iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 6 **Issue:** III **Month of publication:** March 2018

**DOI:** http://doi.org/10.22214/ijraset.2018.3186

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887*
*Volume 6 Issue III, March 2018- Available at www.ijraset.com*

# Division and Replication of Data in Cloud for Optimal Performance and Security - DROPS

Nicy Johnson[1], Remya V R[2], Daniel Williams George[3], Arun Unnikrishnan [4], Rahul C D[5]
[1, 2, 3, 4] *Assistant Professor, University of Calicut, Computer Science Department, I E S College of Engineering, Chittilappilly, Thrissur, Kerala*
[5] *University of Calicut, Computer Science Department, I E S College of Engineering, Chittilappilly, Thrissur, Kerala*

***Abstract*: Cloud storage is basically giving all the data to a third party to store it and to retrieve them whenever we wish. This compromises the security of the data. So high security measures are meant to be taken but, it should be simple and easy to use. To overcome these disadvantages, we come with the technique, Division and replication of Data in the Cloud for Optimal performance and Security (DROPS). In the DROPS methodology, we use many number of cloud servers. To upload a file, it is divided into many fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular file so that even in the case of a successful attack, no meaningful information is revealed to the attacker. The Cloud Manager or simply the CM takes care of all these activities and during the retrieval of a file, the cloud manager collects all the fragments of a file and combines them to form the original file and is given to the user. The main idea is to give added security and protection against all types of attacks, to the data that is being stored in cloud storages***
***Keywords*: Cloud storage,***

## I. INTRODUCTION

Cloud computing is an information technology paradigm, a technique for getting access to shared pools of configurable resources, such as computer networks, servers, storage, applications and services which can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing allows users and enterprises with various computing capabilities to store and process data either in a privately-owned cloud, or on a third-party server located in a data centre, making data-accessing mechanisms more efficient and reliable. It is to be noted that any data stored in such cloud devises are not managed by the owner of the data. The data is being stored usually in the hands of a third party. This leads to many inconveniences among the users. This includes, unavailability of data at times and high risk of the data getting in to unwanted hands. In this project, these main disadvantages of cloud computing have overcome in simple and efficient ways. The main idea is to add more security to the data that is being stored in cloud servers. Instead of storing in the servers directly, like in the conventional methods, the data is first send to a cloud manager. Large number of cloud storage servers are present to store the files. As the data is received by the cloud manager, splits the file into many fragments and stores these fragments in different servers for security reasons. To retrieve a file from the cloud, the cloud manager combines all the fragments of a file and gives is back to the user.

## II. LITRATURE REVIEW

In the work done by S. Manjula, named [1] Division of data in cloud environment for secure data storage, privacy is very much considered in the field of cloud computing and the division of data is a new trend to overcome this security issue. Instead of using public clouds or private clouds, this methodology is implemented in hybrid clouds, which according to the author, is much better in terms of the services provided. The files are first encrypted with the help of RSA algorithm. After successful encryption, the data is divided into many pieces. Copies of these pieces are made and they are stored in the cloud servers. Replication is done to ensure the availability of data even in the case of failure of a cloud server. RSA algorithm is used to encrypt the files before splitting them in to many pieces. This gives an extra layer of protection to the files. Encrypted files are decrypted during the file retrieval process. This encryption and description process with RSA algorithm takes much time to perform, this reduces the performance of the system

In the paper Energy Efficient Data Replication in Cloud Computing Datacenters, [2] by Dejene Boru, the author says that communication resources over a network is a bottleneck in service provisioning for many cloud applications. Therefore, data replication brings databases closer to the users to the users or the cloud applications. Both energy efficiency and bandwidth consumption of the system is improved in addition to the improved Quality of Service as a result of reduced communication delays. Three tire computing architecture is implemented to reduce the time taken to retrieve data from the servers. Additional buffers are

©IJRASET (UGC Approved Journal): All Rights are Reserved

placed at intermediate levels to catch the frequently accessed data. So, time taken to access the data is less. A module called the replica manager is located in the central database and it periodically analyses the data and then the buffers are maintained by it.

## III. PROPOSED SYSTEM

The proposed system aims at keeping all the pros of the existing system, while overcoming some of the drawbacks which are mentioned earlier. In our proposed model, the Cloud manager is the central part, which does all the functions related to the different procedures in connection with the services provided. The cloud storage consists of many individual cloud servers, which stores the files. The cloud manager splits the file in to many fragments and stores each fragment in different servers. The fragmentation is done with the help of fragment threshold. The servers are represented as nodes in the form of a graph and each node is given a color, with respect to the state of that node. Open color is given, if the server doesn't have any fragment of the current file in it. Close color is given if it contains any fragment of the current file. Even in the case of a successful attack, the hacker doesn't get any meaningful information. There is no need for cryptography, as the stolen data will not be of any use. Even if data gets deleted from a server, all data stored in that server will have a copy of it in any other server, so technically data never gets permanently deleted.

### *A. Requirements*

Main requirements for the system is performance and uncompromised security. An android application is developed for the users to make use of our idea. With the android application, the users first have to create an account and once the users have done that, they can login to their account, where they can upload new files to their personal cloud account, view the files that are already uploaded if an and they can also download the files or delete it if they wish. The android app is developed with the help of Android studio. The fragmentation of files are done with a Java program. The program scans the files and makes it in to many small pieces, called fragments. This program is embedded in to the android app.

### *B. Architecture*

The following figure, Fig.1 illustrates our system architecture. This figure gives a brief information about our proposed system. The important two components of the system is the user login/registration module and the cloud manager. The registration module helps users to create an account. The account details are stored in a secure server. The login module checks the credentials entered by the users during login. The data is checked and the user gets access to their account if valid details are given. On successful login, the users get access to their account. Then in the case of a file upload, the file goes to the cloud manager and the rest is taken care by the cloud manager. And during the retrieval of the file also, a request is given to the cloud manager and it returns the file. The cloud manager is the central part and it helps in uploading and downloading the files to the cloud server.

### *C. Cloud Manager*

Cloud manager module is an automated module which runs in the background without user interactions. It mainly deals with the storage strategy of the uploaded file in the cloud server. This module takes charge whenever a new file is uploaded. Any file being uploaded to the cloud, is first passed though the Cloud Management module.

The cloud manager analyses the file and identifies the number of fragments to be created for storing the file. Then the fragmentation replication procedure takes place. During this process, the size of the file is analysed and the file is made in to fragments.

These fragments are to be stored in different nodes. The files are also replicated to ensure the availability of the file even in the case of the failure or unavailability of a server. A copy of each fragment is made for this purpose.

Whenever a request to view or download a file is given to the application, it goes to the cloud manager and the cloud manager looks for the positions in which the fragments are stored and retrieves the fragments from the respective locations.

The look-up table is used to see in which all locations, the fragments are stored. If one location is unavailable, due to any technical problems, the cloud manager gets if from the location where the copy of this file is stored. Replication of files is of great help in such situations. The fragments are then combined to form the original file before it is finally presented before the user.

The download process also uses the same concept. Cloud manager uses the lookup table for searching the fragments associated with a file and collects & binds all such fragments to re-create the file.

This re-created file is sent back the requested user.

©IJRASET (UGC Approved Journal): All Rights are Reserved

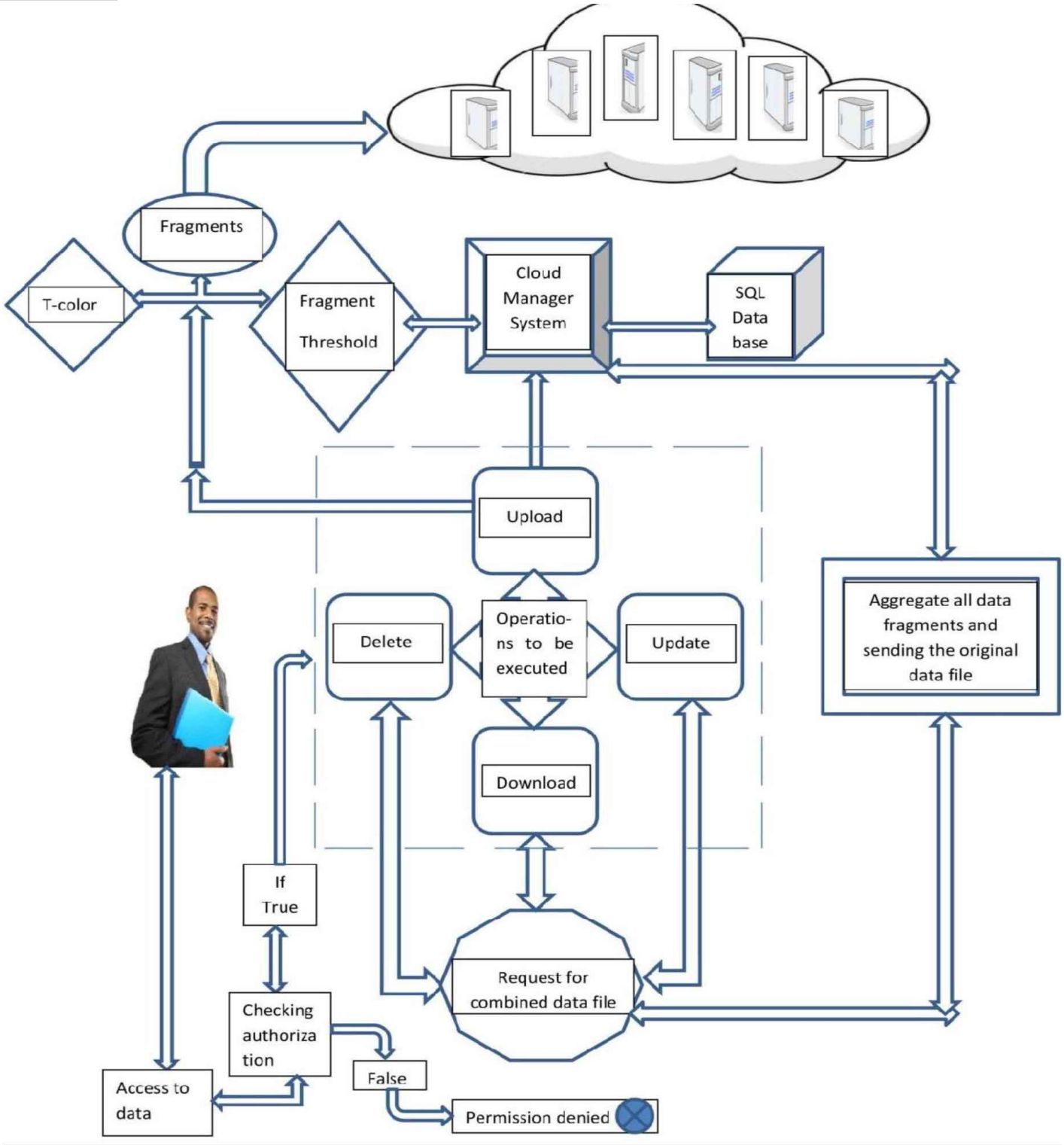



Fig 1. System Architecture

## IV. IMPLEMENTATION

System implementation is the process of changing the theories in to reality. The android app is made with the use of Android studio and all the backend process are done with java and SQLite. The app has a very simple to use user interface. On opening the app, the user is greeted with the login page. By enter valid credentials, the user can login. On successful login, the files uploaded to the user's cloud account can be viewed. New files can be uploaded or existing ones can be deleted. The user has the option to give any

©IJRASET (UGC Approved Journal): All Rights are Reserved

suggestions or feedback to the admin if he has any. Thus, the size of the application can be reduced considerably. Look up table is also implemented in the cloud server. Implementation of a software refers to the final installation of the package in its real environment, to the satisfaction of the intended users and the operation of the system. The people are not sure if the software will work without any errors. This has to be cross checked and necessary changes are to be made before the application is released to the general public.

## V. CONCLUSION

Cloud computing is one of the most commonly used and very useful internet service these days. Its special features like availability and easiness to use makes it very popular. Also, the files stored in the cloud servers can be shared with other people or can be accesses from anywhere with great ease. The risk involved in handing our precious information to a third party many lead many privacy issues. These issues which are discussed earlier are overcome with the use of efficient usage of the cloud servers. Encryption techniques, which are used in traditional systems are avoided, but this “DROPS” technique gives more security without any delay as the encryption and decryption techniques consume lots of time resulting in much slow data processing.

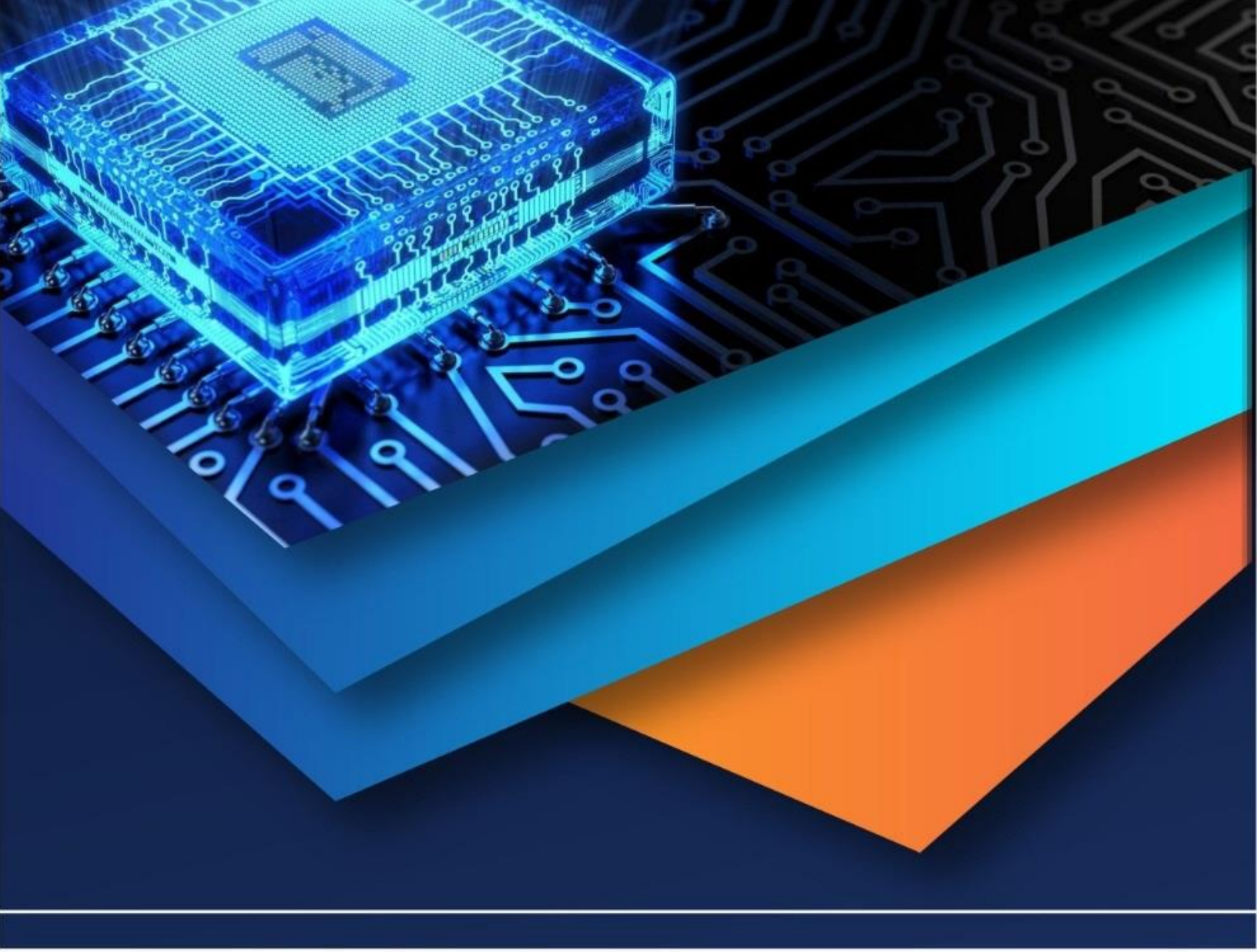
## VI. ACKNOWLEDGMENT

We are greatly thankful to Dr. S. Brilly Sangeetha, Head of Computer Science and Engineering for the vision and the encouragement, which inspired us to make this project. We also show our sincere thanks to Ms. Nicy Johnson, who has been guiding us through out the project. We also extend our thanks to Ms. Remya V R for supporting us and for the encouragement.
Above all, we are thankful to the God Almighty for showering his blessings upon us for this great success.

## REFERENCES

[1] S. Manjula, M. Indra Devi, R Swathia, “Division of data in cloud environment for secure data storage” IEEE International Conference on Computing Technologies and Intelligent Data Engineering
[2] Dejene Boru, Dzmitry Kliazovich, “Energy – Efficient Data Replication in Cloud Computing Datacenters”, IEEE Globecom Workshops (GC Wkshps)
[3] K. Bilal, S. U. Khan, L. Zhang, H. Li, K. Hayat, S. A. Madani, N. Min-Allah, L. Wang, D. Chen, M. Iqbal, C. Z. Xu, and A. Y. Zomaya, “Quantitative comparisons of the state of the art data center architectures,” Concurrency and Computation: Practice and Experience, Vol. 25, No. 12, 2013, pp. 1771-1783.
[4] 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.
[5] G. Kappes, A. Hatzieleftheriou, and S. V. Anastasiadis, “Dike: Virtualization-aware Access Control for Multitenant Filesystems,” University of Ioannina, Greece, Technical Report No. DCS2013-1, 2013.
[6] W. A. Jansen, “Cloud hooks: Security and privacy issues in cloud computing,” In 44th Hawaii IEEE International Conference onSystem Sciences (HICSS), 2011, pp. 1-10

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)