SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V11I4P105

Volume 11 Issue 4, 36-44, April 2024

Original Article

The Design of Security Algorithm RPBB-24-1 in Multi-Way Path over the Distributed Ledger

C. Bagath Basha[1], S. Rajaprakash[2], Nitisha Aggarwal[3], MD Riyazuddin[4], G. Sujatha[5], K. Karthik[6]

[1,5]*Department of Computer Science & Engineering, Kommuri Pratap Reddy Institute of Technology, Autonomous, Telangana, India.*
[2,6]*Department of Computer Science & Engineering, Aarupadai Veedu Institute of Technology, Vinayaka Missions Research Foundation, Tamil Nadu, India.*
[3]*Department of Information Technology, Panipat Institute of Engineering Technology, Haryana, India.*
[4]*Department of Information Technology, Anurag University, Telangana, India.*

[1]*Corresponding Author : chan.bagath@gamil.com*

Received: 05 February 2024 Revised: 05 March 2024 Accepted: 03 April 2024 Published: 30 April 2024

Abstract *- Block Chain is one of the technologies that is gaining popularity in the modern world. The technology in question offers an exceptionally robust level of protection. Users do not have a lot of information about Block Chain, but its security is used to safeguard the data that is sent in several directions. This user continued to utilize the "ChaCha" and RBJ25 algorithms, which are considered to be compact and secure varieties. In this article, we present the new security mechanism that we have decided to call RPBB24-1. Two components make up the RPBB-24-1 approach, which are encryption and decryption. Five stages are involved in the encryption procedure. Assignment of the "Latin Alphabet cod" to PT is the first step in the procedure. Multiplying the number by itself four times using Equation (1) is the second step. Using encrypted data, the third procedure involves swapping the cell values, but the process begins with the 0th cell value from the most recent cell value. The fourth step involves dividing the prime key into the values of the matrix cells. Implementing the "ChaCha" algorithm in the matrix is the fifth step in the procedure. At long last, the ordinary text is transformed into encrypted text. Unlike the encryption procedure, the decryption approach works in the opposite direction. When compared to the approach that is currently in use, the suggested method offers a higher level of security.*

Keywords *- Blockchain, ChaCha, Decryption, Encryption, Performance, RBJ25, RPBB-24-1.*

1. Introduction

Blockchain (BC) technology, which is a decentralized digital ledger system that securely preserves an ever-increasing quantity of data records and transactions, has recently garnered a large amount of interest all around the globe. The public or unauthenticated, the private or authenticated, and the consortium are the three basic characteristics that apply to the accessibility and identification of British Columbia information.

The notion of blockchain is differentiated by its major and distinguishing characteristic, which is the total security of information that is held inside the blocks included within blockchain transactions. There have been several fields in which BC technology has been successfully deployed. When it comes to the use of BC technology for the purpose of exchanging and sharing "network data, records, validation, and security services," an ongoing study is being carried out on the subject of security in the Internet of Things (IoT) sector. There are now a number of organizations that have been granted accreditation working towards the goal of ensuring that the Internet of Things network is compatible, secure, and private.

Blockchain technology is causing a revolution in data modeling, and governments have already used blockchain technology in a number of Internet of Things applications. Because of its remarkable versatility, segmentation, security, and sharing characteristics, it is particularly tempting for a wide variety of applications that fall within the Internet of Things domain. In the Internet of Things (IoT) sector, blockchain technology is playing a crucial part in a number of emerging trends and developments. The fact that a number of Internet of Things services are vulnerable to attacks as well as difficulties is one of the factors that contribute to this problem.

As shown in Figure 1, anonymity is an essential component of blockchain technology played a significant role in maintaining the secrecy of transactions that take place inside networks.

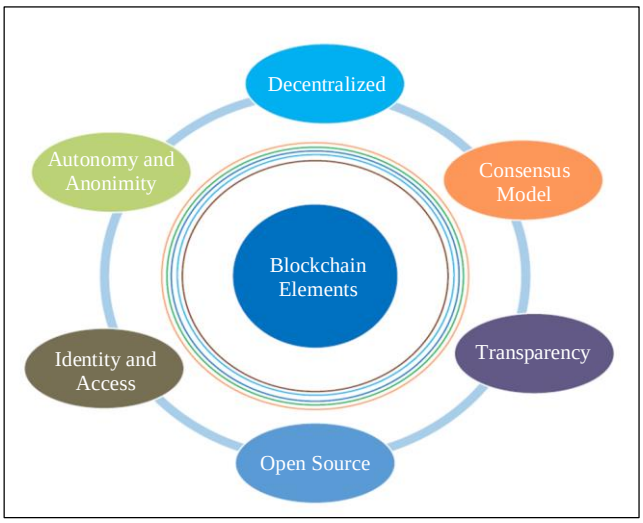

Fig. 1 The elements of blockchain

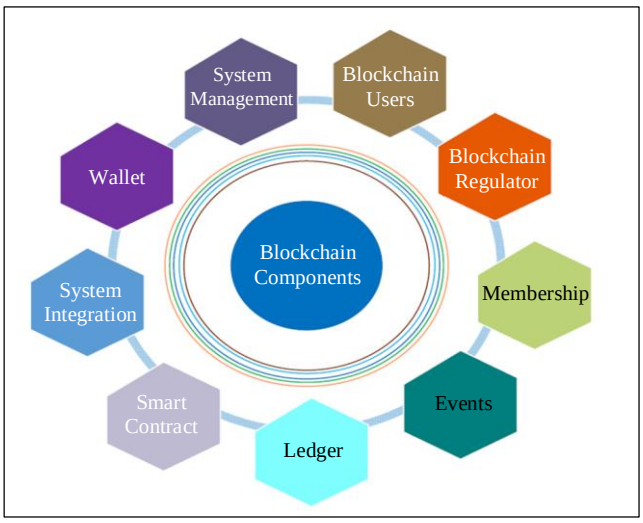

Fig. 2 The components of blockchain

The public nature of the blockchain ledger, on the other hand, makes it difficult to maintain anonymity via the blockchain. In addition, there is no structure in place to guarantee the privacy of user information, and each user is responsible for creating their own address.

In order to improve the privacy of Bitcoin transactions, a specialized Bitcoin mixing service was developed and made available. This service has the power to obscure or perplex the original Bitcoin transaction addresses, which results in an increase in the degree of anonymity. When it comes to blockchain technology, one of the most significant security considerations is the need to make certain that public keys and transactions do not reveal genuine identities.

The diagram in Figure 2 illustrates a wide variety of essential components that make up a blockchain. The descriptions that follow give in-depth explanations for each individual component. A ledger is a database that stores the most recent global status of the transactions performed on a blockchain. In the context of a business network, a smart contract is a piece of code that encapsulates the transactions that it processes.

The retrieval and setting of the ledger state are both triggered by a transaction call. A collection of peers that works together to reliably keep a replicated ledger updated via the use of data and processing constitutes a consensus network. In addition to overseeing the administration of identity and transactional certificates, membership is responsible for overseeing other aspects that are associated with access rights.

Events are notifications that are generated on major actions that occur inside the blockchain, such as the generation of new blocks. Additionally, events may provide notifications that apply to smart contracts that do not include event dissemination.

The development, modification, and monitoring of blockchain components are all made possible via the administration of the system. The wallet is able to manage and protect security credentials in an efficient manner. System Integration: This department is in charge of ensuring that blockchains are seamlessly integrated with external systems, which enables communication in both directions.

2. Literature Survey

In the year 2021, Saurabh Singh and his colleagues had a discussion regarding a variety of “Blockchain security issues such as transactions, network security, and privacy” [1]. In the year 2021, Bhutta and colleagues conducted research on the several uses of blockchain technology in the cryptocurrency known as “Bitcoin”, as well as the difficulties associated with the danger of blockchain security [2].

During the year 2021, Iqbal and his colleagues conducted research on the management of risks associated with blockchain technology. The primary emphasis of their investigation was on two dangers, namely “Sybil” and “double-spending” [3]. Rathore et al. have the idea that blockchain technology with Deep Learning (DL) may provide security. The data will be analyzed using the DL technique, and then predictions will be made using the data. The data will then be utilized to offer security using Blockchain technology [4].

R. A. Mallah and colleagues have examined the security risks associated with blockchain technology and conducted an examination of the numerous mobile risks associated with blockchain [5]. This author, E. A. Shammar et al., investigates the many publications written about blockchain technology with the objective of conducting a survey in the field of security [6]. Among the writers who put up the idea of the blockchain was Junyu Ren and his colleagues. At one point in time, this program was able to cut down on latency [7].

The algorithm of cryptography was the primary topic of discussion among A. J. Cabrera-Gutiérrez and his colleagues in the year 2022. An algorithm that was used to enhance the overall security of the Internet of Things business [8]. Y. Goh and his colleagues, along with other writers, came up with the TDCB D3P approach in the year 2022. Through the use of this technology, harmful activity can be effectively reduced, and the overall network's security may be improved [9]. During the year 2023, P. M. Rao and his colleagues focused their research mostly on the storage, 5G, Internet of Things, V2X, and security of blockchain technology.

In order to concentrate primarily on the survey of technologies that are in between, these technologies are used [10]. When it comes to the "Digital Twin (DT)" environment, the author examines G. Thakur and his colleagues. [11] This environment was used for the purpose of conducting a rigorous investigation of the security of blockchain. "Sec-health" is a technique that was suggested by L. D. Costa and colleagues, and it is based on blockchain technology.

In order to increase the time access in health records and minimize the amount of memory work that is done on the client side, this strategy is used [12]. The author, L. Li, D. Jin, and others, concentrated their attention primarily on the storage in blockchain. This storing approach is used to enhance the support for faults and to give a high level of security [13].

Based on the previously presented work, the "RBJ25" approach, which offers improved security. This author, primarily concentrated on the security of encryption, and the solution that was presented is SRB18. This technique was used to deliver a high level of encryption security at a decent speed.

This author, together with other researchers, conducted research on the seven-stage security approach of RPBB31. The authors, examined ways to increase the level of performance and security. On the basis of the literature review, we are going to present the RajaprakashBagathbasha-24 (RPBB-24-1) approach that has been suggested.

3. Methodology

The RPBB-24-1 methodology has two parts: encryption and decryption. The encryption method has 5 processes. The 1st process is to assign the "Latin Alphabet code" to PT. The 2nd process is to multiply the 4 times using Equation (1). The 3rd process is to swap the cell values using Encrypted data but start the 0th cell value from the last cell value. The 4th process is to divide the prime key in matrix cell values. The 5th process is to apply the "ChaCha" method in the matrix. Finally, the plain text is converted to cipher text, as shown in Figure 4. The decryption method is the reverse of the encryption process.

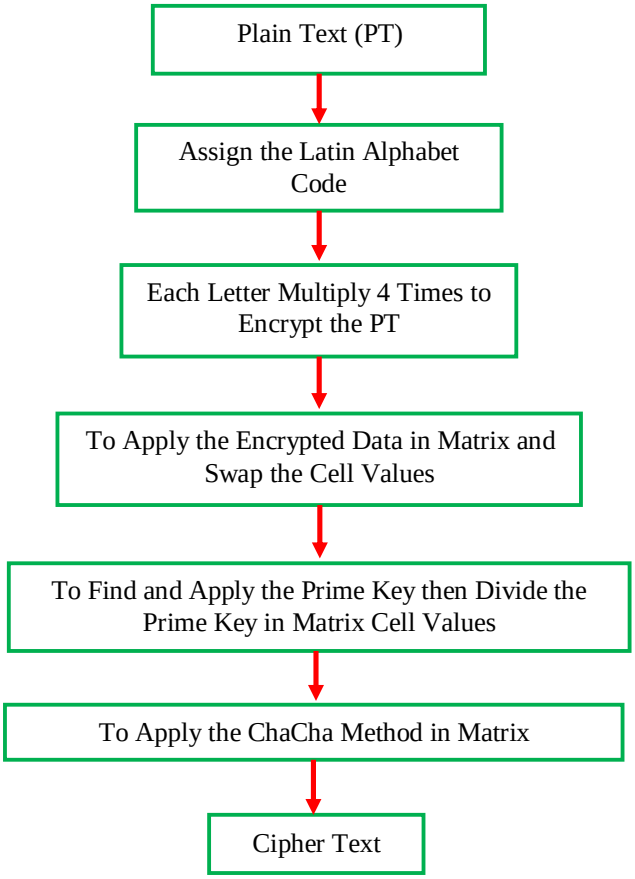

Fig. 3 RPBB-24-1 methodology

3.1. Encryption Algorithm

1. First, we have chosen a secret message as PT.
2. Apply the "Latin alphabet" for PT and convert it to numbers.
3. Each letter number multiply the 4 times to encrypt the PT.

$$
\begin{aligned}
&\text{if } i < n \text{ Then} \\
&C_i - PT_n \\
&C_{ij} = C_{ij} * C_{ij} = R_i * \\
&C_{ij} = (R_i *) * C_{ij} = R_i * \\
&C_{ij} = (R_i *) * C_{ij} = R_i * \\
&C_{ij} = (R_i *) * C_{ij} = R_i * \\
&\text{Where C is Character and R is Remaind} \\
&\qquad i = 0, i = i + 1 \text{ to } n,\ j = j + 1,\ j = 0 \\
&\qquad \text{and } n = \text{number of charaters} \\
&\text{else} \\
&i > n \text{ then Stop } i
\end{aligned}
\tag{1}
$$

4. To apply the encrypted values in matrix A to swap the values, but cell number 0 start from reverse.

5. To find the prime number from the encrypted code or the nearest prime number in the middle letter code.
6. Apply the prime number in matrix A and divide the cell values with the prime key.
7. To apply the ChaCha method in matrix A.

3.2. Decryption Algorithm

1. First, we have to receive a Cipher Text message from the user as CC.
2. Apply the ChaCha Method in matrix CC.
3. Apply the secret prime key in matrix PT and divide the cell values with the prime key.
4. Apply the "Latin alphabet" for the CT message and convert it to numbers.
5. Each letter number is multiplied 4 times to decrypt the CT.

$$\text{if } i < n \text{ Then}$$

$$P_i - CT_n$$

$$P_{i\,j} = P_{i\,j} * P_{i\,j} = R_i *$$

$$P_{i\,j} = (R_i *) * P_{i\,j} = R_i *$$

$$P_{i\,j} = (R_i *) * P_{i\,j} = R_i *$$

$$P_{i\,j} = (R_i *) * P_{i\,j} = R_i * \qquad (2)$$

Where P is Character and R is Remainder

$$i = 0, i = i + 1 \text{ to } n,\ j = j + 1,\ j = 0$$

$$\text{and } n = \text{number of charaters}$$

$$\text{else}$$

$$i > n \text{ then Stop } i$$

6. To apply the decrypted values in matrix PT to swap the values, but cell number 0 start from the reverse.

4. Result & Discussion

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

4.1. Working for Encryption

- PT = BLOCK
  $B-66, L-76, O-79, C-67, K-75$
- $PT = 6676796775$
- Apply Equation 1 to encrypt the PT.

4.1.1. First Character - B=66

$i = 1, j = 1$

$C_{11} = PT_5$

$B = 66$

$C_{11} = 66 * 66$

$C_{11} = 4356/91 \Rightarrow 79$

$j = 2$

$C_{12} = 79 * 66$

$C_{12} = 5214/91 \Rightarrow 27$

$j = 3$

$C_{13} = 27 * 66$

$C_{13} = 1782/91 \Rightarrow 53$

$j = 4$

$C_{14} = 53 * 66$

$C_{14} = 3498/91 \Rightarrow 40$

$C_{14} = 40$

4.1.2. Second Character - L= 76

$i = i + 1,$

$i = 1 + 1 = 2$

$i = 2, j = 1$

$C_{21} = PT_5$

$L = 76, j = 1$

$C_{21} = 76 * 76$

$C_{21} = 5776/91 \Rightarrow 43$

$j = 2$

$C_{22} = 43 * 76$

$C_{22} = 3268/91 \Rightarrow 83$

$j = 3$

$C_{23} = 83 * 76$

$C_{23} = 6308/91 \Rightarrow 29$

$j = 4$

$C_{24} = 29 * 76$

$C_{24} = 2204/91 \Rightarrow 20$

$C_{24} = 20$

4.1.3. Third Character - O= 79

$i = i + 1,$

$i = 2 + 1 = 3$

$i = 3, j = 1$

$C_{31} = PT_5$

$O = 79, j = 1$

$C_{21} = 79 * 79$

$C_{21} = 6241/91 \Rightarrow 53$

$j = 2$

$C_{32} = 53 * 79$

$C_{32} = 4187/91 \Rightarrow 1$

$j = 3$

$C_{33} = 1 * 79$

$C_{33} = 79/91 \Rightarrow 79$

$j = 4$

$C_{34} = 79 * 79$

$C_{34} = 6241/91 \Rightarrow 53$

$C_{34} = 53$

4.1.4. Fourth Character - C= 67

$i = i + 1,$

$i = 3 + 1 = 4$

$i = 4\ j = 1$

$C_{41} = PT_5$

$C = 67,\ j = 1$

$C_{41} = 67 * 67$

$C_{41} = 4489 / 91 \Rightarrow 30$

$j = 2$

$C_{42} = 30 * 67$

$C_{42} = 2010 / 91 \Rightarrow 8$

$j = 3$

$C_{43} = 8 * 67$

$C_{43} = 536 / 91 \Rightarrow 81$

$j = 4$

$C_{44} = 81 * 67$

$C_{44} = 5427 / 91 \Rightarrow 58$

$C_{44} = 58$

4.1.5. Fifth Character - K= 75

$i = i + 1,$

$i = 4 + 1 = 5$

$i = 5\ j = 1$

$C_{51} = PT_5$

$K = 75,\ j = 1$

$C_{51} = 75 * 75$

$C_{51} = 5625 / 91 \Rightarrow 74$

$j = 2$

$C_{52} = 74 * 75$

$C_{52} = 5550 / 91 \Rightarrow 90$

$j = 3$

$C_{53} = 90 * 75$

$C_{53} = 6750 / 91 \Rightarrow 16$

$j = 4$

$C_{54} = 16 * 75$

$C_{54} = 1200 / 91 \Rightarrow 17$

$C_{54} = 17$

- CT=4020535817
- To make a pair and apply the encrypted code in Matrix A, but 0 starts from reverse.

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

- CT pair is (4,0), (2,0), (5,3), (5,8), (1,7)
- The 1st swap values (4,0)

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

- The 2nd swap values (2,0)

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

- The 3rd swap values (5,3)

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

- The 4th swap values (5,8)

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

- The 5th swap values (1,7)

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

- Now, apply the prime key in the CT Matrix.

$$CTP=\begin{bmatrix} \frac{PT_{11}}{79} & \frac{PT_{12}}{79} & \frac{PT_{13}}{79} & \frac{PT_{14}}{79} \\ \frac{PT_{21}}{79} & \frac{PT_{22}}{79} & \frac{PT_{23}}{79} & \frac{PT_{41}}{79} \\ \frac{PT_{43}}{79} & \frac{PT_{32}}{79} & \frac{PT_{24}}{79} & \frac{PT_{44}}{79} \\ \frac{PT_{33}}{79} & \frac{PT_{34}}{79} & \frac{PT_{31}}{79} & \frac{PT_{42}}{79} \end{bmatrix}$$

- Now apply the “ChaCha” Method in the CTP matrix.

$$CC=\begin{bmatrix} \frac{PT_{14}}{79} & \frac{PT_{13}}{79} & \frac{PT_{12}}{79} & \frac{PT_{11}}{79} \\ \frac{PT_{41}}{79} & \frac{PT_{23}}{79} & \frac{PT_{22}}{79} & \frac{PT_{21}}{79} \\ \frac{PT_{44}}{79} & \frac{PT_{24}}{79} & \frac{PT_{32}}{79} & \frac{PT_{43}}{79} \\ \frac{PT_{42}}{79} & \frac{PT_{31}}{79} & \frac{PT_{34}}{79} & \frac{PT_{33}}{79} \end{bmatrix}$$

4.2. Working for Decryption

$$CC=\begin{bmatrix} \frac{PT_{14}}{79} & \frac{PT_{13}}{79} & \frac{PT_{12}}{79} & \frac{PT_{11}}{79} \\ \frac{PT_{41}}{79} & \frac{PT_{23}}{79} & \frac{PT_{22}}{79} & \frac{PT_{21}}{79} \\ \frac{PT_{44}}{79} & \frac{PT_{24}}{79} & \frac{PT_{32}}{79} & \frac{PT_{43}}{79} \\ \frac{PT_{42}}{79} & \frac{PT_{31}}{79} & \frac{PT_{34}}{79} & \frac{PT_{33}}{79} \end{bmatrix}$$

- Now apply the "ChaCha" Method in the CC matrix.

$$PT=\begin{bmatrix} \frac{PT_{11}}{79} & \frac{PT_{12}}{79} & \frac{PT_{13}}{79} & \frac{PT_{14}}{79} \\ \frac{PT_{21}}{79} & \frac{PT_{22}}{79} & \frac{PT_{23}}{79} & \frac{PT_{41}}{79} \\ \frac{PT_{43}}{79} & \frac{PT_{32}}{79} & \frac{PT_{24}}{79} & \frac{PT_{44}}{79} \\ \frac{PT_{33}}{79} & \frac{PT_{34}}{79} & \frac{PT_{31}}{79} & \frac{PT_{42}}{79} \end{bmatrix}$$

- Now apply the prime key 79 in the CT Matrix.

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

- PT = KCOLB
  $K-75, C-67, O-79, L-76, B-66$
- $PT = 7567797666$
- Apply Equation 2 to decrypt the PT.

4.2.1. First Character - K=75

$i=1,\ j=1$

$P_{11}=CT_5$

$K=75$

$P_{11}=75*75$

$P_{11}=5625/91 \Rightarrow 74$

$j=2$

$P_{12}=74*75$

$P_{12}=5550/91 \Rightarrow 90$

$j=3$

$P_{13}=90*75$

$P_{13}=6750/91 \Rightarrow 16$

$j=4$

$P_{14}=16*75$

$P_{14}=1200/91 \Rightarrow 17$

$P_{14}=17$

4.2.2. Second Character - C= 67

$i=i+1,$

$i=1+1=2$

$i=2,\ j=1$

$P_{21}=CT_5$

$C=67,\ j=1$

$P_{21}=67*67$

$P_{21}=4489/91 \Rightarrow 30$

$j=2$

$P_{22}=30*67$

$P_{22}=2010/91 \Rightarrow 8$

$j=3$

$P_{23}=8*67$

$P_{23}=536/91 \Rightarrow 81$

$j=4$

$P_{24}=81*67$

$P_{24}=5427/91 \Rightarrow 58$

$P_{24}=58$

4.2.3. Third Character - O= 79

$i=i+1,$

$i=2+1=3$

$i=3,\ j=1$

$P_{31}=CT_5$

$O=79,\ j=1$

$P_{21}=79*79$

$P_{21}=6241/91 \Rightarrow 53$

$j=2$

$P_{32}=53*79$

$P_{32}=4187/91 \Rightarrow 1$

$j=3$

$P_{33}=1*79$

$P_{33}=79/91 \Rightarrow 79$

$j=4$

$P_{34}=79*79$

$P_{34}=6241/91 \Rightarrow 53$

$P_{34}=53$

4.2.4. Fourth Character - L= 76

$i=i+1,$

$i=3+1=4$

$i=4\ j=1$

$P_{41}=PT_5$

$L=76,\ j=1$

$P_{41}=76*76$

$P_{41}=5776/91 \Rightarrow 43$

$j=2$

$P_{42}=73*76$

$P_{42}=3268/91 \Rightarrow 83$

$j=3$

$P_{43}=83*76$

$P_{43}=6308/91 \Rightarrow 29$

$j=4$

$P_{44}=29*76$

$P_{44}=2204/91 \Rightarrow 20$

$P_{44}=20$

4.2.5. Fifth Character - B= 66

$i = i + 1,$

$i = 4 + 1 = 5$

$i = 5\ j = 1$

$P_{51} = CT_5$

$B = 66,\ j = 1$

$P_{51} = 66 * 66$

$P_{51} = 4356 / 91 \Rightarrow 79$

$j = 2$

$P_{52} = 79 * 66$

$P_{52} = 5214 / 91 \Rightarrow 27$

$j = 3$

$P_{53} = 27 * 66$

$P_{53} = 1782 / 91 \Rightarrow 53$

$j = 4$

$P_{54} = 53 * 66$

$P_{54} = 3498 / 91 \Rightarrow 40$

$P_{54} = 40$

- PT=1758532040
- To make a pair and apply the encrypted code in Matrix A, but 0 starts from reverse.
- PT pair is (1,7), (5,8), (5,3), (2,0), (4,0)
- The 1st swap values (1,7)

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

- The 2nd swap values (5,8)

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

- The 3rd swap values (5,3)

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

- The 4th swap values (2,0)

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

- The 5th swap values (4,0)

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

Table 1. RPBB-24-1 encryption performance

File Size (Bytes)	ChaCha	RBJ25	RPBB-24-1
25	1.69	2.2	2.9
77	1.29	2.6	3.5
110	1.09	3.4	4.1
311	2.73	4.5	4.9
811	2.64	5.3	5.8
1521	3.4	5.5	6.1
6580	2.27	6.8	7.2

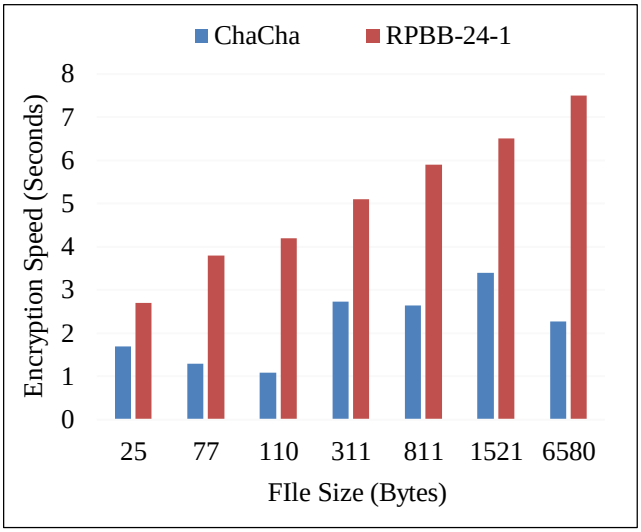

Fig. 4 ChaCha vs. RPBB-24-1 encryption speed

Table 1 shows the comparison of 3 encryption speeds. The proposed method RPBB-24-1 shows good performance of speed when compared to other methods. The proposed method RPBB-24-1 is the performance of the speed 2.9, 3.5,4.1,4.9,5.8,6.1,7.2 in different file sizes good when compared to the existing methods are "ChaCha" in Figure 4, "RBJ25" in Figure 5 and RPBB-24-1 in Figure 6.

Table 2 shows the comparison of 3 decryption speeds. The proposed method RPBB-24-1 shows good performance of speed when compared to other methods. The proposed method RPBB-24-1 is the performance of the speeds 3.1, 3.7, 4.3, 4.7, 5.1, 5.5, 6.2 in different file sizes good when compared to the existing methods are "ChaCha" in Figure 7, "RBJ25" in Figure 8 and RPBB-24-1 in Figure 9.

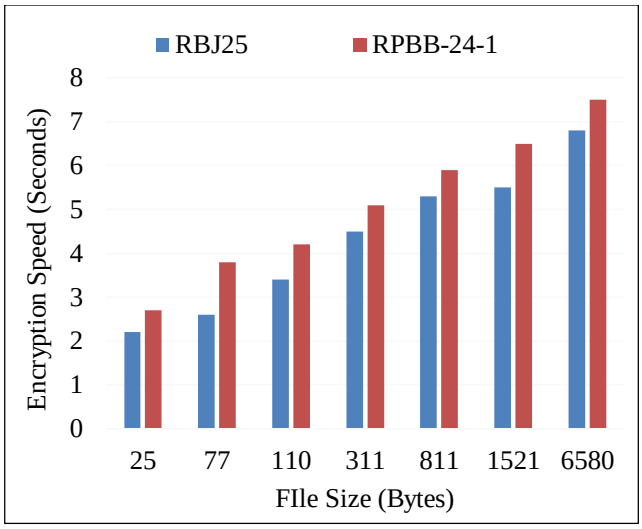

Fig. 5 RBJ25 vs. RPBB-24-1 encryption speed

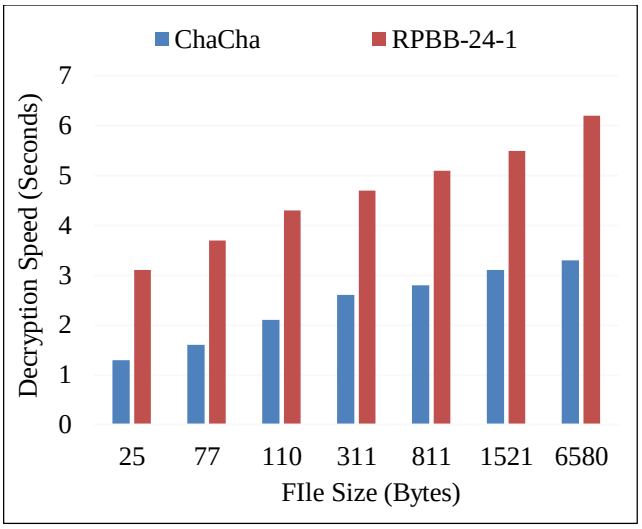

Fig. 7 ChaCha vs. RPBB-24-1 decryption speed

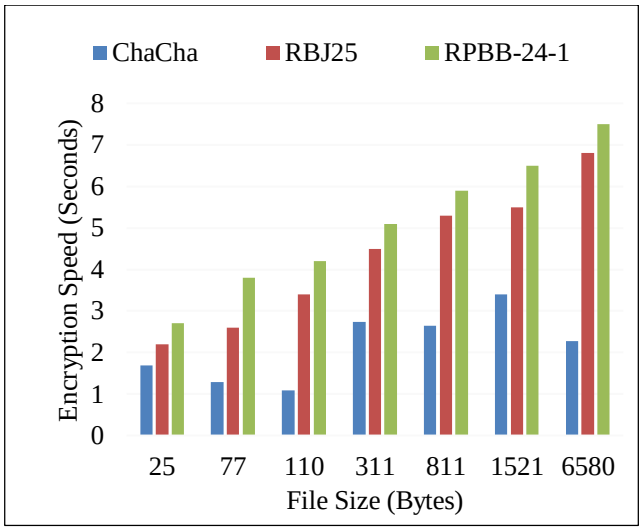

Fig. 6 RPBB-24-1 encryption speed

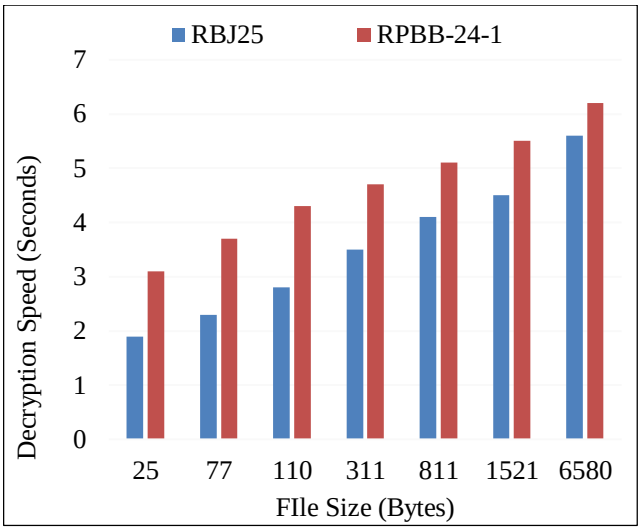

Fig. 8 RBJ25 vs. RPBB-24-1 decryption speed

Table 2. RPBB-24-1 decryption performance

File Size (Bytes)	ChaCha	RBJ25	RPBB-24-1
25	1.3	1.9	3.1
77	1.6	2.3	3.7
110	2.1	2.8	4.3
311	2.6	3.5	4.7
811	2.8	4.1	5.1
1521	3.1	4.5	5.5
6580	3.3	5.6	6.2

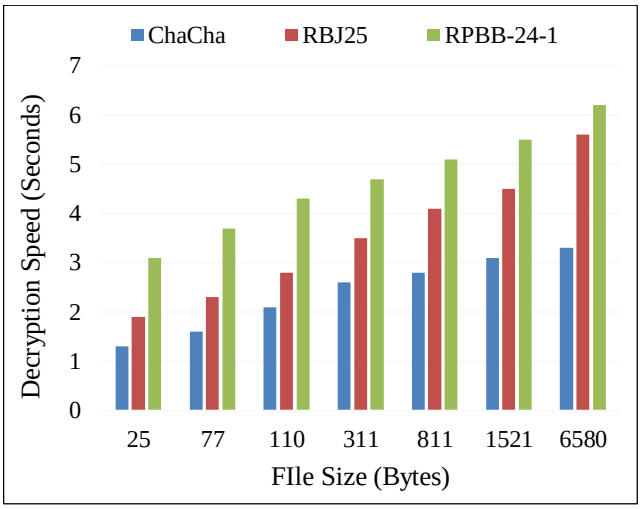

Fig. 9 RPBB-24-1 decryption speed

5. Conclusion

Block Chain is one of the technologies that is one of the most rapidly increasing in the globe. Despite the fact that consumers are not aware of Block Chain, this technology is used to ensure the safety of various data locations. “ChaCha” and “RBJ25” are the names of the minor level of security algorithms that continue to be used by this sort of user.

The RPBB-24-1 security approach is the one that is being offered in this study. Two components, namely encryption and decryption, are included in the RPBB-24-1 approach. The technique of encryption has five different procedures. Within the first step of the procedure, the “Latin Alphabet code” is assigned to PT. Equation (1) is used to perform the second step, which is to multiply the number four times.

The third step involves exchanging the values of the cells with encrypted data, beginning with the value of the 0th cell from the value of the previous cell. The prime key is divided into the values of the matrix cells, which is the fourth procedure. The “ChaCha” approach is used in the matrix, which is the fifth step in the procedure. The ordinary text is finally transformed into encrypted text. This means that the procedure of decryption is the opposite of the encryption approach. When compared to the approach that is currently in use, the suggested method offers a higher level of security.

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 López, 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-Gutiérrez 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] Lina Li et al., “A Secure, Reliable and Low-Cost Distributed Storage Scheme Based on Blockchain and IPFS for Firefighting IoT Data,” *IEEE Access*, vol. 11, pp. 97318-97330, 2023. [CrossRef] [Google Scholar] [Publisher Link]