SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V11I7P125

Volume 11 Issue 7, 280-290, July 2024

Original Article

Blockchain Security System in Multi-Way Direction over Distributed System Using RPBB-24-3 Algorithm

C. Bagath Basha[1], S. Rajaprakash[2], K. Karthik[3], M.D. Riyazuddin[4], S. Kavitha[5], T.K.S. Rathish Babu[6]

[1,5]*Department of Computer Science & Engineering, Kommuri Pratap Reddy Institute of Technology, Telangana, India.*
[2]*Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Tamil Nadu, India.*
[3]*Department of Computer Science & Engineering, Aarupadai Veedu Institute of Technology, Vinayaka Mission's Research Foundation (DU), Tamil Nadu, India.*
[4]*Department of Information Technology, Anurag University, Telangana, India.*
[6]*Department of Computer Science & Engineering, Sridevi Women's Engineering College, Telangana, India.*

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

Received: 12 May 2024 Revised: 14 June 2024 Accepted: 11 July 2024 Published: 26 July 2024

Abstract *- A number of technologies are gaining prominence in the current world, and one of such technologies is the Block Chain. The technology in issue provides an incredibly high degree of security; it is quite resilient. Users are not privy to a great deal of information about Block Chain; nonetheless, the functionality of its security is used to protect the data that is sent in several directions. This particular user proceeded to make use of the "Salsa" and RBJ25 algorithms, both of which are regarded as being compact and secure variations. Within the scope of this paper, we will introduce the new security mechanism that we have chosen to refer to as RPBB24-3. Encryption and decryption are the two components that comprise the RPBB-24-3 method. Both of these components are essential to the process. In order to complete the encryption process, there are five processes needed. In this process, the first step is to use the column functions on GT. The second step in the process is to use the "lattin letter" and multiply the value by four using Equation (1). The third step uses encrypted data to swap the cell values, but the process starts with the 0th cell value from the most recent cell value. In the fourth step, the prime key is split into the values of the matrix cells. The fifth step in the process is to use the "SalSa" method in the grid. Last but not least, the plain text is changed into secret text. The decryption process works the other way around from the encryption process. The suggested method is safer than the standard way that is being used.*

Keywords *- Blockchain, Decryption, Encryption, Performance, RBJ25, RPBB-24-3, Salsa.*

1. Introduction

Blockchain (BC) technology, which is a decentralized digital ledger system that securely retains an ever-growing number of data records and transactions, has lately received a significant amount of attention all over the world. The rising popularity of blockchain technology has fueled this interest. Three fundamental qualities pertain to the accessibility and identification of information belonging to the province of British Columbia. These characteristics are the public or unauthenticated, the private or authenticated, and the consortium. There is a significant and distinctive feature of blockchain that sets it apart from other concepts.

This feature is the complete safety of the information that is stored inside the blocks that are included in blockchain transactions. BC technology has been successfully used in a number of different sectors during its history. Concerning the use of BC technology for the purpose of exchanging and sharing "network data, records, validation, and security services," ongoing research is being conducted on the topic of security in the Internet of Things (IoT) sector. This study is being carried out while the problem is being investigated. There are currently a number of organizations that have been awarded accreditation and are working toward the objective of ensuring that the network that is used for the Internet of Things is compliant, safe, and private. There is already a revolution taking place in the field of data modeling as a result of blockchain technology, and governments have already used blockchain technology in a variety of Internet of Things applications.

It is especially appealing for a broad range of applications that come under the umbrella of the Internet of Things sector because of the exceptional adaptability, segmentation, security, and sharing properties that it has. The Internet of Things (IoT) industry is seeing a variety of new trends and advances, and blockchain technology is playing a significant role in supporting these changes. The fact that many services that are

connected to the Internet of Things are susceptible to assaults as well as challenges is one of the causes that add to the difficulty that we are experiencing.

The fact that anonymity is an important component of blockchain technology is shown in Figure 1. This component has played a key part in the process of preserving the confidentiality of transactions that take place inside networks. The public nature of the blockchain ledger, on the other hand, makes it impossible to retain anonymity via the use of the blockchain. Additionally, there is no structure in place to ensure the privacy of user information, and it is the responsibility of each user to initiate the creation of their specific address.

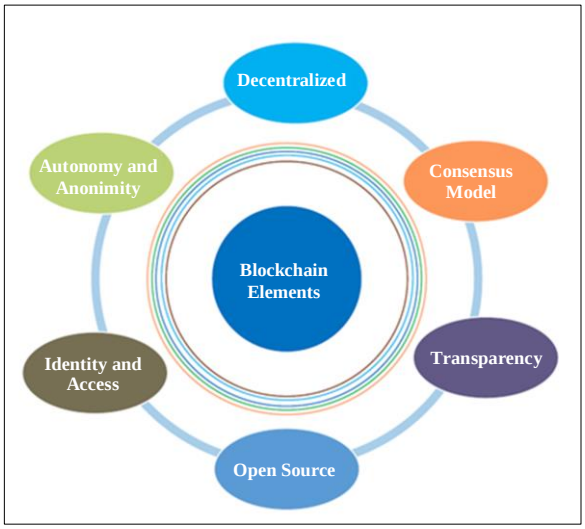

Fig. 1 The elements of blockchain

The development and availability of a dedicated Bitcoin mixing service was done with the intention of enhancing the level of secrecy associated with Bitcoin transactions. This service can disguise or confuse the addresses of the first Bitcoin transactions, which ultimately increases the level of anonymity. When it comes to blockchain technology, one of the most important security issues is the need to ensure that public keys and transactions do not expose true identities. This is one of the most important aspects of blockchain security.

Figure 2 is a graphic that displays a broad range of critical components that are necessary for the construction of a blockchain ecosystem. The following explanations provide detailed explanations for each component that is being discussed. When it comes to blockchain transactions, a ledger is a database that contains the most current global status of the transactions that have been carried out.

A piece of code that encapsulates the transactions that it processes is referred to as a smart contract when it is used in the context of a business application network. A transaction call is what causes both the retrieval of the ledger state and the setting of the ledger state to occur. A consensus network is a set of peers that collaborate in order to consistently keep a replicated ledger updated via the use of data and processing for the purpose of maintaining the ledger.

In addition to being responsible for monitoring the administration of identity and transactional certificates, membership is also accountable for overseeing other components that are linked with access permissions.

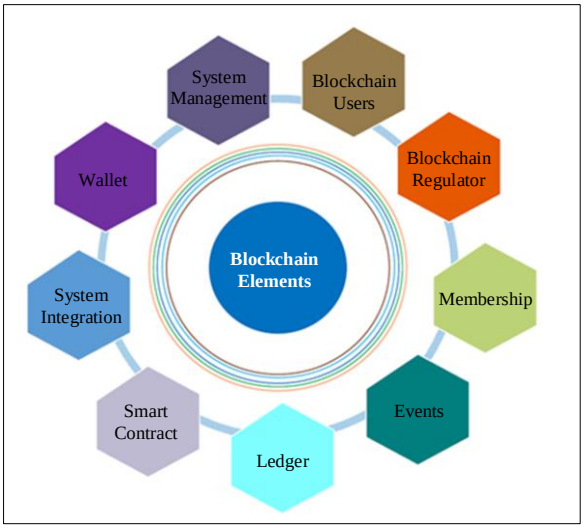

Fig. 2 The components of blockchain

There are a number of significant activities that take place inside the blockchain, such as the creation of new blocks, and events are alerts that are created on these big acts. Furthermore, alerts may be sent by events, and these notifications may be applicable to smart contracts that do not provide event dissemination options.

The management of the system makes it possible to engage in activities such as the construction, modification, and monitoring of components included in the blockchain. It is possible for the wallet to effectively maintain and safeguard security credentials efficiently. The department in charge of system integration is responsible for ensuring that blockchains are connected with external systems in a smooth manner, which permits communication in both ways.

2. Literature Survey

When Saurabh Singh and his colleagues got together in the year 2021, they had a conversation about a number of different “Blockchain security issues such as transactions, network security, and privacy” [1]. During the year 2021, Bhutta and her colleagues carried out a study on the many applications of blockchain technology in the cryptocurrency known as “Bitcoin,” as well as the challenges that are linked with the risk of blockchain security [2].

During the year 2021, Iqbal and his colleagues carried out a study on the management of risks that are related to the technology of blockchain. The two threats that were the major focus of their inquiry were referred to as "Sybil" and "double-spending" [3]. The concept that blockchain technology combined with Deep Learning (DL) may potentially offer security has been proposed by Rathore and others. First, the data will be examined using the DL approach, and then predictions will be created based on the data. Following that, the data will be employed to provide security via the utilization of Blockchain technology [4].

R. A. Mallah and his colleagues have investigated the multiple mobility dangers that are linked with blockchain technology [5]. Additionally, they have also investigated the security concerns that are involved with blockchain technology. This author, E. A. Shammar et al., explores the many articles that have been published on blockchain technology with the intention of carrying out a study on the subject of security [6].

A number of authors, including Junyu Ren and his colleagues, were among those who proposed the concept of the blockchain. This software was able to reduce the amount of delay that was experienced at one point in time [7]. When A. J. Cabrera-Gutiérrez and his colleagues got together in the year 2022, the algorithm of cryptography was the principal subject of conversation that they had. An algorithm was created in order to improve the overall security of the Internet of Things company [8].

It was in the year 2022 that Y. Goh and his colleagues, along with other authors, came up with the TDCB D3P method. The use of this technology may successfully minimize destructive activity, and the overall network's security may be enhanced as a result [9]. In the year 2023, P. M. Rao and his colleagues concentrated the majority of their research efforts on the storage, 5G, Internet of Things, V2X, and security aspects of blockchain technology. The use of these technologies is essential in order to focus largely on the survey of technologies that fall somewhere in the middle [10].

Within the context of the "Digital Twin (DT)" setting, the author investigates G. Thakur and the individuals he collaborates with. [11]. For the goal of carrying out a comprehensive examination of the safety of blockchain technology, this setting was used.

The term "Sec-health" refers to a method that L. D. Costa and his colleagues proposed. This method is based on the concepts of blockchain technology. This method is used in order to maximize the amount of time that may be spent accessing health information while simultaneously reducing the amount of memory work that is performed on the client's end [12].

In particular, the author, L. Li, D. Jin, and a few other individuals focused their attention on the storage that blockchain technology provides. In order to improve the support for faults and to provide a high degree of security [13], this storage strategy is used. This author offered the "RBJ25" strategy, which provides improvements in security. This approach was based on the work the second author and his colleagues had done.

The first author, particularly focussed on the security of encryption, and the solution that was offered is RPBB-24-1. Research on the five-stage security technique of RPBB31 was carried out by the author, Batcha, B.B.C., in collaboration with colleagues from different research institutions. As a result of the examination of the relevant literature, we are going to offer the RajaprakashBagathbasha-24 (RPBB-24-3) technique that has been proposed.

3. Methodology

The RPBB-24-3 method is made up of two parts: encryption and decoding. The encryption process is made up of five steps. In this process, the first step is to use the column functions on GT. The second step in the process is to use the "lattin letter" and multiply the value by four using Equation (1). The third step uses encrypted data to swap the cell values, but the process starts with the 0th cell value from the most recent cell value. In the fourth step, the prime key is split into the values of the matrix cells. The fifth 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 3. The decryption process works the other way around from the encryption process.

3.1. Encryption Algorithm

1. Apply the column operations in the 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.

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

$$T_a - GT_n$$

$$T_{a\,b} = T_{a\,b} * \; T_{a\,b} = R_a * \qquad (1)$$

$$T_{a\,b} = (R_a *) * T_{a\,b} = R_a *$$

$$T_{a\,b} = (R_a *) * T_{a\,b} = R_a *$$

$$T_{a\,b} = (R_i *) * T_{i\,j} = R_i *$$

$$\text{Where T is Character and R is Remainder}$$

$$a = 0, a = a + 1 \text{ to } n, b = b + 1, b = 0$$

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

$$\text{else}$$

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

5. To apply the encrypted values in matrix A for swap the values, but cell number 0 starts from reverse.

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

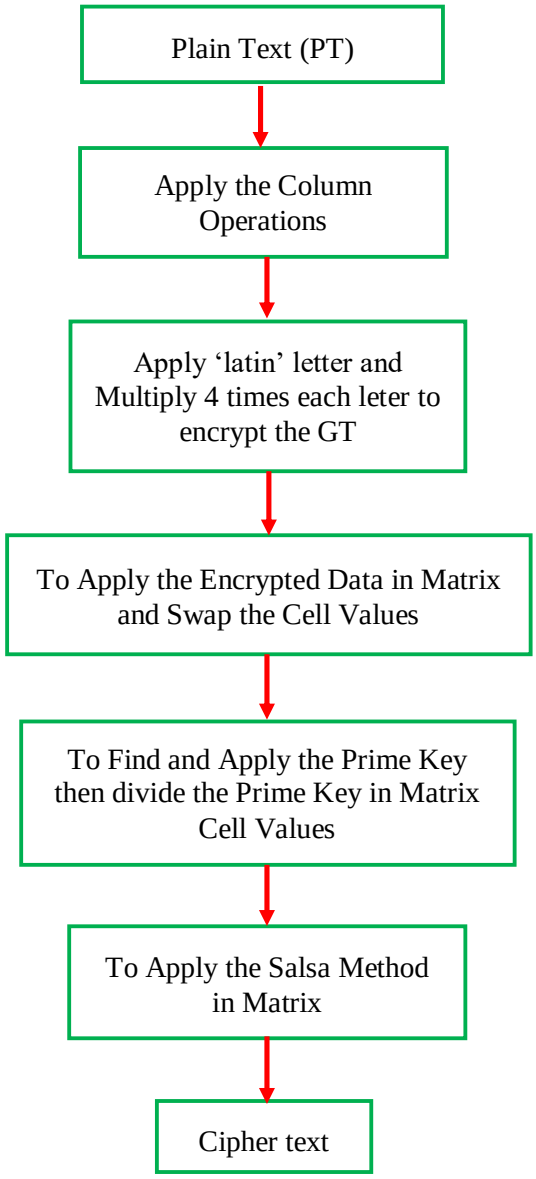

Fig. 3 RPBB-24-3 methodology

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 secret prime key in matrix DT and divide the cell values with the prime key.
4. Apply the "Latin alphabet" for the DT message and convert it to numbers.
5. Each letter number is multiplied 4 times to decrypt the DT.

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

6. To apply the decrypted values in matrix DT for swap the values, but cell number 0 starts from reverse.
7. Finally, apply the column operations in the DT matrix.

4. Result and Discussion

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

4.1. Working for Encryption

4.1.1. Step 1 - Apply the column operations in matrix A

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

4.1.2. Step 2 - To Convert the Number from the Given Text as GT

- GT = MICROSOFT
  $M-77, I-73, C-67, R-82, O-79, S-83, O-79,$
- $F-70, T-84$
  $GT = 77736782\ 7983797084$
- Apply Equation 1 to encrypt the PT.

First Character - M=77

$a = 1, b = 1$

$T_{11} = GT_9$

- $M = 77$

$T_{11} = 77 * 77$

$T_{11} = 5929/91 \Rightarrow 14$

$b = 2$
$T_{12} = 14 * 77$
$T_{12} = 1078/91 \Rightarrow 77$
$b = 3$
- $T_{13} = 77 * 77$
$T_{13} = 5929/91 \Rightarrow 14$
$a = 4$
$T_{14} = 14 * 77$
$T_{14} = 1078/91 \Rightarrow 77$
$T_{14} = 77$

Second Character - I= 73

$a = a + 1,$
$a = 1 + 1 = 2$
$a = 2, b = 1$
- $T_{21} = GT_9$
$I = 73, b = 1$
$T_{21} = 73 * 73$
$T_{21} = 5329/91 \Rightarrow 51$

$b = 2$
$T_{22} = 51 * 73$
$T_{22} = 3723/91 \Rightarrow 83$
$b = 3$
$T_{23} = 83 * 73$
$T_{23} = 6059/91 \Rightarrow 53$
$b = 4$
$T_{24} = 53 * 73$
$T_{24} = 3869/91 \Rightarrow 47$
$T_{24} = 47$

Third Character - C= 67

$a = a + 1,$
$a = 2 + 1 = 3$
$a = 3,\ b = 1$
- $T_{31} = GT_9$
$T = 67, b = 1$
$T_{31} = 67 * 67$
$T_{31} = 4489/91 \Rightarrow 30$

$b = 2$
$T_{32} = 30 * 67$
$T_{32} = 2010/91 \Rightarrow 8$
$b = 3$
$T_{33} = 8 * 67$
$T_{33} = 536/91 \Rightarrow 81$
$b = 4$
$T_{34} = 81 * 67$
$T_{34} = 5427/91 \Rightarrow 58$
$T_{34} = 58$

Fourth Character - R= 82

$a = a + 1,$
$a = 3 + 1 = 4$
$a = 4,\ b = 1$
- $T_{41} = GT_9$
$T = 82, b = 1$
$T_{41} = 82 * 82$
$T_{41} = 6724/91 \Rightarrow 81$

$b = 2$
$T_{42} = 81 * 82$
$T_{42} = 6642/91 \Rightarrow 90$
$b = 3$
- $T_{43} = 90 * 82$
$T_{43} = 7380/91 \Rightarrow 9$
$b = 4$
$T_{44} = 9 * 82$
$T_{44} = 738/91 \Rightarrow 10$
$T_{44} = 10$

Fifth Character - O= 79

$a = a + 1,$
$a = 4 + 1 = 5$
$a = 5, b = 1$
- $T_{51} = GT_9$
$O = 79, b = 1$
$T_{51} = 79 * 79$
$T_{51} = 6241/91 \Rightarrow 53$

$b = 2$
$T_{52} = 53 * 79$
$T_{52} = 4187/91 \Rightarrow 1$
$b = 3$
$T_{53} = 1 * 79$
$T_{53} = 79/91 \Rightarrow 79$
$b = 4$
$T_{54} = 79 * 79$
$T_{54} = 6241/91 \Rightarrow 53$
$T_{54} = 53$

Sixth Character -S= 83

$a = a + 1,$
$a = 5 + 1 = 6$
$a = 6, b = 1$
- $T_{61} = GT_9$
$S = 83, b = 1$
$T_{61} = 83 * 83$
$T_{61} = 6889/91 \Rightarrow 64$

$b = 2$
$T_{62} = 64 * 83$
$T_{62} = 5312/91 \Rightarrow 34$
$b = 3$
$T_{63} = 34 * 83$
$T_{63} = 2822/91 \Rightarrow 1$
$a = 4$
$T_{64} = 1 * 83$
$T_{64} = 83/91 \Rightarrow 83$
$T_{64} = 83$

Seventh Character - O= 79

$a = a + 1,$
$a = 6 + 1 = 7$
$a = 7, b = 1$
- $T_{71} = GT_9$
$O = 79, b = 1$
$T_{71} = 79 * 79$
$T_{71} = 6241/91 \Rightarrow 53$

$b = 2$

$T_{72} = 53 * 79$

$T_{72} = 4187/91 \Rightarrow 1$

$b = 3$

- $T_{73} = 1 * 79$

$T_{73} = 79/91 \Rightarrow 79$

$b = 4$

$T_{74} = 79 * 79$

$T_{74} = 6241/91 \Rightarrow 53$

$T_{74} = 53$

Eight Character - F= 70

$a = a + 1,$

$a = 7 + 1 = 8$

$a = 8, b = 1$

- $T_{81} = GT_9$

$F = 70, b = 1$

$T_{81} = 70 * 70$

$T_{81} = 4900/91 \Rightarrow 77$

$b = 2$

$T_{82} = 77 * 70$

$T_{82} = 5390/91 \Rightarrow 21$

$b = 3$

$T_{83} = 21 * 70$

$T_{83} = 1470/91 \Rightarrow 14$

$b = 4$

$T_{84} = 14 * 70$

$T_{84} = 980/91 \Rightarrow 70$

$T_{84} = 70$

Ninth Character - T= 84

$a = a + 1,$

$a = 8 + 1 = 9$

$a = 9, b = 1$

- $T_{91} = GT_9$

$T = 84, b = 1$

$T_{91} = 84 * 84$

$T_{91} = 7056/91 \Rightarrow 49$

$b = 2$

$T_{92} = 49 * 84$

$T_{92} = 4116/91 \Rightarrow 21$

$b = 3$

$T_{93} = 21 * 84$

$T_{93} = 1764/91 \Rightarrow 35$

$b = 4$

$T_{94} = 35 * 84$

$T_{94} = 2940/91 \Rightarrow 28$

$T_{94} = 28$

- ET=774758105383537028
- To make a pair and apply the encrypted code in Matrix A, but 0 starts from reverse.

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

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

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

- The 2nd swap values (4,7)

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

- The 3rd swap values (5,8)

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

- The 4th swap values (1,0)

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

- The 5th swap values (5,3)

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

- The 6th swap value (8,3)

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

- The 7th swap values (5,3)

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

- The 8th swap values (7,0)

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

- The 9th swap values (2,8)

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

4.1.3. Step 3 - Now Apply the Prime Key in ET Matrix

$$ETP=\begin{bmatrix} \frac{GT_{14}}{53} & \frac{GT_{13}}{53} & \frac{GT_{12}}{53} & \frac{GT_{11}}{53} \\ \frac{GT_{24}}{53} & \frac{GT_{23}}{53} & \frac{GT_{22}}{53} & \frac{GT_{43}}{53} \\ \frac{GT_{42}}{53} & \frac{GT_{33}}{53} & \frac{GT_{32}}{53} & \frac{GT_{34}}{53} \\ \frac{GT_{44}}{53} & \frac{GT_{21}}{53} & \frac{GT_{41}}{53} & \frac{GT_{31}}{53} \end{bmatrix}$$

4.1.4. Step 4 - Now Apply the "Salsa" Method in the ETP Matrix

$$SE=\begin{bmatrix} \frac{GT_{14}}{53} & \frac{GT_{23}}{53} & \frac{GT_{32}}{53} & \frac{GT_{31}}{53} \\ \frac{GT_{24}}{53} & \frac{GT_{33}}{53} & \frac{GT_{41}}{53} & \frac{GT_{11}}{53} \\ \frac{GT_{42}}{53} & \frac{GT_{23}}{53} & \frac{GT_{12}}{53} & \frac{GT_{43}}{53} \\ \frac{GT_{44}}{53} & \frac{GT_{13}}{53} & \frac{GT_{22}}{53} & \frac{GT_{34}}{53} \end{bmatrix}$$

4.2. Working for Decryption

$$SE=\begin{bmatrix} \frac{GT_{14}}{53} & \frac{GT_{23}}{53} & \frac{GT_{32}}{53} & \frac{GT_{31}}{53} \\ \frac{GT_{24}}{53} & \frac{GT_{33}}{53} & \frac{GT_{41}}{53} & \frac{GT_{11}}{53} \\ \frac{GT_{42}}{53} & \frac{GT_{23}}{53} & \frac{GT_{12}}{53} & \frac{GT_{43}}{53} \\ \frac{GT_{44}}{53} & \frac{GT_{13}}{53} & \frac{GT_{22}}{53} & \frac{GT_{34}}{53} \end{bmatrix}$$

4.2.1. Step 1 - Now Apply the "Salsa" Method in the SE Matri

$$SD=\begin{bmatrix} \frac{GT_{14}}{53} & \frac{GT_{13}}{53} & \frac{GT_{12}}{53} & \frac{GT_{11}}{53} \\ \frac{GT_{24}}{53} & \frac{GT_{23}}{53} & \frac{GT_{22}}{53} & \frac{GT_{43}}{53} \\ \frac{GT_{42}}{53} & \frac{GT_{33}}{53} & \frac{GT_{32}}{53} & \frac{GT_{34}}{53} \\ \frac{GT_{44}}{53} & \frac{GT_{21}}{53} & \frac{GT_{41}}{53} & \frac{GT_{31}}{53} \end{bmatrix}$$

4.2.2. Step 2 - Now Apply the Prime Key 53 in the SD Matrix

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

4.2.3. Step 3 - To Convert the Number from the Given Text as DT

- DT =TFOSORCIM

  $T-84, F-70, 0-79, S-83, 0-79, R-82, C-67$
- $I-73, M-77$

  $DT = 8470798379\ 82677377$
- Apply Equation 2 to decrypt the DT.

First Character - T= 84

- $a=1, b=1$

  $T_{11}=GT_9$
- $T=84, b=1$

  $T_{11}=84*84$

  $T_{11}=7056/91 \Rightarrow 49$

  $b=2$

  $T_{12}=49*84$

  $T_{12}=4116/91 \Rightarrow 21$

  $b=3$

  $T_{13}=21*84$

  $T_{13}=1764/91 \Rightarrow 35$

  $b=4$

  $T_{14}=35*84$

  $T_{14}=2940/91 \Rightarrow 28$

  $T_{14}=28$

Second Character - F= 70

- $a=a+1,$

  $a=1+1=2$

  $a=2, b=1$
- $T_{21}=GT_9$

  $F=70, b=1$

  $T_{21}=70*70$

  $T_{21}=4900/91 \Rightarrow 77$

  $b=2$

  $T_{22}=77*70$

  $T_{22}=5390/91 \Rightarrow 21$

  $b=3$

  $T_{23}=21*70$

  $T_{23}=1470/91 \Rightarrow 14$

  $b=4$

  $T_{24}=14*70$

  $T_{24}=980/91 \Rightarrow 70$

  $T_{24}=70$

Third Character - O= 79

- $a=a+1,$

  $a=2+1=3$

  $a=3, b=1$
- $T_{31}=GT_9$

  $O=79, b=1$

  $T_{31}=79*79$

  $T_{31}=6241/91 \Rightarrow 53$

  $b=2$

  $T_{32}=53*79$

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

  $b=3$

  $T_{33}=1*79$

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

  $b=4$

  $T_{34}=79*79$

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

  $T_{34}=53$

Fourth Character -S= 83

$a = a+1,$
$a = 3+1 = 4$
$a = 4, b = 1$

- $T_{41} = GT_9$

$S = 83, b = 1$
$T_{41} = 83*83$
$T_{41} = 6889/91 \Rightarrow 64$

$b = 2$
$T_{42} = 64*83$
$T_{42} = 5312/91 \Rightarrow 34$
$b = 3$
$T_{43} = 34*83$
$T_{43} = 2822/91 \Rightarrow 1$
$a = 4$
$T_{44} = 1*83$
$T_{44} = 83/91 \Rightarrow 83$
$T_{44} = 83$

Fifth Character - O= 79

$a = a+1,$
$a = 4+1 = 5$
$a = 5, b = 1$

- $T_{51} = GT_9$

$O = 79, b = 1$
$T_{51} = 79*79$
$T_{51} = 6241/91 \Rightarrow 53$

$b = 2$
$T_{52} = 53*79$
$T_{52} = 4187/91 \Rightarrow 1$
$b = 3$
$T_{53} = 1*79$
$T_{53} = 79/91 \Rightarrow 79$
$b = 4$
$T_{54} = 79*79$
$T_{54} = 6241/91 \Rightarrow 53$
$T_{54} = 53$

Sixth Character - R= 82

$a = a+1,$
$a = 5+1 = 6$
$a = 6,\ b = 1$

- $T_{61} = GT_9$

$T = 82, b = 1$
$T_{61} = 82*82$
$T_{61} = 6724/91 \Rightarrow 81$

$b = 2$
$T_{62} = 81*82$
$T_{62} = 6642/91 \Rightarrow 90$
$b = 3$
$T_{63} = 90*82$
$T_{63} = 7380/91 \Rightarrow 9$
$b = 4$
$T_{64} = 9*82$
$T_{64} = 738/91 \Rightarrow 10$
$T_{64} = 10$

Seventh Character - C= 67

$a = a+1,$
$a = 6+1 = 7$
$a = 7,\ b = 1$

- $T_{71} = GT_9$

$T = 67, b = 1$
$T_{71} = 67*67$
$T_{71} = 4489/91 \Rightarrow 30$

$b = 2$
$T_{72} = 30*67$
$T_{72} = 2010/91 \Rightarrow 8$
$b = 3$

- $T_{73} = 8*67$

$T_{73} = 536/91 \Rightarrow 81$
$b = 4$
$T_{74} = 81*67$
$T_{74} = 5427/91 \Rightarrow 58$
$T_{74} = 58$

Eight Character - I= 73

$a = a+1,$
$a = 7+1 = 8$
$a = 8, b = 1$

- $T_{81} = GT_9$

$I = 73, b = 1$
$T_{81} = 73*73$
$T_{81} = 5329/91 \Rightarrow 51$

$b = 2$
$T_{82} = 51*73$
$T_{82} = 3723/91 \Rightarrow 83$
$b = 3$
$T_{83} = 83*73$
$T_{83} = 6059/91 \Rightarrow 53$
$b = 4$
$T_{84} = 53*73$
$T_{84} = 3869/91 \Rightarrow 47$
$T_{84} = 47$

Ninth Character - M=77

$a = a+1$
$a = 8+1 = 9$
$a = 9, b = 1$

- $T_{91} = GT_9$

$M = 77$
$T_{91} = 77*77$
$T_{91} = 5929/91 \Rightarrow 14$

$b = 2$
$T_{92} = 14*77$
$T_{92} = 1078/91 \Rightarrow 77$
$b = 3$
$T_{93} = 77*77$
$T_{93} = 5929/91 \Rightarrow 14$
$a = 4$
$T_{94} = 14*77$
$T_{94} = 1078/91 \Rightarrow 77$
$T_{94} = 77$

- DT=287053835310584777
- To make a pair and apply the encrypted code in Matrix SDP, but 0 starts from reverse.

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

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

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

- The 2nd swap values (7,0)

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

- The 3rd swap values (5,3)

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

- The 4th swap values (8,3)

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

- The 5th swap values (5,3)

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

- The 6th swap values (1,0)

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

- The 7th swap values (5,8)

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

- The 8th swap values (4,7)

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

- The 9th swap values (7,7)

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

4.2.4. Step 4 - Apply the Column Operations in Matrix DT as A

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

Table 1. RPBB-24-3 encryption performance

File Size (Bytes)	Salsa	RBJ25	RPBB-24-3
25	1.62	2.2	3.1
77	1.19	2.6	3.8
110	1.39	3.4	4.4
311	2.43	4.5	4.9
811	2.24	5.3	5.9
1521	3.44	5.5	6.6
6580	2.97	6.8	7.5

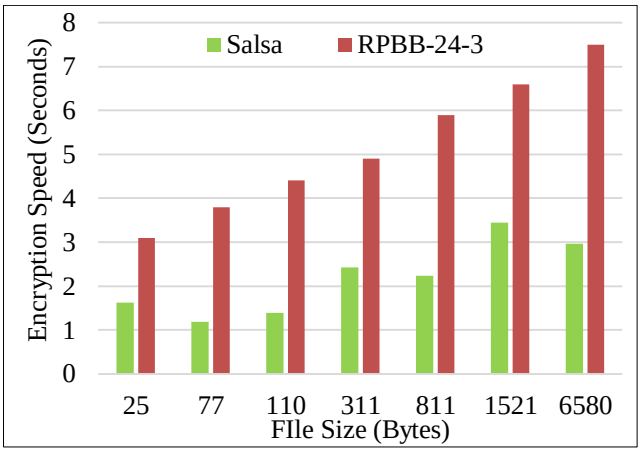

Fig. 4 Salsa Vs RPBB-24-3 encryption speed

These three encryption speeds are compared in Table 1, which may be found here. When compared to other methods,

the RPBB-24-3 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 and RPBB-24-3" in Figure 4, "RBJ25 and RPBB-24-3" in Figure 5, and "Salsa, RBJ25, and RPBB-24-3" in Figure 6, the performance of the speed of the suggested method RPBB-24-3 is 3.1, 3.8,4.4,4.9,5.9,6.6,7.5 in various file sizes. This is an excellent result.

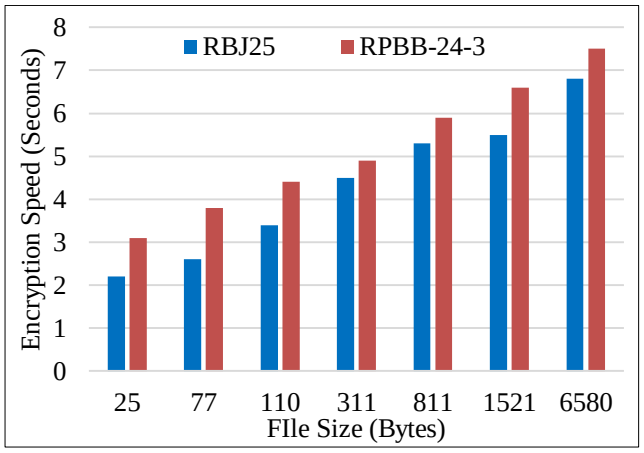

Fig. 5 RBJ25 Vs RPBB-24-3 encryption speed

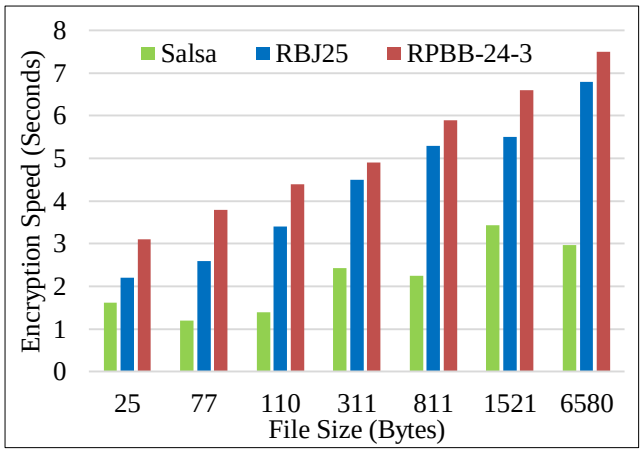

Fig. 6 Salsa, RBJ25, and RPBB-24-3 encryption speed

Table 2. RPBB-24-3 decryption performance

File Size (Bytes)	Salsa	RBJ25	RPBB-24-3
25	1.5	1.9	3.5
77	1.79	2.3	3.9
110	1.91	2.8	4.6
311	2.33	3.5	4.9
811	2.94	4.1	5.4
1521	3.64	4.5	5.9
6580	2.71	5.6	6.5

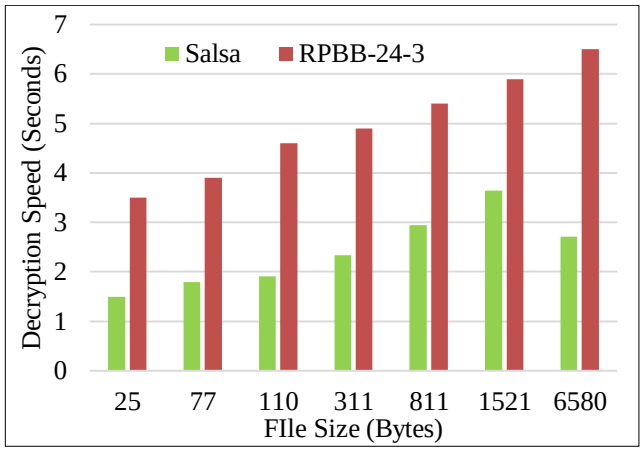

Fig. 7 Salsa Vs RPBB-24-3 decryption speed

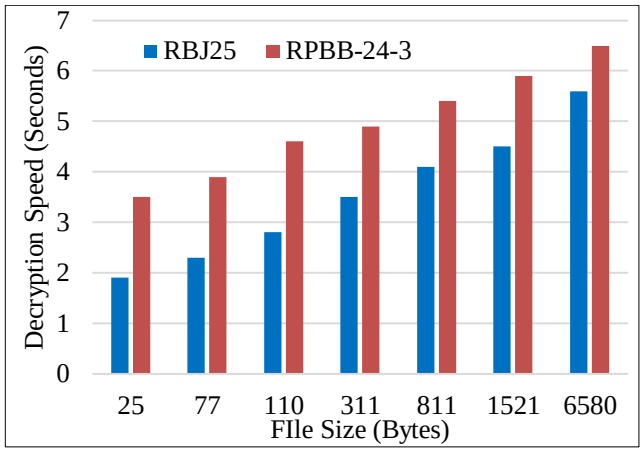

Fig. 8 RBJ25 Vs RPBB-24-3 decryption speed

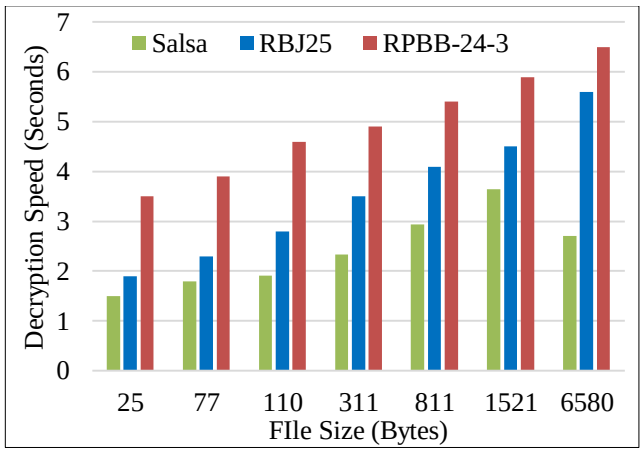

Fig. 9 Salsa, RBJ25, and RPBB-24-3 decryption speed

An examination of the three different decryption speeds is shown in Table 2. When contrasted with other methods, the RPBB-24-3 approach that was suggested demonstrates a really high level of speed performance. The performance of the speed in the suggested method RPBB-24-1 is 3.5, 3.9, 4.6, 4.9, 5.4, 5.9, and 6.5 in various file sizes. This is excellent when

compared to the current techniques, which are "Salsa and RPBB-24-3" in Figure 7, "RBJ25 and RPBB-24-3" in Figure 8, and "Salsa, RBJ25, and RPBB-24-3" in Figure 9.

5. Conclusion

Blockchain is one of the technologies that is significantly expanding at the fastest rate in the world. Block Chain is a technique that is used to secure the protection of multiple data locations despite the fact that users are not aware of what it is. "Salsa" and "RBJ25" are the names of the algorithms that are employed by this kind of user, which are considered to be of a lower degree of security. Within the scope of this investigation, the RPBB-24-3 security technique is the one that is being presented. Two components are incorporated in the RPBB-24-3 method. These components include encryption and decryption. A total of five distinct processes are involved in the encryption approach. The technique begins with the application of the column operations to GT, which is the initial stage. Next, the second step of the method involves using the "lattin letter" and multiplying the value by four using Equation (1). In the third step, the values of the cells are swapped, but the process starts with the 0th cell value from the most recent cell value. Data that is encrypted is used for this process. That which makes up the fourth stage is dividing the prime key into the values of the matrix cells. The "SalSa" method is used inside the matrix in the fifth step of the process. Finally, the plain text is turned into encrypted text. In other words, the process of decryption is the opposite of the process of encryption. The suggested method is safer than the standard way that is 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 Matulevicius, "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] 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]