AC-JBR22 Based On Method To Secure The Data

S. Kishore[1], A. Rajesh[2]
[1,2]*Department of CSE, AVIT, Chennai, Tamil Nadu, India*
[1]*kishore123@gmail.com*

Received: 06.01.2025 Revised: 06.02.2025 Accepted: 16.02.2025 Published:28.02.2025

Abstract - *One of the most important role of the data development security system, which are growth the secret key randomly in AES and Salsa algorithm. Nowadays data security is more important thing in worldwide, because which security system will be decreased the threats and AES algorithm has 16 round and each round has multiple rounds of the process and then Salsa operate the limited rounds only not to given well security. These issues will be solved by the AC-JBR22 operations. This operations has four process. The first 3rd-process will be used the opposite diagonal keys only and 4th-process will be rotated all diagonal keys to the 1strow. Therefore, the new AC-JBR22 operations will do encryption process is very fast and given good security while comparing to the existing operations.*

Keywords - *AES, Salsa, security, speed, encryption, AC- JBR22*

1. Introduction

The information security has become one of the issues which ought to be tended to critically. Actually the rough speed incredibly data equivalent nature and rapidly developing programmability of delineations taking care of units make them an appealing stage for general explanation estimation. The AES estimation is as of now the standard block-figure computation that has follow the “Data Encryption Standard (DES)”.Standard AES computation's very long encryption time makes it unable to satisfy the demand for quick encryption. In light of this, the GPU's (Realistic Dealing with Unit) top show handling limit becomes a hot topic of research due to its higher data move information transfer and improved parallelism. The Cg language does AES encryption estimation based on unparalleled GPU execution handling. The major developments are also examined and distinguished, and the assessment's final result about the estimation's viability is displayed. It has been demonstrated that the estimation speed of an AES computation using a graphics processing unit is significantly faster than an AES computation using a central processing unit. AES key lengths of 128 have 10 rounds, 192 have 12 rounds, and 256 have 14 rounds. The new strategy AESChaCha-JaiBagathRaj22(AC-JBR22).

2. Related work

Creator learned about AES encryption calculation execution of speed with computer processor's [1]. They plan the two plans and those plans determined the throughput utilizing AES [2]. They focus on the key and joining the two primary part as AES and ECC [3]. Creator concentrated on top to bottom of AES calculation and that calculation contrast with existing calculations [4]. They discussed the three principal symmetric based key calculations like "AES, Blowfish", and Salsa20" [5]. They learned about the how to anticipate the information from different sources [6]. Creator concentrated on the co- indivisible numbers top to bottom and applied in lattice [7][9]. They applied the three activities and that tasks are contrast the presentation and different strategies [8]. Creators are focus on the corner to corner keys and typical key [10]. They discussed the AES and executed that strategy [11]. They concentrated on the ideal [12] and indivisible numbers [13]. Creator exchange the typical key and prime key [14]. They anticipate the film audits utilizing AI calculation [15]. They broke down the cryptography calculation and AES calculation [16]. They secure the statistical data by sensor [17]. To detect and secure the cloud data [18]. To protect the data from clone attack [19].

3. Methodology

The new method AC-JBR22 has 4 operations like randomly get the diagonal values from matric data and applied to Equation(1); To apply the calculated reverse diagonal values to the DVRA matrix; and similarly those calculated values will be used to do the swapping process in DVRS matrix; To operate the operations will be moved to the first row for all reverse diagonal values in DVRF matrix.

Algorithm for Encryption

- To discover the any general information and that information converted to the format of matrix.
- To discover the diagonal values randomly from I matrix.
- To apply the random values in Equation(1)
- DVR = a $\frac{az+\alpha z}{a\beta+\alpha\beta}$ Equation (1)
- where DV is diagonal value
- To calculate the DV values and those values will be swap the operations in I matrix.
- To operate the all operations will be moved to the first row of the reverse diagonal values in the I matrix.

4. Discussion

$$\mathbf{I}=\begin{bmatrix} \frac{1X1}{5} & \frac{1B2}{5} & \frac{1C3}{5} & \frac{1Z4}{5} \\ \frac{2A1}{5} & \frac{2X2}{5} & \frac{2Z3}{5} & \frac{2D4}{5} \\ \frac{3A1}{5} & \frac{3Z2}{5} & \frac{3X3}{5} & \frac{3D4}{5} \\ \frac{4Z1}{5} & \frac{4B2}{5} & \frac{4C3}{5} & \frac{4X4}{5} \end{bmatrix}$$

Where I is data

- Let a=23, y=41, α=22, and β=44
- DVRA = $\frac{(23*41)+(22*41)}{(23*44)+(22*44)}$

  where DVRA is Diagonal Values Reverse Applied
- DVRA = $\frac{(943)+(902)}{(1012)+(968)}$

$$\text{DVRA}=\begin{bmatrix} \frac{1X1}{5} & \frac{1B2}{5} & \frac{1C3}{5} & \frac{1Z4}{5} \\ \frac{2A1}{5} & \frac{10X12}{5} & \frac{94Z3}{5} & \frac{2D4}{5} \\ \frac{3A1}{5} & \frac{3Z2}{5} & \frac{3X3}{5} & \frac{3D4}{5} \\ \frac{4Z1}{5} & \frac{4B2}{5} & \frac{4C3}{5} & \frac{96X8}{5} \end{bmatrix}$$

- DVRS Pairs = (94),(39),(02),(10),(12),(96),(80)

  where DVRS Diagonal Values Reverse Swap

1. (9,4)

$$\text{DVRA}=\begin{bmatrix} \frac{1X1}{5} & \frac{1B2}{5} & \frac{1C3}{5} & \frac{1Z4}{5} \\ \frac{2A1}{5} & \frac{10X12}{5} & \frac{3D4}{5} & \frac{2D4}{5} \\ \frac{3A1}{5} & \frac{3Z2}{5} & \frac{3X3}{5} & \frac{94Z3}{5} \\ \frac{4Z1}{5} & \frac{4B2}{5} & \frac{4C3}{5} & \frac{96X8}{5} \end{bmatrix}$$

2. (3,9)

$$\text{DVRA}=\begin{bmatrix} \frac{1X1}{5} & \frac{1B2}{5} & \frac{1C3}{5} & \frac{1Z4}{5} \\ \frac{2A1}{5} & \frac{10X12}{5} & \frac{4Z1}{5} & \frac{2D4}{5} \\ \frac{3A1}{5} & \frac{3Z2}{5} & \frac{3X3}{5} & \frac{94Z3}{5} \\ \frac{3D4}{5} & \frac{4B2}{5} & \frac{4C3}{5} & \frac{96X8}{5} \end{bmatrix}$$

3. (0,2)

$$\text{DVRA}=\begin{bmatrix} \frac{1X1}{5} & \frac{1B2}{5} & \frac{1C3}{5} & \frac{1Z4}{5} \\ \frac{2A1}{5} & \frac{10X12}{5} & \frac{4Z1}{5} & \frac{2D4}{5} \\ \frac{3A1}{5} & \frac{3Z2}{5} & \frac{3X3}{5} & \frac{94Z3}{5} \\ \frac{3D4}{5} & \frac{96X8}{5} & \frac{4C3}{5} & \frac{4B2}{5} \end{bmatrix}$$

4. (1,0)

$$\text{DVRA}=\begin{bmatrix} \frac{1X1}{5} & \frac{1B2}{5} & \frac{1C3}{5} & \frac{1Z4}{5} \\ \frac{2A1}{5} & \frac{10X12}{5} & \frac{4Z1}{5} & \frac{2D4}{5} \\ \frac{3A1}{5} & \frac{3Z2}{5} & \frac{3X3}{5} & \frac{94Z3}{5} \\ \frac{3D4}{5} & \frac{96X8}{5} & \frac{4B2}{5} & \frac{4C3}{5} \end{bmatrix}$$

5. (1,2)

$$\text{DVRA}=\begin{bmatrix} \frac{1X1}{5} & \frac{1B2}{5} & \frac{1C3}{5} & \frac{1Z4}{5} \\ \frac{2A1}{5} & \frac{10X12}{5} & \frac{4Z1}{5} & \frac{2D4}{5} \\ \frac{3A1}{5} & \frac{3Z2}{5} & \frac{3X3}{5} & \frac{94Z3}{5} \\ \frac{3D4}{5} & \frac{4B2}{5} & \frac{96X8}{5} & \frac{4C3}{5} \end{bmatrix}$$

6. (9,6)

$$\text{DVRA}=\begin{bmatrix} \frac{1X1}{5} & \frac{1B2}{5} & \frac{1C3}{5} & \frac{1Z4}{5} \\ \frac{2A1}{5} & \frac{10X12}{5} & \frac{3Z2}{5} & \frac{2D4}{5} \\ \frac{3A1}{5} & \frac{4Z1}{5} & \frac{3X3}{5} & \frac{94Z3}{5} \\ \frac{3D4}{5} & \frac{4B2}{5} & \frac{96X8}{5} & \frac{4C3}{5} \end{bmatrix}$$

7. (8,0)

$$\text{DVRA}=\begin{bmatrix} \frac{1X1}{5} & \frac{1B2}{5} & \frac{1C3}{5} & \frac{1Z4}{5} \\ \frac{2A1}{5} & \frac{10X12}{5} & \frac{3Z2}{5} & \frac{4C3}{5} \\ \frac{3A1}{5} & \frac{4Z1}{5} & \frac{3X3}{5} & \frac{94Z3}{5} \\ \frac{3D4}{5} & \frac{4B2}{5} & \frac{96X8}{5} & \frac{2D4}{5} \end{bmatrix}$$

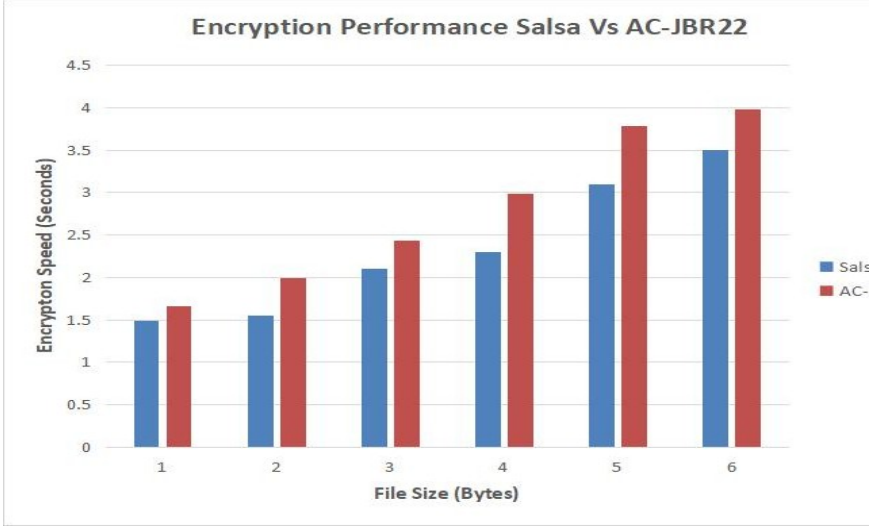

Fig. 1 Performance of the method for Salsa Vs AC-JBR22

From figure 1 show the comparison and performance of the method between Salsa and AC-JBR22. Every operations has speed of encryption are well while comparing to the existing operations of the Salsa. Finally, the graph show it the performance of the proposed and existing operations.

5. Conclusion

Everyday security system will be developed in worldwide. This system growth will be increased day-to-day and discover the random secret key in AES. In this paper, we proposed the method AC-JBR22. This method randomly discover the diagonal values from matric data and applied to Equation(1); To apply the calculated reverse diagonal values to the DVRA matrix; and similarly those calculated values will be used to do the swapping process in DVRS matrix; To operate the operations will be moved to the first row for all reverse diagonal values in DVRF matrix. Therefore, the new AC- JBR22 operations of the speed of encryption process is express and show good security while comparing to the existing operations.

References

[1] Fei Shao, Zinan Chang, and Yi Zhang, “AES Encryption Algorithm Based on the High Performance Computing of GPU”, Proceedings of the Second International Conference on Communication Software and Networks, 2010, PP 588 590.

[2] Shady Mohamed Soliman, Baher Magdy, and Mohamed A. Abd El Ghany, "Efficient Implementation of the AES Algorithm for Security Applications", Proceedings of the Seventeenth IEEE Workshop on Control and Modeling for Power Electronics, Compel 2016, Trondheim, Norway, 2016, PP 206 210.

[3] Nishtha Mathur and Rajesh Bansode, " AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection", Proceedings of the 7th International Conference on Communication, Computing and Virtualization, Mumbai, Maharashtra, India, 2016. PP 1036 1043.

[4] Ako Muhamad Abdullah, 'Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data", Cryptography and Network Security, 2017.

[5] Madhumita Panda and Atul Nag, "Plain Text Encryption Using AES, DES and SALSA20 by Java Based Bouncy Castle API on Windows and Linux", Proceedings of the Second International Conference on Advances in Computing and Communication Engineering, Dehradun, India, 2015, PP 541 548.

[6] 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).

[7] 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).

[8] 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).

[9] 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).

[10] Bagath Basha, C and S. Rajapraksh, S: Enhancing The Security Using SRB18 Method of Embedding Computing. Microprocessor and Microsystems, (2020).

[11] 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).

[12] 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).

[13] 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).

[14] Bagath Basha, C. and Rajaprakash, S.: Securing Twitter Data Using SRB21 Phase I Methodology. International Journal of Scientific & Technology Research, 1952-1955 (2019).

[15] 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).

[16] 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).

[17] Krishnasamy, L., Dhanaraj, R. K., Ganesh Gopal, D., Reddy Gadekallu, T., Aboudaif, M. K., & Abouel Nasr, E. (2020). A Heuristic Angular Clustering Framework for Secured Statistical Data Aggregation in Sensor Networks. Sensors, 20(17), 4937. https://doi.org/10.3390/s20174937

[18] Rajesh Kumar, D., & Shanmugam, A. (2017). A Hyper Heuristic Localization Based Cloned Node Detection Technique Using GSA Based Simulated Annealing in Sensor Networks. In Cognitive Computing for Big Data Systems Over IoT (pp. 307–335). Springer International Publishing. https://doi.org/10.1007/978-3-319-70688-7_13

[19] Sathish, R., & Kumar, D. R. (2013, April). Dynamic Detection of Clone Attack in Wireless Sensor Networks. 2013 International Conference on Communication Systems and Network Technologies. 2013 International Conference on Communication Systems and Network Technologies (CSNT 2013). https://doi.org/10.1109/csnt.2013.110