Asian Journal of Computer Science and Technology
ISSN: 2249-0701 Vol.8 No.S2, 2019, pp. 46-51
© The Research Publication, www.trp.org.in

File Fragmentation to Improve Security in Cloud Using Graph Topology Grid Algorithm: A Survey

S. Abdul Saleem[1] and N. Ramya[2]
[1]Associate Professor, [2]Research Scholar,
[1&2]Department of Computer Science, Jamal Mohamed College (Autonomous), Tiruchirappalli, Tamil Nadu, India
E-Mail: saleemnts@gmail.com, ramyanaga.n@gmail.com

Abstract **- Cloud computing is an emerging patterning that provides computing, communication and storage resources-as-service over a network. In existing system, data stored in a cloud is unsafe due to the eaves dropping and hacking process. To overcome the drawbacks of earlier approaches, Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) methodology is used. The node selection is ensured by means of Graph Topology Grid Algorithm and also data is encrypted here for security. In this process, the common data are divided into multiple nodes and replicate the fragmented data over the cloud nodes. Each data is stored in a different node as fragments in individual locations. In case of any attackers attack a node, no meaningful information will expose to them. The controlled replication of the file fragments is ensured and each of the fragments is replicated only once for the purpose of improved security and minimal retrieval time. In this survey, various relevant approaches were studied and analyzed. Furthermore the DROPS with Graph Topology Grid Algorithm give the better way of security in cloud environment over the earlier approaches.**

Keywords: **Fragmentation, Replication, Graph Topology Grid Data Encryption, DROPS, Cloud Security**

I. INTRODUCTION

Now-a-days, cloud computing plays an important role in internet. It provides many features like flexibility, on-demand services, elasticity, ubiquitous network accesses etc. The advantages of low-cost, flexibility and negligible management comes with security concerns. The data stored in cloud is outsourced to third party that must be secure. Unauthorized access of data is access by any other users and processes should be prevented. In adoption of cloud computing, Security plays very important role [1] [2].

In cloud computing environment, customers of cloud services do not need anything means not going into detail about the implementation and they can get access to their data and complete their computing tasks only by using the Internet connection. Throughout the access to the data and computing, the clients do not know where the data are put away or the location of the data. Thus, here the security issue stands up rapidly. Data security in the cloud computing is more complicated than in the traditional information systems [3]. The existing DROPS scheme ensures that, in the case of a successful attack, no meaningful information is revealed to the attacker. The DROPS methodology fragments the file and makes use of the cloud for replication. The fragments are distributed such that no node in a cloud holds more than single fragments, so that even in a successful attack on the node no significant information is leaked. Node selection is ensured by means of Graph Topology Grid Algorithm. Data is encrypted by using this algorithm. Increasing the cloud computing performance and security in terms of access time. Node selection will help to improve retrieval time, replicate fragments over nodes that generate the highest read/write requests. This approach is shown in Fig.1.

The objectives of this survey include:

1. To design a system that will provide good authentication system which allows only authorized users to enter.
2. To provide a security as well as improve the performance.
3. To provide controlled replication to increase the performance.
4. To improve retrieval time, replicate fragments over nodes that generate highest R/W requests.

This paper is organized as follows, Section I contains the introduction of Cloud Computing, Section II contains the Literature Survey of Security on Cloud data, Section III contains the overall comparison of existing approaches, methodologies, performances, advantages and disadvantages, Section I concludes our survey with future direction of work.

II. LITERATURE SURVEY

The security on cloud storage environment is the greatest issue in the information era. Several new approaches were developed and implemented for the security of cloud data. In our survey, some of the important approaches were discussed for narrow downing our direction of research.

Yang Tang, *et al*., [4], introduced FADE with ABE Encryption approach for securing cloud data. In this approach a quorum of key managers is self-maintained, which are independent of third-party clouds. In today's cloud storage services, FADE acts as an overlay system in that Amazon S3 is topmost and also the work provides insight into security features. In this approach, two new features were designed and implemented. FADE

implementation exports a set of APIs that can be adapted into different data outsourcing application. The concept of policy-based file assured deletion is proceeded in this paper that is a major building block of FADE, the design of FADE that defines the goal, Explaining the design of FADE in achieving access control and assured deletion, Describe the implementation of FADE, Evaluate the FADE and Amazon is topmost, Discussion about related works and review on securing outsourced data storage and conclusion was discussed. Cryptographic keys operations are proposed that enables FADE to achieve security goal. FADE is designed to protect the outsourced data from unauthorized access and to delete the outsourced data. Time performance of FADE is evaluated first. Performance of file upload and download operation is done. Evaluate the time performance of the extension. Related work says, there is no formal study about the implementation of methodologies and performance evaluation. The recent work extends the idea of assured deletion to cloud backup system with version control. The author concluded that a prototype of FADE is demonstrated. The performance is studied is practically and empirically, when its work with Amazon S3. The results provide insight into performance and security when is FADE is deployed in practice.

Abdul Nasir Khan, *et al.,* [5] proposed a lightweight security scheme for the mobile user in the cloud for protecting the mobile user's identity with dynamic credentials. On the basis of performance metrics, the comparison of proposed scheme is made with the existing scheme. Three components are used in the system models; they are the cloud service provider, mobile user and trusted entity. The parameters used to generate the dynamic credential are cloud secret ($CS_{Manager}$), Mobile Secret ($MS_{Manager}$), Current dynamic credential ($S_{current}$) and Packet Counter (N).Using smart phones on the cloud computing, the experiments are performed to evaluate the energy consumption and turnaround. The experiments are performed using dataset. The mobile and cloud secrets are updated using the data portion of the each requests and also the experiments are performed with variable threshold values and average results are presented in the graph. In this scheme, the mobile user needs to store the dynamic credential and secret that are updated on the basis of the cloud-mobile packet exchange. The space complexity of SDGC and proposed scheme is constant. When compared to SDGC, the proposed scheme is lightweight for the mobile device. The author has concluded that comparison is made with the existing system. In the mobile device, experimental results of the proposed scheme improve the turnaround and energy consumption. Future work is based on a dynamic credential generation scheme that reduces the processing burden from a trusted entity to enhance the scalability of the proposed scheme.

Kashif Bilal, *et al.,* [6] proposed a paper in which they focused Quality of Service (QoS). The author analyzed the robustness of the state-of-the-art DCNs (Data Center Network). The major contribution of this paper is presented a multilayered graph modelling of various DCNs. For performing a comparative analysis at various failure scenarios the classical robustness metrics is studied, and presented an inadequacy of the classical network robustness metrics to evaluate the DCNs robustness, proposed new procedures to qualify the DCN robustness. The detailed study of DCN robustness center is not found currently. Topological and robustness of the state-of-the-art DCNs namely: Three Tier, Fat Tree and DCell. Kurant and Thiran proposed a general multi-layered graph model. The authors defined two layers of the network. They are physical and logical. At each layer, real failure is analyzed under various robustness metrics. Two network topologies are generated for DCN architectures: three large networks and three smaller networks. The results of robustness analysis are discussed: 30K networks and 2K of various failure scenarios. The author concluded that the study is made with the structural robustness of the state-of-the-art data center network (DCN) architectures and proposed deterioration metric to quantify the DCN robustness. Based on the percentage change in the graph, the network robustness is evaluated. Deterioration metric illustrated that DCell is the most important among the DCNs.

Radhika Chavan *et al.,* [7] proposed a Graphical Password Authentication Methodology with Fragmentation and Replication technique. This method provides the security and usability of the proposed system. The user uploads the file; it is fragmented and replicated for better performance and security in terms of access time. The data is accessed using replicas. For improving the security, t-colouring method is used to assign the fragments and replicas. The authors focus on the data and authentication system with good performance. Fragmentation is a process, in this process every sensitive file is divided into many fragments in such a way, it is impossible to achieve total file in one try. Data replication means placing a number of replicas on the same server or dissimilar server. Here, the registration process is done by giving information about the user. Then the authorized user login to the system. Graphical Password Authentication methodology is provided for good security purpose. Then it begins the cloud manager system part. The uploaded file gets fragmented; no meaningful information is included in fragments. Fragmentation is done by binary fragmentation. After this, fragments are replicated on the cloud node. Due to this access time becomes low, that increase the performance. At the time of network error or network is not accessible; the fragments are accessed from the replicas within a short period of time. In terms of access time and authentication system, the result focuses on data security and performance.

The authors concluded that when compared to the alphanumeric method, graphical password authentication is increased and secured. Fragmentation is protected using the data from a single point disaster. Replication is useful for maintaining the availability, reliability and performance in failure situations. The future work will save the time and works on some attack.

Ranjana Badra, *et al.*, [8] have proposed a FADE mechanism for secure cloud storage system, it guarantees assured file deletion and improved access control for outsourced data. Even though cloud storage is attractive, nowadays the security of outsourced data becomes the most important issues. The aim of assured file deletion is to provide that based on the request, the cloud client reliably destroy the backup data's. Author has used four modules; they are Data Owner module, Key Manager Module, Storage cloud module and Policy Revocation deletion module. In this approach, each client obtains an ABE-based private access key of a file on the cloud. FADE mechanism uses two independent keys. One is a private control key, it is maintained by the key manager for Assured deletion. Another one is ABE-based access key is used for access control. In this paper, basic FADE architecture is discussed. It guarantees Access control and Assured deletion to the data stored on the third party cloud.

Santosh Ramesh Kadlag, *et al*., [9] mainly concentrated on reducing storage for improving reliability, integrity and privacy user's sensitive data. The file gets divided into fragments using T-Colouring graph technique. The third party Auditor scheme is provided; the audit of the file is stored at cloud and notifies the data owner. Security challenges are supported by using this system, such as authorized duplicate check, integrity, data confidentiality and reliability. De-duplication system improves the storage utilization, by this reliability decreases. The paper proposes a T-Colouring algorithm and Auditing algorithm for improving reliability and integrity. Secret sharing scheme algorithm proposes that data's are splitted into chunks. A chunk is split into blocks, the blocks are accessed incrementally and fragments are allocated using T-Colouring algorithm. File-level and block-level duplication is checked. The t-colouring method selects the nodes for fragment placement. Selection is made, its focus on security and performance in terms of access time. The DROPS methodology uses the concept of centrality to reduce the access time. The t-colouring algorithm is similar to the challenge algorithm in the audit phase. The author has concluded that the distribution de-duplication system to improve the reliability of data. Auditing algorithm improves the integrity and it achieves de-duplication to reduce the storage space utilization, bandwidth uploads and reliability. The input is given in text format. The future work will be based upon extending all types of data including images, multimedia.

S. Suganya, *et al*., [10] have discussed the data replication in a cloud computing data center. To overcome the problem, the author used DROPS methodology. The data is encrypted by using AES (Advanced Encryption Standard Algorithm). For improved security, each node is stored in an individual location. The simulation results reveal the security and performance. Advanced Encryption Standard (AES) is symmetric key cryptography. Blowfish is a symmetric block algorithm. AES has proven reliability. The side-channel attack doesn't use brute-force or theoretical weakness to break a cipher, it rather exploits flaws that have been implemented. It uses AES to encrypt the data. Depending on the cipher version, brute-force attack is faster than AES and demonstrated a technique called a biclique attack that could recover AES keys. Experimental setup says that the communication backbone of cloud computing is Data Center Network (DCN). Three DCN architectures are used. They are three-tier, Fat tree and DCell. The comparative technique performance and DROPS methodology are varying under R/W ratios. The comparative technique shows that the RC savings up to the R/W ratio of 0:50 is increased and the number of writes is decreased that causes the reduction of cost. The results are focused on security and performance. The author concluded that utilized the frequent algorithm (AES) it proves to be a better mechanism to provide efficient replication process to the cloud system and also the comparison of results are made with the existing method of data replication in cloud computing.

Mahesh Kharde, *et al.*, [11] have proposed Fragmentation and Data replication for security and performance issues. In this methodology, files are broken into pieces and replicate the fragments over nodes in the cloud. Each node consists of a particular file of fragments. In case of an attacker attacks a node, no meaning is revealed. Probability to identify any file, it is extremely low. Here, some of the attacks handled by methodology, they are Data Recovery, Cross VM attack, Improve media sanitization, E-discovery, VM escape and VM rollback. For the selection of nodes, two phases are used. In phase one, for the initial placement of fragments the nodes are selected. In phase two, fragments are replicated. For better performance of their work, the results are compared with the fragments replication algorithm. By keeping the number of nodes constant, the number of objects is increased and varied by a read/write ratio. It shows that the performance of the algorithm is reduced with an increase in a number of file fragments. The increase in a number of replicas will decrease the communication cost.

P.D. Patni *et al*., [12] implemented Fragmentation and Replication of data in the cloud (FRDC), addresses the issues related to security and performances. In case of successful attack of a node by an attacker, no meaningful information is revealed to the attacker. To increase the further security T-Colouring method is used. By using this method, it becomes difficult for an attacker to breach the security. It deals with security and performance issues related to cloud storage. Here, the file is uploaded by the client; the cloud manager will encrypt the file, fragments the files into pieces, replicates the file and place the file at a distinct location within the cloud. To increase the performance over the node in replication of fragments, it generates R/W request. The person has to intrude a large number of nodes to obtain significant node. Fragments are stored in a distinct location with the help of T-Colouring. This methodology mainly pays attention to the data security in the cloud. Thus, the author has concluded that the effort needed by a person to breach the security is directly proportional to the number of fragments. During uploading

and downloading the data, there is a moderate increase in the number of fragments that results in a decrease in processing time and increase in performance. By increasing the number of fragments, the uploading time falls sharply with slight increase in encoding time. The comparison is made with the effect of the increase in the number of fragments on uploading and downloading time and increase in the number of fragments with decoding and downloading time.

Dejene Boru *et al*., [13] have addressed a new approach in which provisioning; communication resource becomes a bottleneck for many cloud applications. The evaluation of result is obtained from both the mathematical model and extensive simulations. The author uses two main approaches to making data center for consuming less energy. (i) Shutting the components down and (ii) scaling down the performance. These approaches are applicable to both the computing servers and network switches. In a cloud application, for better reliability and high performance the data resources are brought closer to the physical infrastructure. In this paper a mathematical model for energy consumption, bandwidth demand and delay of the cloud application is focused to develop. The three main performance indicators are Data center energy consumption, available network bandwidth and communication delay. For the performance of evaluation purpose, Green Cloud simulator is developed and it is extended with the required data replication functionality. It is based on the NS2 platform for TCP/IP network simulation. With the increase in data size, Energy consumption of network switches similarly. The optimization of communication delay leads to improvement in the quality of user experience to cloud application. The author has concluded that the replication solution is evaluated based on the development of mathematical model and simulations using Green Cloud.

III. RESULTS AND DISCUSSION

The following Table I give the overall comparison of existing approaches, technologies, methodologies, advantages and disadvantages. The approach of DROPS with Graph Topology Grid discussed in this paper, focus on solving the problems presents in the earlier approaches. Fig.1 depicts the file division and storage in DROPS with Graph Topology Grid approach.

TABLE I COMPARATIVE ANALYSIS

Author Name	Title	Year	Methodology	Performance	Advantages	Disadvantages
Yang Tang, *et al* [4]	Secure Overlay Cloud Storage with Access Control and Assured Deletion	2012	FADE with ABE Encryption	FADE can be viewed as an overlay system atop the underlying cloud.	It provides insight into performance and security when is FADE is deployed.	There is no formal study about the implementation of methodologies and performance evaluation.
Abdul Nasir Khan. M.L *et al*.[5]	Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing.	2013	SDGC (Scheme for Dynamic Credential Generation)	Automatic dynamic credential is generated for the identification of the mobile user in cloud.	It improves the turnaround and energy consumption to mobile user.	Delay occurrence in communication.
Kashif Bilal, *et al*.[6]	On the Characterization of the Structural Robustness of Data Center Networks	2013	DCN Graph Topology	The robustness of the state-of-the-art DCNs (Data Center Network) is analyzed	The network robustness is evaluated based on the percentage is change in the graph structure.	A comparative analysis at various failure scenarios is performed
Radhika Chavan, *et al*. [7]	Cloud Security Solution: Fragmentation and Replication	2013	Graphical password authentication with fragmentation and replication	Data replication at lower levels may significantly increase system performance.	The data collects from replicas within short period	Here, the availability and quality of service is not maintained fully.
RanjanaBadre, *et al*.[8]	Cloud storage with improved access control and assured deletion	2014	FADE mechanism with CP-ABE Encryption	Assured file deletion is provided to cloud clients an option of reliably destroying their backup data's based on the requests.	Access control is guaranteed and Assured deletion to the data stored on the third party.	In a difficult task for outsourced data providers, it provides robust data to users
Santosh Ramesh Kadlag, *et al*. [9]	An Approach for Efficient and Reliable Storage in Cloud Computing Environment	2015	T-Coloring Algorithm with De-duplication	Removing the identical copies of repeating data and it is used reduce the storage space.	It allows minimizing Network delays and bandwidth usage.	Identical data copies of different users will lead to different cipher texts
S.Suganya, et al.[10]	An Optimization And Security Of Data Replication In Cloud Using Advanced Encryption Algorithm	2016	DROPS with AES Encryption	The comparative techniques and DROPS methodology are varying under R/W ratios.	It increased in security level of data accompanied by a slight performance drop.	Possible to store data with duplication.
Mr. Mahesh Kharde, *et al*. [11]	Enhancing Security and Performance by Fragmenting and De-duplication in cloud	2016	Fragmentation with T-coloring approach	File is broken into pieces and replicate this pieces over the nodes in the cloud.	In cloud storage security, it deals with performance and security with respect to retrieval time.	Improper sanitization and malicious VM, due to this the critical information can be leaked.
P.D. Patni, *et al*. [12]	Security Enhancement of Data in Cloud using Fragmentation and Replication	2016	AES with T-Coloring	First File is uploaded by the client, it is encrypted, and then divided into fragments.	It increases the effort of an attacker to intrude the system.	Increasing the number of fragments, the uploading time falls sharply with slight increase in encoding time
DejeneBoru, *et al*. [13]	Energy-Efficient Data Replication in Cloud Computing Data centers	2016	Data Replication Methodology	Green-cloud simulator is developed for the performance,the required data replication functionality is extended.	Reduced communication delays.	Need high performance communication resources

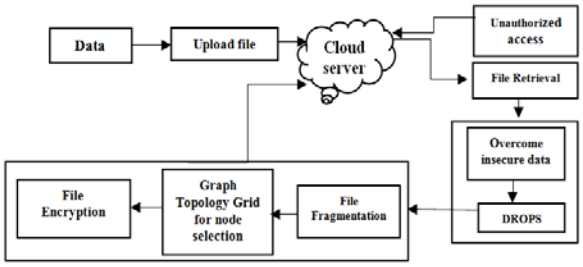

Fig.1 File division and Storage

A. Pseudo Code for Data Partitioning

Input : Upload File to store
Output: File fragments on different servers

Steps involved in file fragmentation
Step 1: Calculate document size.
Step 2: Data Partitioning file:
If File size<=min size or size>=max size Show error message.
Else
Divide report as in keeping with the wide variety of servers with index and extension.
Step 3: Generate private key for encryption.
Step 4: Encrypt respective partition using non-public keys.
Step 5: Save partition sequence, keys and record characteristic.
Step 6: Send every partition at respective garage server.
Step 7: Merging file: Get report walls from garage servers.
Step 8: Extract every partition and Merge report otherwise statistics is corrupted.
Step 9: Decrypt the merged document with key.

Existing T-Colouring approach has following demerits
1. In T-Colouring process, we lose some of the central nodes that may increase the retrieval time.
2. If somehow intruder compromises a node and fragment is obtained then the location of the other fragments can be determined,

This approach of Data Partition and Replication Technique overcomes the limitations of existing approach with high performance, reduced cost and limited data storage space in cloud. It also ensures resilient against threads, attacks and misbehaving server. DROPS methodology is a new field of research in information security in cloud environment. This will provide more secure file storage compared to existing encryption based system. In DROPS methodology, Division and Replication is performing to protect data security and also consider the data retrieval process. Efficient encryption technique applied to encrypt the file fragments. This proposed approach has three parts that are Data Owner, Cloud Service Provider and Data User.

B. Graph Topology Grid

The true representation of the grid is a general graph, where there is no root node; consider the grid topology as a graph. Due to better managing of replica servers and their related nodes, convert the graph structure to hierarchical structure. Here the data grid is modelled to have three tiers, where the tier 0 machines have enormous storage capacity. The tier 1 machines are called as Regional Servers have computing and storage resources. The tier 2 machines are called Local Servers and tier 3 machines are workstations.

Input : Encrypted file fragment
Output: File Replication on different server.

Step 1: Submit jobs to grid.
Step 2: Every request sent to Replica manager of Regional servers.
Step 3: To determine which grid site contains the desired replica (Candidate sites), the Replica manager queries Replica Catalog
Step 4: If the file is not found in lower level then, the Request is send to upper level by manager.
Step 5: Communication cost is determined between requester site and candidate sites.
Step 6: Round Trip Time (RTT) is computed.
Step 7: If (d>RTT) then file is accessed from the remote place or else it replicates the file.
Step 8: Check the storage element of the site selected for replication. If there is no available of storage space then Replica Replacement algorithm is accessed otherwise
Step 9: Threshold Controller checks whether the site has minimum access load. If yes, then communication is made with Reservation Manager.
Step 10: If Reservation Manager succeeds in making the reservations, then Allocation Manager is ready to allocate the resources.
Step 11: Once the Allocation Manager allocated the resources, Replication Placement is performed.
Step 12: If Reservation Manager is not succeeded, then the Lowest Common Ancestor algorithm (LCA) is invoked.
Step 13: LCA returns a site, with this site ID, repeat steps 8 and 9.
Step 14: If the Threshold Controller results maximum access load, choose one of the sibling node and continue step 10 and 11.

IV. CONCLUSION

The main aim of this survey is to analyse the best method for storing resources with security and efficient retrieval time of the resources in cloud environment. DROPS methodology provides the better result when compared with other approaches. In this method, the node selection is ensured by means of Graph Topology Grid Algorithm. This algorithm also encrypts the data for security. In this algorithm, the common data are divided into multiple nodes and fragmented data is replicated over the cloud nodes. Each data is stored in a different node as fragments in individual locations. In case of any attackers attack a node,

no meaningful information will expose to them. This approach provides security at both client levels as well as in network level. Furthermore, it results in increased security level of data with minimal retrieval time. In our future work, we will focus on secure file access with DROPS methodology and time based access control mechanism for providing access control to the data user. It will save the time and resources utilized in downloading and updating the files again.

REFERENCES

[1] A.N. Khan, M.L.M. Kiah, S.U. Khan, and S.A. Madani, "Towards Secure Mobile Cloud Computing: A Survey", *Future Generation Computer Systems, Elsevier*, Vol. 29, No. 5, pp. 1278-1299, 2013.

[2] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computingenvironments", *Procedia Engineering, Elsevier*, Vol. 15, pp. 2852-2856, 2011

[3] Keiko Hashizume, David G Rosado, Eduardo FernndezMedina, and Eduardo B Fernandez, "An analysis of security issues for cloud computing", *Journal of Internet Services and Applications, Springer Open*, 4-5, February 2013.

[4] Tang, Yang, Patrick PC Lee, John CS Lui, and RadiaPerlma, "Secure overlay cloud storage with access control and assured deletion", *IEEE transactions on dependable and secure computing*, Vol. 9, No. 6, pp. 903-316, 2012

[5] Khan, Abdul Nasir, ML Mat Kiah, SajjadA.Madani, and Mazhar Ali, "Enhanced dynamic crendential generation scheme for protection of user identity in mobile-cloud computing", *The Journal of Supercomputing*, Vol. 66, No. 3, pp. 1687-1706, 2013.

[6] Bilal, Kashif, Marc Manzano, Samee U. Khan, EusebiCalle, Keqin Li, and Albert Y. Zomaya, "On the characterization of the structural robustness of data center networks", *IEEE Transactions on Cloud Computing*, Vol. 1, No.1 pp.1-10, 2013.

[7] Radhika Chavan and A. Opera, "Cloud Security Solution: Fragmentation and Replication", *Communication of the ACM*, Vol. 56, No. 2, pp. 64-73, 2013.

[8] Badre, Ranjana, "Cloud storage with improved access control and assured deletion", *International Journal of Innovations in Engineering and Technology (IJIET)*, Vol. 3, No.3, pp. 92-77, 2013

[9] Mr.Santosh Ramesh Kadlag, Prof. Mayur C Akewar, "An Approach for Efficient and Reliable Storage in Cloud Computing Environment , Vol. 3, No.11, 2015.

[10] Suganya, S., and R. Kalaiselvan, "An Optimization and Security of Data Replication in Cloud Using Advanced Encryption Algorithm", *International Journal Of Engineering And Computer Science*, Vol.5, No. 6, pp. 16836-16841, June 2016.

[11] Mr. Mahesh Kharde, Prof.Ashish Kumar, "Enhancing security and Performance by Fragmenting and Deduplication in cloud", *International Journal of Engineering Development and Research (IJEDR), ISSN:2321-9939*, Vol 4, No. 2, pp. 1227-1232, 2016.

[12] P.D. Patni, and S.N.Kakarwal, "Security Enhancement of Data in Cloud using Fragmentation and Replication", *International Journal of Engineering and Management Research (IJEMR)*, Vol. 6, No.5, pp. 492-497, 2016.

[13] Boru, Dejene, DzmitryKkiazovich, FabrizioGranelli, Pascal Bouvry, and Alberet Y. Zomaya, "Energy-efficient data replication in cloud computing datacenters", *Cluster computing*, Vol. 18, No. 1 pp. 385-402, 2015.