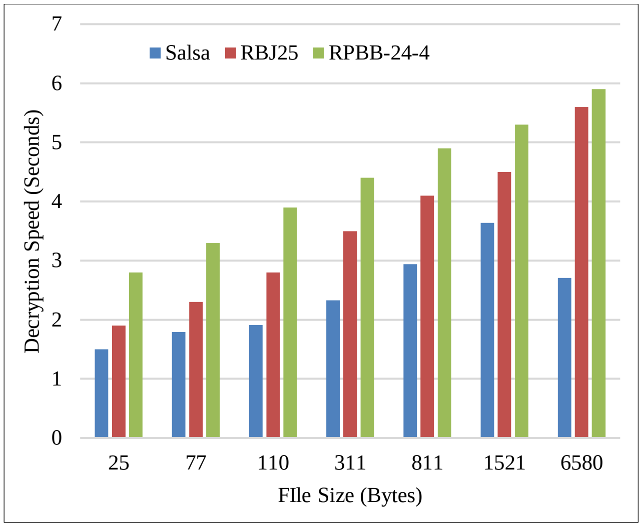

Fig. 8 RPBB-24-4 decryption speed

Table 2. RPBB-24-4 decryption performance

File Size (Bytes)	Salsa	RBJ25	RPBB-24-4
25	1.5	1.9	2.8
77	1.79	2.3	3.3
110	1.91	2.8	3.9
311	2.33	3.5	4.4
811	2.94	4.1	4.9
1521	3.64	4.5	5.3
6580	2.71	5.6	5.9

An examination of the three different decryption speeds is shown in Table 2. When contrasted with other methods, the RPBB-24-4 approach that was suggested demonstrates a really high level of speed performance. The performance of the speed in the suggested method RPBB-24-4 is 2.8, 3.3, 3.9, 4.4, 4.9, 5.3, and 5.9 in various file sizes. This is excellent when compared to the current techniques, which are "Salsa" in Figure 6, "RBJ25" in Figure 7, and RPBB-24-4 in Figure 8.

5. Conclusion

Blockchain is one of the technologies that is considerably increasing at the quickest pace in the globe. Blockchain is one of the technologies as well. In spite of the fact that people are unaware of what blockchain is, it is a method that is used to ensure the safety of numerous data locations throughout the network. "Salsa" and "RBJ25" are the names of the algorithms that are used by this kind of user, which are regarded as having a lesser level of security than other algorithms. The RPBB-24-4 security approach is the one that is being provided here since it falls within the scope of this inquiry.

Within the framework of the RPBB-24-4 approach, two components are integrated. For example, encryption and decryption are included in these components. These components include encryption and decryption. Each of these two elements is necessary for the process to be successful. Additionally, four procedures must be completed in order to finish the encryption process. The application of multiplying the secret prime key in the matrix is the first step in the procedure. Applying the "lattin letter" and multiplying the result by four times using Equation (1) is the second step in the procedure.

Using encrypted data, the third procedure involves swapping the cell values, but the process of Implementing the "SalSa" technique in the matrix is the fourth step in the procedure. After all is said and done, the regular text is converted into encrypted text. In light of this, it may be concluded that the process of decryption goes in the opposite direction of the encryption method. There is a greater degree of security offered by the strategy that has been presented in comparison to the one that is presently being used.

References

[1] Saurabh Singh, A.S.M. Sanwar Hosen, and Byungun Yoon, “Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network,” *IEEE Access*, vol. 9, pp. 13938 - 13959, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Muhammad Nasir Mumtaz Bhutta et al., “A Survey on Blockchain Technology: Evolution, Architecture and Security,” *IEEE Access*, vol. 9, pp. 61048-61073, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Mubashar Iqbal, and Raimundas Matulevičius, “Exploring Sybil and Double-Spending Risks in Blockchain Systems,” *IEEE Access*, vol. 9, pp. 76153-76177, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Shailendra Rathore, Jong Hyuk Park, and Hangbae Chang, “Deep Learning and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT,” *IEEE Access*, vol. 9, pp. 90075-90083, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Ranwa Al Mallah, David Lopez, and Bilal Farooq, “Cyber-Security Risk Assessment Framework for Blockchains in Smart Mobility,” *IEEE Open Journal of Intelligent Transportation Systems*, vol. 2, pp. 294-311, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Elham A. Shammar, Ammar T. Zahary, and Asma A. Al-Shargabi, “A Survey of IoT and Blockchain Integration: Security Perspective,” *IEEE Access*, vol. 9, pp. 156114-156150, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] Junyu Ren et al., “Task Offloading Strategy with Emergency Handling and Blockchain Security in SDN-Empowered and Fog-Assisted Healthcare IoT,” *Tsinghua Science and Technology*, vol. 27, no. 4, pp. 760-776, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Antonio J. Cabrera-Gutierrez et al., “Integration of Hardware Security Modules and Permissioned Blockchain in Industrial IoT Networks,” *IEEE Access*, vol. 10, pp. 114331-114345, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Yunyeong Goh et al., “Secure Trust-Based Delegated Consensus for Blockchain Frameworks Using Deep Reinforcement Learning,” *IEEE Access*, vol. 10, pp. 118498-118511, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] P. Muralidhara Rao et al., “Blockchain Integration for IoT-Enabled V2X Communications: A Comprehensive Survey, Security Issues and Challenges,” *IEEE Access*, vol. 11, pp. 54476-54494, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Garima Thakur et al., “An Effective Privacy-Preserving Blockchain-Assisted Security Protocol for Cloud-Based Digital Twin Environment,” *IEEE Access*, vol. 11, pp. 26877-26892, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Leonardo Da Costa et al., “Sec-Health: A Blockchain-Based Protocol for Securing Health Records,” *IEEE Access*, vol. 11, pp. 16605-16620, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Md. Riyazuddin, and V.V.S.S.S. Balaram, “Diversity Scale by Supervised Learning for Privacy Preserved and Informative Data Publishing,” *Parishod Journal*, vol. 9, no. 2, pp. 872-886, 2020. [Google Scholar] [Publisher Link]

[14] S. Rajaprakash et al., “RBJ25 Cryptography Algorithm For Securing Big Data,” *Journal of Physics: Conference Series*, vol. 1706, pp. 1-8, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] C. Bagath Basha et al., “The Design of Security Algorithm RPBB-24-1 in Multi-Way Path over the Distributed Ledger,” *SSRG International Journal of Electrical and Electronics Engineering*, vol. 11, no. 4, pp. 36-44, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] Bagath Basha Chan Batcha et al., “A Novel Security Algorithm RPBB31 for Securing the Social Media Analyzed Data Using Machine Learning Algorithms,” *Wireless Personal Communications*, vol. 131, pp. 581-608, 2023. [CrossRef] [Google Scholar] [Publisher Link]