Proceedings of the 4th International Conference on Computing and Data Science (CONF-CDS 2022)
DOI: 10.54254/2755-2721/2/20220624

The Security Algorithm ESS-BR22-002 for enhancing the security of the data

S. Rajaprakash, T Indirajith

Aarupadai Veedu Institute Of Technology, Vinayaka Missions Research Foundation, Chennai, Tamil Nadu, India.

thiruindirajith@gmail.com

Abstract. The information age data is impressively more critical in open life, since people's prosperity data just finished up whether or not COVID'19 affected, and besides associated with all clinical issues data. These data used to inspected and expect the clinical issues data by Machine Learning Algorithm, and a while later expected data need more prominent security. Along these lines, we applied the ongoing procedure ChaCha method and that system focused in figuratively speaking "encryption execution" so security is less. In this paper, to apply the new ESS-BR22-001 methodology and this strategy has 8 stages. The 1st stage is finding the K value. The 2nd stage is applying the K value, that is λn is the “order of matrix” and Sk is start from intial values. The 3rd stage is find the Sk values. The 4th stage is to apply the Sk values in the sparse matrix. The 5th stage is sparse matrix values is converted into single line. The 6th stage is pair all the values. The 7th stage is all pair values will be apply in the matrix. The final stage is apply the Salsa operations in the matrix. The new ESS-BR22-002 method has provide security and performance are good while compared to ChaCha method.

Keywords: ChaCha, Encryption, Security, ESS-BR22.

1. Introduction

The continuous age, people's heath issue data extended bit by bit especially COVID'19 data. To examine the COVID'19 data and expect the data by using AI estimation. From Figure 1, the request assumption process is Yes or No. Unpredictable forest area assumption process is Mean Square Error. Gullible bayes figure process is probability. Support vector machine conjecture process is backslide and Yes or No. Decision tree assumption process is tree. Counterfeit mind network assumption process is back spread.

These assumption data is most restricted intel and ought to be secure that data yet security level is low level, so apply the ongoing methodology ChaCha. This procedure is four round cycle and "all inclining characteristics move to the chief area". The encryption time of ChaCha strategy is especially speedy yet security level is very low. Thusly, the new procedure Eigen Sparse Salsa BagathRaj (ESS-BR) 22-002.

DOI: 10.54254/2755-2721/2/20220624

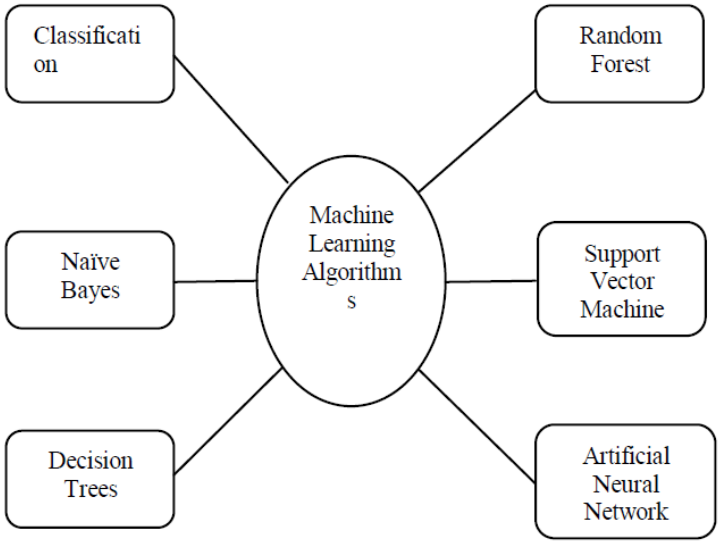

Figure. 1. Machine Learning Algorithms [1].

2. Related Work

The analyzing data with AI estimations and get the show result for certain, computations are differentiated and them. These computations execution showed and particularly basic and appreciate estimation is organization computation [1]. The CBB21 computation is differentiated and Salsa20/4 estimation and principally took a gander at the running time [2]. They separated data with AI estimation and besides inspected data applied the CBB20 computation, and differentiated the running time and Salsa20/4 [3]. They focused on the separated twitter data with AI computation, and besides applied SRB21 security estimation for that data, then, at that point, differentiated the speed time and Salsa [4]. They look at first twitter data then, separated with guessed that data by AI estimation, and applied SRB18 security computation to that data, then differentiated the running time and Salsa for encryption [5]. They proposed the RBJ25 cryptography estimation for general data and differentiated the show and AES and ChaCha for encryption [6]. They focused on the AES and Salsa estimation for encryption security and pondered the display of the proposed security computation is RB20 for encryption time [7].

The CBB22 estimation is proposed and give the security of summarized data. "This computation is broke down the show of the both encryption and interpreting time with Salsa and AES" [8]. They focused on the encryption speed time for Salsa and appeared differently in relation to the proposed SRB21 stage 1 computation [9]. The generally examination the analysis of movies through feeling assessment by gathering and SVM computations [10]. They inspected the huge data and store that data with affirmation process applied for RBJ20 estimation. This estimation has four stages used to protect the data [11]. Different algorithms are used for various security applications [12][13].

3. Methodology

The prediction analyzed data used to apply the new method is ESS-BR22-002 has 8 stages [14]. The 1st stage is finding the K value. The 2nd stage is applying the K value in Equation (1). The 3rd stage is find the Sk values by using Equation (1). The 4th stage is apply the Sk values in the sparse matrix [15]. The 5th stage is sparse matrix values is converted into single line. The 6th stage is pair all the values [16]. The 7th stage is all pair values will be apply in the matrix. The final stage is apply the salsa operations [17].

3.1. Algorithm

Step 1: Input of the public affected Covid'19 positive data.
Step 2: To convert the matrix data format from the positive data.

DOI: 10.54254/2755-2721/2/20220624

Step 3: $\lambda n - Sk\ \lambda n-1 + Sk+1\ \lambda n-2 - Sk+2\ \lambda n-3 - \ldots.. + Sk+\infty\ \lambda n-\infty - Sk=n = 0$
where n = order of the matrix, k=1
Step 4: To find the Sk values using equation 1.
Step 5: To apply the Sk values in the sparse matrix.
Step 6: The sparse matrix values converted into single line.
Step 7: To pair all the values and apply to the matrix.
Step 8: To apply the Salsa operations in the matrix.

$$\text{CP Data}=\begin{bmatrix}-2 & -4 & 2\\ -2 & 1 & 2\\ 4 & 2 & 5\end{bmatrix}$$

Where CP data is Covid Positive data

Encryption Working Process

Using Equation (1)

- $\lambda^n - S_k\ \lambda^{n-1} + S_{k+1}\ \lambda^{n-2} - S_{k+2}\ \lambda^{n-3} - \ldots.. + S_{k+\infty}\ \lambda^{n-\infty} - S_{k=n} = 0$
  where n = order of the matrix, k=1
- n=3, k=1
- $\lambda^3 - S_1\ \lambda^2 + S_2\ \lambda - S_3 = 0$

To find S_1 value

- S_1= sum of main diagonal element values
- $S_1 = 4$

To find S_2 value

- $S_2=\begin{vmatrix}1 & 2\\ 2 & 5\end{vmatrix}+\begin{vmatrix}-2 & 2\\ 4 & 5\end{vmatrix}+\begin{vmatrix}-2 & -4\\ -2 & 1\end{vmatrix}$
- $S_2=-27$

To find S_3 value

- $S_3=-2\begin{vmatrix}1 & 2\\ 2 & 5\end{vmatrix}-(-4)\begin{vmatrix}-2 & 2\\ 4 & 5\end{vmatrix}+2\begin{vmatrix}-2 & -4\\ -2 & 1\end{vmatrix}$
- $S_3=-90$
- $\lambda^3 - S_1\ \lambda^2 + S_2\ \lambda - S_3 = 0$
- $\lambda^3 - 4\lambda^2 - 27\lambda + 90 = 0$
- $$\begin{array}{r|cccc} 3 & 1 & -4 & -27 & 90\\ & 0 & 3 & -3 & -90\\ \hline & 1 & -1 & -30 & 0\end{array}$$
- $\lambda^2 - \lambda - 30 = 0$
- $\lambda=5, \lambda=-6$
- Now, all λ values will be apply to the sparse matrix. The first two λ values in the two diagonal cells and second λ values in the 3rd diagonal cell, then remaining one λ value will be store in the lower diagonal cell and another one λ value will be store in the upper diagonal cell in the matrix.

$$\text{SM}=\begin{bmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}$$

Where SM is sparse matrix

DOI: 10.54254/2755-2721/2/20220624

$$SM=\begin{bmatrix} 1 & 1 & 5 \\ 0 & -1 & 0 \\ -30 & 0 & -6 \end{bmatrix}$$

- (1,1), (5,0), (-1,0), (-3,0), (0,-6)

$$CP=\begin{bmatrix} -2 & -4 & 2 \\ -2 & 1 & 2 \\ 4 & 2 & 5 \end{bmatrix}$$

- Pair (1,1)

$$CP=\begin{bmatrix} -2 & -4 & 2 \\ -2 & 1 & 2 \\ 4 & 2 & 5 \end{bmatrix}$$

- Like this remaining pair operations will do Pairs -(5,0), (-1,0), (-3,0).

- Pair (0,-6)

$$CP=\begin{bmatrix} 4 & 2 & 2 \\ -4 & 1 & -2 \\ -2 & 2 & 5 \end{bmatrix}$$

- To apply the Salsa operations

$$CP=\begin{bmatrix} 4 & 1 & 5 \\ -4 & 2 & 2 \\ -2 & 2 & -2 \end{bmatrix}$$

4. Result & Discussion

The proposed algorithm ESS-BR22-002 “encryption performance compared with ChaCha. ChaCha concept is the all diagonal values move to the 1st column” [18][19]. The three by three matrix has “24 bytes of fie size; the six by six matrix has 76 bytes of file size; the ten by ten matrix has 312 bytes of file size [20][21]; the fifteen by fifteen matrix has 812 bytes of file size; the twenty by twenty matrix has 1531 bytes of file size; and the forty by forty matrix has 6580 bytes of file size” as shown in the Table 1 [22][23].

From Fig.2, the ESS-BR22-002 method and has compared the encryption speed in seconds [24][25]. The encryption performance of “the speed 1.69 (s), 1.29 (s), 2.73 (s), 2.64 (s), 3.4 (s), and 2.27 (s) for the ChaCha”, and 2 (s), 2.5 (s), 2.9 (s), 3.1 (s), 3.7 (s) and 3.9(s) for the ESS-BR22-002 [26][27]. The ESS-BR22-002 gives “more protection of the data; when compared to existing techniques” [28][29].

DOI: 10.54254/2755-2721/2/20220624

Table 1. ESS-BR22-002 encryption performance

File Size	ChaCha	ESS-BR22-002
24	1.69	2
76	1.29	2.5
312	2.73	2.9
822	2.64	3.1
1531	3.4	3.7
6580	2.27	3.9

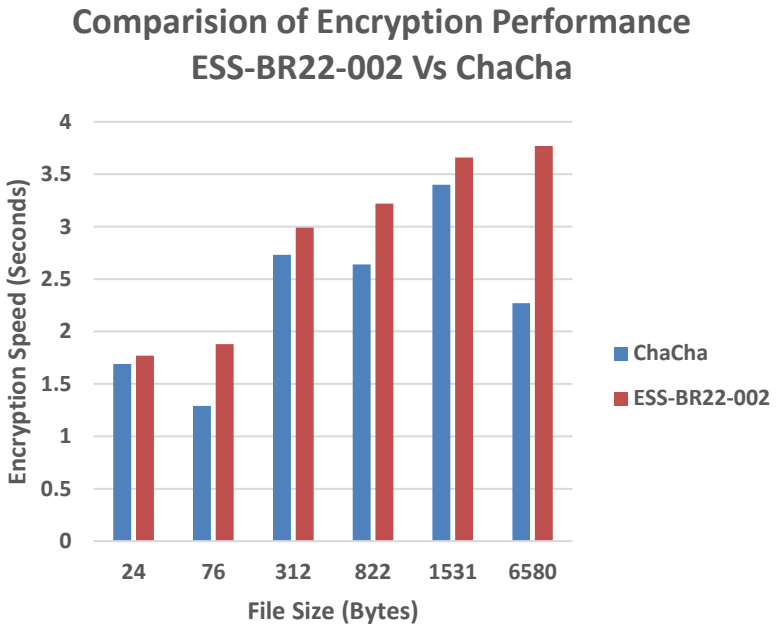

Figure. 2. Encryption performance

5. Conclusion

The present information is widely more tremendous in open life, since individuals' success information just shut whether COVID'19 impacted, furthermore connected with all clinical issues information. These information used to investigated and anticipate the clinical issues information by Machine Learning Algorithm, and some time later expected information need more essential security. In this way, we applied the continuous framework ChaCha strategy and that procedure centered in a manner of speaking "encryption execution" so security is less. In this paper, to apply the new ESS-BR22-002 framework and this system has 8 stages. The 1st stage is finding the K value. The 2nd stage is applying the K value in Equation (1). The 3rd stage is find the Sk values by using Equation (1). The 4th stage is apply the Sk values in the sparse matrix. The 5th stage is sparse matrix values is converted into single line. The 6th stage is pair all the values. The 7th stage is all pair values will be apply in the matrix. The final stage is applying the Salsa operations in the matrix. The new ESS-BR22-002 method has provide security and performance are good while compared to ChaCha method.

References

[1] Bagath Basha, C and Somasundaram K: A Comparative Study of Twitter Sentiment Analysis Using Machine Learning Algorithms in Big Data. International Journal of Recent Technology and Engineering, 591-599 (2019).

DOI: 10.54254/2755-2721/2/20220624

[2] Bagath Basha, C and Rajaprakash, S: Applying The CBB21 Phase 2 Method For Securing Twitter Analyzed Data. Advances in Mathematics: Scientific Journal, 1085-1091 (2020).
[3] Bagath Basha, C. Rajaprakash, S. Muthuselvan, P. Saisatishsunder, and Alekhya Rani, SVL: Applying the CBB20 Algorithm for Twitter Analyzed Data. In: First International Conference on Advances in Physical Sciences and Materials, Coimbatore, Tamil Nadu, India, (2020).
[4] Bagath Basha, C and Rajaprakash, S: Applying the SRB21 Phase II Methodology for Securing Twitter Analyzed Data. In: International Confererence on Mechanical Electronics and Computer Engineering, (2020).
[5] Bagath Basha, C and S. Rajapraksh, S: Enhancing The Security Using SRB18 Method of Embedding Computing. Microprocessor and Microsystems, (2020).
[6] Rajaprakash, S. Bagath Basha, C. Muthuselvan, S. Jaisankar, N. and Ravi Pratap Singh: RBJ25 Cryptography Algorithm For Securing Big Data. In: First International Conference on Advances in Physical Sciences and Materials, Coimbatore, Tamil Nadu, India, (2020).
[7] Karthik, K. Bagath Basha, C. Bhaswanth Thilak, U. Sai Kiran, T. and Raj J.: Securing Social Media Analyzed Data Using RB20 Method. Advances in Mathematics: Scientific Journal, 3 (2020).
[8] Bagath Basha, C. Rajaprakash, S. Harish, V.V.A., Krishna, M.S. and Prabhas, K.: Securing Twitter Analysed Data Using CBB22 Algorithm. Advances in Mathematics: Scientific Journal, 1093-1100 (2020).
[9] Bagath Basha, C. and Rajaprakash, S.: Securing Twitter Data Using SRB21 Phase I Methodology. International Journal of Scientific & Technology Research, 1952-1955 (2019).
[10] Jaichandran, R. Bagath Basha, C. Shunmuganathan, K. L. Rajaprakash, S. and Kanagasuba Raja, S.: Sentiment Analysis of Movies on Social Media using R Studio. International Journal of Engineering and Advanced Technology, 8 (2019).
[11] Rajaprakash, S. Jaisankar, N. Bagath Basha, C. Jayan, A. Sebastian, G.: RBJ20 Cryptography Algorithm for Securing Big Data Communication using Wireless Networks. WorldS4, Springer, LNNS Book Series (ISSN: 237 – 3370, London, 499-507 (2022).
[12] Sathishkumar V E, Changsun Shin, Youngyun Cho, "Efficient energy consumption prediction model for a data analytic-enabled industry building in a smart city", Building Research & Information, Vol. 49. no. 1, pp. 127-143, 2021.
[13] Sathishkumar V E, Youngyun Cho, "A rule-based model for Seoul Bike sharing demand prediction using Weather data", European Journal of Remote Sensing, Vol. 52, no. 1, pp. 166-183, 2020.
[14] Sathishkumar V E, Jangwoo Park, Youngyun Cho, "Seoul Bike Trip duration prediction using data mining techniques", IET Intelligent Transport Systems, Vol. 14, no. 11, pp. 1465-1474, 2020.
[15] Sathishkumar V E, Jangwoo Park, Youngyun Cho, "Using data mining techniques for bike sharing demand prediction in Metropolitan city", Computer Communications, Vol. 153, pp. 353-366, 2020.
[16] Sathishkumar V E, Yongyun Cho, "Season wise bike sharing demand analysis using random forest algorithm", Computational Intelligence, pp. 1-26, 2020.
[17] Sathishkumar, V. E., Wesam Atef Hatamleh, Abeer Ali Alnuaim, Mohamed Abdelhady, B. Venkatesh, and S. Santhoshkumar. "Secure Dynamic Group Data Sharing in Semi-trusted Third Party Cloud Environment." Arabian Journal for Science and Engineering (2021): 1-9.
[18] Chen, J., Shi, W., Wang, X., Pandian, S., & Sathishkumar, V. E. (2021). Workforce optimisation for improving customer experience in urban transportation using heuristic mathematical model. International Journal of Shipping and Transport Logistics, 13(5), 538-553.
[19] Pavithra, E., Janakiramaiah, B., Narasimha Prasad, L. V., Deepa, D., Jayapandian, N., & Sathishkumar, V. E., Visiting Indian Hospitals Before, During and After Covid. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 30 (1), 111-123, 2022.

DOI: 10.54254/2755-2721/2/20220624

[20] Easwaramoorthy, S., Moorthy, U., Kumar, C. A., Bhushan, S. B., & Sadagopan, V. (2017, January). Content based image retrieval with enhanced privacy in cloud using apache spark. In International Conference on Data Science Analytics and Applications (pp. 114-128). Springer, Singapore.

[21] Sathishkumar, V. E., Agrawal, P., Park, J., & Cho, Y. (2020, April). Bike Sharing Demand Prediction Using Multiheaded Convolution Neural Networks. In Basic & Clinical Pharmacology & Toxicology (Vol. 126, pp. 264-265). 111 RIVER ST, HOBOKEN 07030-5774, NJ USA: WILEY.

[22] Subramanian, M., Shanmuga Vadivel, K., Hatamleh, W. A., Alnuaim, A. A., Abdelhady, M., & VE, S. (2021). The role of contemporary digital tools and technologies in Covid-19 crisis: An exploratory analysis. Expert systems.

[23] Babu, J. C., Kumar, M. S., Jayagopal, P., Sathishkumar, V. E., Rajendran, S., Kumar, S., ... & Mahseena, A. M. (2022). IoT-Based Intelligent System for Internal Crack Detection in Building Blocks. Journal of Nanomaterials, 2022.

[24] Subramanian, M., Kumar, M. S., Sathishkumar, V. E., Prabhu, J., Karthick, A., Ganesh, S. S., & Meem, M. A. (2022). Diagnosis of retinal diseases based on Bayesian optimization deep learning network using optical coherence tomography images. Computational Intelligence and Neuroscience, 2022.

[25] Liu, Y., Sathishkumar, V. E., & Manickam, A. (2022). Augmented reality technology based on school physical education training. Computers and Electrical Engineering, 99, 107807.

[26] Sathishkumar, V. E., Rahman, A. B. M., Park, J., Shin, C., & Cho, Y. (2020, April). Using machine learning algorithms for fruit disease classification. In Basic & clinical pharmacology & toxicology (Vol. 126, pp. 253-253). 111 RIVER ST, HOBOKEN 07030-5774, NJ USA: WILEY.

[27] Sathishkumar, V. E., Venkatesan, S., Park, J., Shin, C., Kim, Y., & Cho, Y. (2020, April). Nutrient water supply prediction for fruit production in greenhouse environment using artificial neural networks. In Basic & Clinical Pharmacology & Toxicology (Vol. 126, pp. 257-258). 111 RIVER ST, HOBOKEN 07030-5774, NJ USA: WILEY.

[28] Sathishkumar, V. E., & Cho, Y. (2019, December). Cardiovascular disease analysis and risk assessment using correlation based intelligent system. In Basic & clinical pharmacology & toxicology (Vol. 125, pp. 61-61). 111 RIVER ST, HOBOKEN 07030-5774, NJ USA: WILEY.

[29] Kotha, S. K., Rani, M. S., Subedi, B., Chunduru, A., Karrothu, A., Neupane, B., & Sathishkumar, V. E. (2021). A comprehensive review on secure data sharing in cloud environment. Wireless Personal Communications, 1-28.