International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Security Enhanced Model for Cloud Data Based on Dynamic Data Fragmentation and Replication (DDFR)

P. Peter Jose, S.P.Victor

Abstract: ***Nowadays cloud computing is utilized in several IT capabilities like smart industry with IoTs, Mobile computing, etc., It is happen through outsourcing data to a third-party administrative control which is great application of cloud. But this leads to data leakage through attacks. A high level of data security is required on the data stored in cloud nodes. This paper enhances the security and data availability by dynamic fragmentation and replication process. The fragmentation is performed in runtime to create the fragments according to the available virtual machine. The replication aims to enhance the better load balance with less number of replicas. Bee colony algorithm is used for finding the best node in replication. The AES encryption approach is used for encrypting the fragments. This approach does not provides the original data if any attacks happened successfully.***

Keywords: Cloud computing, data fragmentation, data security, Replication, AES, cryptography

I. INTRODUCTION

Cloud computing allows their user to store and retrieve the digital data anywhere. The cloud data storage replaces the physical storage system in various organizations which is owned and maintained by several hosting organizations. Data security, Retrieval time, load balancing and Data reliability have been widely concerned for outsourcing the data [1]. The recent studies consider the Data fragmentation and the Replication process as a solution for above mentioned issues [2]. The Data fragmentation is performed in two methods: Static and Dynamic. The static fragmentation first creates the fragments and stores them while execution. Dynamic fragmentation creates the fragments based on the available resource and stores them simultaneously. The dynamic fragmentation process improves the scalability and efficiency of while outsourcing the data File replication process reduces the node overloading when the cloud node gets multiple requests at a time [3]. Replication reduces the retrieval time in an efficient manner. This is done by distributing the widely used files replica nodes. The contribution of the proposed works is

- An outsourced data scheme is proposed that enhance both the performance and security by fragmenting the cloud user file and replicates those file in various location.
- The dynamic fragmentation generates the fragments based on the number of virtual machine availability. That significantly reduces the number of fragments that improves the throughput and reduces the delay time and response time.
- The replication process improves the load balancing and data reliability by performing the multiple times replica placement. In addition the proposed replication model generates the minimal replicas to utilize the available storage resources effectively.
- The proposed Dynamic Data Fragmentation and Replication (DDFR) method ensure the security of the fragmented data through the AES encryption techniques.

The remaining section of this paper is organized as: Section II discusses the literature review on data fragmentation and replication process. In addition the encryption techniques are also reviewed for cloud data security. Section III describes the existing Encryption techniques and their drawbacks in detail. Section IV explains the proposed methodology of DDFR approach with its architecture. Section V presents the Experimental setup of the implementation and the obtained result. The Conclusion and the direction for the future study of this research is discussed in Section VI.

RELATED WORKS

Amjad Alsirhani et al [4] proposed a scheme to enhance the database security using data fragmentation. The combination of encryption techniques is introduced to maintain the data confidentiality. Through this scheme the author distributes the database over the cloud with level of security using the encryption combination.

Nelson Santos and Giovanni L. Masala [5] proposed a security model for NoSQL Database using data fragmentation. Authors apply the pattern fragmentation techniques to convert the data into chunks. The system obtains a layer of security on the data instead of applying encryption schemes.

di Vimercati et al [6] presents the model for Data Confidentiality in cloud data using fragmentation and encryption techniques. The symmetric encryption is adopted for uploaded data in cloud. Yu-Ju Chen et al [7] applies the dynamic replication techniques for cloud data centers to achieve great availability and reliability of data in cloud. This system achieves less response time and lessens the system overhead.

Revised Manuscript Received on March 30, 2020.
* Correspondence Author
P. Peter Jose* Research Scholar Department of Computer Science, Bharathiar University, Coimbatore.
Dr S.P.Victor Associate Professor, Department of Computer Science, St. Xavier's College (Autonomous), Palayamkottai.

Uras Tos et al [8] presents a data replication model for improving the performance and service provider profit. This approach estimates the query response time and execute the replication process.

N.Mansouri and M.M.Javidi [9] develops a Prefetching-aware Data Replication methods for enhance the availability of cloud data. With the file access history replication scheme determines the connection of the files and retrieve the widely accessed files.

The proposed approach aim at achieving high data availability with data confidentiality while outsourcing the data files. The proposed architecture is shown in figure 1. The proposed framework is executed during the outsourcing process. The data user uploads the data file in cloud server. Then Encryption process is carried out on the data using AES algorithm. After that the dynamic fragmentation is executed based on the runtime feedback of available Virtual machines. Eventually the replication is performed to store the data file in different cloud node.

II. PROPOSED METHODOLOGY

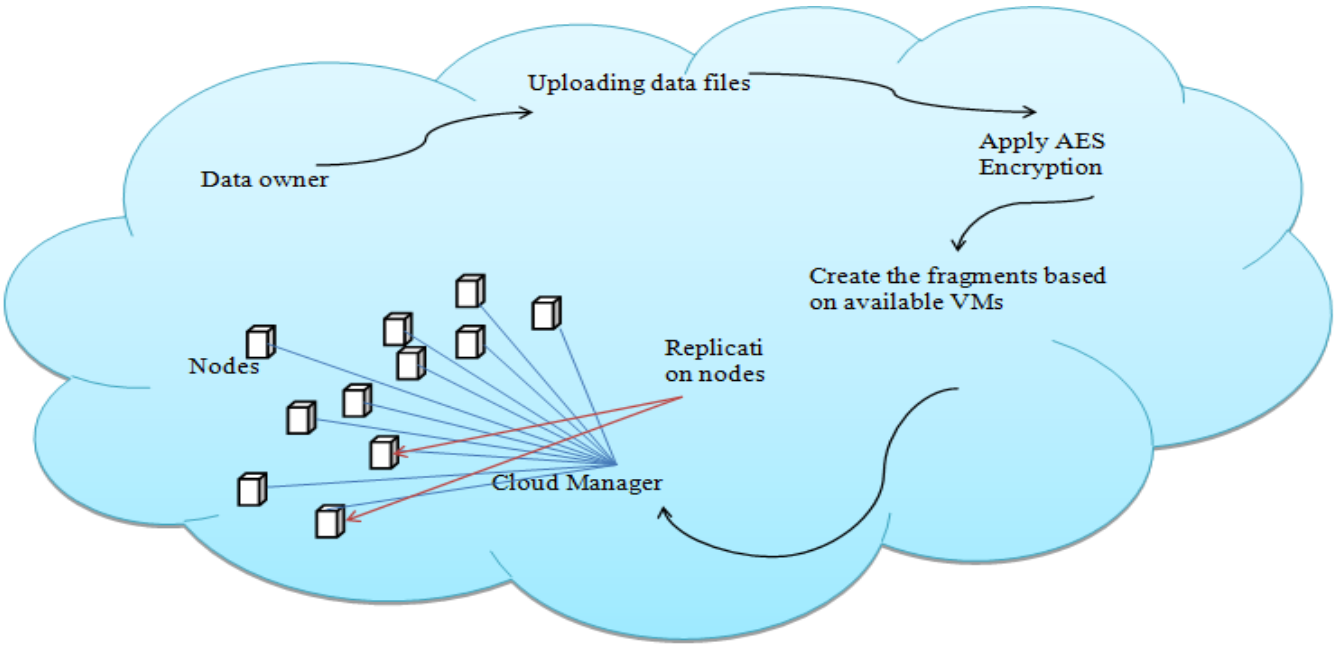
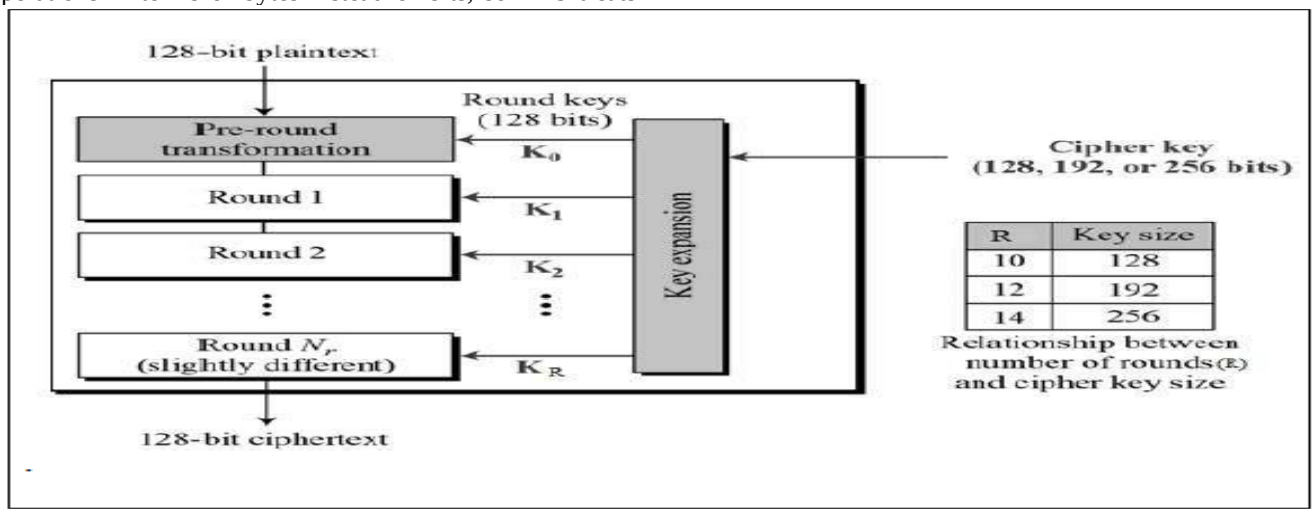


Figure 1. Architecture of the proposed model

Advanced Encryption Standard (AES)

AES is one of the powerful symmetric algorithm which is commonly used for enhancing the security. Our model used the 128 bit block and key for encryption. AES is variable and depended to the length of the key. AES performs all its operations in terms of bytes instead of bits, so AES treats the 128 bit as 16byte. This 16 byte is arranged in a 4X4 matrix. AES uses 10 series for 128-bit keys, 12 series for 192-bit keys and 14 series for 256-bit keys. Each of these series uses a different 128-bit series key, which is intended from the original AES key.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds (R) and cipher key size

Figure 2. AES Structure.

Data fragmentation

The security of cloud computing depend on each node security instead of entire node. If one node got any successful attack the other nodes can has the possibility for vulnerability. The data owner worried about the security concerns when outsourcing the data to third party control. To overcome this issue fragmentation is applied in the proposed system to ensure the security. Initially the number of virtual machine is captured during the execution and the fragmentation is carried out to create data chunk from.

The possibility of successful attack on this model is evaluated by the following scenario. Consider a cloud node with N numbers and p number of data files fragments. Let a be the number of successful intrusions on distinct nodes, such that s>z. The probability that s number of victim nodes contain all of the z sites storing the file fragments (represented by P(s,z)) is given as:

$$F(a,p) = \frac{\binom{a}{p}\binom{N-a}{s-p}}{\binom{N}{s}}$$

If the values of N, a, p are 30, 10 and 7 then $F(a,p) = 0{:}0046$. However if the values of N, a, p are 50, 20 and 15 then $F(a,p) = 0{:}000046$. From this scenario it is clear that increasing value in N gives a less possibilities for successful attack.

The figure 3 shows the overall flow chart of encryption, fragmentation and Replication process. The replication finds the best nodes for storing the fragments. While retrieving the data it's reduced the waiting time and fetches the data effectively.

The data replication is performed based on the Artificial Bee Colony (ABC) optimization. In ABC half of the bees perform as workers and the remaining bees acts as guardians. The ABC for selecting the best node for replication process is performed as mentioned in [10].

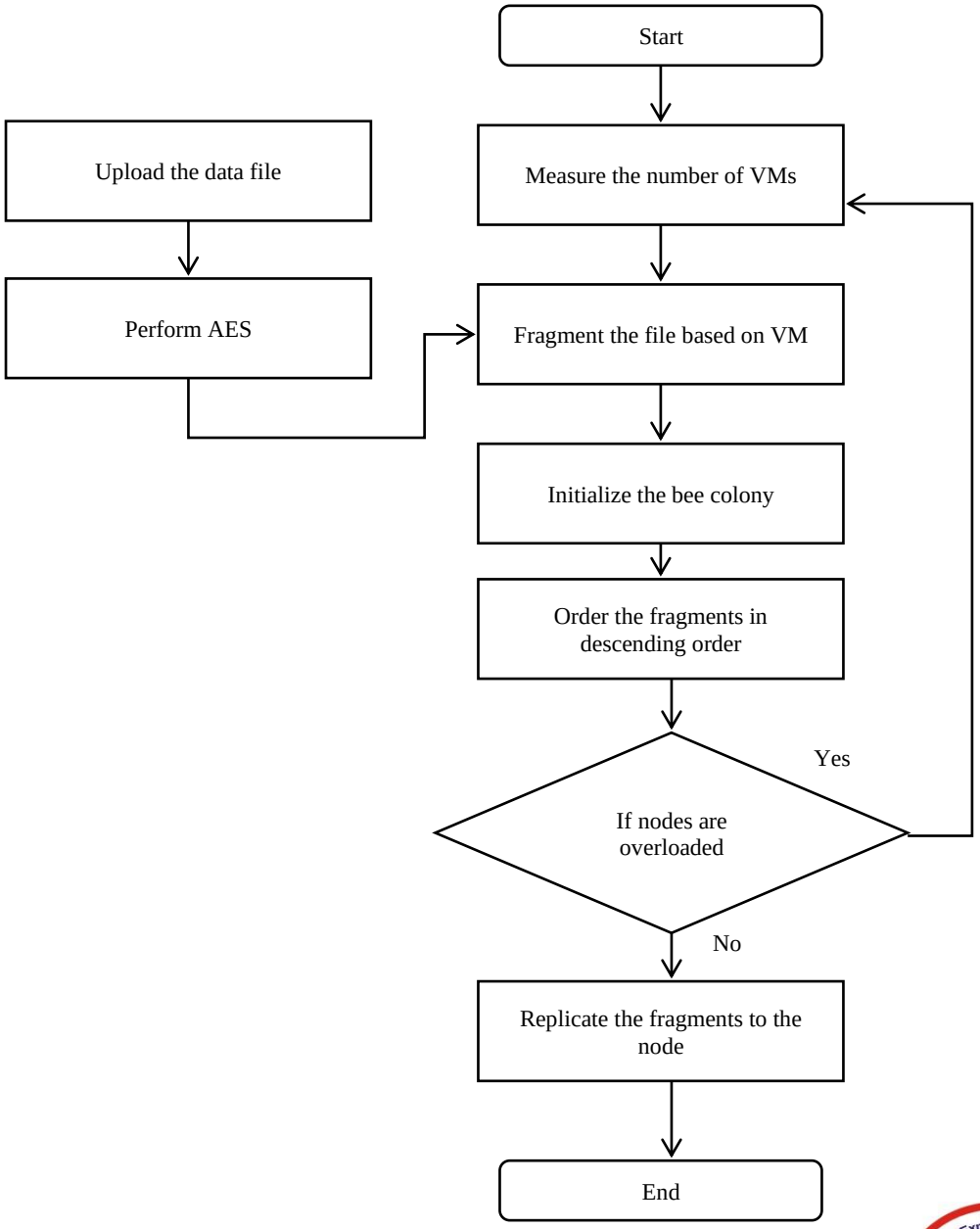


Figure 3. Flow chart of proposed model

III. EXPERIMENTAL RESULT

The proposed work performance is estimated in this section. The experiment was carried out in Java based Netbeans IDE. The cloud setup and the simulation modeling are utilized through Cloudsim Tool. It is a Java Library that supports the cloud computing simulation with help of cloud related modeling through the jar files. The performance metrics such as Response time, Throughput and Memory utilization is measured. The formula for calculating the performance metrics is given in table 2.

Table 1. Formulas of Performance parameter.

No	Performance Metrics	Formula
1	Response Time	Response Time $= \sum_{i=0}^{n} Execution\_StartTime$
2	Throughput	Throughput $= {Workload}/{Finish\ Time}$

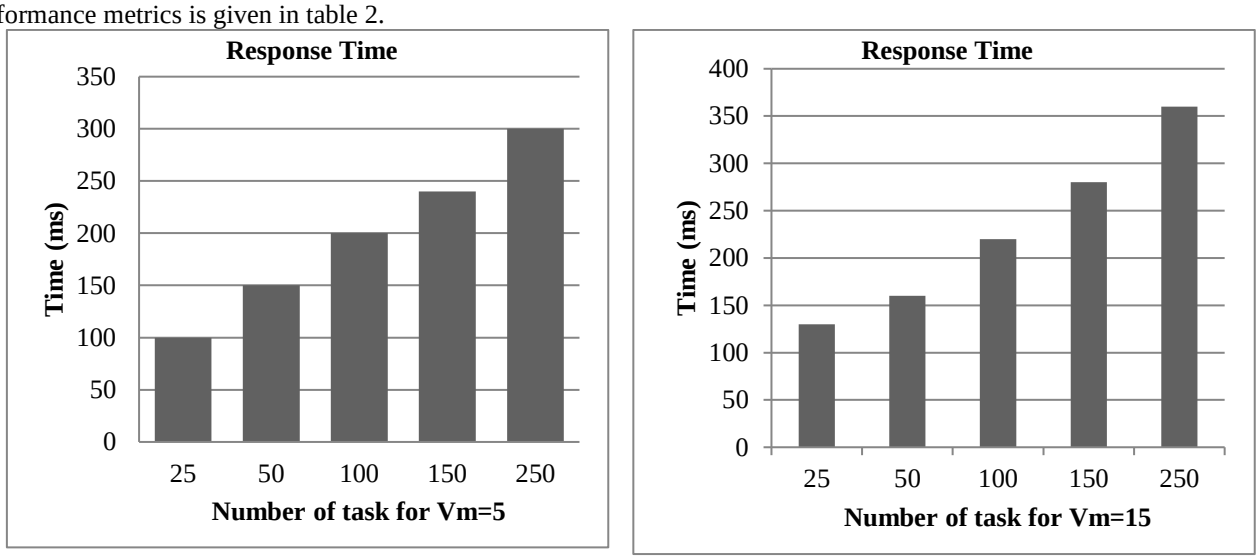


Figure 4. The Result of Throughput Time.

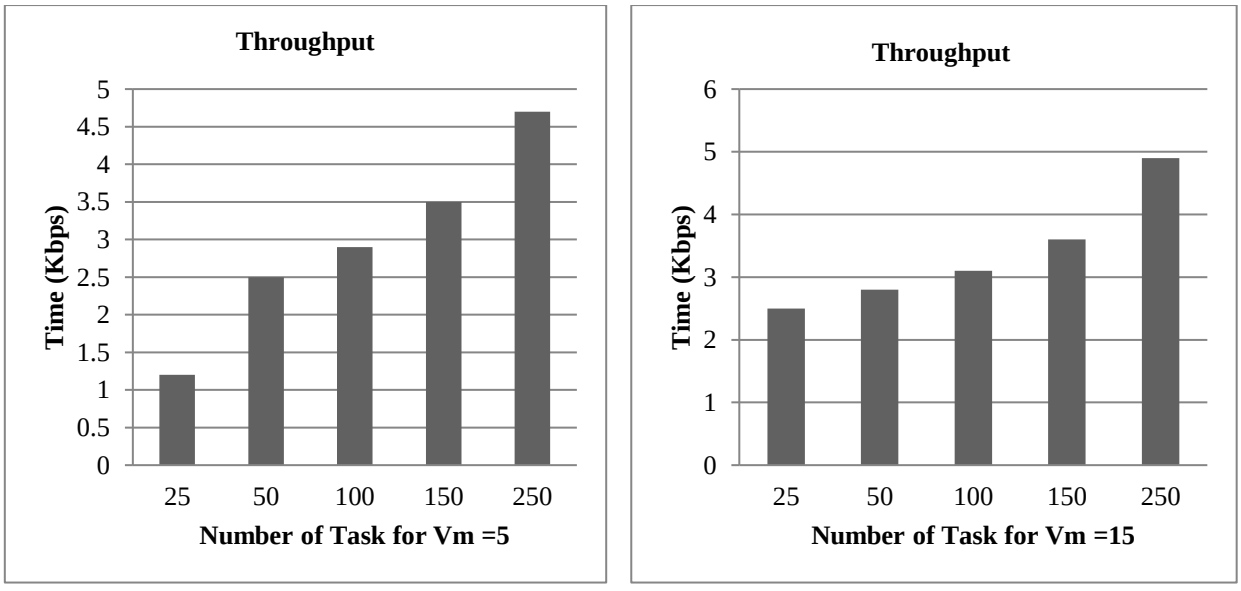


Figure 5. The Result of Throughput Time.

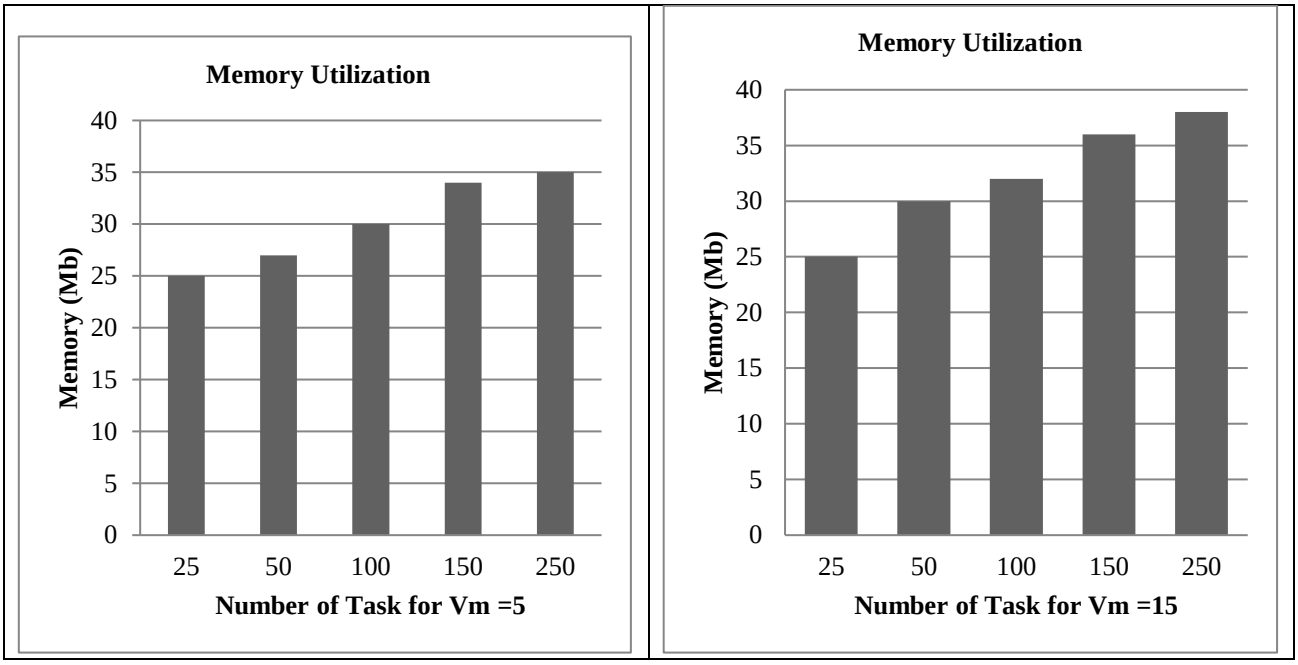


Figure 6. The Result of Memory Utilization.

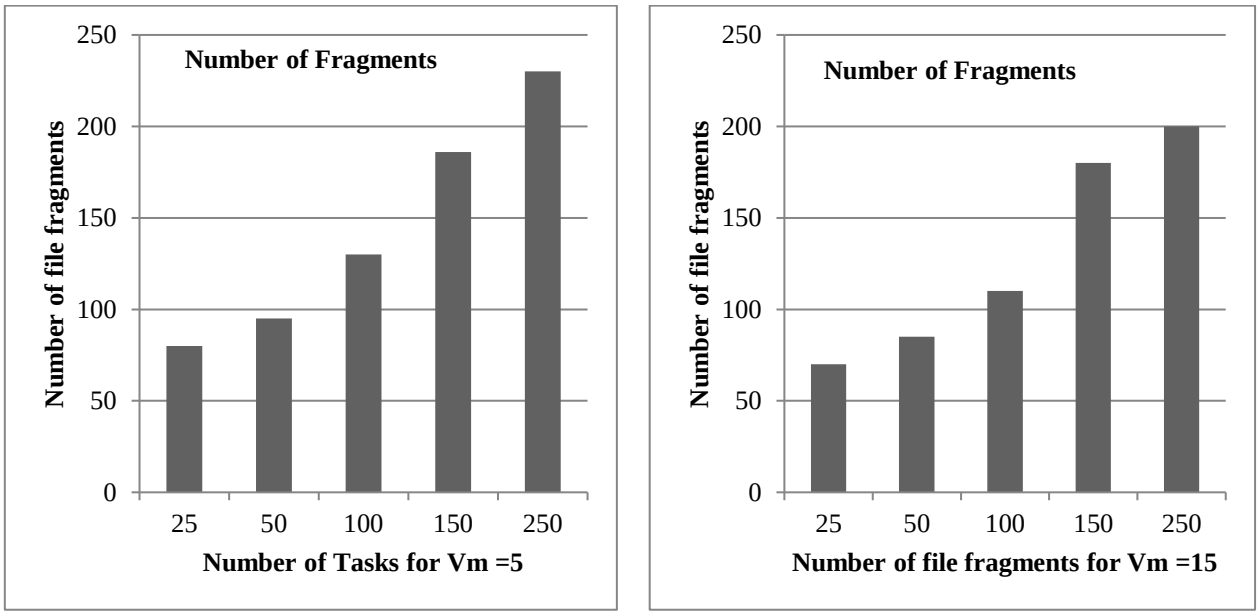


Figure 7. The Result of Fragemenation.

Figure 2 to 4 shows the result of Response Time, Throughput, Memeory Utilized and number of fragementaion. From the above result it is clear that the proposed techniques provides the efficient result. This system reduces the response time and increase throughput. The runtime fragmentation option and AES encryption provides the security to the system. The Replication process ensure the high data availability to the cloud user.

IV. CONCLUSION

Data fragmentation and replication are important problems in outsourcing data. The aim of this study is to enhance the security of the cloud data through data fragmentation and Replication process. To achieve this goal the dynamic fragmentation scheme is applied and the artificial bee colony algorithm is adopted. The security of the overall model is maintained by the AES encryption techniques. The system model utilizes the Cloudsim for implement the cloud based experiment that provides the efficient result. The performance of the system is evaluated based on the number of tasks and the size of the virtual machines. The high throughput 4.9 Kbps is achieved. Likewise the retrieval time is also reduced. Increasing size in virtual machine does not exceed 350 Ms in retrieving the data. In addition the cpu memory utilization and the number of fragment is also evaluated for showing the performance of the presents study.

In Future this research can be done to reduce the number of replicas and develops the model to delete the redundant replicas.

REFERENCES

1. Sun, ShengYao, WenBin Yao, BaoJun Qiao, Ming Zong, Xin He, and XiaoYong Li. "RRSD: A file replication method for ensuring data reliability and reducing storage consumption in a dynamic Cloud-P2P environment." Future Generation Computer Systems 100 (2019): 844-858.
2. Ali, Mazhar, Kashif Bilal, Samee U. Khan, Bharadwaj Veeravalli, Keqin Li, and Albert Y. Zomaya. "Drops: division and replication of data in cloud for optimal performance and security." IEEE Transactions on Cloud computing 6, no. 2 (2015): 303-315.
3. Raouf, Ahmed E. Abdel, Nagwa L. Badr, and Mohamed Fahmy Tolba. "Dynamic distributed database over cloud environment." In International Conference on Advanced Machine Learning Technologies and Applications, pp. 67-76. Springer, Cham, 2014.
4. H. Shen, An efficient and adaptive decentralized file replication algorithm in P2P file sharing systems, IEEE Trans. Parallel Distrib. Syst. 21 (6) (2010) 827–840.
5. Alsirhani, Amjad, Peter Bodorik, and Srinivas Sampalli. "Data Fragmentation Scheme: Improving Database Security in Cloud Computing." In Recent Trends in Computer Applications, pp. 115-138. Springer, Cham, 2018.
6. Santos, Nelson, and Giovanni L. Masala. "Big data security on cloud servers using data fragmentation technique and NoSQL database." In International Conference on Intelligent Interactive Multimedia Systems and Services, pp. 5-13. Springer, Cham, 2018.
7. di Vimercati, Sabrina De Capitani, Robert F. Erbacher, Sara Foresti, Sushil Jajodia, Giovanni Livraga, and Pierangela Samarati. "Encryption and fragmentation for data confidentiality in the cloud." In Foundations of security analysis and design VII, pp. 212-243. Springer, Cham, 2013.
8. Chen, Yu-Ju, Wan-Chi Chang, and Pi-Chung Wang. "Dynamic Replication Scheduling for Cloud Datacenters Based on Workload Statistics." In 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), pp. 1093-1096. IEEE, 2019.
9. Tos, Uras, Riad Mokadem, Abdelkader Hameurlain, Tolga Ayav, and Sebnem Bora. "Ensuring performance and provider profit through data replication in cloud systems." Cluster Computing 21, no. 3 (2018): 1479-1492.
10. khalili azimi, Saedeh. "A Bee Colony (Beehive) Based Approach for Data Replication in Cloud Environments." In Fundamental Research in Electrical Engineering: The Selected Papers of The First International Conference on Fundamental Research in Electrical Engineering, pp. 1039-1052. Springer Singapore, 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.