Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 3, MaRCH-2018

Distribution and Duplication of Records in Darken for Optimal Performance and Safety

V Gokula Krishnan[1], M Poomani Raj[2], T Kalidas[3], H Ronak[4]

Associate Professor[1], UG Scholars[2,3,4]
Department of Computer Science and Engineering
Panimalar Institute of Technology, Chennai, Tamil Nadu, India

gokul_kris143@yahoo.com[1], poomaniraj10@gmail.com[2], kalidasparkash5@gmail.com[3], ronakhjoshi1997@yahoo.com[4]

ABSTRACT – Now a day in cloud the data security is the major problem. various third party provide cloud storage to us but person who use that don't know whether the data is secured in cloud are not to avoid data hacking from cloud here the data are fragmented and stored into various data servers the fragmentation of data is done using fragmented key and using that key the data is again retrieved an given back to the user due to fragmentation data and data also protected using an T-Coloring theorem the data are fragmented and stored in various data servers the hacker would get only an small part of information which would not be useful to him.

KEYWORDS – Centrality, Cloud Security, Fragmentation, Replication, Performance.

I. INTRODUCTION

Cloud computing is use to deliver computing service using internet. Cloud computing is used to access the pooled resources required for computing through our browser's window. Cloud computing is referred to an application and service which run of many number of system in virtualized resource using internet protocol and network standards. In cloud computing we use public or private network which is created using many no of system to provide scalable infrastructure for application file system and data's.

The five characteristic of cloud computing is:

1. On-demand self-service
2. Resource pooling
3. A broad network access
4. Rapid elasticity
5. Measured service

Cloud computing consist of servicing modes such as

1. Software as a Service (SAAS)
2. Platform as a Service (PAAS)
3. Infrastructure as a Service (IAAS)

Software as a Service is a licensed service which provides cloud based on pay per use model. It is used for billing purposes, provided by Google, Mails, and Facebook. Platform as a service is use to provide services such as building, delivering and deploying web applications. It is provided by Google app engine, Microsoft azure, Zoho. Infrastructure as a service is based on demand self-service and scalable service. Providers are amazon elastic computing cloud, go grid etc.

Cloud deployment models are:

1. Public cloud
2. Private cloud
3. Hybrid cloud

Public clouds are made available for public usage it is provided by Google app engine, azure and IBM. Private cloud is used by organization it is provided by VMware cloud infrastructure, amazon VPC. Hybrid cloud is a combination of various public and private networks which is a provided by an organization called Google.

II. LITERATURE SURVEY

Data replication [2] proposes a novel replication solution which in addition to traditional performance metrics, such as availability of network bandwidth, optimizes energy efficiency of the system. Moreover, the optimization of communication delays leads to improvements in quality of user experience of cloud applications. The performance evaluation is carried out using GreenCloud – the simulator focusing on energy efficiency and communication processes in cloud computing data centers. The obtained results confirm that replicating data closer to data consumers, i.e., cloud applications, can reduce energy consumption, bandwidth usage, and communication delays significantly. There is no single optimal approach [11] to foster both security and legal compliance in an Omni-applicable manner. Moreover, the approaches that are favorable from a technical perspective appear less appealing from a regulatory point of view, and vice versa. The few approaches that score sufficiently in both these dimensions lack versatility and ease of use, hence can be used in very rare circumstances only.

Security and Privacy-Enhancing Multi cloud Architecture [12] cloud computing platforms are widely used today, there still exist plenty of research gaps to be addressed. Reliability of cloud services still remains a big challenge. On the other hand, with the increase in the infrastructure and design complexity of clouds, they are becoming big consumers of energy and leaving enormous carbon footprints. Energy efficiency, reliability and scalability are among the foremost concerns in cloud computing in these days. Researchers are striving to find the optimized and applicable solutions for the challenges. In this paper, we identified the need of a reliability-aware and energy-aware resource provisioning policy to improve the availability of the services of

cloud by reducing the energy consumption. We have developed algorithms [13] to allocate correlated data shares in large-scale peer-to-peer data grids. To support scalability, we represent the data grid as a two-level cluster based topology and decompose the allocation problem into two sub-problems: the OIRSP and OISAP. The OIRSP determines which clusters need to maintain share replicas, and the OISAP determines the number of share replicas needed in a cluster and their placements.

Heuristic algorithms are developed for the two sub-problems. First, the secure storage mechanisms developed in this paper can also be used for key storage. In this alternate scheme, critical data objects are encrypted and replicated. Use of Firewall [14] within the organization network along with IDS is very effective away of implementing a security. Distribution of NIDS among different departments makes it more immune to Intrusion and avoids the problem of single point of failure. Distributed nature of NIDS results in early Detection of attacks launched from organizations against organization itself. DoS/DDoS/Probing attack launched from the organization can't affect the entire organization as it gets detected and blocked at NIDS of the Department itself. Novel Architecture for Intrusion-Tolerant Distributed Intrusion Detection System using Packet Filter Firewall and State Transition Tables.

III. PROBLEM DEFINITION

Outsourcing data to a third-party administrative control, as is done in cloud computing, gives rise to security concerns. The data compromise may occur due to attacks by other users and nodes within the cloud. Therefore, high security measures are required to protect data within the cloud. However, the employed security strategy must also take into account the optimization of the data retrieval time. In this paper, we propose Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. In the DROPS methodology, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Moreover, the nodes storing the fragments are separated with certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments. Furthermore, the DROPS methodology does not rely on the traditional Cryptographic techniques for the data security; thereby relieving the system of computationally expensive methodologies. We show that the probability to locate and compromise all of the nodes storing the fragments of a single file is extremely low. We also compare the performance of the DROPS methodology with ten other schemes. The higher level of security with slight performance overhead was observed.

IV. EXISTING SYSTEM

The off-site data storage cloud utility requires users to move data in cloud's virtualized and shared environment that may result in various security concerns. Pooling and elasticity of a cloud, allows the physical resources to be shared among many users. The data outsourced to a public cloud must be secured. Unauthorized data access by other users and processes must be prevented as discussed above, any weak entity can put the whole cloud at risk. In such a

scenario, the security mechanism must substantially increase an attacker's effort to retrieve a reasonable amount of data even after a successful intrusion in the cloud.

Disadvantages

- The data compromise may occur due to attacks by other users and nodes within the cloud.
- The employed security strategy must also take into account the optimization of the data retrieval time

V. DESIGN GOALS

Access control: Initial, licensed cluster members are able to access the cloud information. Second, unauthorized users cannot access the cloud information at any time, and revoked users won't be capable of accessing the cloud once they're revoked.

Data confidentiality: Data confidentiality needs that unauthorized users aren't capable to access the content of the stored information and difficult issue for information confidentiality for dynamic clusters. Specifically, new users ought to access the information stored within the cloud before their participation, and revoked users are unable to access the information once the revocation. Data owner can store the information on the cloud and share among the cluster members and data owner can modify the information and delete the information within the cloud.

Efficiency: every user data are stored in separate cloud server if an hacker try's to access data from an particular server he would only get an specific part of data which would not cant any full detail about the project .

VI. PROPOSED SYSTEM

Here collectively approach the issue of security and performance as a secure data replication problem. Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that judicially fragments user files into pieces and replicates them at strategic locations within the cloud. The division of a file into fragments is performed based on a given user criteria such that the individual fragments do not contain any meaningful information. Each of the cloud nodes contains a distinct fragment to increase the data security.

Advantages

- The implications of TCP in cast over the DROPS methodology need to be studied that is relevant to distributed data storage and access
- To improve data retrieval time, the nodes are selected based on the centrality measures that ensure an improved access time.

VII. SYSTEM ARCHITECTURE

The architecture model consists of 3 main completely different entities: The Cloud Server, user files.

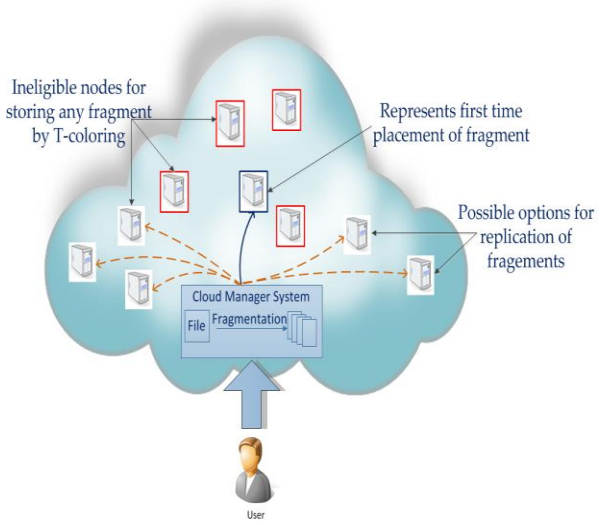

Figure 1. System Architecture

Cloud Server: Cloud is the massive repository of resources. Cloud is accountable for storing all user information and granting access to the file among a cluster to different cluster members based on public revocation list which is maintained by group manager. We have a tendency to assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user information, but can attempt to learn the content of the stored information.

User file: Here the user file is stored in cloud by fragmenting the data of user into small pieces and stored in different cloud servers for securing the data in cloud

VIII. MODULE DESCRIPTION

Develop Cloud Manager System

In this phase user registration process take place. For registration user need to register using valid email Id. The password for the user is sent to email using this the user can login in to cloud account. This process is done in phase 1.

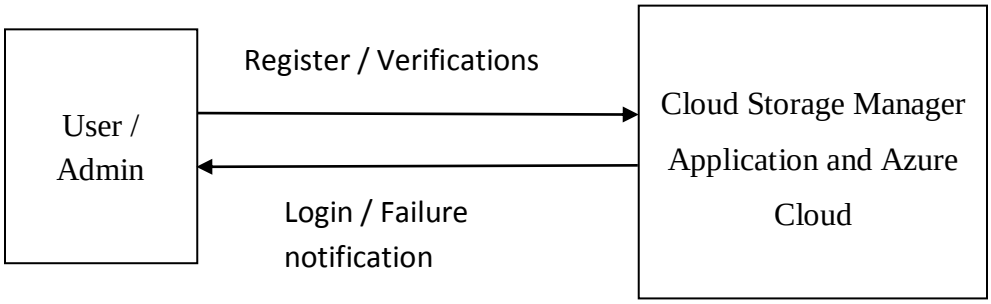

Figure 2. Cloud Manager System

Coloring and Fragmentations

In this phase the data provided by the user is stored in cloud before storing the data is fragmented into five pieces. Each piece is given a separate code to identify the data and all data is shuffle. Shuffling of data is done using t-coloring approach .and data is stored in data base using Manchester's algorithm

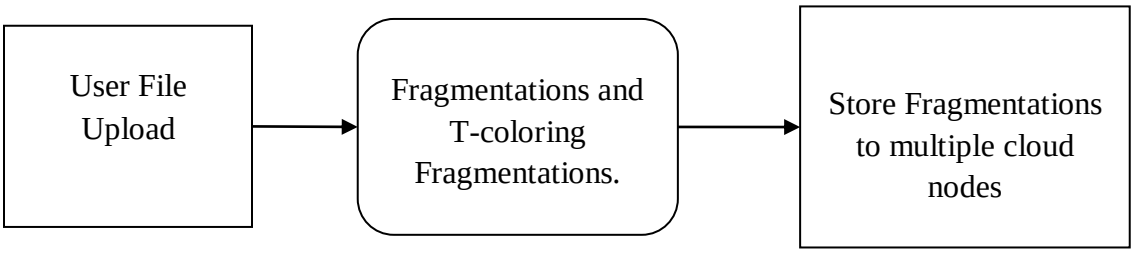

Figure 3. Coloring and Fragmentation

Requesting and Replication

In this user send a data file to the cloud. The cloud manager system receive the file and perform fragmentation, in the first cycle of nodes used for fragmentation over selected node, and second cycle of nodes selection for fragments replication. The fragmentation threshold of the data file is specified to be generated by the file owner. The file owner can specify the fragmentation threshold in terms of either percentage or the number and size of different fragments. Here we use T-coloring approach to store the fragmented data into various location of server and uses Manchester's algorithm to place the fragmented data in various servers.

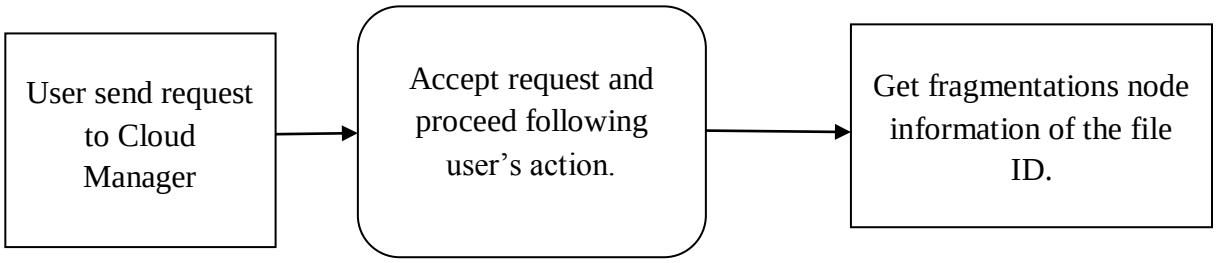

Figure 4. Requesting and Replication

Managing Status and Download Files

When a user send a download request the cloud manager collect all the data from different location of server and reassemble it in single file. After the reassembling of file is done the user can download the file from the dashboard. Therefore every request for download file is stored in cloud manager

Figure 5. Managing Status and Downloading Files

IX. EXPERIMENTAL RESULTS

The below displayed are the results of the module implementation. These screenshots show the User Interface through which the modules are being developed.

For registration user need to register using valid email Id. The password for the user is sent through email using this user can login In to cloud account.

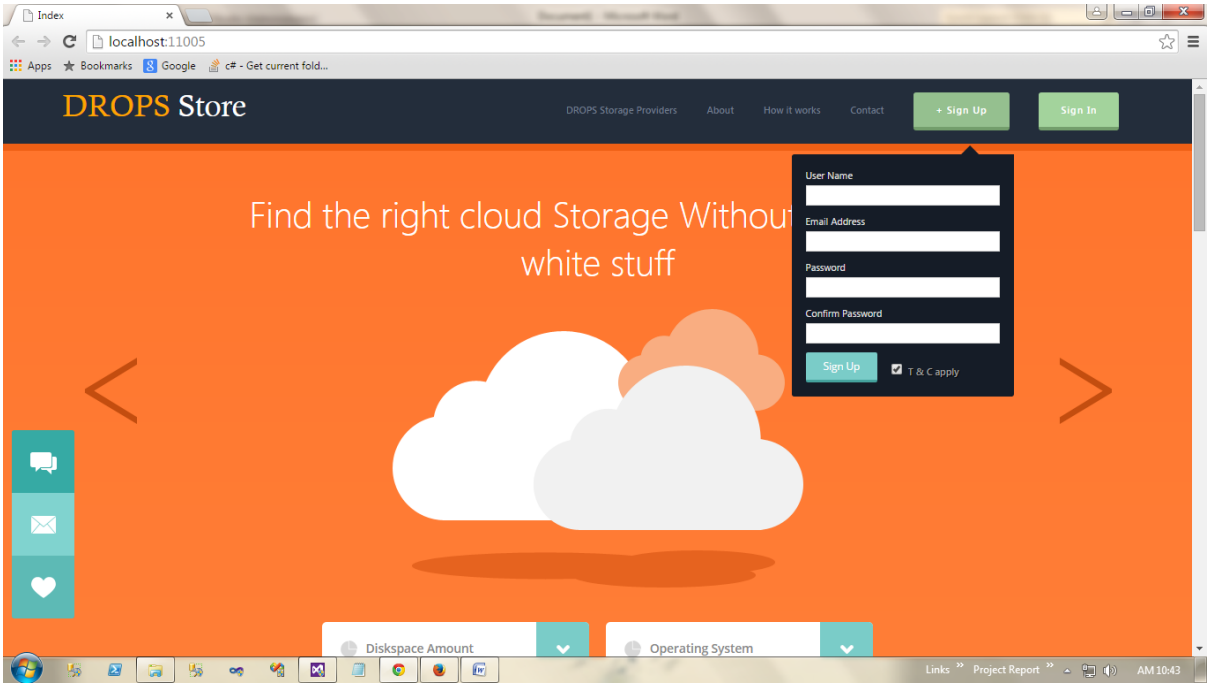

Figure 6. Creating a New Member

The data provided by the user is stored in cloud before storing the data is fragmented into five pieces. Each piece is given a separate code to identify the data and all data is shuffle. Shuffling of data is done using t-coloring approach .and data is stored in data base using Manchester's algorithm.

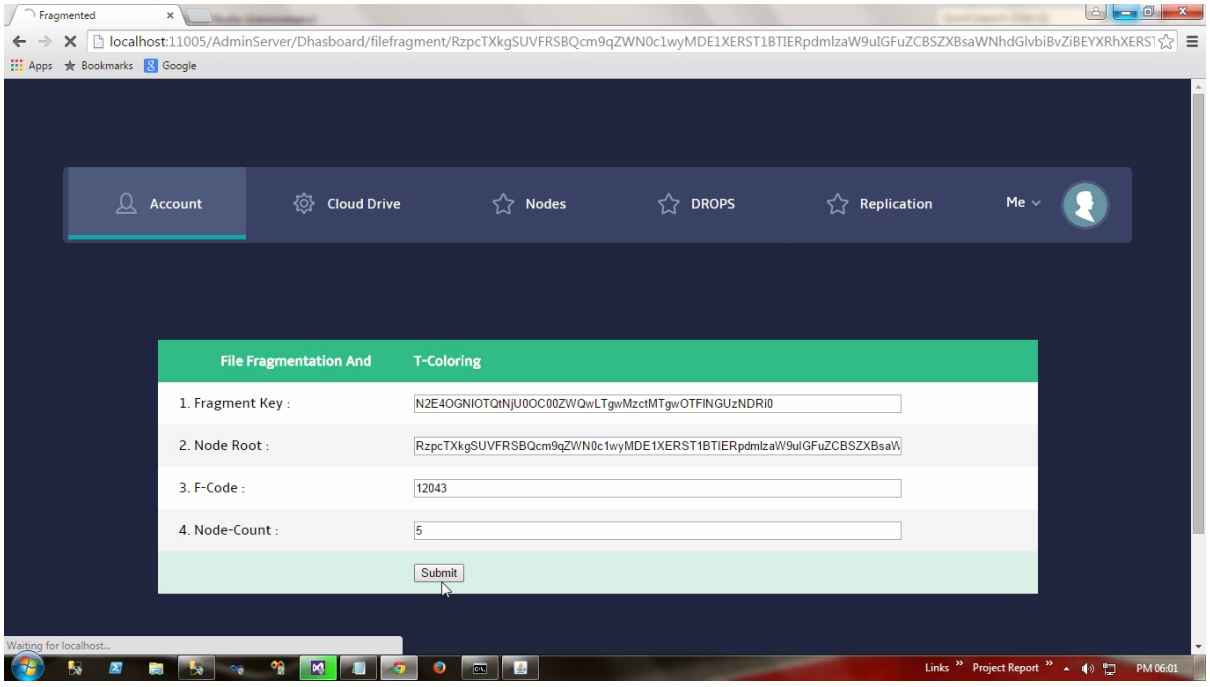

Figure 7. Uploading a File

Here the user sends the request to the cloud manager that he need to download his file which is securely stored in cloud

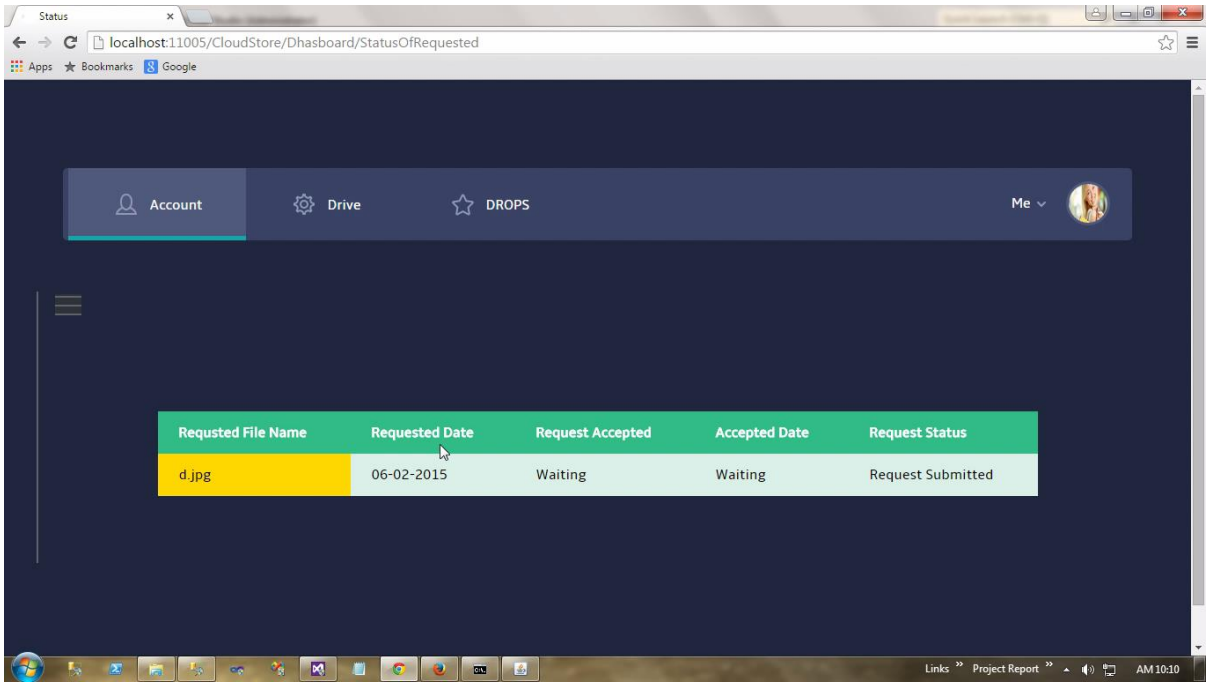

Figure 8. Requesting a File

Here the cloud manager verify the user details and his data in cloud and collect all his data from various location of cloud and arrange it in order and that download link to user and thus the user can download the file from his dashboard.

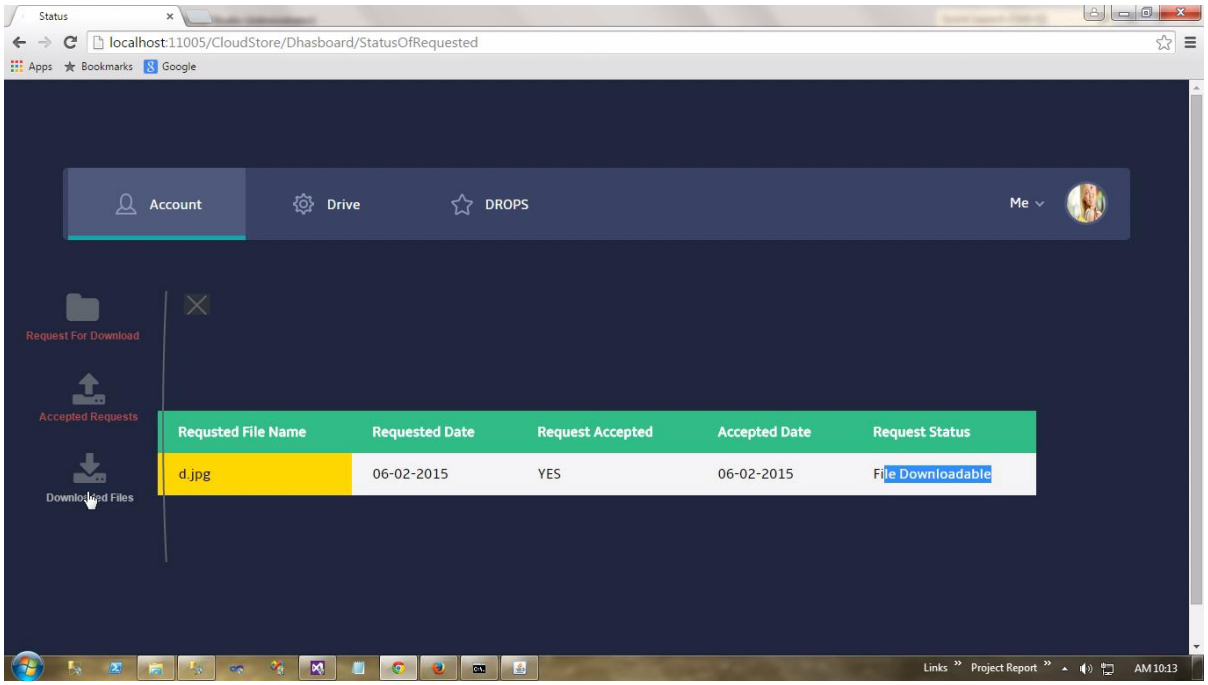

Figure 9. Downloading Link of a File

Therefore the data from cloud is download by the user which is provide by the cloud manager and can be accessed by the user for father usage of his project are his work.

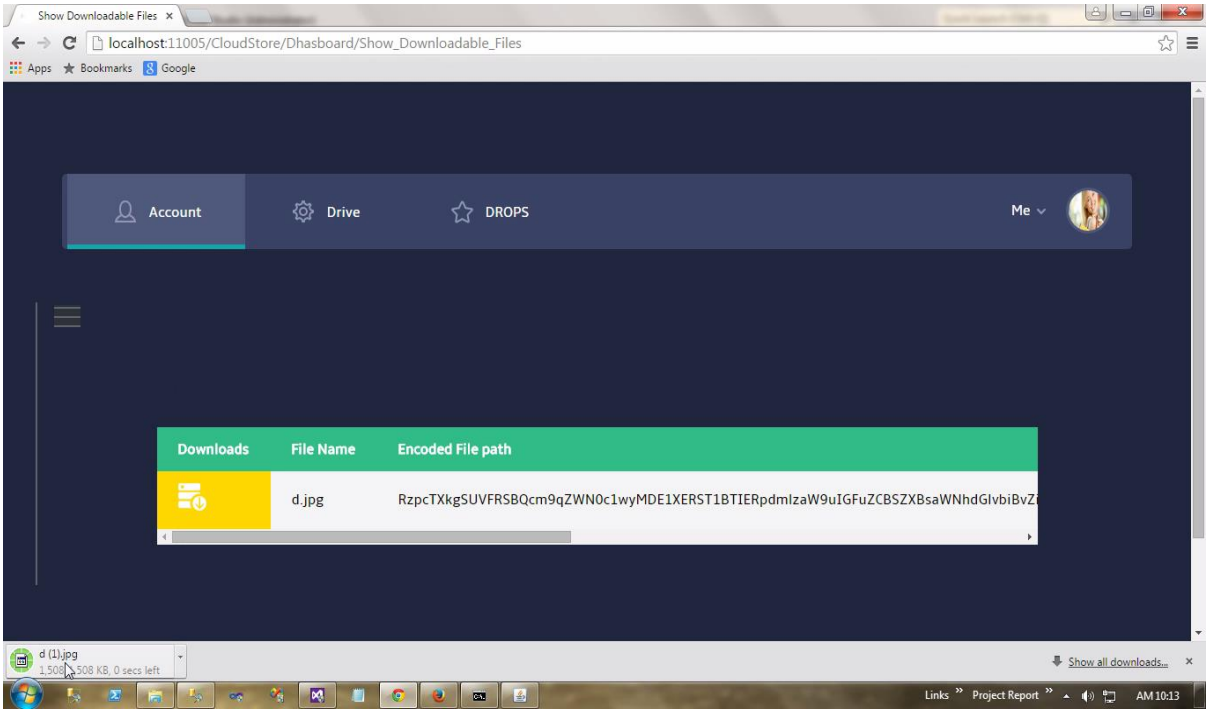

Figure 10. Path of Download File

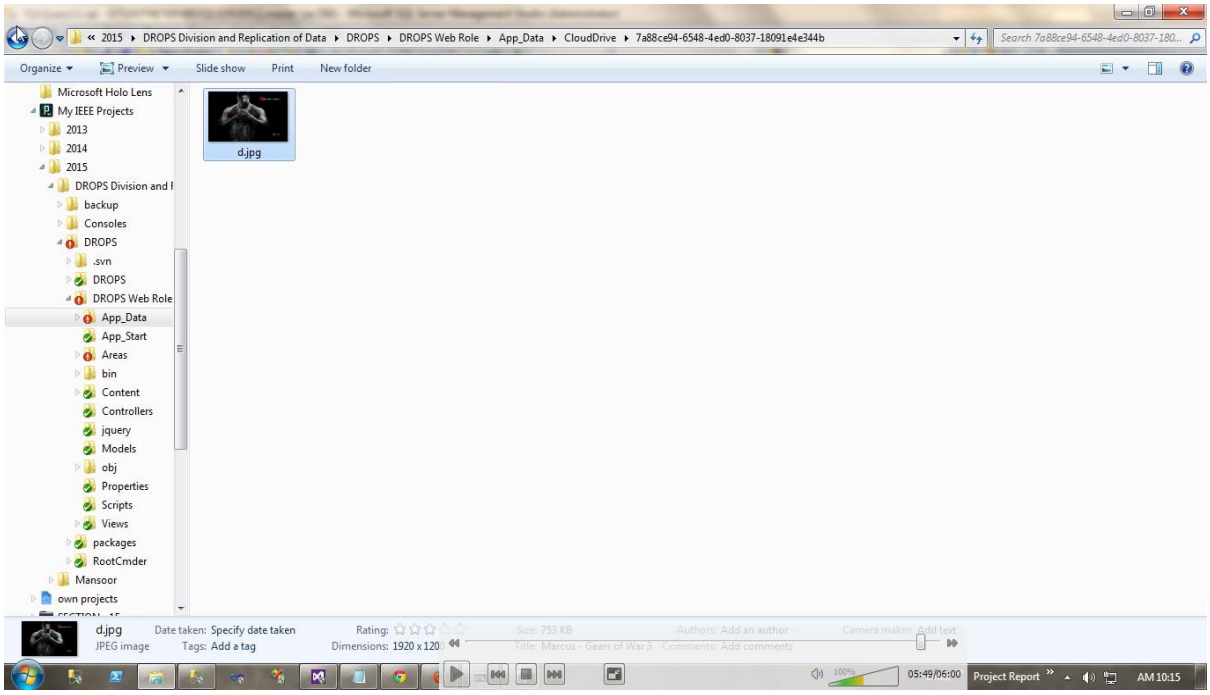

Figure 11. Uploaded User File

X. CONCLUSION

This project focuses on data security on cloud. Now a day most of the people use cloud to store data in cloud there are various security constraint in cloud. Since the data in cloud are not secured the data in cloud are separated and stored in various data centers using Manchester's algorithm and the data are separated by using t-coloring process and fragmentation key. Thus the data hacking is reduced from cloud.

REFERENCES

[1]. K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A. Zomaya, "On the characterization of the structural robustness of data center networks," IEEE Transactions on Cloud Computing, Vol. 1, No. 1, 2013, pp. 64-77.

[2]. 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.

[3]. Y. Deswarte, L. Blain, and J-C. Fabre, "Intrusion tolerance in distributed computing systems," In Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy, Oakland CA, pp. 110-121, 1991.

[4]. B. Grobauer, T.Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," IEEE Security and Privacy, Vol. 9, No. 2, 2011, pp. 50-57.

[5]. W. K. Hale, "Frequency assignment: Theory and application, Proceedings of the IEEE, Vol. 68, No. 12, 1980, pp. 1497-1514.

[6]. 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.

[7]. 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.

[8]. L. M. Kaufman, "Data security in the world of cloud computing, "IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.

[9]. Y. Tang, P. P. Lee, J. C. S. Lui, and R. Perlman, "Secure overlay cloud storage with access control and assured deletion," IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 6,Nov. 2012, pp. 903-916.

[10]. M. Tu, P. Li, Q. Ma, I-L. Yen, and F. B. Bastani, "On the optimal placement of secure data objects over Internet," In Proceedings of 19th IEEE International Parallel and Distributed Processing Symposium, pp. 14-14, 2005.

[11]. Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono and Ninja Marnau, "Security and Privacy-Enhancing Multicloud Architectures", IEEE Transactions on Dependable and Secure Computing, Vol. 10, No. 4, July/August 2013.

[12]. Yogesh Sharma, Bahman Javadi, Weisheng Si, "On the Reliability and Energy Efficiency in Cloud Computing", Proceedings of the 13th Australasian Symposium on Parallel and Distributed Computing (Aus PDC 2015), Sydney, Australia, 27 - 30 January 2015.

[13]. G. Aruna Kranthi, D. Shashi Rekha, "Protected data objects replication in data grid", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, January 2012.

[14]. Dr. S.G. Bhirud Vijay Katkar, "Novel Architecture for Intrusion-Tolerant Distributed Intrusion Detection System using Packet Filter Firewall and State Transition Tabels, "International Journal of Computer Applications (0975 – 8887) Volume 8– No.11, October 2010.

[15]. Dimitrios Zissis, Dimitrios Lekkas, Department of Product and Systems Design Engineering, University of the Aegean, Syros 84100, Greece in 2010.