International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-6, April 2020

Ensuring Cloud Security Scheme with Hybrid Encryption Technique using AES_RSA for Fragmented Data

P. Peter Jose, S. P. Victor

Abstract: ***Cloud storage provides the enormous benefits to the cloud user. Especially the data accessibility feature that allows the user to access their data anywhere any time. But cloud computing maintain the distributed environment for storing the data which increase the risk of data leakages. A suitable solution to reduce the security risk is to deploy encryption mechanism. Ensuring security on cloud storage is still a challenging issue. In this paper a hybrid encryption techniques is proposed with three powerful algorithms such as Advanced Encryption Standard, Rivest–Shamir–Adleman (RSA) and MD5. The Encryption scheme executes between the fragmentation and replication process. The proposed hybrid framework strength the security of cloud data. If any successful attacks occurs the attackers does not able to discover the plaintext. The implementation was carried out with the help of Clousim framework. The performance of this study is compared with prior encryption techniques.***

Keywords: Cloud Storage, Security, Hybrid Encryption, AES, RSA, MD5.

I. INTRODUCTION

Cloud computing model offers the massive computation capacity at reasonable cost. It acts as the bone for IT industries and many organizations. The entire details such as employee's information, sales and stocks, machinery operation, customer relationship management activities are running with the help of cloud technology. Several features are introduced nowadays but security regarding issues is still remains [1]. There are various chances to have a security issues in cloud due to faulty equipment, attackers and some mistaken action performed. Among these, criminal intent is still remains due to advanced technology.

The possible solution is to employ the encryption technique to secure the data [1]. Encryption concept protects the data from attackers. Different methods have been proposed by various research scholars to get out of these problems [2-3]. Compared to symmetric encryption Asymmetric encryption is the most suitable encryption approach for data transition, due to the elimination of key management existed in symmetric encryption.

Another framework in enhancing the security is done through data fragmentation and replication.

Revised Manuscript Received on April 30, 2020.
***** Correspondence Author
Peter Jose P.*, Ph.D., Department of Cloud Computing, Bharathiyar University, Coimbatore, Tamil Nadu, India.
Dr. S. P. Victor, Associate Professor, Computer Science, St. Xavier's College Palayamkottai, Tamil Nadu, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

The fragmentation divides the data file into number of chunks based on the available virtual machine and the replication store the fragments in different location The present study focus on ensuring the security of outsourcing data in fragmentation and replication process.

The contribution of the proposed study

- The proposed scheme focuses on both security and performance. The introduced hybrid encryption technique enhances the security of the outsourced data.
- The hybrid algorithm utilized the benefits of three powerful encryption algorithms such as AES, RSA and Md5.
- This scheme divides the file into fragments and replicates them into different nodes that strength the security of the system.
- The retrieval time and the encryption time is reduced significantly.

The remaining section of this paper is organized as follows: the literature review on cloud security on prior encryption techniques is discussed in section 2. Section 3 discusses the prior encryption techniques in detail. Section 4 highlights the proposed three factor encryption techniques with AES, RSA and MD5. The experimental setup and the result obtained in this research are described in section 5. Eventually the summary of the study is given in section 6.

II. RELATED WORKS

The prior research on RSA, AES and encryption on fragmented data in cloud computing is discussed in this section.

Yinghui Zhang et al [4] introduced an attribute privacy protection for outsourced data in mobile computing. The novel scheme called *match then decrypt* is proposed for fast decryption. Sakinah Ali Pitchay et al [5] employs the combination of both AES and RSA for file access in cloud using usb devices. This mechanism simplifies the process for user not to fully memorize the randomly generated keys. The access for file download will be allowed once the system detects the usb device with private keys.

Nandita Sengupta and Ramya Chinnasamy [6] developed the hybrid encryption techniques with Data encryption standard (DES) and CAST algorithm to secure the data from brute force and birthday attacks. Shefali ojha and Vikram Rajput [7] combines the AES and MD5 encryption to secure the cloud authentication. Liu Zhenhua et al [8] introduced a hybrid security scheme with searchable encryption. The cloud can applies the fine grained deduplication after attaching the cipher into bloom filter tree. This study achieved the fine grained access control through the hybrid encryption.

Kanika Sharma et al [9] presents an enhanced RSA based encryption technique to secure the patient sensitive data over cloud. The authors separated the users and data owners based on the domain of health information.

Through this key management complexity has been reduced efficiently. This study allows the data owners to have full control on their data that improves the confidentiality of the data owners and prevents the data from semantic attacks.

Yogita S. Gunjal et al [10] introduced the policy attribute based encryption scheme for maintaining the difficulty in access control. The system secures against the collusion attack. Rupali Sharma and Bharti Joshi [11] develops a hybrid scheme with Identity Based Encryption (IBE) and Attribute Based Encryption (ABE) to ensure the revocation and security on cloud data.

Akshita Bhandari et al [12] creates a hybrid encryption using RSA and AES to improves the trustworthiness in servers. This scheme reduces the memory size, cost and consumption time. The attacks such as timing and brute force have been prevented in this approach.

III. EXISTING ENCRYPTION ALGORITHM

Advanced Encryption Standard (AES)

AES is the symmetric encryption with block of three modes such as 128 bit, 192 and 256 bit. Our study used the 128 bit block for encryption and decryption. Figure 1 shows the key size and the number of round performed during the execution. From this figure it is clear that the number of round in AES algorithm is depends upon the key length.

	Block Size Nb words	Key Length Nk words	Number of Rounds Nr
AES–128-bits key	4	4	10
AES–192-bits key	4	6	12
AES–256-bits key	4	8	14

Figure 1. AES key types

AES enhance the security of data using the four steps: Key Expansion, Initial round, Initial round and Final Round.

Table 1. Important steps with its operations

Steps	Operations
Key Expansion	Carried out with key schedule
Initial round	Only Performs the AddRoundKey operation
Round	Perform four important operations SubBytes, ShiftRows, MixColumns, and an AddRoundKey
Final Round	Works same as Round step without mixcolumns operations.

AES Encryption

The Encryption can be applied in the form of various transformations in a fixed number of iterations, called rounds. During the encryption the number of rounds is selected based on the key length. In the proposed system the key length is 128 bits, therefore the number of iteration required are10. (Nr = 10).

AES Decryption

The encryption process is performed in reverse order to obtain the original data. In the present study the block size is 128 therefore with the 128 bit block all four operations has to be performed in reverse manner. Among the four operations AddRoundKey is same for decryption and the other three has inverse such as Inverse SubBytes, Inverse ShiftRows, and Inverse MixColumns.

RSA

The RSA was developed in 1978[13]. The modulus n is the product of two large prime's p and q, public key and private key are obtained by:

$$e = d - 1 \; mod \; \emptyset(n)$$

The formula for encrypting the plaintext with public key n and e is given below.

$$C = Me \; (mod \; n)$$

Where M denotes the input such that $0 < M$, C denotes the output

$$M = C \; d \; (mod \; n)$$

Message Digest 5 (MD5)

The Md5 is the advanced version of MD4 algorithm. MD5 can process the plaintext at any length and generates the ciphertext with 128 bits. The working procedure of MD5 with 512 bit block is shown in Fig. 2. The demerits of this approach are its simplicity and the collision [14]. Therefore brute force attack is possible when Md5 is utilized for encryption.

Figure 2 shows the working of md5 with 512 bit block. To overcome the disadvantages in all above algorithm our study implements the combination of all three in a single encryption model.

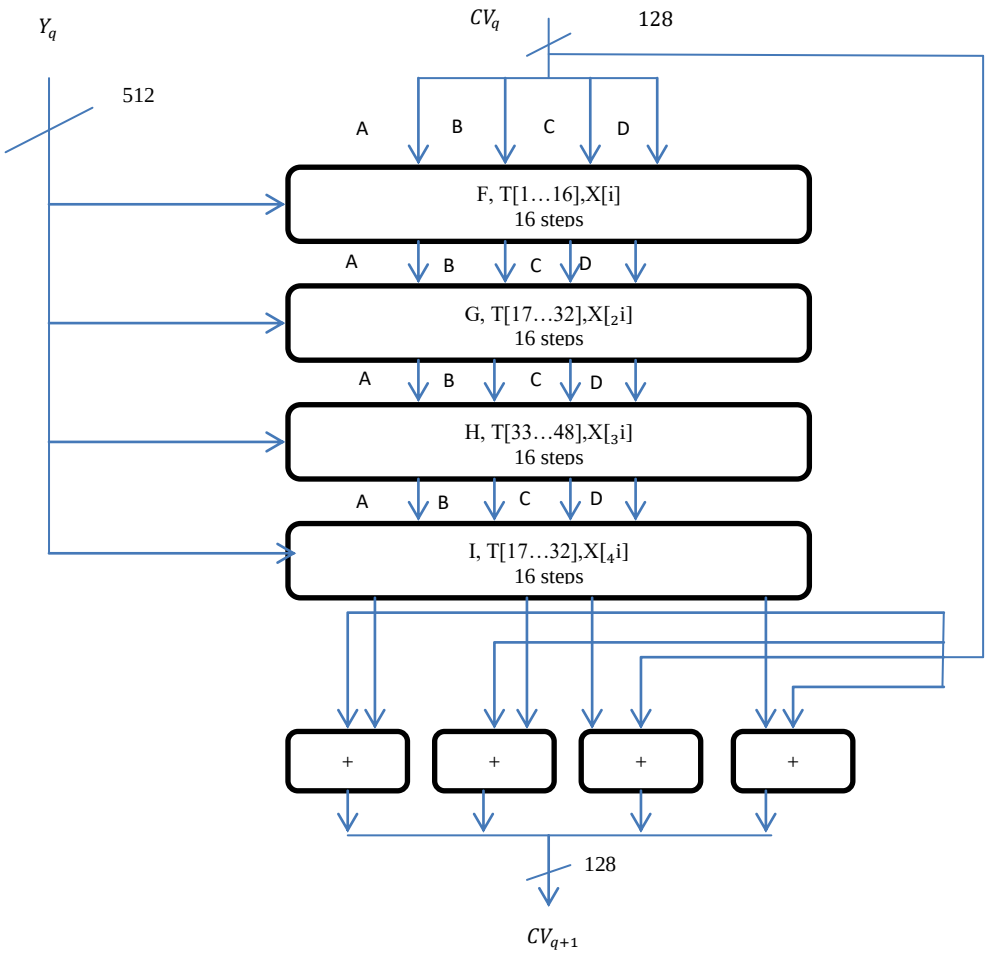
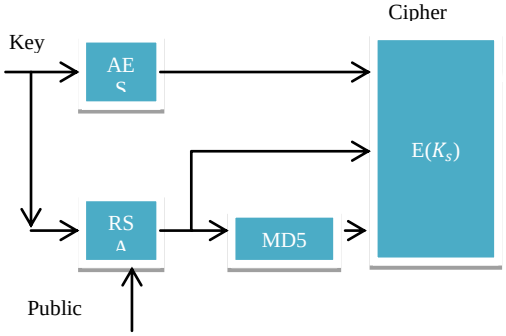


Figure 2. MD5 with 512 bit block

IV. PROPOSED METHODOLOGY

The proposed system ensures the security of cloud storage by applying the fragmentation and replication process with hybrid encryption technique. In our previous study [15] concept of fragmentation and Replication have discussed. Hence this study focuses on encryption part alone. The AES and RSA algorithm is combined with MD5 encryption technique to develop the hybrid security on cloud data. Initially the uploaded user data is fragmented and encrypted with Secret key using AES and the secret key of AES is encrypted with RSA algorithm. In order to strength the security MD5 hash function is includes in this approach. The working procedure of the present study is given in figure 3.



The proposed architecture shows that the uploaded file is encrypted with three layer security scheme. The algorithm procedure is given in Table 2. The procedure only covers the encryption part of the fragmented files.

Procedure of Hybrid Encryption

Initialize the Cloudsim with datacenter, Virtual machine, etc
For all files do
Generate a secret key with the key length of 40-448 bits
Apply RSA to encrypt the Key, K_s
Obtain Cipher text by applying AES
Generate 512 bit Message Digest using MD5 algorithm for the Encrypted Message

$$HM = MD5(E(ME))$$

For all message do
Generate $KS, E(ME), HM$
. End for
Send $CM = KS + E(ME) + HM$
End for
Disconnect the session
End

V. EXPERIMENT EVALUATION

The present study is implemented with the java and Cloudsim jar for cloud based simulation. Java is the powerful language allows the user to create the user interface with simple effort. Java has enormous supporting libraries for algorithm and other software packages. The proposed study develops the user interface with Netbeans IDE. The performance of the hybrid encryption is compared with AES, RSA and MD5. The comparative result is analyzed based on the time taken for encryption, Throughput, response time for the entire data outsourcing system which contains fragmentation and replication and memory utilized.

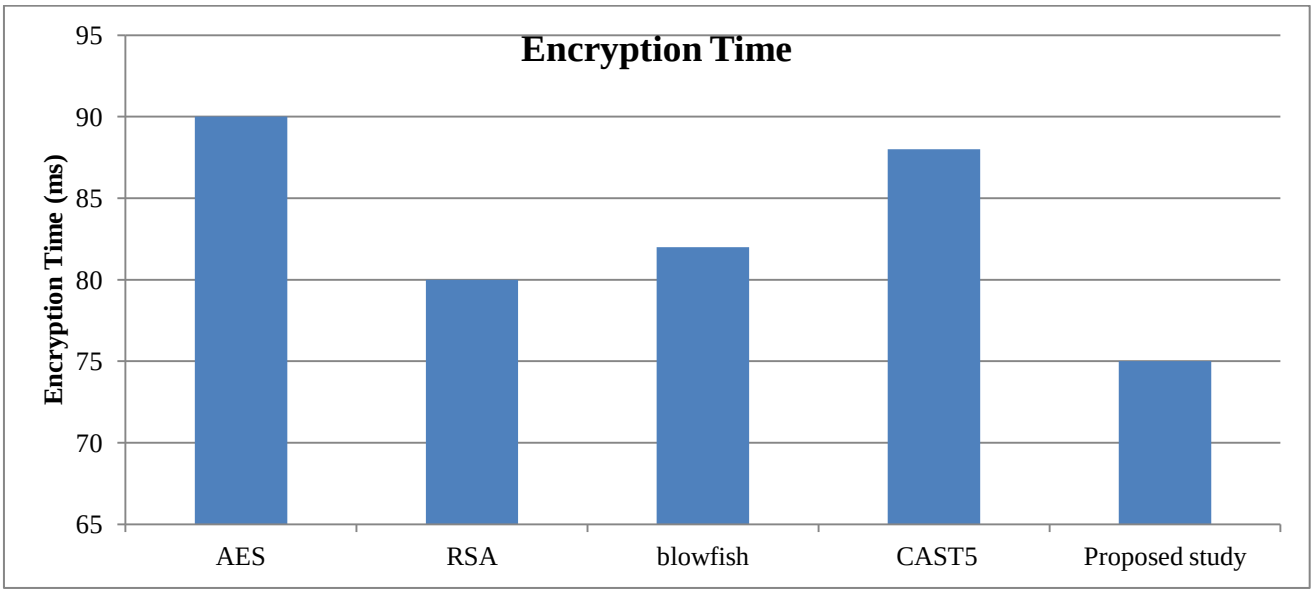


Figure 3 Encryption Time Report

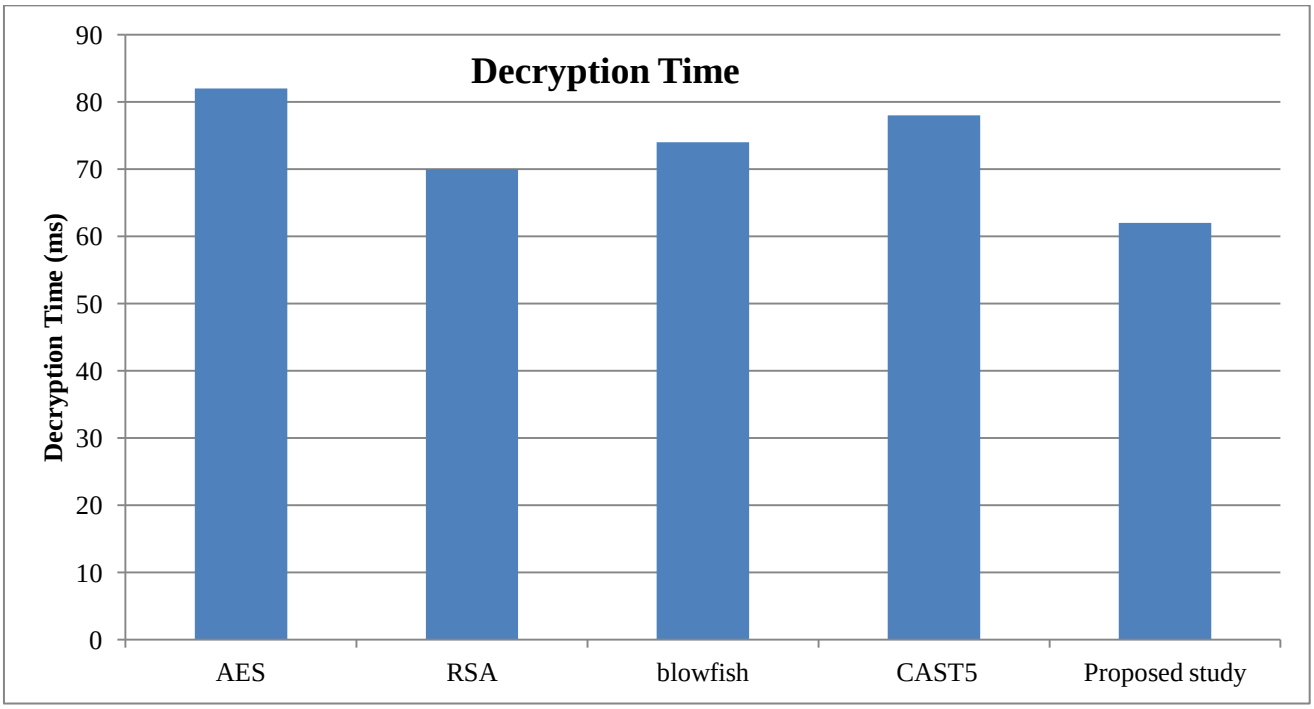


Figure 4. Decryption Time Report

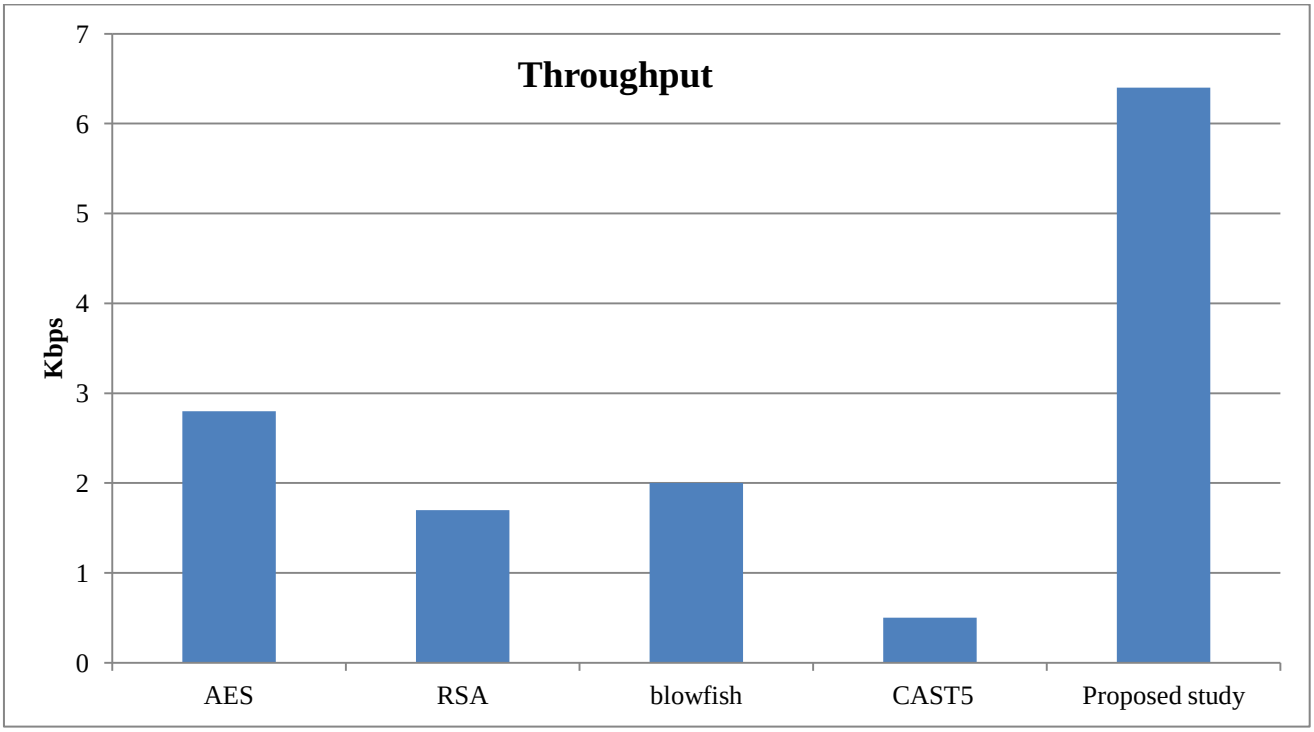


Figure 5. Throughput comparison

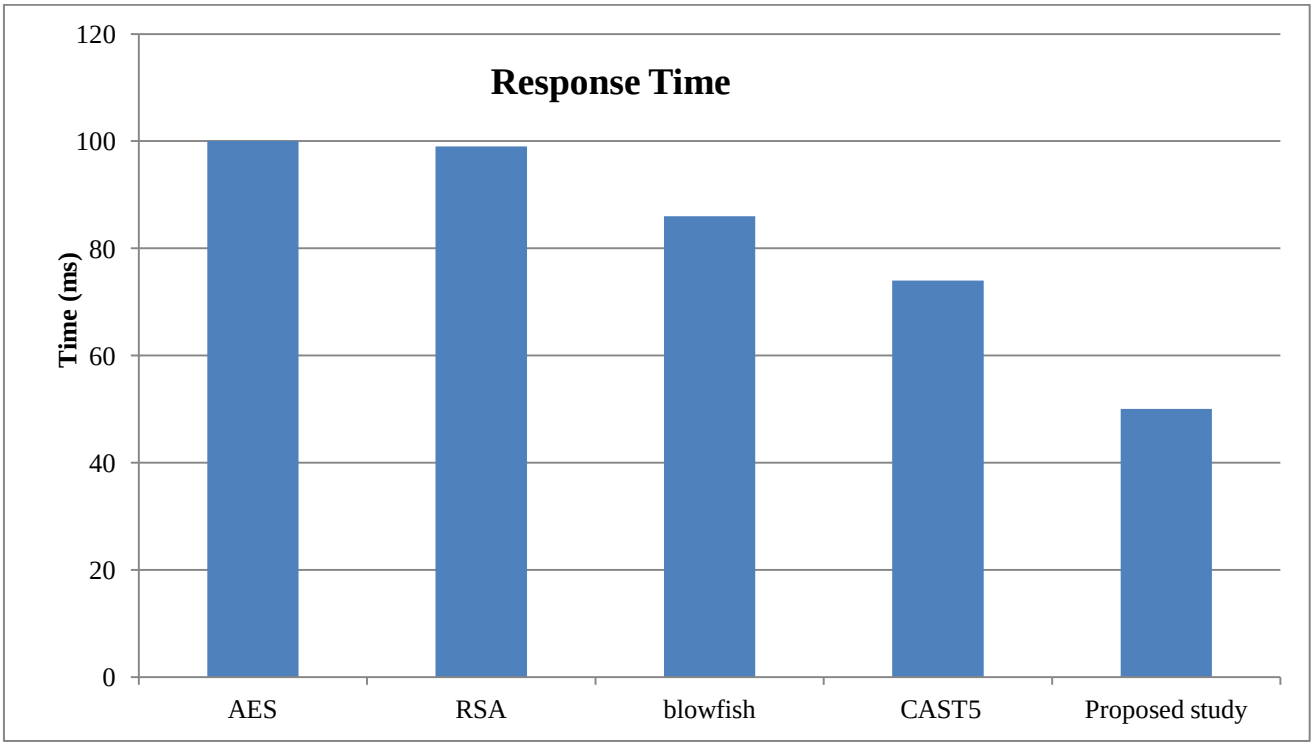


Figure 6. Response Time Comparison

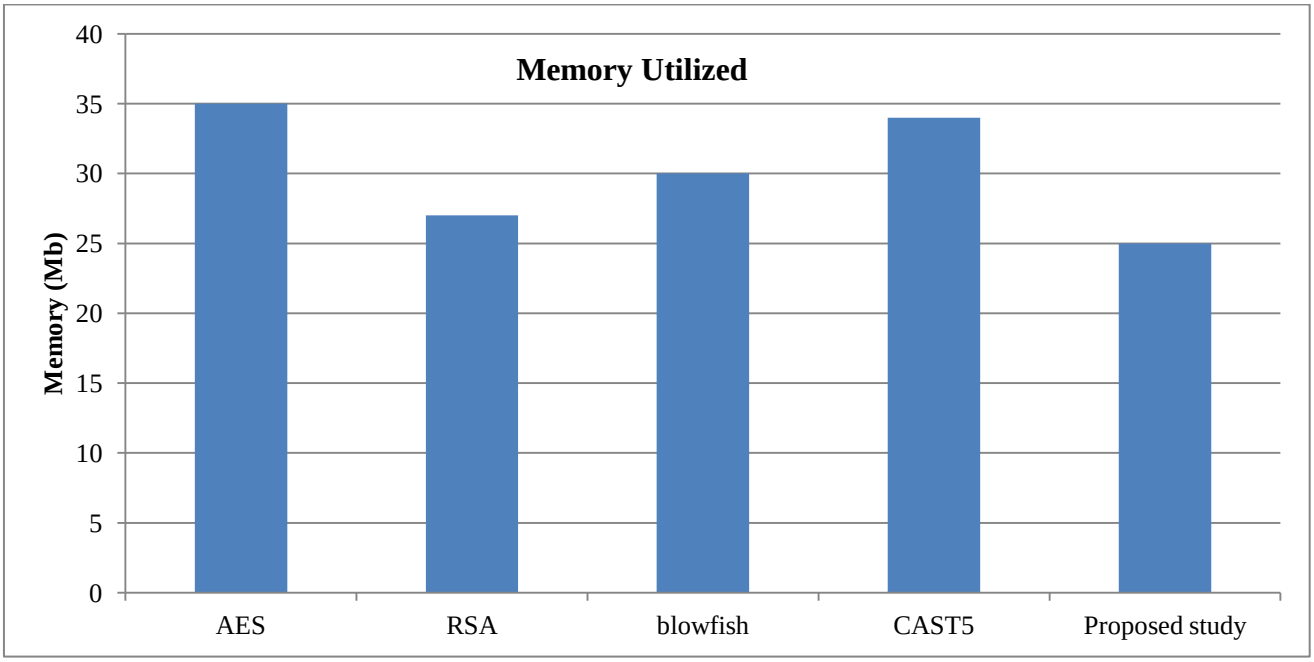


Figure 7. Memory Utilization Report

Figure 4 to 8 shows the performance evaluation report of the proposed approach with existing techniques. The present study obtains the higher throughput of 6.4 kbps, very low encryption time, decryption time and response time such as 75 ms, 62ms and 50 ms respectively. Similarly the present system achieved low memory utilization of 25 mb. Compared to other algorithm the proposed approach achieved the best result in metrics.

VI. CONCLUSION

The contribution of the study is to improve the security of the outsourced data in cloud. To achieve the goal our study focuses on fragmentation and replication process with hybrid security. Therefore a hybrid encryption technique is designed with AES, RSA and MD5 techniques. A combination of both symmetric and a symmetric encryption techniques is used to develop a secure system. A robust approach is proposed with 128 bit block and cipher key that prevent the data from brute-force attack and birthday problems.

The entire system performed well with the help of Netbeans and Cloudsim jar. Obtained a best result for throughput, response time, Encryption and memory utilization. This application can work well in 3G and 4G LTE environments.

REFERENCES

1. Liu, Joseph K., Kaitai Liang, Willy Susilo, Jianghua Liu, and Yang Xiang. "Two-factor data security protection mechanism for cloud storage system." *IEEE Transactions on Computers* 65, no. 6 (2015): 1992-2004.
2. Ilyas, Muhammad, Talha Naqash, and Sajjad Hussain Shah. "Encryption and Decryption of Mobile Security Using AES and GOST Algorithms." In *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pp. 769-772. IEEE, 2018.
3. Chang, Victor, and Muthu Ramachandran. "Towards achieving data security with the cloud computing adoption framework." *IEEE Transactions on Services Computing* 9, no. 1 (2015): 138-151.
4. Zhang, Yinghui, Xiaofeng Chen, Jin Li, Duncan S. Wong, Hui Li, and Ilsun You. "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing." *Information Sciences* 379 (2017): 42-61.
5. Pitchay, Sakinah Ali, Wail Abdo Ali Alhiagem, Farida Ridzuan, and Madihah Mohd Saudi. "A proposed system concept on enhancing the encryption and decryption method for cloud computing." In *2015 17th UKSim-AMSS International Conference on Modelling and Simulation (UKSim)*, pp. 201-205. IEEE, 2015.
6. Sengupta, Nandita, and Ramya Chinnasamy. "Contriving hybrid DESCAST algorithm for cloud security." *Procedia Computer Science* 54 (2015): 47-56.
7. Ojha, Shefali, and Vikram Rajput. "AES and MD5 based secure authentication in cloud computing." In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pp. 856-860. IEEE, 2017.
8. Zhenhua, Liu, Kang Yaqian, Li Chen, and Fan Yaqing. "Hybrid cloud approach for block-level deduplication and searchable encryption in large universe." *The Journal of China Universities of Posts and Telecommunications* 24, no. 5 (2017): 23-34.
9. Sharma, Kanika, Alka Agrawal, Dhirendra Pandey, R. A. Khan, and Shail Kumar Dinkar. "RSA based encryption approach for preserving confidentiality of big data." *Journal of King Saud University-Computer and Information Sciences* (2019).
10. Gunjal, Yogita S., Mahesh S. Gunjal, and Avinash R. Tambe. "Hybrid attribute based encryption and customizable authorization in cloud computing." In *2018 International Conference On Advances in Communication and Computing Technology (ICACCT)*, pp. 187-190. IEEE, 2018.
11. Sharma, Rupali, and Bharti Joshi. "H-IBE: Hybrid-identity based encryption approach for cloud security with outsourced revocation." In *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, pp. 1192-1196. IEEE, 2016.
12. Bhandari, Akshita, Ashutosh Gupta, and Debasis Das. "Secure algorithm for cloud computing and its applications." In *2016 6th International Conference-Cloud System and Big Data Engineering (Confluence)*, pp. 188-192. IEEE, 2016.
13. R. L. Rivest, A. Shamir and L. Adleman "A method for obtaining digital signatures and public-key cryptosystems" Communications of the ACM, vol. 21, pp. 120-126, 1978.
14. X. Wang, D. Feng, X. Lai and H. Yu, "Collisions for Hash Functions," in *Crypto*, 2004.
15. P. Peter Jose, S.P.Victor, "An Improved Model to Increase Retrieval Time and Security by Data Fragmentation and Replication Process in Cloud" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019.

AUTHORS PROFILE

Peter Jose P., has completed M.C.A Degree in Computer Applications from Sacred Heart College, Tirupattur in the year 2009. He is doing his Part Time Ph.D (Cloud Computing) in Bharathiyar University, Coimbatore, Tamil Nadu 641046, India. His research area is Cloud Computing. He has published1 research articles in the refereed International journals with good impact factor.

Dr. S. P. Victor, has completed his Ph.D. in Computer science in M.S.University Tirnuelveli in the year of 2005. Currently working as Associate Professor of Computer Science, St. Xavier's College Palayamkottai, with over 30 years of teaching experience. Functioned as the Head of the Department of Computer Science and Director of the Research Centre for six years. Functioned as the Dean of Science of the College for three years. Having Strong educational background with a Master degree in Computer Applications, M.C.A, Master degree in Engineering, M.E (CSE) and a Ph.D degree. Recognized as a research guide by the Manonmaniam Sundaranar University, Tirunelveli. He has published around 116 research articles in the refereed International journals with good impact factor. Guiding students in the areas like Cloud computing, Data mining, Web mining, Graph mining, Networks, and Image processing.