E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

A SURVEY ON DATA SECURITY & ACCOUNTABILITY IN CLOUD

Mr. Hrushikesh Joshi[1], Dr. Prof. Suhas Patil[2] and Prof. Mahesh Pavaskar [3]
[1] M.Tech Student, Dept of Computer Engineering, B. V. U. College of Engineering,
Pune, Maharashtra 411043, India
hrushikeshjj@yahoo.com
[2] Head of the Computer Engg Dept, B. V. U. College of Engineering,
Pune, Maharashtra 411043, India
shpatil@bvucoep.edu.in
[3] Asst. Prof, Dept of Computer Engineering, MIT Academy of Engg,
Alandi, Pune, Maharashtra, India
pavaskarmahesh@gmail.com

Abstract
Cloud is one of the emerging environments supporting data storage and access activities. It has changed the traditional way of file systems and database transactions which proved tedious for both the user and the developer. However cloud promised various issues of versatility, flexibility, extensibility, accountability of data etc. With the advantages of the Cloud come the security issues. In this project we have come up with an idea of providing data security and integrity. In cloud computing the user data is stored at large data centers and the storage may not be trustworthy. In this project we are attempting to resolve this conflict by providing security by using various algorithms like SLAs, digital signatures, encryption and decryption methods etc. We are also providing a user friendly interface. The security is also provided at the internal level as the TPA monitors and keeps a track of database admin activities taking place.

Keywords: Third Party Auditor, Cloud Vendor/Cloud Service Provider, Cloud Computing, Data Security and Integrity Verification.

1. INTRODUCTION

Cloud computing is becoming one of the next IT industry buzz words: users move out their data and applications to the remote Cloud and then access them in a simple and pervasive way.[1-4] Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services.[6]

2. BACKGROUND AND MOTIVATION

The rapid growth in field of “cloud computing” also increases severe security concerns. Security has remained a constant issue for Open Systems and internet, when we are talking about security cloud really suffers. Lack of security is the only hurdle in wide adoption of cloud computing. Cloud computing is surrounded by many security issues like securing data, and examining the utilization of cloud by the cloud computing vendors. The wide acceptance www has raised security risks along with the uncountable benefits, so is the case with cloud computing[6-8]. The boom in cloud computing has brought lots of security challenges for the consumers and service providers. How the end users of cloud computing know that their information is not having any availability and security issues? Every one poses, Is their information secure? [1].Through our project we are likely to solve such security issues evolved in cloud computing with high level of efficiency, low cost and can be deployed in a limited time frame.

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

3. PROBLEM STATEMENT

3.1 Existing System

Three different network entities can be identified as follows:

- User: users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.
- Cloud Service Provider (CSP): a CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.
- Third Party Auditor (TPA): an optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request [4].

In cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, cooperated and distributed manner. Data redundancy can be employed with technique of erasure-correcting code to further tolerate faults or server crash as user's data grows in size and importance. Thereafter, for application purposes, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data [2-3]. The most general forms of these operations we are considering are block update, delete, insert and append. As users no longer possess their data locally, it is of critical importance to assure users that their data are being correctly stored and maintained. That is, users should be equipped with security means so that they can make continuous correctness assurance of their stored data even without the existence of local copies. In case those users do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the tasks to an optional trusted TPA of their respective choices. In our model, we assume that the point-to-point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead. Note that we don't address the issue of data privacy in this paper, as in Cloud Computing, data privacy is orthogonal to the problem we study here [5].

3.2 Proposed System

In this system we are likely to provide an OTP system at the user level. The OTP system will generate a verification code which the user needs to enter during registration. Further this code will be verified by the TPA and only after his approval the user registration will be completed. Next comes the uploading and downloading of files. While uploading the original data will be sent to the CSP and a copy of it would be sent to the TPA for verification. After a simple yes/no message from the TPA the original file will be processed further for fragmentation and encryption by the CSP. This will also reduce the overhead considerably. The rights to modify, update or delete will only reside with the owner of the data thereby ensuring an optimal level of security. Internally the DB admin is also monitored by the TPA in order to keep a check on any form of malicious activity. Data lost can also effectively retrieved using standby servers (RAID LEVEL 1).Other specifications in the proposal include digital signatures, captchas, SLAs.

4. MODULES

4.1 Data Security

There are a number of security issues/concerns associated with cloud computing. In cloud computing user's data is saved in large data centres where data management is not trustworthy .In order to ensure good quality of service we are providing OTP technology to ensure the correct user , encryption of data ,fragmentation of data and alert systems .These tasks will be monitored by the TPA and would take necessary action in case of any malicious activity takes place [4-6].

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

4.2 Accountability

User's need to be able to ensure that their data are handled according to the service level agreements made at the time they sign on for services in the cloud. We propose a novel approach, namely Cloud Information Accountability (CIA) framework, based on the notion of information accountability. Information accountability focuses on keeping the data usage transparent and trackable. One of the main innovative features of the CIA framework lies in its ability of maintaining lightweight and powerful accountability that combines aspects of access control, usage control and authentication. By means of the CIA, data owners can track not only whether or not the service-level agreements are being honoured, but also enforce access and usage control rules as needed [2].

5. SYSTEM MODEL

Representative network architecture for cloud data storage is illustrated in Figure 1. Three different network entities can be identified as follows:

- User: users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.
- Cloud Service Provider (CSP): a CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.
- Third Party Auditor (TPA): an optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request. In cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, cooperated and distributed manner. Data redundancy can be employed with technique of erasure-correcting code to further tolerate faults or server crash as user's data grows in size and importance. Thereafter, for application purposes, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data.

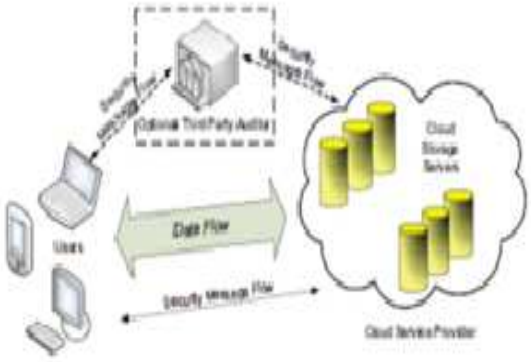

Fig.1 Data Storage Architecture[4]

The most general forms of these operations we are considering are block update, delete, insert and append. As users no longer possess their data locally, it is of critical importance to assure users that their data are being

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

correctly stored and maintained. That is, users should be equipped with security means so that they can make continuous correctness assurance of their stored data even without the existence of local copies. In case those users do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the tasks to an optional trusted TPA of their respective choices. In our model, we assume that the point-to-point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead [4].

5.1 Data Storage and Security

Storing of user data in the cloud despite its advantages has many interesting security concerns which need to be extensively investigated for making it a reliable solution to the problem of avoiding local storage of data. Many problems like data authentication and integrity, outsourcing encrypted data and associated difficult problems dealing with querying over encrypted domain were discussed in research literature. Cloud computing has raised a range of important privacy and security issues. Such issues are due to the fact that, in the cloud, users' data and applications reside—at least for a certain amount of time—on the cloud cluster which is owned and maintained by a third party. Concerns arise since in the cloud it is not always clear to individuals why their personal information is requested or how it will be used or passed on to other parties. To date, little work has been done in this space, in particular with respect to accountability. Pearson et al. have proposed accountability mechanisms to address privacy concerns of end users and then develop a privacy manager. Their basic idea is that the user's private data are sent to the cloud in an encrypted form, and the processing is done on the encrypted data. The output of the processing is deobfuscated by the privacy manager to reveal the correct result. However, the privacy manager provides only limited features in that it does not guarantee protection once the data are being disclosed. The Cloud Information Accountability framework proposed conducts automated logging and distributed auditing of relevant access performed by any entity, carried out at any point of time at any cloud service provider [4-6].

5.2 Data Integrity and Verification

Cloud computing environment is constructed based on open architectures and interfaces; it has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability. We call such a distributed cloud environment as a multi-Cloud (or hybrid cloud). Often, by using virtual infrastructure management (VIM), a multi-cloud allows clients to easily access his/her resources remotely through interfaces such as Web services provided by Amazon EC2. It is crucial to offer an efficient verification on the integrity and availability of stored data for detecting faults and automatic recovery. Moreover, this verification is necessary to provide reliability by automatically maintaining multiple copies of data and automatically redeploying processing logic in the event of failures. To check the availability and integrity of outsourced data in cloud storages, researchers have proposed two basic approaches called Provable Data Possession (PDP) and Proofs of Retrievability (POR) [5].

5.3 Data Framework for Multi-Cloud Storage

Although existing PDP schemes offer a publicly accessible remote interface for checking and managing the tremendous amount of data, the majority of existing
PDP schemes are incapable to satisfy the inherent requirements from multiple clouds in terms of communication and computation costs. To address this problem, we consider a multi-cloud storage service as illustrated in Figure 1. In this architecture, a data storage service involves three different entities: Clients who have a large

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

amount of data to be stored in multiple clouds and have the permissions to access and manipulate stored data; Cloud Service Providers (CSPs) who work together to provide data storage services and have enough storages and computation resources; and Trusted Third Party (TTP) who is trusted to store verification parameters and offer public query services for these parameters [5,6].

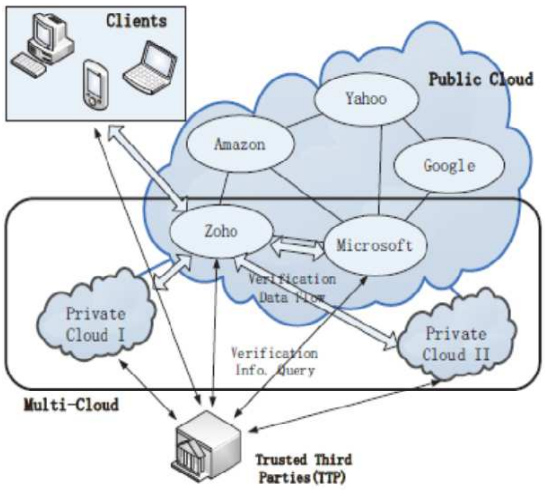

Fig.2 Integrity Verification of Cloud[5]

In this architecture, we consider the existence of multiple CSPs to cooperatively store and maintain the clients' data. Moreover, a cooperative PDP is used to verify the integrity and availability of their stored data in all CSPs [5].

6. ARCHITECHTURE

6.1 User Registration

Initially when the user registers for the first time, the request is first sent to the TPA. The TPA verifies the email id and sends a verification code to the user on his cell phone using the OTP. The user is supposed to enter this code on the screen within a valid time of 2 to 3 minutes. This code is again verified by the TPA and after his approval the user is registered to use the cloud services.

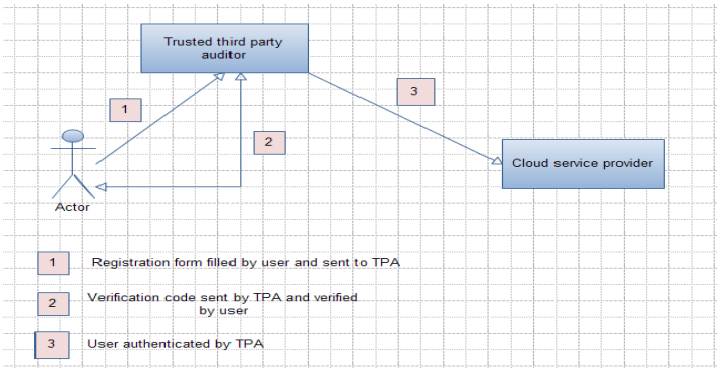

Fig.3 Registration of User

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

6.2 Uploading of File

While uploading, the user data is sent in a queue and the TPA monitors this data and sends a simple yes/no signal towards CSP. This considerably reduces overheads. If the TPA signals yes, the CSP accepts the data. In CSP, the data is encrypted and fragmented to store in its respective data server. For eg, if a data file contains an image and a video clip, the image is stored at a different server and a video clip at a different server. Else the TPA signals no to the CSP sends a message to the user to send the data again.

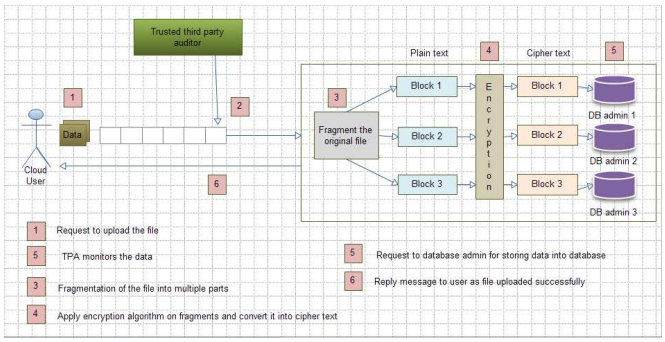

Fig. 4 Uploading in Cloud

6.3 Downloading of File

A download can be performed by any normal user. He just needs to send a download request to the CSP and the required data is decrypted and is downloaded in the original format. The rights to modify, update and delete resides only with the owner. Any normal user cannot modify the data.

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

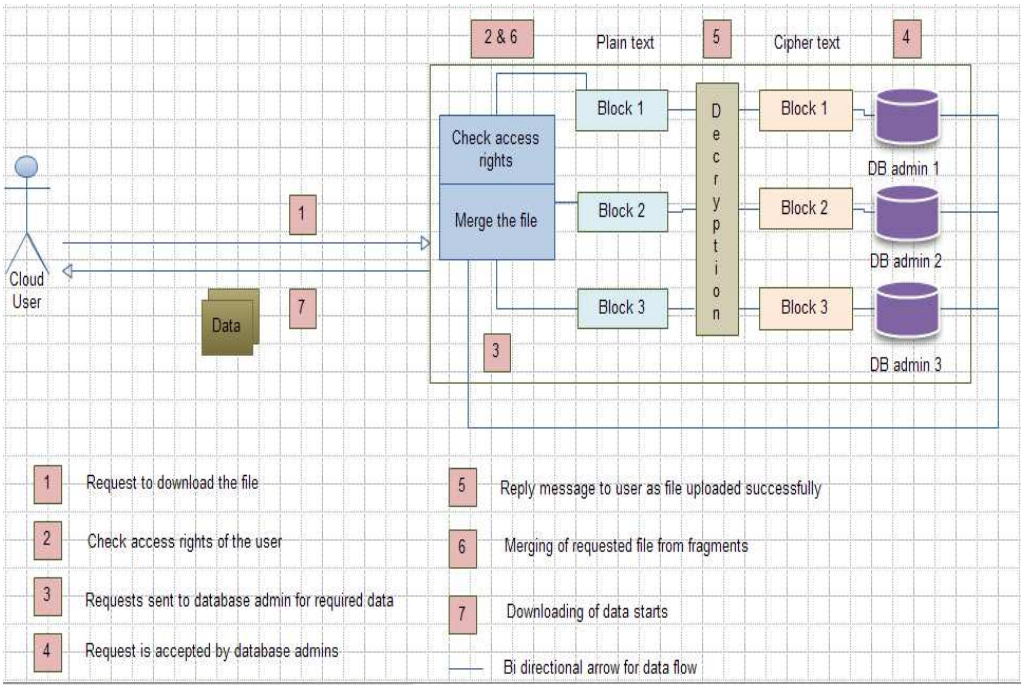

Fig. 5 Downloading from Cloud

6.4 Alert generation

TPA monitors the data internally too. He keeps a check on the internal activities taking place. If suppose database admin is trying to modify the data, the TPA generates an alert.

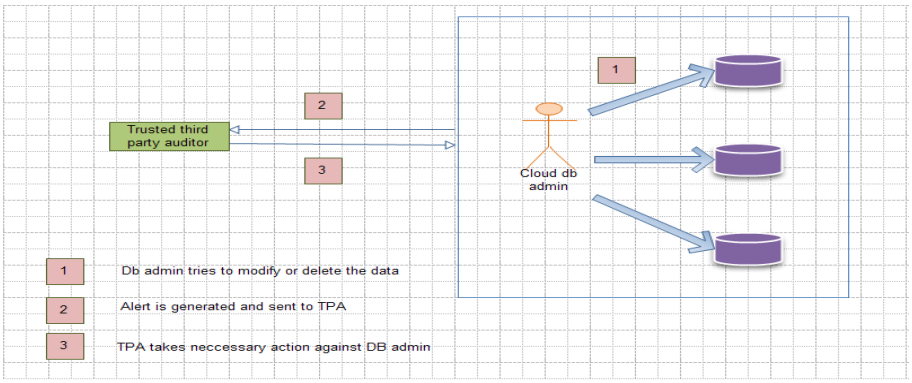

Fig. 6 Alert Message Generation

7. CONCLUSION

Cloud computing is a new technology widely studied in recent years. Now there are many cloud platforms both in industry and in academic circle. How to understand and use these is a big issue. In this paper we described various security issues related to cloud and gave our proposed system based on the existing system .Thus

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

cloud computing provides a low cost super computing services to users. Our system proposal ensures security and integrity with effective utilization of available resources.

Acknowledgment

I am thankful to my guide Prof. Dr. Suhas Patil & Co-guide Prof. Mrs. S. S. Dhotre for their guidance and encouragement for the proposed project and paper work.

References

[1] Mladen A. Vouch, —"Cloud Computing Issues, Research and Implementations", Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246

[2] Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud ", IEEE transactions on dependable and secure computing, vol. 9, no. 4, july/august 2012.

[3] D.J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigen-baum, J. Hendler, and G.J. Sussman, "Information Accountability," Comm. ACM, vol. 51, no. 6, pp. 82-87, 2008.

[4] Cong Wang, Qian Wang, and Kui Ren ,'' Ensuring Data Storage Security in Cloud Computing.''.

[5] Yan Zhu, Hongxin Hu, Gail-Joon Ahn,"Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage." ,IEEE Transactions On Parallel And Distributed Systems, Digital Object Indentifier 10.1109/TPDS.2012.66.

[6] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Senior Member, IEEE, Mengyang Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage ",IEEE transactions on parallel and distributed systems

[7] Dawn Song, Elaine Shi, and Ian Fischer, University of California, Berkeley Umesh Shankar, Google, "Cloud Data Protection for the Masses ",IEEE Computer Society,Jan 12

[8] Salvatore J. Stolfo, Malek Ben Salem, Angelos D. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud", Defense Advanced Research Projects Agency (DARPA)