ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Fragmenting the Data in Cloud for Enhancing Security and Performance.

Praveen Paul*, and Ramya G Franklin.

Department-MCA, Faculty of Computing, Sathyabama University, Chennai-600119,Tamilnadu, India.

ABSTRACT

Cloud computing is growing technology which attract consumer by providing offers such as unlimited virtual dynamic storage resources, space, computation and reduced cost etc. The user share sensitive data in cloud which provides high security problem in cloud. Third–party administration control is main concern in security outsourcing data in cloud computing. Because of unauthorized user access data in cloud, data damage might be occurs. So, high security needed to prevent the data within cloud. In order to protect the data of user Division and Replication of Optimal Performance (DROPS) is utilized in this paper. DROPS technique increases security in cloud and solve performance issues. In cloud computing, third-party administration control increase security concerns in cloud. Due to the attacks by nodes and other users in cloud data compromise might occur. High security is needed to prevent data in cloud. By using replication and fragmentation in cloud the data protected. In DROPS technique, the file divided into fragments and fragmented data replicate over cloud nodes. Every node stores single fragment of data confirms that even successful attack in that significant information not revealed to attacker.

Keywords: DROPS, T-coloring, fragmentation, Third–party administration control.

Corresponding author

ISSN: 0975-8585

INTRODUCTION

Basically cloud computing is specified by self-serviced, on-demand, resource pooling, network accesses, flexibility and steady services. The above cloud computing characteristics become it a important candidate for organization, business, and own user for adoption. The advantages of greater flexibility, negligible management, and low-cost come with more security issues is one of important reason for those prohibiting the cloud computing adoption. The outsourced data must be secured in public cloud. Data access from unauthorized user also must be protected.

Any weak aspect can becomes the whole cloud computing at risk. In this scheme, the security device must substantially increase an effort of attacker to recover a reasonable data amount even after victorious intrusion in cloud. Providers started using VPN (Virtual private network) services for data transmission [1]. Now days, more people are relation with cloud services for get advantages from application like instant messaging, Email, software of business application and low cost web services [2]. Cloud computing is combine of many computing areas and became more famous in recent years. Normally cloud provides storage, services, application and computing over by internet. Furthermore, cloud computing helps to reduce the cost of capital, provides the flexibility based on the resource provisioning [3]. Cloud provides various types or services based on the needs; these are 1) Platform as a service (PaaS), 2) Infrastructure as a service (IaaS), 3) Software as a service (SaaS). For achieving a secure cloud, it is important to secure all joining entities. In any type of the system, it must be needed that highest type of system security [2]. The data storage of cloud needs users to outsource their data in remote location of cloud storage that may chance for different security issues. Elasticity and pooling of cloud computing, helps the resources of physical to be distributed among more users [5]. Better performance and security are required for huge scale systems. In this proposed system we concentrate the two issues such as performance and security for overcome these issues [6]. When the file in storage place is not divided then if any single attack happens on file, it causes more chances full details of file. So It is crucial to divide the file for increase the security level [7]. In our proposed system our aim is to provide the security on outsourced file by using the fragment technique.

RELATED WORK

The authors [8] have proposed an analysis over cloud computing for the issues of security and have proposed solution within that. The proposed solution over security concerned with cloud computing data. The [9] have concerned the same security issues within quality of service parameter for data security. They had discussed over the misbehavior of server division of data for checking the data integrity for helping the pre-computation token. These previous work is not supporting the dynamic insertion supports. The process is ensuring the case of data availability for failure of link communication. The authors [10] have proposed a data replication process over the center of cloud computing bandwidth and energy-efficiency for the system. The result is being obtained through the design solution guide for replication of data future. The [11] had also concerned within the data replication and energy efficiency in the data center of cloud computing, the data replication is distributing the geographical distribution of cloud computing and proposing the solution of novel replication for the additional metrics of performance as bandwidth, network availability energy efficiency optimization of the system. The optimization delay of the communication leads a quality improvement over the cloud application with user experience. The data allocation and fragmentation is distributing the environment of database management for improving the concurrency level automatically, the system throughput is increasing the query process [12]. The technique of fragmentation has been used to split the files for enhancing the security at server side which have local file as an input and producing the output as a fragmented file. The attacker is being uncertain about the location information for improving the security which causes the successful attack. The author [13] have proposed duplicate replica for the fragmented portion by fragmenting the replica and managing the attack over useful contents. The fragmented replica is replacing the damaged replica and combining all the original fragmentation by reconstructing original fragmentation [14]. The security is being a major concern for essential large-scale system in cloud, where both are utilizing the user end services. The replication and security must have to be balanced with one service but not within the least service at other side. The performance is optional that providing automatic mechanism for updating the fragment identification and necessary fragment [15]. The fragments are being encrypted before storing the content and allow identical files to get detect with high probability and several encryption techniques for generating secure keys.

ISSN: 0975-8585

OVERVIEW PROPOSED WORK

The DROPS (Division and Replication of Optimal Performance and Security) techniques solve the performance and security problem. The nodes in the cloud separated with definite distance by using T-coloring and the fragment of the single file store in different node. To avoid replication problem we proposed DROPS technique which fragments files and replicates the strategic locations in cloud. The DROPS prevent the attacks even if attack is severe no meaningful data revealed to attacker. Non- cryptographic scheme is proposed to make retrieval and placement on data. Using these techniques we control the file fragments replication.

3.1 OVERALL ARCHITECTURE

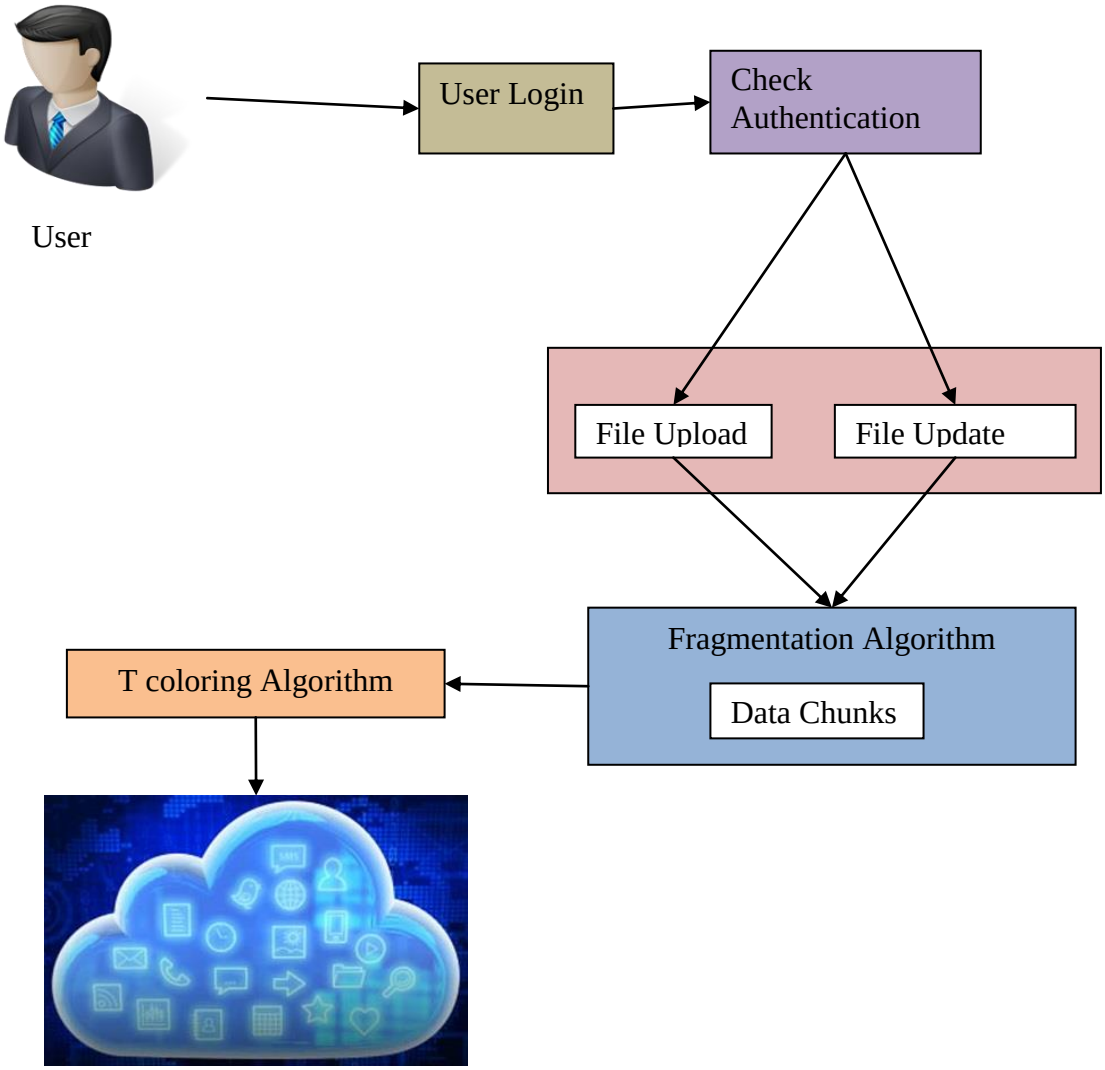


Figure: 1 Cloud manager system

DROPS FRAME WORK

Replication is used for preserving accessibility in every failure situations or load conditions through this availability and performance can improve. Excessive replication achieves overall performance degradation and high storage cost due to extreme bandwidth use. DROPS appreciate with data fragments so it is better. DROPS method used in cloud storage protection system which deals with data security and retrieval time performance. The data fragmented into many fragments and distributed in multiple nodes of cloud. By using Toloring the nodes separated randomly in cloud. In one node can able to store single fragment only. Using DROPS method user upload and download file.

ISSN: 0975-8585

DROPS PROCESS AND ALGORITHM

Using DROPS method file split into various fragment. For Security and Optimal Performance in cloud Division and Replication is used. When selecting the node in cloud keeping focus on performance and security. For enhanced access time we have to choose central nodes offered in cloud storage. DROPS technique uses centrality to reduce access time.

T-COLORING ALGORITHM FOR FRAGMENTS ALLOCATION:

T-coloring technique selects nodes in cloud for fragment placement by keeping focus on performance and security. The central node in cloud network gives improved access time. The DROPS method utilize centrality concept to decrease the access time. Centrality concludes central node based on various measures. T-coloring restricts node selection at hop distance. T-coloring gives more security performance in the cloud. The fragments are stored in different node so location of fragments can't able to determine.

ALGORITHM: FRAGMENTATION

Step 1: I = {I1;I2,…,IN}
Step 2: i = {sizeof(i1); sizeof(i2),…,sizeof(iN)}
Step 3: data = {open_data, close_data}
Step 4: cen = {cen1; cen2,….,cenM}
Step 5: data ←open_data ∀ i
Step 6: cen ←ceni ∀ i
Step 7: for each Ik > I do
Step 8: choose C^i |C^i indexof(max(ceni))
Step 9: if $data_{C^i}$ = open_data andc_i >= ik then
Step 10: S^i←Ik
Step 11: Ci ←Ci – Ik
Step 12: $data_{C^i}$ ←close_ data
Step 13: $C^{i'}$←distance(C^i; T
Step 14: $data_{C^i}$ ← close_data
Step 15: end if
Step 16: end for

RESULT AND DICUSSION

USER LOGIN

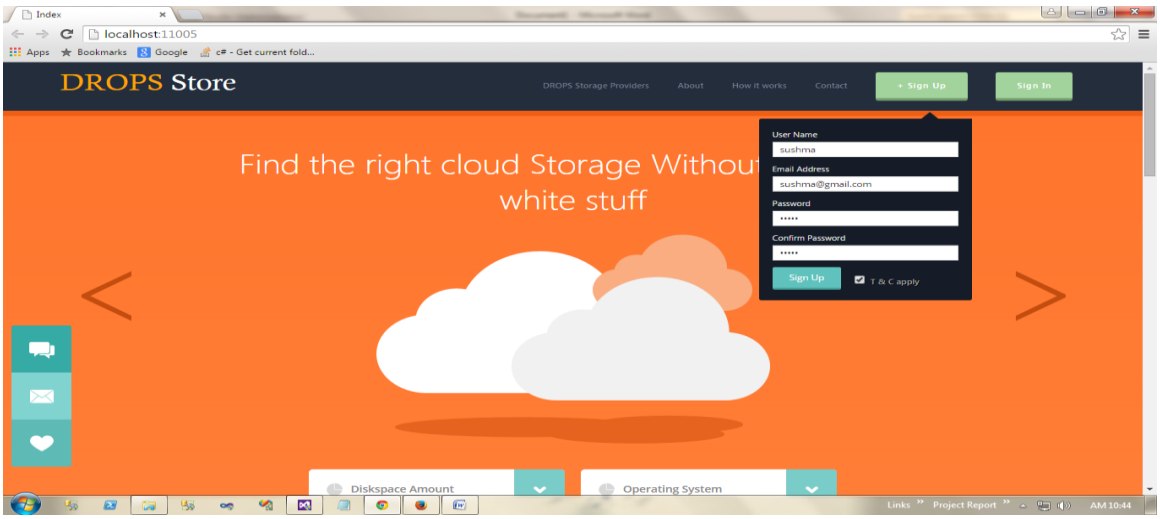


Figure: 2 User login

ISSN: 0975-8585

Figure 2 shows user login. The user have to login to access the cloud. By giving username and password the user login the cloud.

FILE UPLOAD

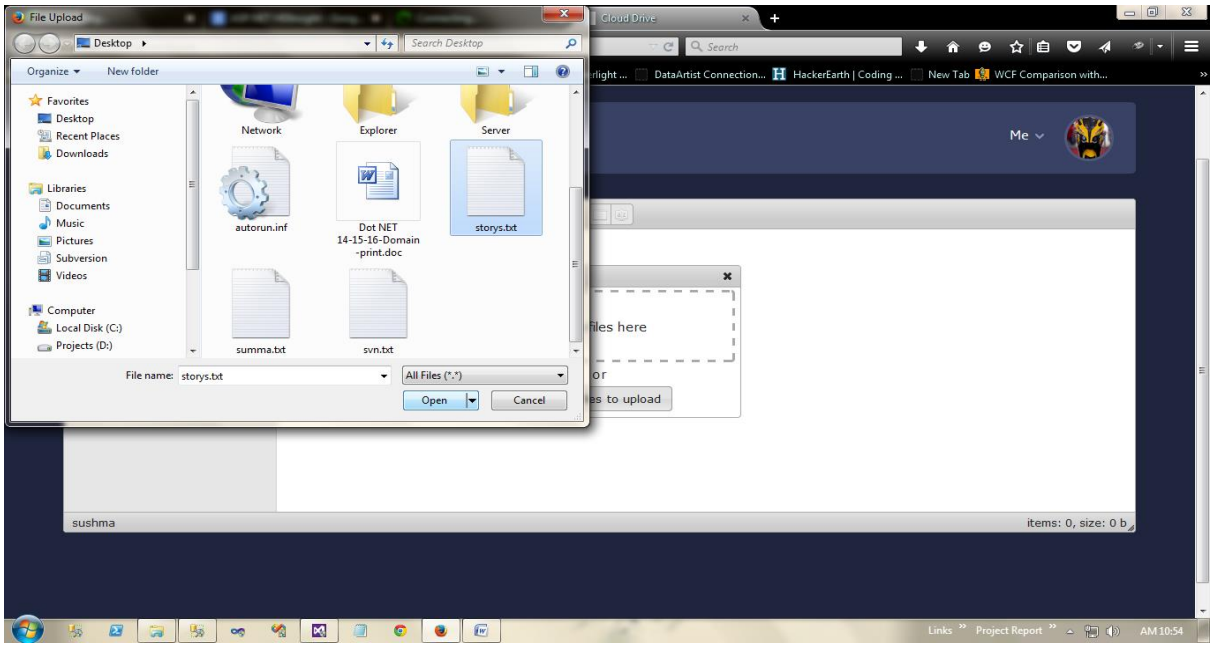
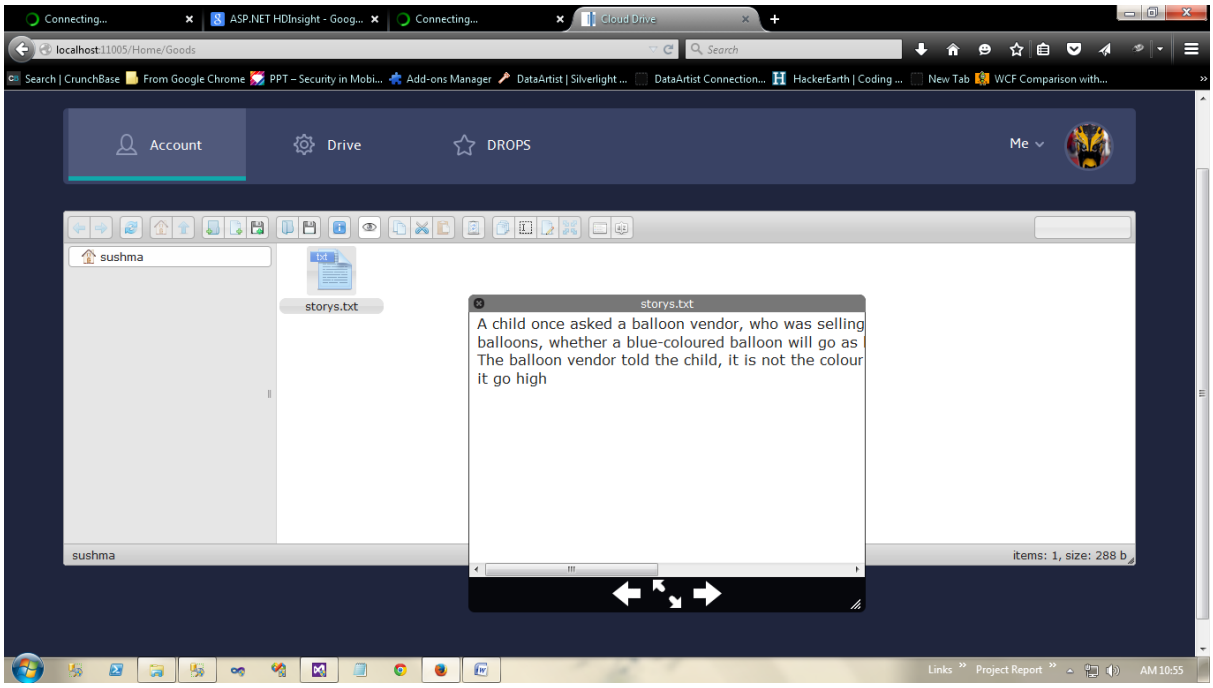


Figure: 3 File upload

Figure 3 shows file upload. The user has to select the file to upload the file into cloud. After selecting user upload the file into cloud.

FILE MODIFICATION



Figure; 4 File modification

ISSN: 0975-8585

Figure 4 shows file modification. If user wants to modify the content he/she can able to modify in cloud itself.

FILE DOWNLOAD

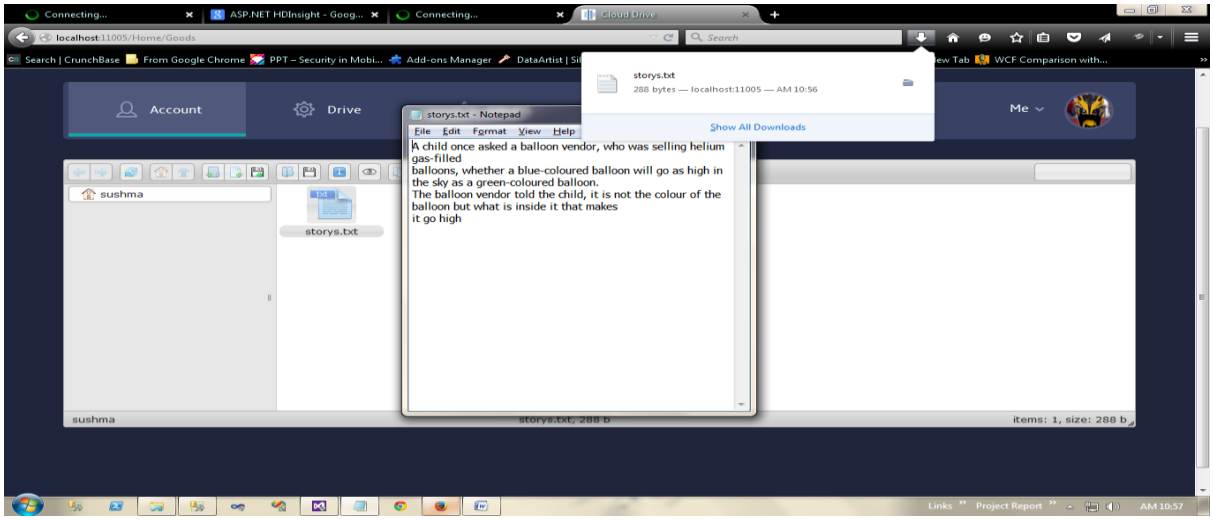


Figure: 5 File download

Figure 5 shows file download. If the user wants the file in their system he/she have to download the file in their system.

CONCLUSION

To deal security problem T-coloring is used in Cloud services. However, fragments data store in node based on the centrality there may chance to reduce user data security. So we proposed DROPS technique to divide the file into fragments and replicated the fragments of file into each node in cloud. Using T-coloring the nodes are separated into certain distance and each node can store only one fragment. The DROPS and T-coloring distribute the data in various nodes. Through this we can achieve security in cloud service system.

REFERENCES

[1] L. M. Kaufman, —Data security in the world of cloud computing, || IEEE Security and Privacy, 2009;7(4): 61-64.

[2] Issa M. Khalil ,Abdallah Khreishah,Salah Bouktif, Azeem Ahmad , ||Security concerns in cloud computing||, 10th International Conference on Information Technology: New Generations , 2013.

[3] A. R. Khan, M. Othman, S. A. Madani, S. U. Khan, —A survey of mobile cloud computing application models, IEEE Communications Surveys and Tutorials, DOI: 10.1109/SURV.2013.062613.00160.

[4] M. Hogan, F. Liu, A.Sokol, and J. Tong, —NIST cloud computing standards roadmap, NIST Special Publication, July 2011.

[5] [5] D. Zissis and D. Lekkas, —Addressing cloud computing security issues, Future Generation Computer Systems, Vol. 28, No. 3, 2012, pp. 583-592.

[6] A. Mei, L. V. Mancini, and S. Jajodia, —Secure dynamic fragment and replica allocation in large-scale distributed file systems, IEEE Transactions on Parallel and Distributed Systems, Vol. 14, No. 9, 2003, pp. 885-896.

[7] Manisha Kalkal*, Sona Malhotra, Replication for Improving Availability & Balancing Load in Cloud Data Centres —,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, 2015.

[8] Akhil Behl and Kanika Behl,||An analysis of cloud computing security issues, IEEE 2012.

[9] Bharti Dhote, A.M. Kanthe ,||Secure Approach for Data in Cloud Computing, International Journal of Computer Applications (0975 – 8887) Volume 64– No.22, February 2013.

[10] W. A. Jansen, —Cloud hooks: Security and privacy issues in cloud computing, In 44th Hawaii IEEE International Conference on System Sciences (HICSS), 2011, pp. 1-10.

[11] D.Boru, D.Kliazovich, F.Granelli, P.Bouvry, and A.Y.Zomaya, —Energy-efficient data replication in cloud computing datacenters, In IEEE Globecom Workshops, 2013, pp. 446-451.

[12] Nicoleta - Magdalena Iacob (Ciobanu), Fragmentation and Data Allocation in the Distributed Environments,Annals of the University of Craiova, Mathematics and Computer Science Series Volume 38(3), 2011.

[13] DROPS: Division and Replication of Data in Cloud for Optimal Performance and SecurityMazhar Ali, Student Member, IEEE, Kashif Bilal, Student Member, IEEE, Samee U. Khan, Senior Member, IEEE, BharadwajVeeravalli, Senior Member, IEEE, Keqin Li, Senior Member, IEEE, and Albert Y. Zomaya, Fellow, IEEE

[14] T. Loukopoulos and I. Ahmad, "Static and adaptive distributed data replication using genetic algorithms," Journal of Parallel and Distributed Computing, Vol. 64, No. 11, 2004, pp.1270-1285.

[15] DROPS: Division and Replication of Data inCloud for Optimal Performance and Security Mazhar Ali, Student Member, IEEE, Kashif Bilal, Student Member, IEEE, Samee U. Khan, Senior Member, IEEE, Bharadwaj Veeravalli, Senior Member, IEEE, Keqin Li, Senior Member, IEEE, and Albert Y. Zomaya, Fellow, IEEE

[16] A. Mei, L. V. Mancini, and S. Jajodia, "Secure dynamic fragment and replica allocation in large-scale distributed file systems,"IEEE Transactions on Parallel and Distributed Systems, 2003;14(9): 885-896.