Guaranteeing Cloud Security Scheme with Hybrid Encryption Technique utilizing AES_RSA for Divided Data

P. Peter Jose, S. P. Victor

Abstract:

Distributed storage system gives the tremendous advantages to the cloud client. Particularly the information availability include that permits the client to get to their information anyplace any time. In any case, distributed computing keep up the dispersed climate for putting away the information which increment the danger of information spillages. A reasonable answer for decrease the security hazard is to send encryption component. Guaranteeing security on distributed storage is as yet a difficult issue. In this paper a cross variety encryption technique is proposed with three incredible calculations, for example, Rivest–Shamir–Adleman (RSA), Advanced Encryption Standard and MD5. The Encryption plot performs between the discontinuity and duplication measure. The proposed mixture system quality the security of cloud information. On the off chance that any fruitful assaults happen the assailants doesn't ready to find the plaintext. The usage was done with the assistance of Cloud sim structure. The presentation of this examination is contrasted and earlier encryption methods.

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

I. INTRODUCTION

Distributed computing model offers the enormous calculation limit at sensible expense. It goes about as the bone for IT businesses and numerous associations. The whole subtleties, for example, worker's data, deals and stocks, hardware activity, client relationship the board exercises are running with the assistance of cloud innovation. A few highlights are presented these days yet security with respect to issues is still remains [1]. There are various chances to have a security issues in cloud due to defective equipment, assailants and some stirred up action performed. Among these, criminal point is still stays due to flow edge advancement.

The feasible arrangement is to utilize the encryption strategy to make sure about the information [1]. Encryption idea secures the information from attackers. Various techniques have been proposed by different exploration researchers to escape these issues [2-3]. Asymmetric encryption is the appropriate encryption approach contrasted with symmetric encryption for information change, because of the end of key administration occurred in symmetric encryption.

Additional system in upgrading the security is completed through data fragmentation and replication. The discontinuity partitions the information record into number of pieces' dependent on the accessible virtual machine and the duplication store the sections in various area the current examination center around guaranteeing the security of redistributing information in fracture and replication measure.

- The proposed plot centers on both security and execution. The presented mixture encryption procedure improves the security of the re-appropriated information.
- The cross breed calculation used the advantages of three incredible encryption calculations, for example, Md5, AES and RSA.
- This conspire separates the document into parts and reproduces them into various hubs that quality the security of the framework.
- The fetching time and the encryption time is decreased altogether.

The rest of the section of this paper is sorted out as follows: the literature review on cloud security on previous encryption methods is discussed in section 2. Section 3 discusses the earlier encryption techniques. Section 4 highpoints the proposed three factor encryption techniques with MD5, AES and RSA. The experimental operation and the outcome obtained in this research are defined in section 5. Finally the summary of the study is given in section 6.

II. RELATED WORKS

In the following section is discussing about previous studies about RSA, AES encryption on fragmenting the data in distributed computing. Yinghui Zhang et al [4] Invented a protecting the outsourced data using attribute privacy protection in mobile computing. The novel scheme called *match then decrypt* is proposed for fast decryption.

Sakinah Ali Pitchay et al [5] utilizes the blend of both AES and RSA for record access in cloud utilizing usb gadgets. This instrument improves the cycle for client not to completely retain the haphazardly created keys. The entrance for record download will be permitted once the framework distinguishes the usb gadget with private keys. Nandita Sengupta and Ramya Chinnasamy [6] built up the crossover encryption methods with Data encryption standard (DES) and CAST calculation to make sure about the information from animal power and birthday assaults. Shefali ojha and Vikram Rajput [7] joins the AES and MD5 encryption to make sure about the cloud verification. Liu Zhenhua et al [8] presented a half breed security plot with accessible encryption. The cloud can apply the fine grained deduplication in the wake of appending the code into sprout channel tree. This examination accomplished the fine grained admittance control through the half breed encryption.

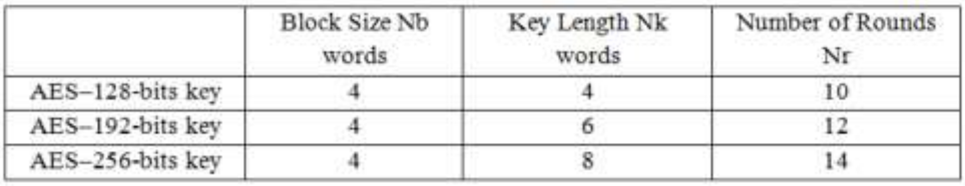
Kanika Sharma et al [9] presents an upgraded RSA based encryption procedure to make sure about the patient touchy information over cloud. The creators isolated the clients and information proprietors dependent on the area of wellbeing data. Through this key administration intricacy has been decreased proficiently. This investigation permits the information proprietors to have full control on their information that improves the privacy of the information proprietors and keeps the information from semantic assaults.

Yogita S. Gunjal et al [10] presented the arrangement property based encryption plot for keeping up the trouble in access control. The framework makes sure about against the intrigue assault. Rupali Sharma and Bharti Joshi [11] builds up a crossover conspire with Identity Based Encryption (IBE) and Attribute Based Encryption (ABE) to guarantee the denial and security on cloud information. Akshita Bhandari et al [12] creates a hybrid encryption AES improve the security of information utilizing the four stages: Key Expansion, Initial round, Initial round and Final Round.

III. EXISTING ENCRYPTION ALGORITHM

Advanced Encryption Standard (AES)

AES is the symmetric encryption with square of three modes, for example, 128 bit, 192 and 256 bit. Our investigation utilized the 128 digit block for encryption and decoding. Figure 1 shows the key size and the quantity of round performed during the execution. From this figure obviously the quantity of round in AES calculation is relies on the key length inverse such as Inverse Sub Bytes, Inverse Shift Rows, and Inverse Mix Columns.



	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

Figure1. AES key types

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.

Encryption

The Encryption can be applied as different changes in a fixed number of cycles, called adjust. During the encryption the quantity of rounds is chosen dependent on the key length. In the proposed framework the key length is 128 pieces, subsequently the quantity of cycle required are10. (Nr = 10).

AES Decryption

The encryption cycle is acted backward request to acquire the first information. In the current investigation the square size is 128 along these lines with the 128 cycle block every one of the four activities must be acted backward way. Among the four activities AddRoundKey is same for unscrambling and the other three has workers. This plan lessens the memory size, cost and utilization time. The assaults, for example, timing and animal power have been forestalled in this methodology.

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.

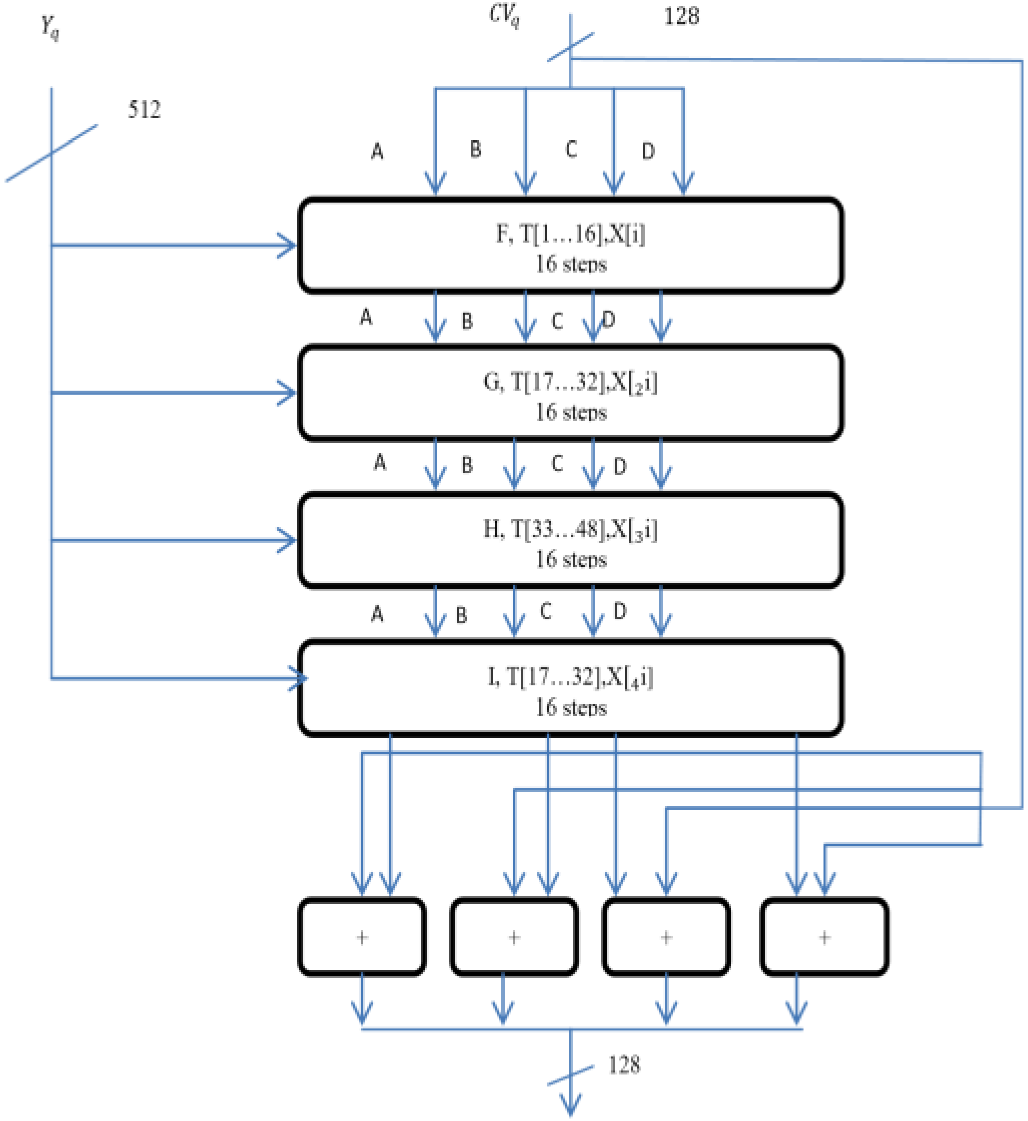
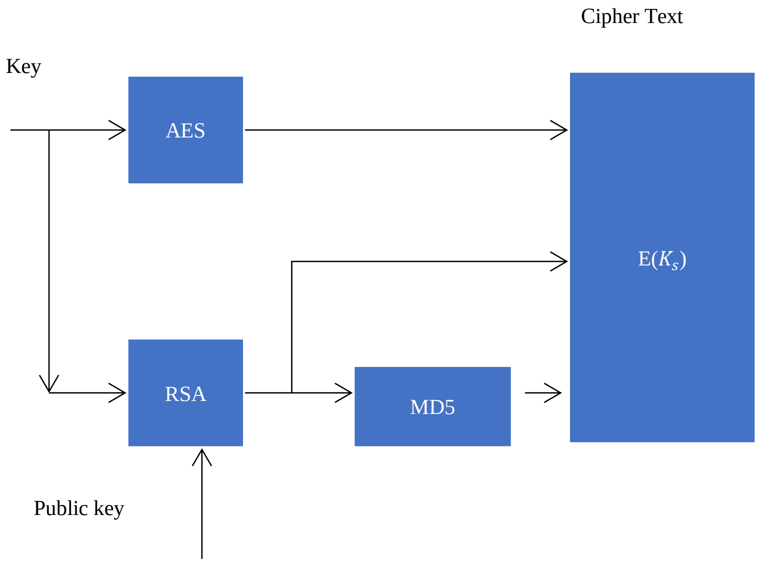


Figure 1. MD5 with 512 bit block

IV. PROPOSED METHODOLOGY

The proposed framework guarantees the security of distributed storage by applying the discontinuity and replication measure with half and half encryption procedure. In our past investigation [15] idea of fracture and Replication have examined

Thus this examination centers around encryption part alone. The AES and RSA calculation is joined with MD5 encryption procedure to build up the mixture security on cloud information. At first the transferred client information is divided and encoded with Secret key utilizing AES and the mystery key of AES is encoded with RSA calculation. So as to quality the security MD5 hash work is remembers for this methodology. The working system of the current investigation is surrendered



The proposed engineering shows that the transferred document is encoded with three layer security plot. The calculation strategy is given in Table 2. The method just covers the encryption part of the divided documents.

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 current examination is executed with the java and Cloudsim container for cloud based reenactment. Java is the ground-breaking language permits the client to make the UI with basic exertion. Java has tremendous supporting libraries for calculation and other programming bundles. The proposed investigation builds up the UI with Net beans IDE. The exhibition of the crossover encryption is contrasted and AES, RSA and MD5. The similar outcome is dissected dependent on the time taken for encryption, Throughput, reaction time for the whole information re-appropriating framework which contains fracture and replication and memory used.

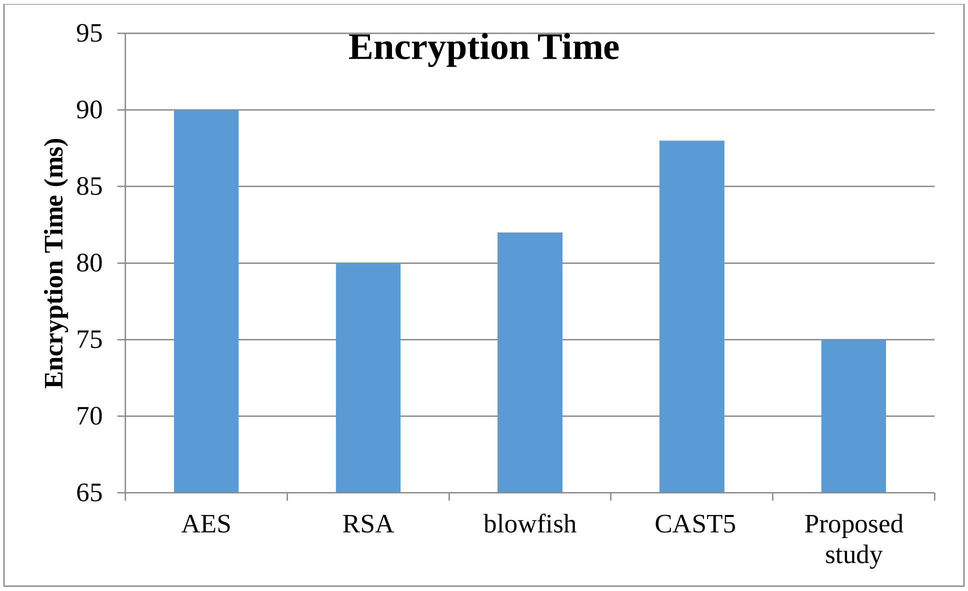


Figure 2 Encryption Time Report

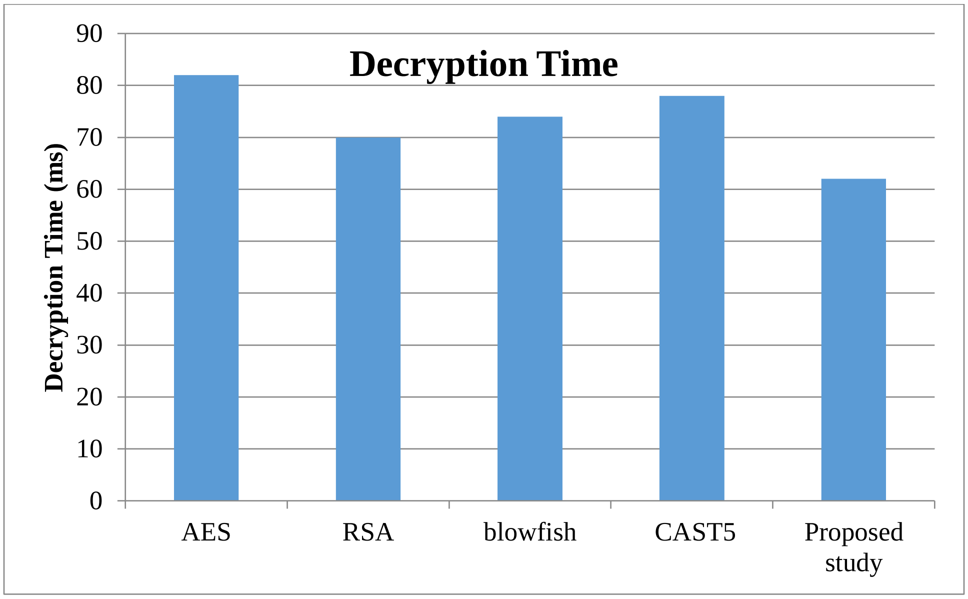


Figure 3. Decryption Time Report

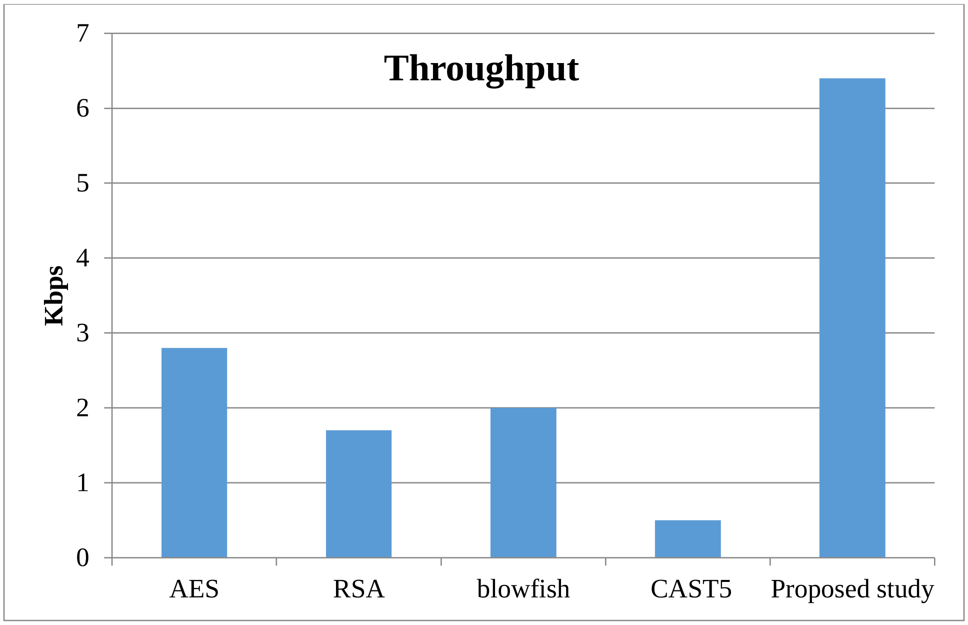


Figure 4. Throughput comparison

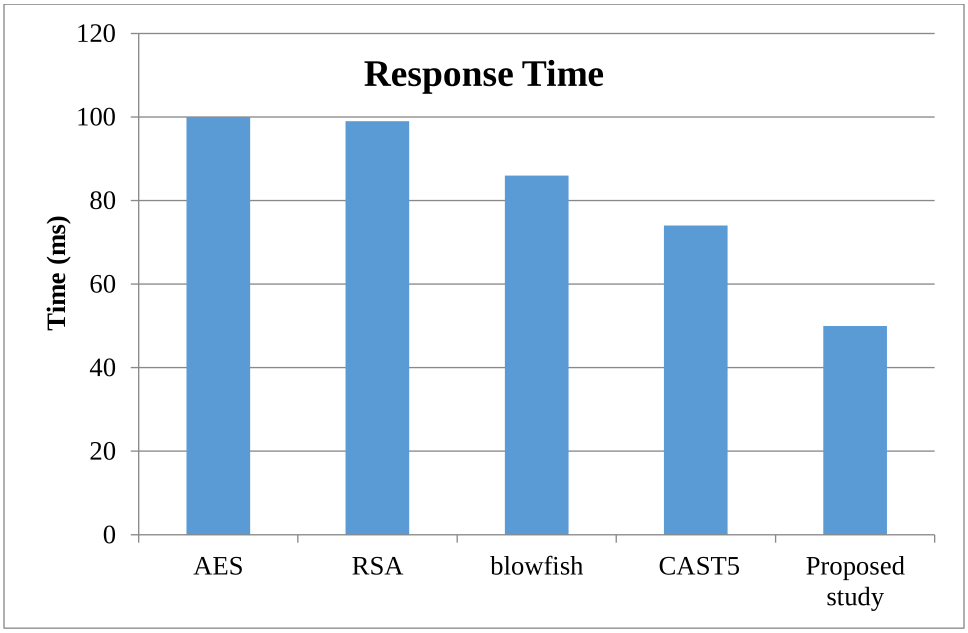


Figure 5. Response Time Comparison

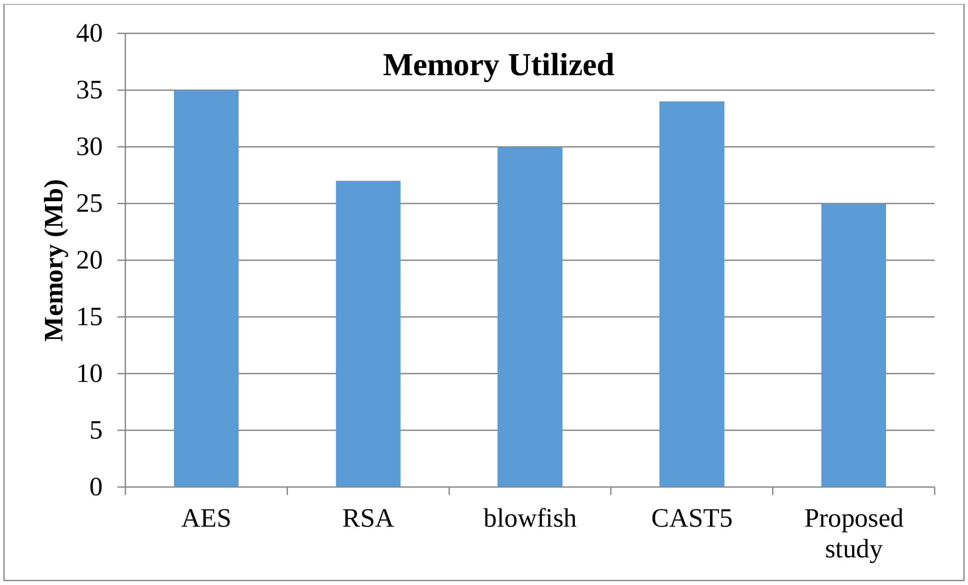


Figure 6. Memory Utilization Report

Figure 4 to 8 shows the exhibition assessment report of the proposed approach with existing strategies. The current investigation gets the higher throughput of 6.4 kbps, low encryption time, decoding time and reaction time, for example, 75 ms, 62ms and 50 ms individually. Additionally the current framework accomplished low memory usage of 25 mb. Contrasted with other calculation the proposed approach accomplished the best outcome in measurements.

VI CONCLUSION

The current examination is executed with the java and Cloudsim container for cloud based reenactment. Java is the ground-breaking language permits the client to make the UI with basic exertion. Java has tremendous supporting libraries for calculation and other programming bundles. The proposed investigation builds up the UI with Net beans IDE. The exhibition of the crossover encryption is contrasted and AES, RSA and MD5. The similar outcome is dissected dependent on the time taken for encryption, Throughput, reaction time for the whole information re-appropriating framework which contains fracture and replication and memory used.

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.