IMPLEMENTATION OF EFFICIENT CONTROL ACCESS AND DATA INTEGRITIY IN MULTI CLOUD

[1]Shivakumar K.Honawad, [2]Praveen S.Challagidad

Abstract— **The usage of single cloud provider affecting the user's data and cloud service failure. Data intrusion, Data Integrity, and Service availability leads too many problems for the users of cloud computing. Data intrusion will leads to the modification of the stored data in a cloud. Due to downfall of the cloud server leads to the service unavailability to the users. Corrupting the stored data in cloud will not maintain integrity of the data to users. This paper focuses on data storage and data accessing from multi-clouds, it also overcomes the service availability problem. It avoids the accessing of corrupted data from the cloud and makes the user to access the non corrupted data from the cloud. The efficient algorithm for file upload and efficient algorithm for file download is used. The multi cloud concept has been used. The main aim of this paper is to get the data in non violated form from the cloud to user.**

Index Terms— **cloud computing, data integrity, cloud corruption and data intrusion.**

I. INTRODUCTION

Cloud computing is a subscription-based service where those can obtain networked storage space and computer resources. The use of cloud computing has increased rapidly in many organizations. Small and medium companies use cloud computing services for various reasons, including because these services provide fast access to their applications and reduce their infrastructure costs.

The cloud makes it possible for user to access user information from anywhere at any time. While a traditional computer setup requires user to be in the same location as user data storage device, the cloud takes away that step. The cloud removes the need for user to be in the same physical location as the hardware that stores user data. User cloud provider can both own and house the hardware and software necessary to run user home or business applications.

This is especially helpful for businesses that cannot afford the same amount of hardware
and storage space as a bigger company. Small companies can store their information in the cloud, removing the cost of purchasing and storing memory devices. Additionally, because user only need to buy the amount of storage space user will use, a business can purchase more space or reduce their subscription as their business grows or as they find they need less storage space.

One requirement is that user needs to have an internet connection in order to access the cloud. This means that if user want to look at a specific document user have housed in the cloud, user must first establish an internet connection either through a wireless or wired internet or a mobile broadband connection. The benefit is that user can access that same document from wherever users are with any device that can access the internet. These devices could be a desktop, laptop, tablet, or phone. This can also help user business to function more smoothly because anyone who can connect to the internet and user cloud can work on documents, access software, and store data. Imagine picking up user Smartphone and downloading a pdf document to review instead of having to stop by the office to print it or upload it to user laptop. This is the freedom that the cloud can provide for user.

Cloud computing has now emerged to become one of the best methods for companies wanting to revamp and enhance their IT infrastructures. However, there are certain issues and problems associated with cloud computing. Needless to say, it is very advantageous for everyone to adapt to new technology, but it is also wise to recognize some of the risks associated with this technology, so as to avoid the possibility of future issues. Here, some information on the risks associated with cloud computing, along with suggestions on how to deal with the same.

The use of cloud computing has increased rapidly in many organizations. Small and medium companies use cloud computing services for various reasons, because these services provide fast access to their applications and reduce their infrastructure costs.

Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multi-clouds", "inter-cloud" or "cloud-of-clouds".

Generally speaking, most cloud computing service providers are already familiar with the issues involved and can deal with them right at the beginning. This makes the process more of less safe for users. But it also implies that users make wise decisions while choosing their service provider. Users need to clarify all their doubts and issues with the service provider before choosing them.

The increasing popularity of cloud storage is leading organizations to consider moving data out of their own data centers and into the cloud. However, success for cloud storage providers can present a significant risk to customers; namely, it becomes very expensive to switch storage providers.

Data outsourcing or database as a service is a new paradigm for data management in which a third party service provider hosts a database as a service. The service provides data management for its customers and thus obviates the need for the service user to purchase expensive hardware and software, deal with software upgrades and hire professionals for administrative and maintenance tasks. Since using an external database service promises reliable data storage at a low cost it is very attractive for companies. Such a service would also provide universal access, through the Internet to private data stored at reliable and secure sites.

A. Types of clouds

There are different types of clouds that one can subscribe to depending on needs. As a home user or small business owner, will most likely use public cloud services.

- Public Cloud - A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space.
- Private Cloud - A private cloud is established for a specific group or organization and limits access to just that group.
- Community Cloud - A community cloud is shared among two or more organizations that have similar cloud requirements.
- Hybrid Cloud - A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community.

II. RELATED WORK

Cloud computing is not without its risks, the truth remains that these risks are definitely manageable with some effort taken on the part of the company involved. The risks in cloud computing can be overcome with necessary precautions. The service failure can be overcome by redundant data storage using multi cloud. The data loss can be overcome by storing the single copy of data in multiple clouds at one time. The users of the cloud computing can be provided the data integrity by multi-cloud storage .Hence the the major issues of cloud computing are cloud service failure, data loss and data integrity. These all issues can be overcome by using multi cloud storage and file comparison while accessing.

The reliability and security of data stored in the cloud still remain major concerns. DepSky a system that improves the availability, integrity and confidentiality of information stored in the cloud through the encryption, encoding and replication of the data on diverse clouds that form a cloud-of-clouds. They deployed the system using four commercial clouds and used PlanetLab to run clients accessing the service from different countries. They observed that the protocols improved the perceived availability and in most cases, the access latency when compared with cloud providers individually. [1]. Due to the fact that data will be shared with a third party, an un-trusted server is dangerous and unsafe for the user.NetDB2 architecture, known as NetDB2 Multi-Shares (NetDB2-MS). It is based on multi-service providers and a secret sharing algorithm instead of encryption. It shows a significant improvement in performance for data storage and retrieval for various query types [2]. The increasing popularity of cloud storage is leading organizations to consider moving data out of their own data centers and into the cloud. However, success for cloud storage providers can present a significant risk to customers; namely, it becomes very expensive to switch storage providers. In this work, the authors make a case for applying RAID-like techniques used by disks and file systems, but at the cloud storage level. They argue that striping user data across multiple providers can allow customers to avoid vendor lock-in, reduce the cost of switching providers, and better tolerate provider outages or failures. They introduce RACS, a proxy that transparently spreads the storage load over many providers [3]. Cloud computing is a disruptive technology with profound implications not only for Internet services but also for the IT sector as a whole. Still, several outstanding issues exist, particularly related to service-level agreements (SLA), security and privacy, and power efficiency on application and data security over the cloud. This work intends to develop a framework by which the security methodology varies dynamically from one transaction/communication to another. One of the pieces of the framework might be focused on providing data security by storing and accessing data based on meta-data information. This would be more like storing related data in different locations based on the meta-data information which would make information invaluable if a malicious intent user recovers it [4]. The concept of multi-clouds put forward that cloud computing must not stop by means of a particular cloud. By means of a multi-share technique replicating the data into multi-clouds may possibly decrease the threat of data intrusion and augment data integrity [5]. In this work a scalable privacy preserving algorithms for data outsourcing has been described. Instead of encryption, which is computationally expensive, they use distribution on multiple data provider sites and information theoretically proved secret sharing algorithms as the basis for privacy preserving outsourcing. The technical contributions of this work is the establishment and development of a framework for efficient fault-tolerant scalable and theoretically secure privacy preserving data outsourcing that supports a diversity of database operations executed on different types of data, which can even leverage publicly available data sets [6].

III. IMPLEMENTATION

Implementation of efficient control access and data integrity in Multi cloud is a process which consists of two models.i.e Upload and Download.

A. Upload process model

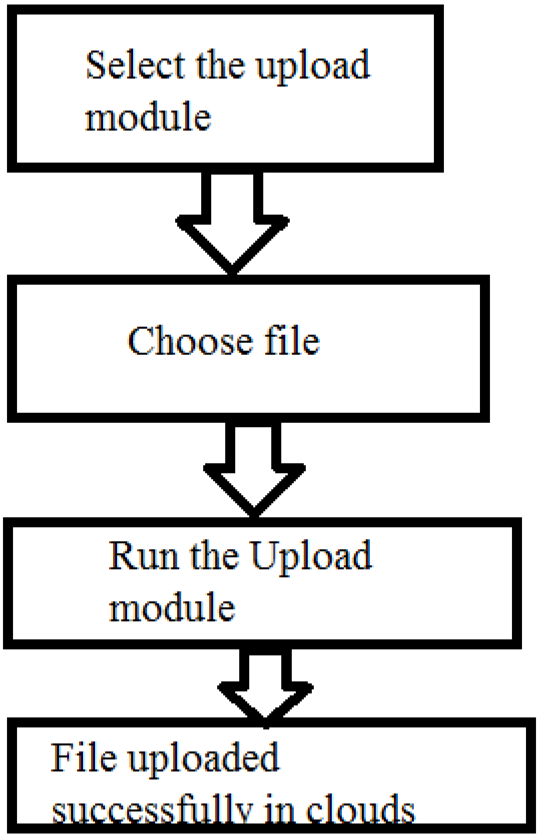

Fig 1 Upload process model

The upload process is structured into a three phases as follows

- Phase-I:The user selects the upload module first to store data into clouds
- Phase-II: Then the user choose file to upload
- Phase-III: In this phase the upload module is executed the data is stored in multi cloud

B. Download process model

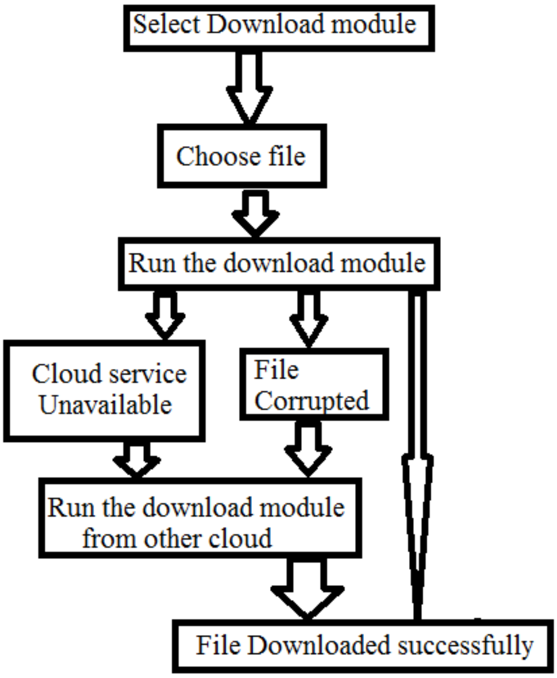
Select Download module
Choose file
Run the download module
Cloud service Unavailable
File Corrupted
Run the download module from other cloud
File Downloaded successfully

Fig 2 Download process model

The Download process is structured into a three phases as follows

- Phase-I: The user selects the download module first to access data from cloud.
- Phase-II: Then the users choose file to download
- Phase-III: In this phase the download module is executed. The file is downloaded successfully. If the cloud is inactive or file is corrupted, then file is downloaded from other cloud by executing download module.

C. Basic architecture

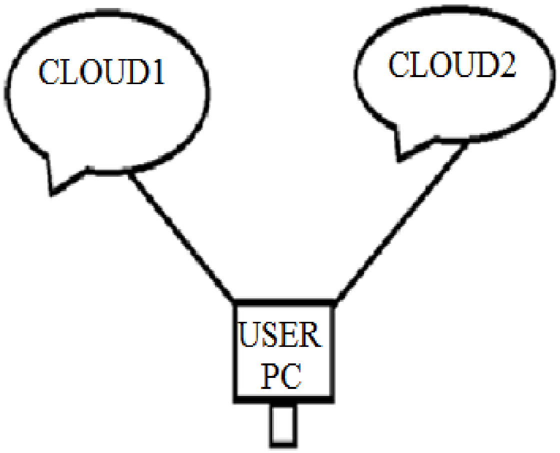

Fig 3 architecture

The above architecture has been followed for the implementation of the work. The architecture contains three parts user pc, cloud1 and cloud2.The major models for the implementation of this work are upload and download module. The user is storing his data in multi cloud when upload module executed, when download module executes user get data from any of the cloud user choose. Hence the above architecture is basic architecture for this project. This work has been implemented by taking two clouds.

D. Efficient Algorithm for file Upload

```
Step 1: Choose a file (text or doc)
Step 2: Generate Checksumbit for a file
        Checksumbit=^*~1672+filename+@7834$%
Step 3: Attach Checksumbit to file
Step 4: Upload file to clouds
```

- **Working**

  This algorithm has been used in the implementation for uploading a file in Multi-Cloud. The file may be a text document or a word document. When user select a file to upload initially a Checksumbit is generated for the file, Then file is attached with Checksumbit and finally uploaded into clouds.

E. Efficient Algorithm for file Download

```
Step 1: Select a cloud sever to download file from it
Step 2: If Cloud server is active go to step 3 else go to step 9
Step 3: Choose a file (text or doc) from cloud
Step 4: Compare Checksumbit of file from cloud with Checksumbit of same file in user database
Step 5: If matches go to step 7
Step 6: If not matches go to step 8
Step 7: Download a file from cloud to user pc
Step 8: Choose a same file from other cloud go to step 4
Step 9: Select another Cloud go to step 1
```

- **Working**

  This algorithm has been used in the implementation for downloading a file from a Cloud. The file from cloud may be text document or a word document. Initially a cloud server is selected to download file from it, if the server is active then it proceeds otherwise select another server .when server is active the user choose file to download from cloud. Then the Checksumbit of file from cloud is compared with Checksumbit of file from user database. if matches the file is downloaded in user pc.if not matches get a same file from other cloud compare Checksumbit and download in user pc.

IV. Conclusion

Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Furthermore, data intrusion leads to many problems for the users of cloud computing.

The purpose of this work is to use multi-cloud service to avoid service availability problem, to avoid data loss due to redundant data storage and to maintain data integrity for users of cloud computing.

REFERENCES

[1] Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6thConf. on Computer systems, 2011, pp. 31-46.

[2] M.A. AlZain and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service", 44th Hawaii Intl. Conf. on System Sciences (HICSS), 2011, pp. 1-9.

[3] H. Abu-Libdeh, L. Princehouse and H. Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240.

[4] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 34(1), 2011, pp 1-11.

[5] C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring data storage security in cloud computing", ARTCOM'10: Proc. Intl. Conf. on Advances in Recent Technologies in Communication and Computing, 2010, pp. 1-9.

[6] D. Agrawal, A. El Abbadi, F. Emekci and A. Metwally, "Database Management as a Service: Challenges and Opportunities", ICDE'09:Proc.25thIntl. Conf. on Data Engineering, 2009, pp. 1709-1716.

First Author
Shivakumar K.Honawad B.E (IS), M.Tech (CSE)*(pursuing)
SecondAuthor
Praveen S.Challagidad assistant professor cse dept,bec bagalkot
B.E (CSE), M.Tech (CSE), Ph.d (pursuing)