Bbrp21 Technique Used To Store And Secure The Data In Cloud Storage Database

S. Alangaram [1], M. Thilagarani [2], S.Keerthika [3], R.Sathyaraj[4], S.Sankarganesh[5]
[1]Assistant Professor, Department of IT, Jaya Engineering College, Chennai,
[2,3,4]Assistant Professor, Department of CSE, Velalar College of Engineering and Technology,Erode.
[5]Assistant Professor, Department of CSE, PSR Engineering College,Sivakasi,

1 alangaram1985@gmail.com, 2 thilagaranim@gmail.com, [3]keerthivs97@gmail.com ,
[4]sathyarajvcet@gmail.com, [5]sankarganesh@psr.edu.in

Abstract: The current globe is data globe. This data produced using online media; this data is unhindered data; this data could be store in cloud storage database; this data have not incredible security; hereafter to beat this issue we apply the Salsa technique. This technique successfully hack the data from the software engineers. BBRP21 strategy has 5 phases. 1. To apply the mystery key S. 2. To discover the n esteem with the assistance of k. 3. Apply the n esteem proper condition. 4. To trade a and b esteems from left in matrix. 5. To find the mystery prime key S. 6. To find the X_1 and X_2 values from prime numbers. 7. To find the $\overline{X}_1$ and $\overline{X}_2$ values. 8. To find the standard deviation values with the help of equation 3 and 4. 9. To trade a and b esteems from left in matrix. 10. To locate the T-test values and pair it that numbers from left to right. After applied these steps will be stored in cloud storage. The BBRP21 strategy gives extraordinary security while appearing differently in relation to Salsa technique.

Keywords: BBRP21, Cloud, Encryption, Decryption, Prime, T-test, Salsa

1. INTRODUCTION

The current globe is data globe. This data produced using online media; this data is unhindered data; this data could be stored in cloud storage database; this data have not incredible security; from now on to beat this issue we apply the Salsa technique. This procedure adequately hack the data from the software engineers. The extra revolutions XOR for ChaCha is deficiency assault [1]. This creator is utilized new hash idea for key speculating and ending condition [2]. Creator was presented thw bricklayer assault for investigation of ChaCha [3]. They basically focuse the security for Double A [4]. They made new plan for secure quick and adaptable calculation [5]. SRB18 strategy used to give security to information [6]. SRB21 Phase 1 and SRB21 Phase 2 strategy used to give security to information [7][8]. CBB21, CBB22, CBB20, and RBJ25 techniques are used to give security to information [9][10][12][13]. Presented the novel strategy BBRP(Bagath Basha and RajaPrakash) 2.

Table 1. Encryption Algorithm

Steps	Encryption Algorithm
i	To multiply the secret key ‘S’ in given matrix.
Ii	To find the n value with the help of ‘K’
iii	If n is even number where n=2k $a^n+b^n = (a+b)\ (a^{n-1}- a^{n-2}b+ a^{n-3}b^2…-b^{n-2}a+b^{n-1})$ **(1)**
iv	To apply the n value in equation (1)
v	To merge the step 4 values from left to right.
vi	Step 5 values will be apply in given matrix.

vii	To find a prime numbers in given matrix IP.
viii	Equally separate the two parts of prime numbers and apply those values in equation (2), (3), and (4).
ix	T-Test Formula = $(\overline{X}_1 - \overline{X}_2)/\sqrt{((S_1^{\ 2}/N_1)+(S_2^{\ 2}/N_2))}$ **(2)**
x	To find the values for equation (2) with the help of equation (3) and (4).
xi	$\overline{X}_1 = \sum X_1 / N_1 \qquad \overline{X}_2 = \sum X_2 / N_2$ **(3)**
xii	$S_1 = \sqrt{\sum (X_1 - \overline{X}_1)^2 /(N_1 - 1)} \qquad S_2 = \sqrt{\sum (X_2 - \overline{X}_2)^2 /(N_2 - 1)}$ **(4)**
xiii	To pair the T-test value from left to right and swap it those numbers.

Table 2. Decryption Algorithm

Steps	**Decryption Algorithm**
i	To find a prime numbers in matrix TTED.
ii	Equally separate the two parts of prime numbers.
iii	$S_1 = \sqrt{\sum (X_1 - \overline{X}_1)^2 /(N_1 - 1)} \qquad S_2 = \sqrt{\sum (X_2 - \overline{X}_2)^2 /(N_2 - 1)}$ **(5)**
iv	$\overline{X}_1 = \sum X_1 / N_1 \qquad \overline{X}_2 = \sum X_2 / N_2$ **(6)**
v	T-Test Formula = $(\overline{X}_1 - \overline{X}_2)/\sqrt{((S_1^{\ 2}/N_1)+(S_2^{\ 2}/N_2))}$ **(7)**
vi	To merge the values step 5 from right to left and swap it those numbers.
vii	To find the n value with the help of ‘K’
viii	If n is even number where n=2k $a^n+b^n = (a+b)\ (a^{n-1} - a^{n-2}b + a^{n-3}b^2 \ldots -b^{n-2}a+b^{n-1})$ **(8)**
ix	To apply the n value in equation (5)
x	To merge the step 4 from right to left.
xi	Step 5 values will be apply in given matrix.
xii	To divide the secret key ‘S’ in given matrix.

Encryption

$$A = \begin{bmatrix} 112/7 & 113/7 & 114/7 \\ 115/7 & 116/7 & 117/7 \\ 118/7 & 119/7 & 120/7 \end{bmatrix}$$

Where A is Matrix A

- To multiply the key S=2 in matrix A

$$EA = \begin{bmatrix} 224/7 & 226/7 & 228/7 \\ 230/7 & 232/7 & 234/7 \\ 236/7 & 238/7 & 240/7 \end{bmatrix}$$

Where EA is Encryption Matrix A

- To find the n value: a=2,b=3, k=2,n=4
- **n is even number**

<u>Using Equation (1)</u>

- $a^2+b^3= (2+3)(2^{4-1}-2^{4-2}3+2^{4-3}3^2-2^{4-4}3^3+3^{4-3}2-3^{4-2}2+3^{4-1})$
- $a^2+b^3= (5)\ (2^3-2^2 3+2^1 9-2^0 27+3^1 2-3^2 2+3^3)$
- $a^2+b^3= (5)(16-12+18-54+6-18+27)$
- $a^2+b^3= (5)(-17)$
- $a^2+b^3= (5,1), (7,0)$

Pair-1 (5,1)

$$EA = \begin{bmatrix} 232/7 & 226/7 & 228/7 \\ 230/7 & 224/7 & 234/7 \\ 236/7 & 238/7 & 240/7 \end{bmatrix}$$

Pair-2 (7,0)

$$EA = \begin{bmatrix} 236/7 & 226/7 & 228/7 \\ 230/7 & 224/7 & 234/7 \\ 232/7 & 238/7 & 240/7 \end{bmatrix}$$

- Prime Numbers – 1, 3, 5, 7
- X_1= 1, 3
- X_2 = 5, 7

<u>Using Equation (3) and (6)</u>

- $\overline{X}_1 = \sum X_1 / N_1$
  - $\overline{X}_1$ = (1+3)/2
  - $\overline{X}_1$ =4/2
  - $\overline{X}_1$ =2
- $\overline{X}_2 = \sum X_2 / N_2$

- ○ $\overline{X}_2$=(5+7)/2
- ○ $\overline{X}_2$=6

Table 3. X_1 and X_2 Values

X_1	$(X_1-\overline{X}_1)$	$(X_1-\overline{X}_1)^2$	X_2	$(X_2-\overline{X}_2)$	$(X_2-\overline{X}_2)^2$
1	-1	1	5	-1	1
3	1	1	7	1	1
	$\sum(X_1-\overline{X}_1)^2$	2		$\sum(X_2-\overline{X}_2)^2$	2

<u>Using Equation (4) and (5)</u>

- $S_1=\sqrt{\sum(X_1-\overline{X}_1)^2/(N_1-1)}$ $\qquad S_2=\sqrt{\sum(X_2-\overline{X}_2)^2/(N_2-1)}$
- $S_1=\sqrt{(2/(2-1))}$ $\qquad S_2=\sqrt{(2/(2-1))}$
- $S_1=\sqrt{(2/1)}$ $\qquad S_2=\sqrt{(2/(1))}$
- $S_1=1.41$ $\qquad S_2=1.41$

<u>Using Equation (2) and (7)</u>

- T-Test Formula = $(\overline{X}_1-\overline{X}_2)/\sqrt{((S_1{}^2/N_1)+(S_2{}^2/N_2))}$
- T-Test Formula = $(2-6)/\sqrt{((1.41^2/2)+(1.41^2/2))}$
- T-Test Formula = $-4/\sqrt{((1.60/2)+(1.60/2))}$
- T-Test Formula = $-4/\sqrt{((1.60+1.60)/2))}$
- T-Test Formula = $-4/\sqrt{(3.2/2)}$
- Pair the T-test value from left to right (4,3) (2,2) and swap it those numbers.

Step 1:

Pair 3 (4,3)

$$\text{TTEA} = \begin{bmatrix} 236/7 & 226/7 & 230/7 \\ 228/7 & 224/7 & 234/7 \\ 232/7 & 238/7 & 240/7 \end{bmatrix}$$

Where TTEA is T-Test Encryption A

Step 2:

Pair 3 (2, 2)

$$\text{TTEA} = \begin{bmatrix} 236/7 & 226/7 & 230/7 \\ 228/7 & 224/7 & 234/7 \\ 232/7 & 238/7 & 240/7 \end{bmatrix}$$

Decryption

- Pair the T-test value from right to left (2,2), and (3,4) and swap it those numbers.

$$\text{TTDA} = \begin{bmatrix} 236/7 & 226/7 & 230/7 \\ 228/7 & 224/7 & 234/7 \\ 232/7 & 238/7 & 240/7 \end{bmatrix}$$

Where TTDA is T-Test Decryption A

Pair 1: (2,2)

$$\text{TTDA} = \begin{bmatrix} 236/7 & 226/7 & 230/7 \\ 228/7 & 224/7 & 234/7 \\ 232/7 & 238/7 & 240/7 \end{bmatrix}$$

Pair 2: (3, 4)

$$\text{TTDA} = \begin{bmatrix} 236/7 & 226/7 & 228/7 \\ 230/7 & 224/7 & 234/7 \\ 232/7 & 238/7 & 240/7 \end{bmatrix}$$

Using Equation (8)

Pair-3 (0,7)

$$\text{DA} = \begin{bmatrix} 232/7 & 226/7 & 228/7 \\ 230/7 & 224/7 & 234/7 \\ 236/7 & 238/7 & 240/7 \end{bmatrix}$$

Pair-4 (1,5)

$$\text{DA} = \begin{bmatrix} 224/7 & 226/7 & 228/7 \\ 230/7 & 232/7 & 234/7 \\ 236/7 & 238/7 & 240/7 \end{bmatrix}$$

- To divide the key S=2 in matrix DA

$$\text{A} = \begin{bmatrix} 112/7 & 113/7 & 114/7 \\ 115/7 & 116/7 & 117/7 \\ 118/7 & 119/7 & 120/7 \end{bmatrix}$$

2. CONCLUSIONS

The current globe is data globe. This data produced using online media; this data is unhindered data; this data could be stored in cloud storage database; this data have not incredible security; hereafter to beat this issue we apply the Salsa technique. This technique successfully hack the data from the software engineers.

BBRP21 strategy has 5 phases. 1. To apply the mystery key S. 2. To discover the n esteem with the assistance of k. 3. Apply the n esteem proper condition. 4. To trade a and b esteems from left in matrix. 5. To find the mystery prime key S. 6. To find the X_1 and X_2 values from prime numbers. 7. To find the $\overline{X}_1$ and $\overline{X}_2$ values. 8. To find the standard deviation values with the help of equation 3 and 4. 9. To trade a and b esteems from left in matrix. 10. To locate the T-test values and pair it that numbers from left to right. After applying these steps could be stored in cloud storage database. The BBRP21 technique gives great security while contrasted and Salsa strategy. Later on, to add the prime variables tasks of the information security.

REFERENCES

[1] *S V Dilip Kumar, Sikhar Patranabis, Jakub Breier, Debdeep Mukhopadhyay, Shivam Bhasin†, Anupam Chattopadhyay, and Anubhab Baksi, "A Practical Fault Attack on ARX-like Ciphers with a Case Study on ChaCha20", Workshop on Fault Diagnosis and Tolerance in Cryptography,* ***(2017)****,pp.33-40.*

[2] *P. A. Babu and J. J. Thomas, "Freestyle, a randomized version of ChaCha for resisting offline brute-force and dictionary attacks", IEEE Transactions on Information Forensics and Security,* ***(2018)****.*

[3] *A. Adomnicai, J. J. A. Fournier, and L. Masson, "Bricklayer Attack: A Side-Channel Analysis on the ChaCha Quarter Round", Progress in Cryptology International Conference on Cryptology,* ***(2017)****.*

[4] *B. Mazumdar, S.K. S. Ali and O. Sinanoglu, "Power Analysis Attacks on ARX: An Application to Salsa20", IEEE 21st On-Line Testing Symposium,* ***(2015)****,Halkidiki, Greece.*

[5] *C. Watt, J. Renner, N. Popescu, S. Cauligi, and D. Stefan, "CT-Wasm: Type-Driven Secure Cryptography for The Web Ecosystem", Proceedings of the ACM on Programming Languages,* ***(2019)****, pp. 77:1-77:29.*

[6] *C. B. Basha and S. Rajaprakash, "Enhancing The Security Using SRB18 Method of Embedding Computing", Microprocessors and Microsystems, 103125,* ***(2020)****.*

[7] *C. B. Basha and S. Rajaprakash, "Securing Twitter Data Using Srb21 Phase I Methodology", International Journal of Scientific & Technology Research, vol. 8, no. 12,* ***(2019)****, pp.1952–1955.*

[8] *C. B. Basha and S. Rajaprakash, "Applying the SRB21 Phase II Methodology for Securing Twitter Analyzed Data", AIP Conference Proceedings of the International Conference on Mechanical, Electronics and Computer Engineering, 2271,* ***(2020)****.*

[9] *C. B. Basha and S. Rajaprakash, "Applying The CBB21 Phase 2 Method For Securing Twitter Analyzed Data", Advances in Mathematics: Scientific Journal, vol. 9, no. 3,* ***(2020)****, pp.1085-1091.*

[10] *C. B. Basha, S. Rajaprakash,, V. V. A. Harish, M. S. Krishna, K. Prabhas, "Securing Twitter Analysed Data Using CBB22 Algorithm", Advances in Mathematics: Scientific Journal, vol. 9, no. 3,* ***(2020)****, pp.1093-1100.*

[11] *C. B. Basha and K. Somasundaram, "A Comparative Study of Twitter Sentiment Analysis Using Machine Learning Algorithms in Big Data", International Journal of Recent Technology and Engineering, vol. 8, no. 1,* ***(2019)****, pp. 591-599.*

[12] *C. B. Basha, S Rajaprakash, S Muthuselvan P Saisatishsunder, and SVL Alekhya Rani, "Applying the CBB20 Algorithm for Twitter Analyzed Data",*

Journal of Physics: Conference Series - First International Conference on Advances in Physical Sciences and Materials, Coimbatore, Tamil Nadu, India.

[13] S Rajaprakash, C Bagath Basha, S Muthuselvan, N Jaisankar and Ravi Pratap Singh, "RBJ25 Cryptography Algorithm For Securing Big Data", Journal of Physics: Conference Series - First International Conference on Advances in Physical Sciences and Materials, Coimbatore, Tamil Nadu, India.