Suitable encrypting algorithms in Parallel Processing for improved efficiency

Sampath Kumar Tallapally\textsuperscript{1} and Dr. B. Manjula\textsuperscript{2}
\textsuperscript{1}Department of Computer Science & Engineering, SR University, Warangal, Telangana, India
\textsuperscript{2}Dept, of CS, Kakatiya University, Warangal, Telangana, India.
Email: tsk0707@gmail.com

Abstract. Cryptographic algorithms play a vital role in providing security to the data and from malicious attacks. Now a day’s storing the data in the Cloud became essential for organizations to reduce the overhead of securing the data within the organization. “Stream ciphers” are more vulnerable to attacks when compared to “Block Ciphers”. In this article we used java platform to evaluate and compare all the block cipher techniques used for converting plain text to cipher text and we have identified the best block cipher technique which can be used in cloud.

Keywords: AES, EC, CBC, CF, OF, CTR, Cloud Computing

1. Introduction
Securing information over internet can be done with the help of Cryptography which is done by encrypting the information (plain text to cipher text that is in non readable and non understandable format) as with the encrypting algorithms and decrypting the information (cipher text to plain text) is taken with the help of decrypting algorithms and a key is used to encrypt [1] and further decrypt [4] the text by using the implementation of a physical key [2] which is further locks or encrypts the data so that only someone with the right key can unlock or decrypt the data. These algorithms can be further classified into two types that is symmetric algorithms [3] and asymmetric algorithms [2] where symmetric algorithms comprises of a similar key (secret key) s the encryption and decryption are the probable information generated which is based on the asymmetric algorithms using the dissimilar (public private) keys for performing encrypting and decrypting of the information[4, 5].

With the rapid increase in the size of key that is used for performing the encryption as the strength of the cipher further advances as it is hard to analyze the data streams as the key size is directly proportional to the strength of the cipher [6, 7]. A file which needs to be transmitted over network which contains sensitive information can be done in two ways one is stream ciphers and other is block ciphers where a “Stream” is the which is frequently utilized based on the speed and straightforwardness of data to be further executed and implied in applications as the plaintext comes in amounts of mysterious length which is considerably safe when associated in the block ciphers that are implemented on specific size of data blocks that comprises of distinct rounds [8-10].
One of the technique that enables concurrent processing is called as the “Parallel Processing” where the task implemented will evolve to further enhance the processing speed of transactions or instructions in a computer system as the main task of parallel processing is to improvise the computer computing capabilities which are further boosted based on the throughput on which the processing speed is based for imparting the processing in a given time span [11, 12].

A Thread is an individual and independent part of any of the application which can be executed simultaneously used for faster outputs as we creating more than one thread for an application is called multithreaded application which has the applications advantages such as: 1) Responsiveness [13] 2) Faster executions [14] 3) Enhanced system utilization [15] 4) Simplified sharing and communication [16] 5) Parallelization [17]

2. Background
When stream ciphers and block ciphers are compared with each other stream ciphers are strong [5]. The term “Confusion Hides” is the association among cipher text and the key as well as the “Diffusion” which is initially not visible in the association in between cipher text and plain text as the block ciphers have high diffusion and stream ciphers have low diffusion because the block ciphers are immune to injection where as stream ciphers are not and block ciphers that slowly encrypts where as stream ciphers are fast encrypters as they are used when we deal with small amount of sensible data whereas block ciphers are used when we want operate on huge amount of data such as cloud Computing where we deal with huge amount of data so we need to use block ciphers, below are certain modes [18].
Table 1. Summary of modes

| Mode               | Formulas                                               | Cipher Text | E- P | D- P | RRA |
|--------------------|--------------------------------------------------------|-------------|------|------|-----|
| “Electronic Codebook” | “Y_i=F(PlainText_i, Key)”                           | “Y_i”       | Yes  | Yes  | Yes |
| “Cipher Block Chaining” | “Y_i=PlainText_i XOR CipherText_{i-1}” | “F(Y, Key) CipherText_0=IV” | No    | Yes  | Yes |
| “Cipher Feedback”   | “Y_i=CipherText_{i-1}”                               | “Plaintext XOR F(Y, Key) CipherText_0=IV” | No    | Yes  | Yes |
| “Output Feedback”   | “Y_i=F(Y_{i-1},Key)”                                 | “Plaintext XOR Y_i” | No    | No   | No  |
| “Counter”           | “Y=F(IV+g(i),Key)”                                   | “Plaintext XOR Y_i” | Yes  | Yes  | Yes |

E-P: Encryption parallelizable D-P: decryption parallelizable RRA: Random Read Access

Electronic Codebook- The message or File is partitioned into fixed blocks, and each block is encoded independently. The weakness of the strategy is absence of dispersion. Since ECB encodes indistinguishable plaintext hindends into indistinguishable ciphertext squares.

Cipher Block Chaining- Each block of “plaintext is XORed with the past cipher text block before being encoded along these lines where each cipher text block relies upon all plaintext obstructs to that point and to make each message interesting and an instatement vector must be utilized in the principal block”.

In the following equations C denotes cipher text, P denotes plain text and E denotes encryption and D denotes decryption function and k denotes the key.

Mathematical formula for CBC encryption is

\[ C_i = E_K(P_i \oplus C_{i-1}). \]  \hspace{1cm} (1)
\[ C_0 = IV, \]  \hspace{1cm} (2)

Mathematical formula for CBC decryption is

\[ P_i = D_K(C_i) \oplus C_{i-1}. \]  \hspace{1cm} (3)
\[ C_0 = IV. \]  \hspace{1cm} (4)

Cipher Feedback is implemented in the mod of CFB which is almost relative to the CBC that converts a squared figure into a considerable self synchronizing stream figure as the fundamental activity which is same as the specifically for implementing the CFB as it is decoded and is practically indistinguishable from implementing the CBC encryption which is implemented backward based on the aspect

\[ P_i = E_K(C_{i-1}) \oplus C_i; \]  \hspace{1cm} (5)
\[ C_i = E_K(C_{i-1}) \oplus P_i; \]  \hspace{1cm} (6)
\[ C_0 = IV. \]  \hspace{1cm} (7)

Output Feedback is implemented on the OFB [6] mode that converts a block figure into set of coordinates that are mapped to the stream figure which develops the blocks of key streams and further XOR operation is performed over the plaintext blocks to attain the cipher text which is similar to the stream figures as the flipping of a piece of cipher text that produces the flipped bit in the plaintext as the similar area and its attained property permits numerous errors or faults in the revising codes to
work based on the probable events which is applied before the encryption operation as the balance attained for the XOR activity performs the encryption and decoding which are essentially equivalent and attainable.

\[ C_j = P_j \oplus O_j \]  
(8)

\[ P_j = C_j \oplus O_j \]  
(9)

\[ O_j = E_k (I_j) \]  
(10)

\[ I_j = O_{j-1} \]  
(11)

\[ I_0 = IV \]  
(12)

Counter: Is the counter mode that transforms the block figure into a stream of figures that produces the following key streams that obstruct for encoding the progressive estimations as the counter which can be represented based on the capacity attained for delivering the succession to ensure that the capability in a genuine augmentation over the counter value which is attained and is least difficult and is a part of mainstream data as it is the generic deterministic info as the work is almost questionable.

Experimental Setting: In this study we used a laptop of i3 processor with 8 GB of RAM, WIN 7 as our Operating System and used Java 10 as our platform and GIT-HUB libraries to carry out our experiment[20].

Our main objective of this work is to identify best block cipher technique which can be used in cloud which uses parallel computing for performing the task assigned to it and to have better results.

3. Implementation of parallel encryption algorithm
In the present era of “high performance computing” the process of adapting the distributed computing for forming the clusters which have the properties such as more power with lower cost workstations or desktop computers are linked within the fast communication interfaces for attaining he maximum performance which is considered to be “Parallel Computing (PC)” [6]. By enhancements in the processing speed or communication speed of microprocessor with respect to their clock speeds we have attained maximum performance in the areas of public domains that also includes the implementation of robust software such as “operating system, compiler tools and message passing libraries, make cluster based computing” which tends to be economical and cost effective while processing the data in node or server machine based on the communication speeds and more over a processor is also considered to be a program which shares the data between distinct objects called as the process by passing messages between them.

The predominant “Message Passing Interface (MPI)” is the basic approach which is identified to be best and mature method for implementing the same execution process in parallel programming because of its features or qualities such as simplicity and robustness while implementing the “Application Program Interface (API)” in Java for evaluating the methodology using the parallel machines to form and utilize the implementation of clusters. In the present trend message passing is considered to be the most vital or important aspect in implementing of parallel processing paradigm for performing encryption over the MPI based clusters without any issues.

Merely the performance aspects of parallel algorithm clearly relies over the input size as well as the hardware architecture where the parallel computing is implemented as it includes the ram size, processor capacity, established communication procedure and the network architecture for implementing distinct types of parallel architectures that handles over input and output of data with distinct key sizes and processing iterations for measuring the run time complexity for evaluating the parallel algorithms with respect to serial implementation is considered[19].

4. Simulation results:
We have taken the AES algorithm for implementing the encrypting algorithm that comprises the distinct modes of operations and it is also based on the standard encryption algorithm in recent years as the block cipher comprises of the block length of 128 bits and AES is comprises of three distinct key lengths of (128, 192, or 256) bits and for performing the simulation process we need to assume
that the key length is of 128 bits and we have implemented the simulation over all the five algorithms and illustrated the results in Table 1 based on which it is observed that CTR and EC modes are quicker while converting the plain text into cipher text [6].

**Table 2. Random results attained**

| Block Cipher Algorithm | Encryption Time Key Length | File Size (MB) |
|------------------------|----------------------------|----------------|
|                        | 128 | 192 | 256 |                |
| EC                     | 1450 | 1562 | 1978 | 50             |
| CBC                    | 1833 | 1658 | 1963 | 48             |
| CF                     | 1700 | 1635 | 1985 | 40             |
| OF                     | 1685 | 1688 | 1920 | 45             |
| CTR                    | 1548 | 1547 | 1921 | 49             |

And the equaling histogram attained in is illustrated in figure 3.

4.1. Based on the implemented block cipher techniques for attaining the performance we identified that only Counter and Electronic Code Book are eligible to be executed on parallel machines because of their independent nature we executed these two techniques on multithreaded java environment assuming that each thread is executing on distinct core of the computer to utilize the CPU to a maximum extent and had the following results for different file sizes.
When Electronic Codebook and Counter modes are technically compared with each other EC is most vulnerable to cryptanalysis and Counter mode is resistant as it is capable of performing distinct attacks because it combines the features of Stream Ciphers in generating the ounce value used as an input into the algorithm[21-23].

5. Conclusion
From the above analysis and results we conclude that Counter mode is the best option to be used when using Cloud for encrypting the text and further dividing and executing parallel by using the concept of threads. Every file under execution will comprises of one or more files of plain text for different threads is implemented to attain the equal or similar sizes but the conversion speed to cipher text is not at equal pace, so we used suitable data structures to merge those blocks in to original order that complexity need to be added. And we have compared and found the best five algorithms that can be used in future aspects out of which when implemented the block cipher over parallel computing only EC and CTR have yielded the acceptable performance.

6. References
[1] Ali Shaik, M. 2020 Time series forecasting using vector quantization International Journal of Advanced Science and Technology vol 29(4) pp 169-175
[2] Shaik, M.A. 2019 A survey on text classification methods through machine learning methods International Journal of Control and Automation vol 12(6) pp 390-396
[3] Shaik, M.A., Sampath Kumar, T., Praveen, P., Vijayaprakash, R. 2019 Research on multi-agent experiment in clustering International Journal of Recent Technology and Engineering vol 8(4) pp 1126-1129
[4] S Mounika, T Sampath Kumar 2019 Client –requirement fulfil QOS in multi server for max beneficial in cloud computing International Journal of Advanced Science and Technology vol 7(3) 201-209
[5] P Praveen, B Rama, T Sampath Kumar 2017 An efficient clustering algorithm of minimum Spanning Tree Proceedings of the 3rd IEEE International Conference on Advances in Electrical and Electronics, Information, Communication and Bio-Informatics, AEEICB
[6] T Sampath Kumar, B Manjula, D Srinivas 2017 A new technique to secure data over cloud Journal of Advanced Research in Dynamical and Control Systems vol 21(4) pp 123-127
[7] Shaik, M.A. 2018 Protecting Agents from Malicious Hosts using Trusted Platform Modules (TPM) Proceedings of the International Conference on Inventive Communication and Computational Technologies, ICICCT vol 8 pp 559-564

[8] Mohammed Ali Shaik, P.Praveen, Dr. R. Vijaya Prakash 2019 Novel Classification Scheme for Multi Agents Asian Journal of Computer Science and Technology Vol.8(3) pp 54-58

[9] R Ravi Kumar, M Babu Reddy, P Praveen 2019 An evaluation of feature selection algorithms in machine learning International Journal of Scientific and Technology Research, vol 7 pp. 142-149

[10] P Praveen, C Jayanth Babu 2019 Big Data Clustering: Applying Conventional Data Mining Techniques in Big Data Environment Lecture Notes in Networks and Systems.

[11] B Rama, P Praveen, H Sinha, T Choudhury 2017 A study on causal rule discovery with PC algorithm International Conference on Infocom Technologies and Unmanned Systems: Trends and Future Directions, ICTUS

[12] R Ravi Kumar, M Babu Reddy, P Praveen 2017 A review of feature subset selection on unsupervised learning Proceedings of the 3rd IEEE International Conference on Advances in Electrical and Electronics, Information, Communication and Bio-Informatics, AEEICB

[13] Sheshikala M, Kothandaraman D, Vijaya Prakash R, Roopa G 2019 Natural language processing and machine learning classifier used for detecting the author of the sentence Int J Recent Technol Eng vol 8(3) pp 936-939

[14] Pasha SN, Ramesh D, Kodhandaraman D, Salauddin MD 2019 An research to enhance the old manuscript resolution using deep learning mechanism Int J Innov Technol Explor Eng vol 8(6) pp 1597-1599

[15] Mothe R, Tharun Reddy S, Chythanya KR, Supragna Reddy Y 2019 Challenges, open research issues and tools in bigdata analytics Int J Recent Technol Eng vol 8(11) pp 2634-2641

[16] Dadi R, Salauddin, Pasha SN, Harshavardhan A, Kumarawamy P 2019 Adapting best path for mobile robot by predicting obstacle size Int J Innov Technol Explor Eng vol 8(9) pp 200-202

[17] Pramod Kumar P, Sandeep CH, Naresh Kumar S. 2018 An overview of the factors affecting handovers and effective highlights of handover techniques for next generation wireless networks Indian J Public Health Res Dev vol 9(11) pp 722-725

[18] Jamalpur Bhavana, Komuravelly Sudheer Kumar 2018 Implementation of Bow model Towards Obtaining Discriminative Features of the Images International Journal of Advanced Science and Technology vol 28 pp 17-25

[19] Harshavardhan A, Suresh Babu Dr and Venugopal T Dr 2016 “3D Surface Measurement through Easy-snap Phase Shift Fringe Projection”, Springer conference International Conference on Advanced Computing and Intelligent Engineering Proceedings of ICACIE 1 179-186

[20] Harshavardhan A, Suresh Babu Dr and Venugopal T Dr 2017 “An Improved Brain Tumor Segmentation Method from MRI Brain Images” 2017 2nd International Conference On Emerging Computation and Information Technologies (ICECIT) IEEE 1–7. DOI.org (Crossref) doi:10.1109/ICECIT.2017.8453435.

[21] Mahender K, Kumar TA and Ramesh KS 2019 Simple transmit diversity techniques for wireless communications Advances in Intelligent Systems and Computing 669 329-342 10.1007/978-981-10-8968-8_28

[22] Rajasri I, Gupta AVSSKS and Rao YVD 2016 Generation of Egs: Hamming Number Approach Procedia Engineering 144 537-542 10.1016/j.proeng.2016.05.039

[23] Seena Naik K and Sudarshan E 2019 Smart healthcare monitoring system using raspberry Pi on IoT platform ARPN Journal of Engineering and Applied Sciences 14(4) 872-876.