SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V12I7P118

Volume 12 Issue 7, 253-263, July 2025

Original Article

Implementing The CS25-1 Algorithm for Multi-Way Distributed Blockchain Security

C. Bagath Basha[1], S. Rajaprakash[2], K. Karthik[3], TKS Rathish Babu[4], Maha Yousif Rizgalla Sulieman[5], Rasitha Banu GulMohamed[6]

[1]*Department of Computer Science & Engineering, Kommuri Pratap Reddy Institute of Technology, Autonomous, Hyderabad, Telangana, India.*
[2]*Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu, India.*
[3]*Department of Computer Science and Engineering, Aarupadai Veedu Institute of Technology, Vinayaka Mission's Research Foundation (DU), Chennai, Tamil Nadu, India.*
[4]*Department of Computer Science & Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.*
[5]*Health Education Program, Department of Public Health, College of Nursing and Health Sciences, Jazan University, Jazan, Jazan Province, Saudi Arabia.*
[6]*Health Informatics Program, Department of Public Health, College of Nursing and Health Sciences, Jazan University, Jazan, Jazan Province, Saudi Arabia.*

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

Received: 12 May 2025 Revised: 14 June 2025 Accepted: 13 July 2025 Published: 31 July 2025

Abstract - *Blockchain is a rapidly developing technology that has been widely known for its high data security features. Although it is mostly utilized to encrypt data in transit, the underlying processes tend to be misinterpreted by the public. In this paper, a new lightweight encryption scheme called CS25-1, inspired by small but secure algorithms like Salsa and RB20, is proposed. CS25-1 employs a six-step encryption and decryption process, designed to render information more secure yet still be effective. The process, also referred to as CS25-1, is thus: Create Two Secret Messages: Begin with the writing of two plaintext messages that are to be encrypted. Encrypt First Message: Each character of the first message is encrypted with a predecided secret code and then multiplied by four to add complexity. Matrix Mapping (First Message): The encrypted values are then placed within a matrix to create structural obfuscation. Encrypt the Second Message: The second message is encrypted using the secret code, followed by multiplication by four. Matrix Mapping (Second Message): The second group of encrypted values is mapped into a second matrix. Prime Key Division: A hidden prime number is employed subsequently to divide the values in each of the two matrices, providing yet another level of cryptographic hardness. The decryption algorithm proceeds to undo the steps in sequence to obtain the original plaintexts. This multi-layered approach enhances conventional encryption strategies by providing double-message encoding, matrix transformation, and prime-based division as collective methods of strengthening against brute-force and analytical attacks.*

Keywords - *Decryption, Encryption, Performance, RB20, CS25-1.*

1. Introduction

In recent years, "Blockchain (BC) technology" has made its way into the majority of different businesses. This is mostly due to the fact that it offers a novel and effective method for storing and sending data in a way that is both traceable and safe. Concurrently, as smart environments continue to develop, an increasing amount of data is produced, which must be handled and stored in a securely protected manner.

In fact, blockchain is making a significant contribution to the protection of users' data and the preservation of the anonymity of network participants. Additionally, blockchain technology has shown itself to be the most suitable ledger for the movement and storage of data; A range of "industries", including industry and logistics, health, banking, and so on, are now being accepted by a large number of companies all over the globe. In addition, the use of BC technology within the sector alleviates congestion, the danger of data loss, the possibility of data theft, and the possibility of cost inflation. Blockchain technology is a technology that operates on layers. As shown in Figure 1, the infrastructure layer is responsible for encapsulating the time-stamped data blocks and exercising control over the storage of the nodes. Both the platform layer and the distributed computing layer are made up of numerous

consensus methods and security regulations, such as hashing operations. The platform layer is made up of the Web Application Programming Interface (API). Additionally, the application layer is accountable for bringing programmability to blockchain, and it is made up of commercial apps that are built on blockchain technology. In spite of the fact that we deal with a significant volume of data in smart settings. One of the capabilities of "blockchain technology" is its ability to handle the complexity of a distributed architecture that contains various devices and apps. To be more specific, "blockchain technology" has lately been recognized as an essential infrastructure for the management of transactions in the Metaverse. The ultimate objective of smart environments is to make it easier for residents to access a variety of services.

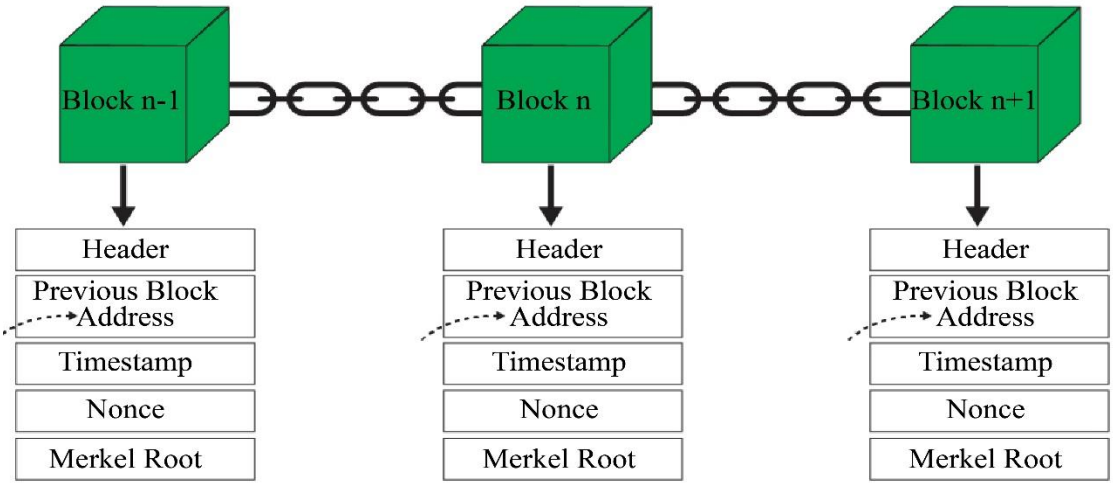

Fig. 1 The structure of the blockchain

2. Literature Survey

Several concerns about blockchain technology were mentioned by the author. In order to study the security risk, it is used [1, 2] They spoke about the assaults that were committed by criminals and analyzed the safety of the criminal activity. The author conducted research on the composition and structure of the blockchain, which is used for the purpose of analyzing and comparing the different levels of security [3]. In order to design the two primary security measures, such as double-spending and sybil, they conducted an analysis of the numerous dangers.

This established approach was used in order to put the security into effect [4]. The author S. Rajaprakash and others, the writer came up with the "RB20" method, which is safer [5]. The author postulated the levels of SRA. It is the responsibility of this layer to ensure that the blockchain remains secure. They conducted an analysis of the unique characteristics of the key and controlled the vulnerability using four different security measures [6]. Along with other experts, the author, Batcha, B.B.C., looked into RPBB31's seven-stage security method [7]. In light of the public mode, they conducted research on the interchange of data and provided assistance for the voting system [8]. This method was used to transmit the data to the blockchain. The author conducted research on the different levels of protocol in the security industry. For "the purpose of evaluating the effectiveness" of the performance, several techniques are used [9]. The blockchain hyperledger and the capabilities of the reaction for speed and security were both something that they invented. For the purpose of implementing security, this capability is used [10]. The author concentrated mostly on the characteristics of the Internet of Things and compared them to the different characteristics of blockchain [11]. The majority of their attention is directed to the various learning with security. An improvement in the performance of the security is achieved by the use of federated learning. The author made a proposal on the safety of deep learning and conducted an analysis of the many activities that pertain to the safety of blockchain data [12]. Other writers, including one named Basha, C. B., looked into ways to boost performance and safety [13]. The reencryption of the data that is exchanged in the blockchain of the Internet of Things is evaluated by them. The purpose of this reencryption operation is to demonstrate the effectiveness of the data security [14]. The author, C. Bagath Basha et al., mostly talked about how to make encryption safer, and the answer they came up with is RPBB-24-1. This method was used to "provide a high level of protection for encryption" at a good speed. Based on the study of the literature, we will show the "ChanS25" (CS25-1) method that was proposed

3. Methodology

The suggested technique, CS25-1, is a process of encryption and decryption comprising six primary steps. Generate Two Secret Messages – Start by generating two separate secret messages. Encrypt the First Message – Assign a "secret code to every letter of the first message and then

multiply the value obtained by four". Matrix Mapping (First Message) – Place the encrypted values of the first message in a matrix. Encrypt the Second Message – Follow the same process by applying the secret code to every letter of the second message and multiplying the result again by four. Matrix Mapping (Second Message) – Put each encrypted output of the second message into a second matrix. Use Prime Key Division – Divide the matrix values using a secret prime key to encrypt further. Copy and Paste the Key. Finally, the plaintext is converted to a securely encrypted ciphertext, as shown in Figure 2.

Algorithm for encryption:

1. First, we have to pick two "secret messages" as PT.
2. The first secret message is changed to the numbers from the "Latin alphabet" for PT, and each letter is multiplied by four to "encrypt" the FET.
3. Use the initial "encrypted" text values in matrix PT for "swap the values".
4. The second secret message uses the same method as the first secret message to encipher the SET.
5. To use the secret prime key to divide the SET matrix.

Algorithm for decryption:

1. The secret prime key is used to multiply the DDT matrix.
2. Therefore, we have to "receive Cipher Text message from user" as DDT.
3. First, decrypt the secret message and translate it into the numbers of the "Latin alphabet" for DDT. Then, multiply each letter by 4 times to decrypt the FDT.
4. To use the first decrypted text values in matrix DDT for "swap the values".
5. Once again, the second secret message is used as the first decrypted secret message to "encrypt" the SDT.
6. To use the "decrypted values in matrix" FDT for "swap the values".

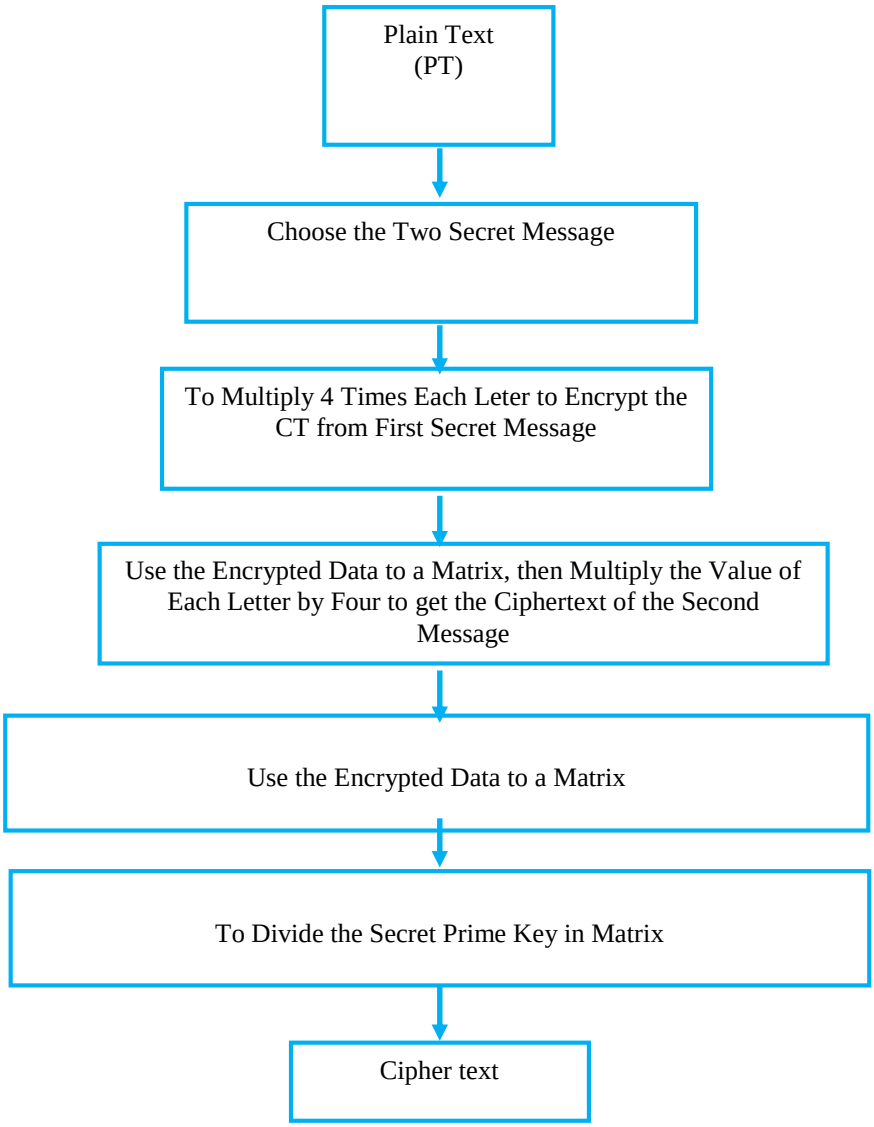

Fig. 2 CS25-1

4. Result & Discussion

$$PT=\begin{bmatrix} TP_{11} & TP_{12} & TP_{13} & TP_{14} \\ TP_{21} & TP_{22} & TP_{23} & TP_{24} \\ TP_{31} & TP_{32} & TP_{33} & TP_{34} \\ TP_{41} & TP_{42} & TP_{43} & TP_{44} \end{bmatrix} \quad (1)$$

4.1. Working for Encryption

- To choose the two secret keys as PT
- First secret key "GOLD" and second secret key "DIAM".
- PT=GOLD
- $G-71, O-79, L-76, D-68$

$$PT = 71797668$$

- Apply Equation (1) [12].

4.1.1. First Character -G 71

- $a=1, b=1$

$$T_{11} = PT_4$$
$$G-71, b=1$$
$$T_{11} = 71*71$$
$$T_{11} = 5041/91 \Rightarrow 36b=2$$
$$T_{12} = 36*71$$
$$T_{12} = 2556/91 \Rightarrow 8$$
$$b=3$$
$$T_{13} = 8*71$$
$$T_{13} = 568/91 \Rightarrow 22$$
$$a=4$$
$$T_{14} = 22*71$$
$$T_{14} = 1562/91 \Rightarrow 15$$
$$T_{14} = 15$$

4.1.2. Second Character - O= 79

- $a=a+1,$

$$a=1+1=2$$
$$a=2, b=1$$
$$T_{21} = PT_4$$
$$O=79, b=1$$
$$T_{21} = 79*79$$
$$T_{21} = 6241/91 \Rightarrow 53b=2$$
$$T_{22} = 53*79$$
$$T_{22} = 4187/91 \Rightarrow 1$$
$$b=3$$
$$T_{23} = 1*79$$
$$T_{23} = 79/91 \Rightarrow 79$$
$$b=4$$
$$T_{24} = 79*79$$
$$T_{24} = 6241/91 \Rightarrow 53$$
$$T_{24} = 53$$

4.1.3. Third Character - L 76

- $a=a+1,$

$$a=2+1=3$$
$$a=3, b=1$$
$$T_{31} = PT_4$$
$$L=76, b=1$$
$$T_{31} = 76*76$$
$$T_{31} = 5776/91 \Rightarrow 43b=2$$
$$T_{32} = 43*76$$
$$T_{32} = 3268/91 \Rightarrow 83$$
$$b=3$$
$$T_{33} = 83*76$$
$$T_{33} = 6308/91 \Rightarrow 29$$
$$b=4$$
$$T_{34} = 29*76$$
$$T_{34} = 2204/91 \Rightarrow 20$$
$$T_{34} = 20$$

4.1.4. Fourth Character - D 68

- $a=a+1$

$$a=3+1=4$$
$$a=4, b=1$$
$$T_{41} = PT_4$$
$$T=68, b=1$$
$$T_{41} = 68*68$$
$$T_{41} = 4624/91 \Rightarrow 74b=2$$
$$T_{42} = 74*68$$
$$T_{42} = 5032/91 \Rightarrow 27$$
$$b=3$$
$$T_{43} = 27*68$$
$$T_{43} = 1836/91 \Rightarrow 16$$
$$b=4$$
$$T_{44} = 16*68$$
$$T_{44} = 1088/91 \Rightarrow 87$$
$$T_{44} = 87$$

- FET=15532087
- To form a pair, apply the First Encrypted Text (FET) in a matrix.
- FET=(1,5), (5,3), (2,0), (8,7)

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

- First swap values (1,5)

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

- Second swap values (5, 3)

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

- Third swap values (2, 0)

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

- Fourth swap values (8, 7)

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

- PT=DIAM

- $D-68, I-73, A-65, M-77$

$PT = 68736577$

4.1.5. First Character - D 68

- $a = 1, b = 1$

$$T_{11} = PT_4$$
$$T = 68, b = 1$$
$$T_{11} = 68 * 68$$
$$T_{11} = 4624/91 \Rightarrow 74b = 2$$
$$T_{12} = 74 * 68$$
$$T_{12} = 5032/91 \Rightarrow 27$$
$$b = 3$$
$$T_{13} = 27 * 68$$
$$T_{13} = 1836/91 \Rightarrow 16$$
$$b = 4$$
$$T_{14} = 16 * 68$$
$$T_{14} = 1088/91 \Rightarrow 87$$
$$T_{14} = 87$$

4.1.6. Second Character - I= 73

- $a = a + 1,$

$$a = 1 + 1 = 2$$
$$a = 2, b = 1$$
$$T_{21} = GT_9$$
$$I = 73, b = 1$$
$$T_{21} = 73 * 73$$
$$T_{21} = 5329/91 \Rightarrow 51b = 2$$
$$T_{22} = 51 * 73$$
$$T_{22} = 3723/91 \Rightarrow 83$$
$$b = 3$$
$$T_{23} = 83 * 73$$
$$T_{23} = 6059/91 \Rightarrow 53$$
$$b = 4$$
$$T_{24} = 53 * 73$$
$$T_{24} = 3869/91 \Rightarrow 47$$
$$T_{24} = 47$$

4.1.7. Third Character - A= 65

- $a = a + 1,$

$$a = 2 + 1 = 3$$
$$a = 3, b = 1$$
$$T_{31} = PT_4$$
$$F = 65, b = 1$$
$$T_{31} = 65 * 65$$
$$T_{31} = 4225/91 \Rightarrow 39b = 2$$
$$T_{32} = 39 * 65$$
$$T_{32} = 2535/91 \Rightarrow 78$$
$$b = 3$$
$$T_{33} = 78 * 65$$
$$T_{33} = 5070/91 \Rightarrow 65$$
$$b = 4$$
$$T_{34} = 65 * 65$$
$$T_{34} = 4225/91 \Rightarrow 39$$
$$T_{34} = 39$$

4.1.8. Fourth Character - M=77

- $a = a + 1$

$$a = 3 + 1 = 4$$
$$a = 4, b = 1$$
$$T_{41} = PT_4$$
$$M = 77$$
$$T_{41} = 77 * 77$$
$$T_{41} = 5929/91 \Rightarrow 14b = 2$$
$$T_{42} = 14 * 77$$
$$T_{42} = 1078/91 \Rightarrow 77$$
$$b = 3$$
$$T_{43} = 77 * 77$$
$$T_{43} = 5929/91 \Rightarrow 14$$
$$a = 4$$
$$T_{44} = 14 * 77$$
$$T_{44} = 1078/91 \Rightarrow 77$$
$$T_{44} = 77$$

- SET=87473977

- SET=(8,7), (4,7), (3,9), (7,7)

- First swap values (8, 7)

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

- Second swap values (4, 7)

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

- Third swap values (3, 9)

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

- Fourth swap values (7, 7)

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

- Use the secret prime key "59" for division in the matrix.

$$\text{DET}=\begin{bmatrix} \frac{TP_{13}}{59} & \frac{TP_{22}}{59} & \frac{TP_{11}}{59} & \frac{TP_{32}}{59} \\ \frac{TP_{31}}{59} & \frac{TP_{14}}{59} & \frac{TP_{23}}{59} & \frac{TP_{21}}{59} \\ \frac{TP_{24}}{59} & \frac{TP_{12}}{59} & \frac{TP_{33}}{59} & \frac{TP_{34}}{59} \\ \frac{TP_{41}}{59} & \frac{TP_{42}}{59} & \frac{TP_{43}}{59} & \frac{TP_{44}}{59} \end{bmatrix}$$

4.2. Working for Decryption

$$\text{DDT}=\begin{bmatrix} \frac{TP_{13}}{59} & \frac{TP_{22}}{59} & \frac{TP_{11}}{59} & \frac{TP_{32}}{59} \\ \frac{TP_{31}}{59} & \frac{TP_{14}}{59} & \frac{TP_{23}}{59} & \frac{TP_{21}}{59} \\ \frac{TP_{24}}{59} & \frac{TP_{12}}{59} & \frac{TP_{33}}{59} & \frac{TP_{34}}{59} \\ \frac{TP_{41}}{59} & \frac{TP_{42}}{59} & \frac{TP_{43}}{59} & \frac{TP_{44}}{59} \end{bmatrix} \quad (2)$$

- Use the secret prime key "59" for multiplication in the DDT matrix.

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

- DT=MAID

- $M-77, A-65, I-73, D-68$

$$DT = 77657368$$

- Apply Equation (2) [12].

4.2.1. First Character - M=77

- $a=1, b=1$

$$T_{11}=PT_4$$
$$M=77$$
$$T_{11}=77*77$$
$$T_{11}=5929/91 \Rightarrow 14b=2$$
$$T_{12}=14*77$$
$$T_{12}=1078/91 \Rightarrow 77$$
$$b=3$$
$$T_{13}=77*77$$
$$T_{13}=5929/91 \Rightarrow 14$$
$$a=4$$
$$T_{14}=14*77$$
$$T_{14}=1078/91 \Rightarrow 77$$
$$T_{14}=77$$

4.2.2. Second Character - A= 65

- $a=a+1,$

$$a=1+1=2$$
$$a=2, b=1$$
$$T_{21}=PT_4$$
$$F=65, b=1$$
$$T_{21}=65*65$$
$$T_{21}=4225/91 \Rightarrow 39b=2$$
$$T_{22}=39*65$$
$$T_{22}=2535/91 \Rightarrow 78$$
$$b=3$$
$$T_{23}=78*65$$
$$T_{23}=5070/91 \Rightarrow 65$$
$$b=4$$
$$T_{24}=65*65$$
$$T_{24}=4225/91 \Rightarrow 39$$
$$T_{24}=39$$

4.2.3. Third Character - I= 73

- $a=a+1,$

$$a=2+1=3$$
$$a=3, b=1$$
$$T_{31}=GT_9$$
$$I=73, b=1$$
$$T_{31}=73*73$$
$$T_{31}=5329/91 \Rightarrow 51b=2$$
$$T_{32}=51*73$$
$$T_{32}=3723/91 \Rightarrow 83$$
$$b=3$$
$$T_{33}=83*73$$
$$T_{33}=6059/91 \Rightarrow 53$$
$$b=4$$
$$T_{34}=53*73$$
$$T_{34}=3869/91 \Rightarrow 47$$
$$T_{34}=47$$

4.2.4. Fourth Character - D 68

- $a=a+1,$

$$a=3+1=4$$
$$a=4, b=1$$
$$T_{41}=PT_4$$
$$T=68, b=1$$
$$T_{41}=68*68$$
$$T_{41}=4624/91 \Rightarrow 74b=2$$
$$T_{42}=74*68$$
$$T_{42}=5032/91 \Rightarrow 27$$
$$b=3$$

$$T_{43} = 27 * 68$$
$$T_{43} = 1836/91 \Rightarrow 16$$
$$b = 4$$
$$T_{44} = 16 * 68$$
$$T_{44} = 1088/91 \Rightarrow 87$$
$$T_{44} = 87$$

- DT=77394787
- To make a pair, apply the First Decrypted Text (FDT) in the matrix.
- DT=(7,7), (3,9), (4,7), (8,7)
- First swap values (7, 7)

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

- Second swap values (3,9)

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

- Third swap values (4,7)

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

- Fourth swap values (8,7)

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

- SDT=DLOG
- $D-68, L-76, O-79, G-71$

$$SDT = 68767971$$

- Apply Equation (2) [12].

4.2.5. First Character - D 68

- $a = 1, b = 1$

$$T_{11} = PT_4$$
$$T = 68, b = 1$$
$$T_{11} = 68 * 68$$
$$T_{11} = 4624/91 \Rightarrow 74b = 2$$
$$T_{12} = 74 * 68$$
$$T_{12} = 5032/91 \Rightarrow 27$$
$$b = 3$$
$$T_{13} = 27 * 68$$
$$T_{13} = 1836/91 \Rightarrow 16$$
$$b = 4$$
$$T_{14} = 16 * 68$$
$$T_{14} = 1088/91 \Rightarrow 87$$
$$T_{14} = 87$$

4.2.6. Second Character - L 76

- $a = a + 1,$

$$a = 1 + 1 = 2$$
$$a = 2, b = 1$$
$$T_{21} = PT_4$$
$$L = 76, b = 1$$
$$T_{21} = 76 * 76$$
$$T_{21} = 5776/91 \Rightarrow 43b = 2$$
$$T_{22} = 43 * 76$$
$$T_{22} = 3268/91 \Rightarrow 83$$
$$b = 3$$
$$T_{23} = 83 * 76$$
$$T_{23} = 6308/91 \Rightarrow 29$$
$$b = 4$$
$$T_{24} = 29 * 76$$
$$T_{24} = 2204/91 \Rightarrow 20$$
$$T_{24} = 20$$

4.2.7. Third Character - O= 79

- $a = a + 1,$

$$a = 2 + 1 = 3$$
$$a = 3, b = 1$$
$$T_{31} = PT_4$$
$$O = 79, b = 1$$
$$T_{31} = 79 * 79$$
$$T_{31} = 6241/91 \Rightarrow 53b = 2$$
$$T_{32} = 53 * 79$$
$$T_{32} = 4187/91 \Rightarrow 1$$
$$b = 3$$
$$T_{33} = 1 * 79$$
$$T_{33} = 79/91 \Rightarrow 79$$
$$b = 4$$
$$T_{34} = 79 * 79$$
$$T_{34} = 6241/91 \Rightarrow 53$$
$$T_{34} = 53$$

4.2.8. Fourth Character -G 71

- $a = a + 1$

$$a = 3 + 1 = 4$$
$$a = 4, b = 1$$
$$T_{41} = PT_4$$
$$G - 71, b = 1$$
$$T_{41} = 71 * 71$$
$$T_{41} = 5041/91 \Rightarrow 36b = 2$$

$$T_{42} = 36 * 71$$
$$T_{42} = 2556/91 \Rightarrow 8$$
$$b = 3$$
$$T_{43} = 8 * 71$$
$$T_{43} = 568/91 \Rightarrow 22$$
$$a = 4$$
$$T_{44} = 22 * 71$$
$$T_{44} = 1562/91 \Rightarrow 15$$
$$T_{44} = 15$$

- SDT=87205315
- SDT=(8,7), (2,0), (5,3), (1,5)
- First swap values (8,7)

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

- Second swap values (2, 0)

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

- Third swap values (5,3)

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

- Fourth swap values (1, 5)

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

Table 1. CS25-1 encryption performance

File Size (Bytes)	Salsa	RB20	CS25-1
32	0.99	1.23	2.43
67	1.49	1.95	2.96
105	2.1	2.44	3.45
298	2.98	3.6	4.67
799	3.54	4.9	5.32
1431	4.4	5.8	6.21
5480	4.79	6.6	6.91

Table 1 shows the performance of the three “encryption” speeds. The novel method CS25-1 is showing better “performance of speed” when compared to other methods. The novel method “CS25-1 is the speed of the performance, is 2.43, 2.96, 3.45, 4.67, 5.32, 6.21, and 6.91in various file sizes and also good performance when compared to other methods “RB20 in Figure 3, Salsa in Figure 4”, and the novel method in Figure 5.

Table 2 shows the performance of the three “decryption” speeds. The novel method CS25-1 is showing better “performance of speed” when compared to other methods. The novel method “CS25-1 is the speed of the performance” is 2.52, 2.88, 3.59, 4.89, 5.53, 6.23, and 7.41 in various file sizes and also good performance when compared to other methods “RB20” in Figure 6, “Salsa” in Figure 7, and the novel method in Figure 8.

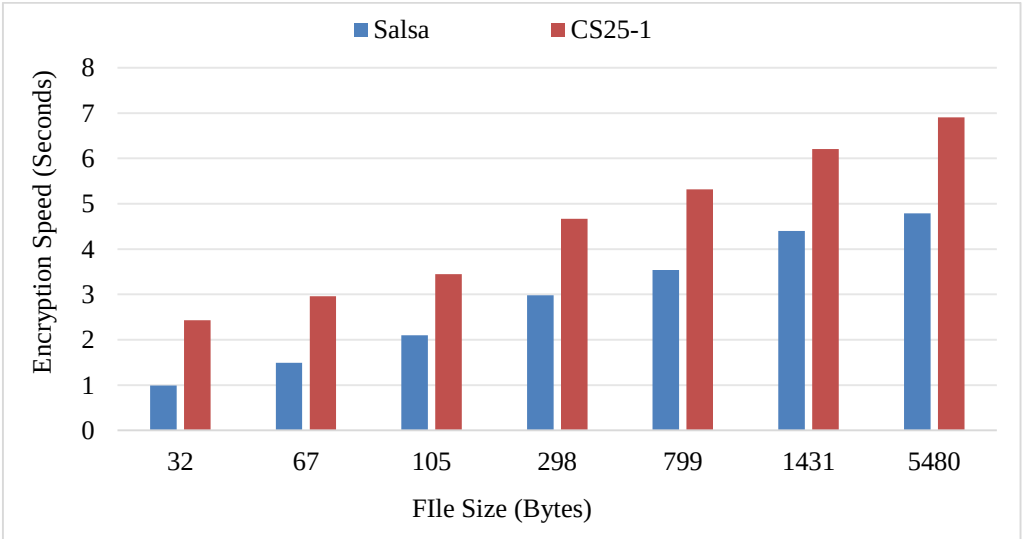

Fig. 3 Encryption speed (a)

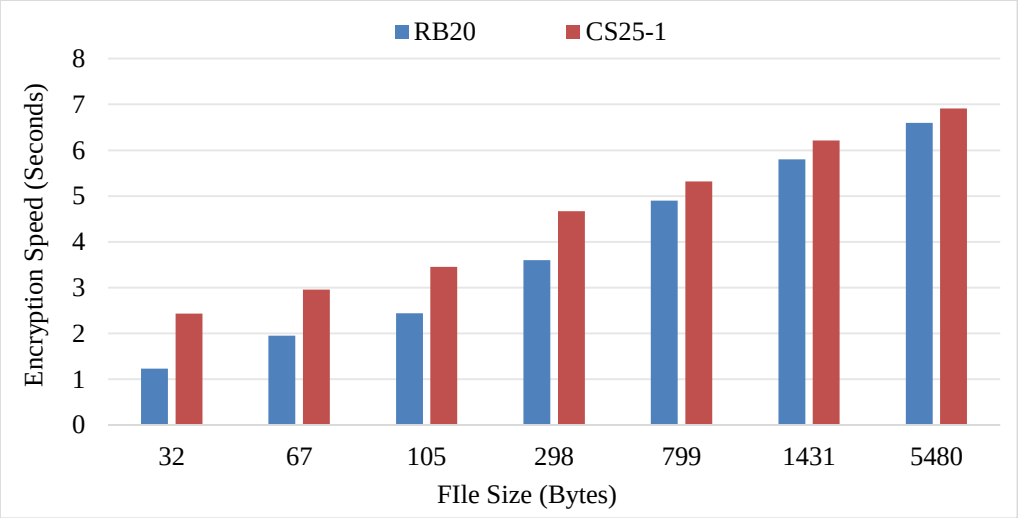

Fig. 4 Encryption speed (b)

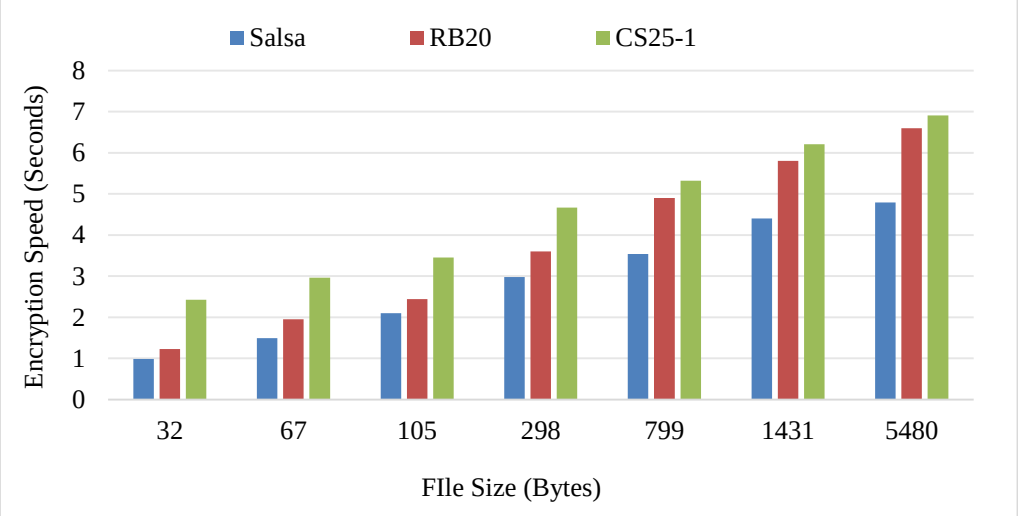

Fig. 5 CS25-1 encryption speed

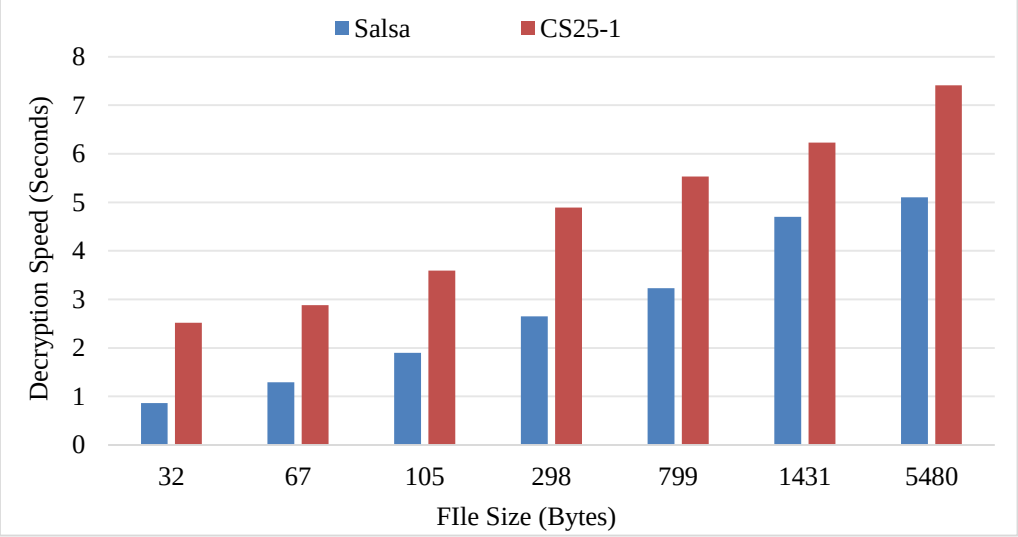

Fig. 6 Decryption speed (a)

Table 2. CS25-1 decryption performance

File Size (Bytes)	Salsa	RB20	CS25-1
32	0.86	1.73	2.52
67	1.29	2.1	2.88
105	1.9	2.89	3.59
298	2.65	3.43	4.89
799	3.23	4.63	5.53
1431	4.7	5.45	6.23
5480	5.1	6.23	7.41

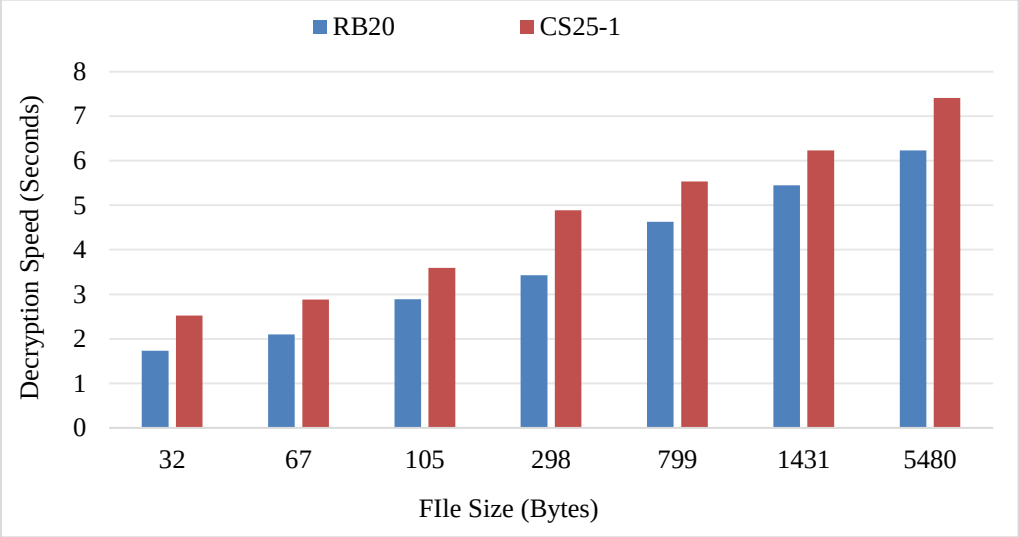

Fig. 7 Decryption speed (b)

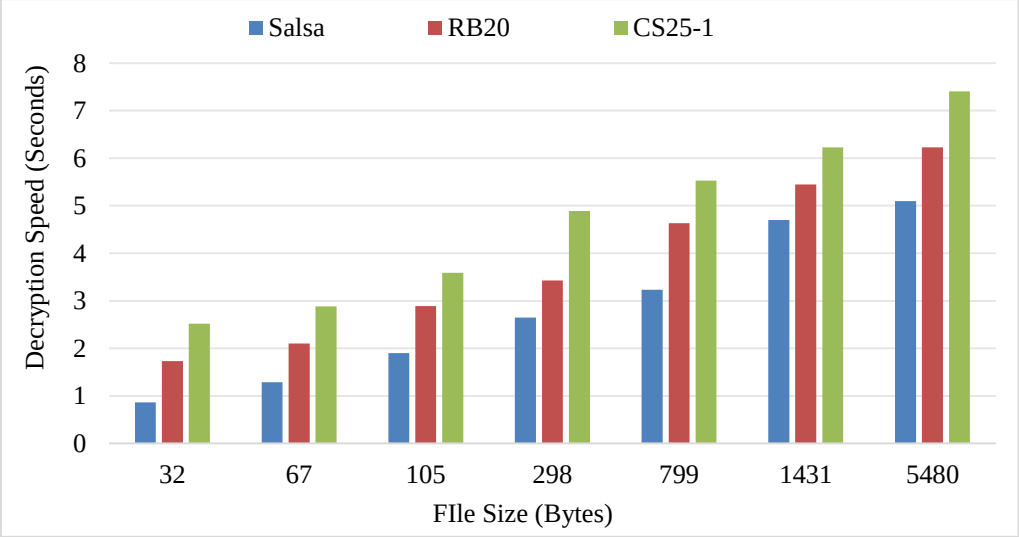

Fig. 8 CS25-1 decryption speed

5. Conclusion

Blockchain is among the world's fastest-growing technologies. Though most individuals are not well familiar with its mechanism, it has a crucial role in protecting information on different platforms. In contrast to this improvement, most users still insist on simple encryption methods like Salsa and RB20, which provide very limited security. This work proposes a novel encryption scheme referred to as CS25-1 aimed at offering increased security using an orderly six-step approach: Create Two Secret Messages – Start by creating two individual secret messages. Encrypt the First Message – For every letter of the first secret message, use a secret code and multiply its worth by four.

Store in Matrix – Store the resultant encrypted data in a matrix. Encrypt the Second Message – Do the encryption on the second secret message the same way: add the secret code and divide by four. Store in Second Matrix – Place this second encrypted result in a second matrix. Apply Prime Key Division – Divide values in the matrices with a secret prime key, wrapping up the encryption process. This converts the plaintext into ciphertext. Decryption is merely the opposite of these actions, and hence, the original message can be retrieved correctly. As compared to prevailing standard practices, CS25-1 is a more potent and secure mechanism for data encryption.

References

[1] 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]

[2] Suhyeon Lee, and Seungjoo Kim, "Blockchain as a Cyber Defense: Opportunities, Applications, and Challenges," *IEEE Access*, vol. 10, pp. 2602-2618, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Mohammad Wazid, Ashok Kumar Das, and Youngho Park, "Generic Quantum Blockchain-Envisioned Security Framework for IoT Environment: Architecture, Security Benefits and Future Research," *IEEE Open Journal of the Computer Society*, vol. 5, pp. 248-267, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] 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]

[5] Ivan Homoliak et al., "The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 341-390, firstquarter, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Yongfeng Huang et al., "Smart Contract Security: A Software Lifecycle Perspective," *IEEE Access*, vol. 7, pp. 150184-150202, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[7] 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. 31, no. 1, pp. 581-608, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Weiqi Dai et al., "PRBFPT: A Practical Redactable Blockchain Framework with a Public Trapdoor," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 2425-2437, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] Yong Wang et al., "Cloud-Assisted EHR Sharing with Security and Privacy Preservation via Consortium Blockchain," *IEEE Access*, vol. 7, pp. 136704-136719, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[10] Zeeshan Zulkifl et al., "FBASHI: Fuzzy and Blockchain-Based Adaptive Security for Healthcare IoTs," *IEEE Access*, vol. 10, pp. 15644-15656, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Nathalie Tan Yhe Huan, and Zuriati Ahmad Zukarnain, "A Survey on Addressing IoT Security Issues by Embedding Blockchain Technology Solutions: Review, Attacks, Current Trends, and Applications," *IEEE Access*, vol. 12, pp. 69765-69782, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] Oumaima Fadi et al., "A Survey on Blockchain and Artificial Intelligence Technologies for Enhancing Security and Privacy in Smart Environments," *IEEE Access*, vol. 10, pp. 93168-93186, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] 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]

[14] Kwame Opuni-Boachie Obour Agyekum et al., "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1685-1696, 2022. [CrossRef] [Google Scholar] [Publisher Link]