ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.3, 1093–1100
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.3.34 Spec. Issue on RDESTM-2020

SECURING TWITTER ANALYSED DATA USING CBB22 ALGORITHM

C. BAGATH BASHA, S. RAJAPRAKASH[1], VENNA VENKATA ALLURI HARISH, MALLINENI SURESH KRISHNA, AND KAIVARAM PRABHAS

ABSTRACT. Today's world is data world especially social media data, so without data we cannot process anything in the current world. This social media analysed data need security, and also available more algorithm like AES, DES, Salsa, and etc... In In this paper, discuss two existing algorithm such has AES and Salsa and proposed CBB22 algorithm by modifying the Salsa. The proposed algorithm has five stages. The first stage is identifying the prime numbers in the twitter analyzed data matrix, the second stage is to apply the prime number in quadratic equations in the matrix, the third stage is to merge all numbers into a single row, the fourth stage is to form a pair from left to right side from third process, and fifth stage is to swap the cell values with the help of pair from the given matrix. The proposed algorithm calculate the time and compared with both AES and Salsa. The proposed algorithm provides high security while comparing to both existing algorithms.

1. INTRODUCTION

Today's world people heart is social media like Twitter and Facebook. These social media used to users tweet and re-tweet many information from anywhere in the world through the Internet. These tweets are used to analyze the positive or negative tweets, and make polarity score. This polarity score predict the future trends, so need security of the polarity score because this score data can be easily hacked, and changing the score result can face the lot of issues,

[1]*corresponding author*

Key words and phrases. CBB22, Encryption, Decryption, Quadratic Form.

such has company brands, world economic status, and etc...The machine learning algorithm used to predict the future with the help of Twitter [1] and movie reviews with performance [2], Salsa20 used the secret key is 256 bits [3], and it is faster than AES (Advanced Encryption Standard) and provides better security [4]. AES algorithm execution time is high and security also perfect. Salsa20/20 round versions are Salsa20/12, Salsa20/8, Salsa20/5, Salsa20/6, Salsa20/7, and finally Salsa20/4 rounds [5, 6]. SRB21 algorithm used to swap the prime number and secret key [7] . We produce a novel algorithm Chan Bagath Basha22(CBB22) in this current work.

2. Methodology: CBB22 Algorithm

CBB22 algorithm has five stages. The first stage is identifying the prime numbers in the twitter analyzed data matrix, the second stage is to apply the prime number in quadratic equations in the matrix, the third stage is to merge all numbers into a single row, the fourth stage is to form a pair from left to right side from third process, and fifth stage is to swap the cell values with the help of pair from the given matrix as shown in Table 1 and Table 2.

3. Implementation of cbb22 encryption algorithm

This section explained the CBB22 encryption algorithm below

$$A = \begin{bmatrix} 1 & 4 & 8 & 5 \\ 2 & 3 & 6 & 7 \\ 4 & 12 & 10 & 11 \\ 13 & 15 & 17 & 18 \end{bmatrix},$$

where A is analyzed twitter data matrix.

Step 1: Secret keys are stored in the upper triangle cells. Upper triangle secret keys are $a_{12} = 4, a - 13 = 8, a_{14} = 5, a_{23} = 6, a_{24} = 7, a_{34} = 11.$

Step 2:1st cell operations will be add this two values. $a_{12} = (a_{12} + a_{21})/2$, $a_{21} = (a_{12} + a_{21})/2$,

$$E = \begin{bmatrix} 1 & 3 & 8 & 5 \\ 3 & 3 & 6 & 7 \\ 4 & 12 & 10 & 11 \\ 13 & 15 & 17 & 18 \end{bmatrix},$$

where E is encryted matrix.

Step 3: 2nd cell operations will be add this two values.$a_{13} = (a_{13} + a_{31})/2$, $a_{31} = (a_{13} + a_{31})/2$,

$$E = \begin{bmatrix} 1 & 3 & 6 & 5 \\ 3 & 3 & 6 & 7 \\ 6 & 12 & 10 & 11 \\ 13 & 15 & 17 & 18 \end{bmatrix}.$$

Step 4: 3rd cell operations will be add this two values. $a_{14} = (a_{14} + a_{41})/2$, $a_{41} = (a_{14} + a_{41})/2$,

$$E = \begin{bmatrix} 1 & 3 & 6 & 9 \\ 3 & 3 & 6 & 7 \\ 6 & 12 & 10 & 11 \\ 9 & 15 & 17 & 18 \end{bmatrix}.$$

Step 5: 4th cell operations will be add this two values. $a_{23} = (a_{23} + a_{32})/2$, $a_{32} = (a_{23} + a_{32})/2$,

$$E = \begin{bmatrix} 1 & 3 & 6 & 9 \\ 3 & 3 & 9 & 7 \\ 6 & 9 & 10 & 11 \\ 9 & 15 & 17 & 18 \end{bmatrix}.$$

Step 6: 5th cell operations will be add this two values. $a_{24} = (a_{24} + a_{42})/2$, $a_{42} = (a_{24} + a_{42})/2$,

$$E = \begin{bmatrix} 1 & 3 & 6 & 9 \\ 3 & 3 & 9 & 11 \\ 6 & 9 & 10 & 11 \\ 9 & 11 & 17 & 18 \end{bmatrix}.$$

Step 7: 6th cell operations will be add this two values.$a_{34} = (a_{34} + a_{43})/2$, $a_{43} = (a_{34} + a_{43})/2$,

$$E = \begin{bmatrix} 1 & 3 & 6 & 9 \\ 3 & 3 & 9 & 11 \\ 6 & 9 & 10 & 14 \\ 9 & 11 & 14 & 18 \end{bmatrix}.$$

Step 8: To convert the quadratic form from matrix from Step 7 using equation 1.

$$E(x,y) = 1x_{11}^2 + 3x_{22}^2 + 10x_{33}^2 + 18x_{44}^2 + 3x_{12}y_{21} + 6x_{13}y_{31} + 9x_{14}y_{41} + 9x_{23}y_{32}$$
$$+11x_{24}y_{42} + 14x_{34}y_{43} + 18x_{44}y_{44}$$

TABLE 1. CBB22 ENCRYPTION ALGORITHM

STEPS	CBB22 ENCRYPTION
1	Extracting the data from Twitter.
2	Analyzed twitter data are stored in the matrix A.
3	To create secret keys for principal diagonal cell of the matrix.
4	To add the upper and lower triangle cell values except diagonal values in the matrix.
5	Added values should be divided by 2, and store it in appropriate places in the matrix.
6	To form the quadratic form from the matrix using below equation.
7	$E(x_1, ...x_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_i a_j x_i x_j$ where $E(x_1, ...x_n)$ is encrypted matrix, $a_i a_j$ are matrix values, and $x_i x_j$ are matrix cell places. **Equation (1)**

4. IMPLEMENTATION OF CBB22 DECRYPTION ALGORITHM

This section explained the CBB22 decryption algorithm below

$$D(x,y) = 1x_{11}^2 + 3x_{22}^2 + 10x_{33}^2 + 18x_{44}^2 + 3x_{12}y_{21} + 6x_{13}y_{31} + 9x_{14}y_{41} + 9x_{23}y_{32}$$
$$+11x_{24}y_{42} + 14x_{34}y_{43} + 18x_{44}y_{44}$$

TABLE 2. CBB22 DECRYPTION ALGORITHM

STEPS	CBB22 DECRYPTION
1	To get the encryption matrix data.
2	Encryption data are stored in the matrix D.
3	To convert a matrix form using below equation.
4	$D(x_1, ...x_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_i a_j x_i x_j$ where $D(x_1, ...x_n)$ is decrypted matrix, $a_i a_j$ are matrix values, and $x_i x_j$ are matrix cell places. **Equation (2)**
5	Upper and lower triangle values should be added same values except diagonal cell values.
6	To find a decryption secret key for upper triangle values in the matrix.
7	To store the decryption secret key in upper triangle cell values except diagonal cell values.
8	To minus the secret key numbers and store it lower triangle places except diagonal cell values using below equations.
9	LTA=LTA-UTA (OR) UTA-LTA **Equation (3)** where LTA is Lower Triangle and UTA is Upper Triangle.

Step 1: To convert the matrix from quadratic form using equation 2.

$$D = \begin{bmatrix} 1 & 3 & 6 & 9 \\ 3 & 3 & 9 & 11 \\ 6 & 9 & 10 & 14 \\ 9 & 11 & 14 & 18 \end{bmatrix},$$

where D is a decryption matrix.

Step 2: 1st cell operations will be add this two values. $a_{34} = (a_{34} + a_{43})$, $a_{43} = (a_{34} + a_{43})$

Step 3: 2nd cell operations will be add this two values. $a_{24} = (a_{24} + a_{42})$, $a_{42} = (a_{24} + a_{42})$

Step 4: 3rd cell operations will be add this two values. $a_{23} = (a_{23} + a_{32}$, $a_{32} = (a_{23} + a_{32})$

Step 5: 4th cell operations will be add this two values. $a_{14} = (a_{14} + a_{41})$, $a_{41} = (a_{14} + a_{41})$

Step 6: 5th cell operations will be add this two values. $a_{13} = (a_{13} + a_{31})$, $a_{31} = (a_{13} + a_{31})$

Step 7: 6th cell operations will be add this two values. $a_{12} = (a_{12} + a_{21})$, $a_{21} = (a_{12} + a_{21})$

Step 8: To get the decryption keys from sender are $a_{12} = 4, a - 13 = 8,\ a_{14} = 5, a_{23} = 6, a_{24} = 7, a_{34} = 11.$

Step 9: To store the decryption upper triangle secret key values in the appropriate cells.

Step 10: To find the lower triangle values using equation 3:

$$D = \begin{bmatrix} 1 & 4 & 8 & 5 \\ 6 & 3 & 6 & 7 \\ 4 & 12 & 10 & 11 \\ 13 & 15 & 17 & 18 \end{bmatrix}.$$

5. Conclusion

The proposed algorithm CBB22 by modifying the Salsa to enhance further security. CBB22 algorithm compared with AES and Salsa algorithms; 1) N round in CBB22, 16 round in AES, and quarter round in Salsa; 2) Time is high both CBB22 and AES, and time is less in Salsa; 3) Security is more high in CBB22, Security is good in AES, and Security is less in Salsa; 4) Data is converted to equation in CBB22 and data not converted to equation both AES and Salsa. The proposed algorithm provides high security because data converted to equation while compared to both existing algorithms. In future, to add more operations for data security.

References

[1] C. Bagath Basha, K. Somasundaram: *A Comparative Study of Twitter Sentiment Analysis Using Machine Learning Algorithms in Big Data*, Inter. J. of Rec. Tech. and Eng., **8**(1) (2015), 310–324.

[2] B. PANG, L. LEE, S. VAITHYANATHAN: *Thumbs up? Sentiment classification using machine learning techniques*, Pro. of the Con. on Emp. Met. in Nat. Lan. Pro., Philadelphia, 2002.

[3] Z. SHAO, L. DING: *Related-Cipher Attack on Salsa20*, Fou. Inter. Conf. on Comp. and Inf. Sci., Chongqing, China; 2012.

[4] M. ALMAZROOIE, A. SAMSUDIN, M. M. SINGH: *Improving the Diffusion of the Stream Cipher Salsa20 by Employing a Chaotic Logistic Map*, J. of Infor. Proc. Sys., **11**(12) (2019), 1952–1955.

[5] S. FISCHER, W. MEIER, C. BERBAIN, J. BIASSE, M. J. B. ROBSHAW: *Non-Randomness in eSTREAM Candidates Salsa20 and TSC-4*, Ind. Lec. N. in Com. Sci., R. Barua and T. Lange, eds., Springer, Berlin, Heidelberg, 2006.

[6] D. J. BERNSTEIN: *The Salsa20 Family of Stream Ciphers*, N. St. Ci. Des.: The eST. Fin., Lec. Not. in Com. Sc., M. Robshaw and O. Billet, eds., Berlin: Springer, 2008.

[7] C. BAGATH BASHA, S. RAJAPRAKASH: *Securing Twitter Data Using Srb21 Phase I Methodology*, Inter. J. of Sci. and Tech. Res., **8**(12) (2019), 1952–1955.

Department of Computer Science and Engineering
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation
Chennai, Tamil Nadu, India
E-mail address: chan.bagath@gmail.com

Department of Computer Science and Engineering
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation
Chennai, Tamil Nadu, India
E-mail address: rsaiilamaran@gmail.com

Department of Computer Science and Engineering
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation
Chennai, Tamil Nadu, India
E-mail address: vennaharish12@gmail.com

Department of Computer Science and Engineering
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation
Chennai, Tamil Nadu, India
E-mail address: sureshkrishna240@gmail.com

Department of Computer Science and Engineering
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation
Chennai, Tamil Nadu, India