Object based Accountability Framework for Information Sharing in Cloud Computing

Pradeep Singh
M.Tech Student
Lovely Professional University
Phagwara, Punjab, India

Parminder Singh
Assistant Professor
Lovely Professional Univeristy
Phagwara, Punjab, India

Avinash Kaur
Assistant Professor
Lovely Professional University
Phagwara, Punjab, India

ABSTRACT
Cloud computing is one of the biggest thing in computing in recent time. Cloud computing uses the internet and the central remote servers to support different data and applications. Cloud computing is that emerging technology which is used for providing various computing and storage services over the Internet. In the cloud computing, the internet is viewed as a cloud. Internet users can receive services from a cloud as if they were employing a super computer which be using cloud computing. Accountability is one of the major reforms that are provided in cloud environment. Because of this we can restrict the use of the user information by the third party. The user is pre informed when his or her information is shared with some third party or any organization. The accountability provides the uses the Object oriented approach for holding all that information. The information is shared with the concerned user prior to the misuse of that information To Whom It May Concern. The study also focuses on web application framework to enhance the security of cloud computing.

Keywords
Cloud computing, log manager, Learning agent, attacks, SLA, Electronic Data Sharing Agreements (e-DSA), Object Base accountability (OBA).

1. INTRODUCTION
Cloud computing is an emerging new technology that is use in the information technology field. It uses the internet and central remote servers to support the various data and applications. Hence, cloud computing is an internet based technology. The cloud computing flexibility is a function of the allocation of resources on user request. Cloud computing provides the act of uniting. [9] In the cloud computing, the internet is viewed as a cloud. By the use of cloud computing, the capital and operational costs can be cut.

1.1 Architecture of Cloud Computing:
Cloud computing system is divides into two sections:

- **Front end**
- **Back end**

They connect to each other through the internet. The front end is the side the computer user. In the front end side, all the applications are presents that are required to access cloud computing system. The back end is the cloud section of the system. In the back end system, various computers, servers and data storage systems are presents that create the cloud of computing services. [10] [11] [12]. In the cloud computing, each application has its own server. The central server helps in administers the system, monitoring traffic and client demands

1.2 Virtualization:
In the cloud computing, clouds are divided into three parts, as, Public Clouds, Private Clouds and the Hybrid Clouds. Virtualization is very useful concept in context of cloud systems. Virtualization means something that is not real. Virtualization is a software implementation of computer. It helps to execute different programs like a real machine. Virtualization is related to cloud computing, because it can be used by end users. The end users can use various services of the cloud. Virtualization can be classified in two different parts:

- Full virtualization
- Partial virtualization

1.3 Full Virtualization
In case of full virtualization, the complete installation of one machine is done on another machine. [13]It will result in a virtual machine which will have all the software that are presents in the actual server. The full virtualization is used for many purposes.

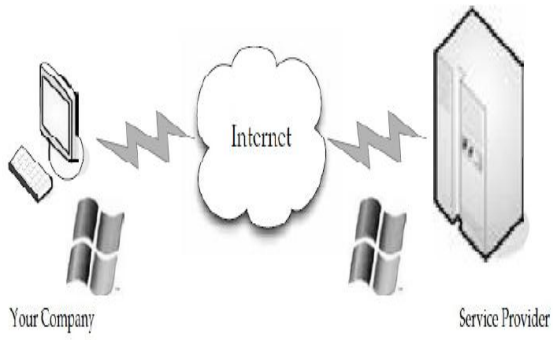

Fig 1: Full virtualization

- Sharing a computer system among different users
- It helps to Isolates users from each other and from the control program
- Emulating hardware on another machine

1.4 Partial virtualization
In partial virtualization, the hardware allows multiple operating systems to run on single machine by efficient use of system resources such as memory and processor. [14] In this case, the services are not fully available. These services are provided partially. [13]

It has the following advantages:

- **Disaster recovery:** It helps in the disaster recovery.

- **Migration:** in the virtualization, hardware can be replaced easily, hence migration of different parts of a new machine is faster.
- **Capacity management:** In a virtualized environment, it is easier and faster to add more hard drive capacity and processing power.

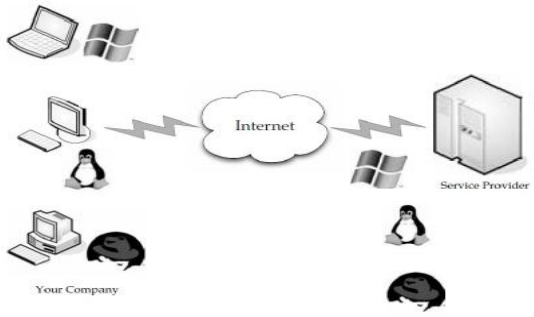

Fig 2: Partial virtualization

2. RELATED WORK

[4]The center for discussion is the reliable cloud environment. The organizations can reduce the cost by offloading of data and using the cloud computing services. But, to reduce the confidentiality violations, the cloud has provided the option of encryption. It is an effective and very secure way of storing data to the service provider. The companies are benefited because they reduce their incurring cost by using the cloud services or we can say by outsourcing computation-on-demand. (Santos 2009) In this paper, the author has proposed a design of a platform called TCCP. TCCP will allow IaaS service providers like Amazon to give a closed box environment to its user which will ensure a confidential execution of guest virtual machine.

[3]The center of discussion of this paper circles around security concerns related to the data storage in the cloud environment. The cloud system is an internet based development process and with the availability of high network bandwidth and reliable and flexible network connections is making it even more possible for user to user the cloud services. Also, the cloud environment provides an effective and more productive way of development and deployment. Cloud computing just doesn't act as a data warehouse as the data is frequently updated by the user time to time. Cloud computing allows to move the large applications and databases to be moved to large datacenters, where the management of the data may not be trustworthy. That data can be seen or used by some other individual or organization which is not a trustworthy option for a user or an Organization. This paper discuss about an effective and flexible distributed system for the correctness of user data in the cloud environment. (C. e. Wang 2010)

[5]It describes the various schemes that are used in the security of cloud computing. Cloud computing allows the user to buy the services they needed instead of owning that services prior to its use. This helps to reduce the incurring cost of that service, software that the user needs to use. It helps in increasing the accountability. (Ko 2011) The security in the cloud computing is a big issue. For this purpose, data transparency, the access in the cloud environment and the lack-ness of data ownership clarity were surfaced. Here, the outcome of this paper is to propose a new scheme, which helps in providing security to cloud computing. This scheme finds out the various previous security and privacy concerns. Here the data centric approach is use and which helps in increasing privacy and security of data in the cloud environment. (Ko 2011)

[6]Cloud environment or cloud computing is one most rapidly emerging concept which is providing different computing and storage and other services. It is next generation architecture of IT solutions. In the cloud computing, the internet is viewed as a cloud. Cloud computing provides the various IT services. It may help in gaining efficiency and effectiveness in the development and the deployment and may save the extra incurring cost. But, on the other hand, it contains many security challenges. The security concerns with the data storage are the major concern in the cloud environment. This discussion proposes a new scheme called third party auditor. It helps in providing the trustful authentication to user. (Han 2011)

[7]The main focus of this discussion is on data security in cloud computing. In the cloud environment, the data and the applications are available on the web servers. The cloud computing systems divide the applications in two scenarios: The front-end and the back-end. All the cloud systems doesn't have the same interface i.e. all the cloud systems run with their own operating system. The cloud uses protocols and uses different software's also called middleware. The cloud system keeps the information of all of its users and keeps it on devices. This information is required to enable the server to retrieve data. Cloud computing allows to share distributed resources and software's which helps user to use resources at convenient cost by using the facility of pay-per-use i.e. they pay only for the services they use from the cloud..(Jose 2011)

The internet is used by the cloud computing as the communication medium. This discussion has proposed a model in which the cloud computing system is integrated with cluster load balancing. (Jose 2011)

[2]The main issue of discussion of this paper is data security and privacy protection. Nowadays many organizations are understanding the benefits of using their data and applications in the cloud environment and implementing the measures for data security and privacy protection in the cloud environment. The use of cloud computing may help in gaining efficiency and effectiveness in the development and the deployment and may save the extra incurring cost. The major concern that is associated with the cloud computing are the security and the privacy concerns of the user. The users are not happy with the idea of handing over their data to other individual or to some organization. It concerns the privacy of and security of user's data. Also, in corporate area, the people are afraid that some key information might not get leaked in this process. Because the data or information is shared on the cloud environment, lack of proper security measures may lead to leak of key information to unwanted personnel or organization. This paper is about providing a precise and all round analysis of security and privacy issues of cloud environment. (Chen 2012)

[8]This discussion is about the private cloud that is used for the disaster recovery. The outcome of this discussion proposes to build a framework for disaster recovery. The discussion proposes to build a prototype system that is based on IaaS architecture. The prototype system is constructed by several private cloud computing fabrics. In such scenario, distributed storage system is used to build a private cloud fabric. The distributed storage system is used to handle the large file systems. The distributed storage system will be able to keep running as one large file system when some private cloud

fabric does not work by any troubles. Here, it further show inter cloud cooperation framework. (Satoshi Togawa 2013)

[1]It is a world where words like e-commerce and online transaction and cloud sharing are very much used. The main objective of all these is to automate the activity of manual transaction through the online way of sharing data or say online transaction. (Casassa-Mont 2014)But the problem with these approaches is that the user is always having a doubt that what is going to the information that is shared by him/her. The data can be misused or can be used for fraud transaction etc. So these problems are affecting the assurance of the online transaction or data sharing concepts. The discussion is about the possible reason why the users don't take the sharing data in cloud environment a good approach. In the manual transaction, User do have a contractual agreement referring to certain rules and constraints that will be obeyed by both the parties between which the transaction is going on. Similarly, the online transaction also provide the same thing with the help of E-DSA (Electronic Data Sharing Agreement)

The E-DSA is a human-readable and machine-process able contract regulating how organizations or any individuals share data with one-another or among themselves. The E-DSA automates the two main purposes/processes i.e. verification and validation and generate policies which are enforced through a manageable and consistent lifecycle. These policies can be deployed into and used by software infrastructure controlling the flow of data among organization or individuals that are involved in the agreement. The violations of these policies can also be tracked back to the policies statements that are mentioned in the E-DSA. (Casassa-Mont 2014)

3. EXISTING WORK ON INFORMATION ACCOUNTABILITY

Cloud computing is used as for the purpose of computation, as a platform and as a services also. It is an environment where the user does not need his/her own infrastructure and they can use the cloud services on pay per use basis. But security is one of the major concerns in cloud environment and while using web applications on cloud computing it play a very important role because it helps to keep our secret information confidential. In the Existing system, the user can share information over the cloud using the Electronic Data Sharing Agreements (e-DSA). [1] In this, many rules and policies are defined between the user and the local service provider. This agreement is a way to give the user an option to have the accountability of his data or information over the cloud.

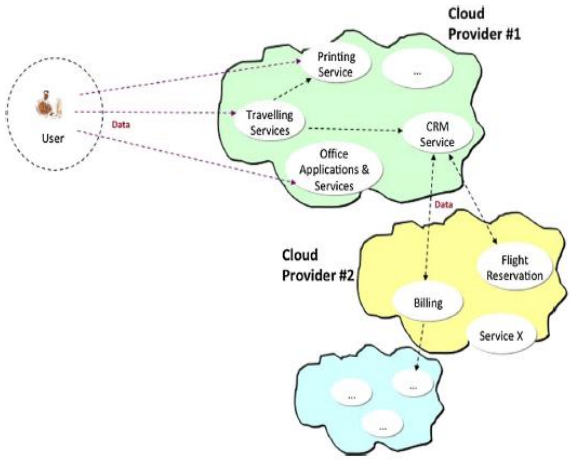

Figure 3: Data sharing with web application [1]

If the user accepts the rules and the policies of the agreement, he is liable to get the accountability information of the data or information that is shared by him over the cloud. This was how the existing system provides the accountability to the user. [1]

In the previous system, the e-DSA was divided into following:

1. End User
2. e-DSA Management
3. e-DSA Authoring
4. e-DSA Analyzer
5. e-DSA Deployment
6. e-DSA Enforcement
7. Service

This all mentioned integrally used in the e-DSA to provide a singular way of providing this service. Along with that, many roles were also defined. Suppose, once the agreement is done between the user and the local service provider, after that if a data is available over the server for more than year, it will be deleted after that. [1]

The thing is that if once the agreement is finalized between the user and the local service provider, it is the responsibility of the local service provider to retain the security and the privacy of the user data. If the service provider shares the user data with another service provider, he needs to inform the user about that. So that the user gets to know that his information is shared with some other service provider that can use his information.

These are some points that were taken into consideration while developing this new framework because it provides better option over this existing system.

3.1 Major Drawback of Existing System

There were major drawbacks in the previous or the existing system which is why the new framework model with an object oriented approach is used. The object oriented approach provides a more granular control over the data accountability as compared to the existing or the previous system available. The major drawbacks were that, in the previous technologies, the user is unaware of what is happening to the information shared by that user and who, why and when that data is accessed. This created a dilemma in the minds of the user regarding the security aspects with the data in the cloud environment. The user has no awareness of his data being used by some other individual or an organization without the proper permission or authentication and there was no accountability of that provided to the user. [1] The other drawback is that the previous technologies were prone to many security attacks like Man-In-Middle. The main reason for that, earlier the agreement was done between the user and the local service provider. So, if the user gets relocated for some reason, he needs to make another service agreement with new local service provider which is a big concern. But, with the object oriented approach in the new framework mode, we can overcome the need of such local service providers because we can use service brokers which a better and reliable option as compared to local service providers

4. PROPOSED FRAMEWORK

Security of web application in cloud computing is a very challenging task. If we talk about the security of web application like online payment application the security is

highly required because here we have to exchange our import information like act. Number etc. which is very confidential. To protect our confidential information we need to provide security on both channels, means from web application to bank verification and from we application to payment receiver.

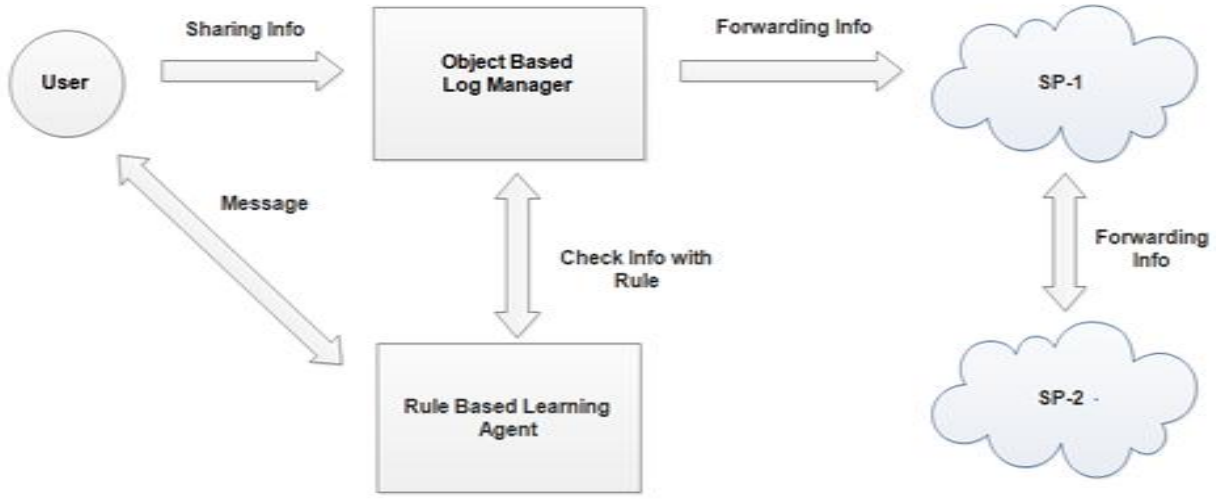

Fig 4: Object Based Accountability Framework

In my proposed methodology I am using an object based log manager which is integrated with a Rule Based Learning Agent.

4.1 Object-based Log Manager

Object-based log manager store the log of shared file in XML format. Whenever the new instance of file is shared with any service provider or service provider share the information with another service provider, the log will be stored by log manager. Object based technique is used for taking accountability of shared information.

4.2 Rule-based learning Agent

The Rule Based Learning Agent is used to define some rule for the object based log manger. The three types of rule defined are as follows:

- Public
- Protected
- Private

Three type of access will be provided to the shared information. Learning Agent store the information with SLA (service level agreement). If any service provider violate the rule of information sharing, immediate result will sent to user with all the information that When, why, how the information has been shared by your service provider.

5. MEASURABLE OUTCOMES

Within the timeframe of the project, Object Based Accountability (OBA) Framework will have:

- The main objective of this was to develop middleware services for the users which uses cloud environment. Cloud uses protocols and uses different software's also called middleware. The cloud system keeps the information of all of its users and keeps it on devices.
- The other thing is to publish standard guidelines which provide an overall aspect of the accountability factor to the business group that are going to indulge in the cloud environment.
- The third thing is that once the middleware is developed, it needs to be tested whether it actually provides the accountability to the user of his/her information/data, which is shared around in the cloud environment.
- The fourth thing is to provide the user with the information of how the data or information shared by the user is going around in the cloud environment and who can or who is actually accessing that data and if he allowed to or not. This all is managed through the accountability of the data over the cloud environment. And to see if user can get hold of information of how his/her data is used over cloud.
- To provide the above mentioned measures to provide user a more secure and private way of his data handling over cloud, we uses Deffi-helman algorithm which a provides a way to privately communicate a user's data over cloud.
- To provide training for developers, cloud service providers and users, and business legal and regulatory communities on how they can implement accountability. They are provided with proper guidelines and tools to implement that.

6. CONCLUSION

Cloud environment or cloud computing is one most rapidly emerging concept which is providing different computing and storage and other services. In the cloud computing, the internet is viewed as a cloud. The users can use the services provided by the cloud environment as per their requirement on pay per use basis. The cloud provides the service of storing data on the cloud instead of our own devices which makes it ubiquitous. The main purpose of this paper is to provide accountability to any user who is using the cloud services using a more modular and granular way using object oriented

approach. Using the object oriented approach, a new framework is developed which provides the accountability to the user. By using this framework, the user gets to know that who can or who had accessed his private information and when. This provides user with a reliable option to the user to track the activities happening over his private data. The user can get to know why and where his information was accessed along with other specific information's. So, if any other individual or any other organization tries to misuse that data, the user will get to know what data has been used or altered or if any other modification is done over his data. But, these services will only be available if the user uses the middleware provided by us. If the user do so, all the policies that were defined were for the data protection divides the data into two part. Object Manager, Role Base learning agent. The information is kept on the middleware framework divided among these two parts. With the help of this, we can keep the record of each and every data of the user and so we can provide full accountability to the user of his data usage over the cloud environment. This paper concludes this whole scenario of this new middleware framework and its working aspects with regards to accountability factor. With the advent of these solution into the cloud environment, the cloud environment has mitigated the major concern issues which were there in the cloud environment. The cloud environment has grown its effectiveness over internet because of a large number of services and platforms that are made available to the user. Hence, the cloud environment has become a favored solution to the user or organizations

7. REFERENCES

[1] M. e. a. Casassa-Mont, "Towards safer information sharing in the cloud," International Journal of Information Security, pp. 1-16, 2014.

[2] D. a. H. Z. Chen, "Data security and privacy protection issues in cloud computing," Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, 2012.

[3] C. e. a. Wang, "Privacy-preserving public auditing for data storage security in cloud computing," INFOCOM, 2010 Proceedings IEEE, 2010.

[4] N. K. P. G. a. R. R. Santos, "Towards trusted cloud computing," Proceedings of the 2009 conference on hot topics in cloud computing, 2009.

[5] R. K. e. a. Ko, "Trust Cloud: A framework for accountability and trust in cloud computing," Services (SERVICES), 2011 IEEE World Congress on. IEEE, 2011.

[6] S. a. J. c. X. Han, "Ensuring data storage security through a novel third party auditor scheme in cloud computing," Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on, 2011.

[7] G. J. A. C. S. a. D. C. S. Jose, "Implementation of Data Security in Cloud Computing," International Journal of P2P Network Trends and Technology, pp. 1-3, 2011.

[8] K. K. Satoshi Togawa, "Private Cloud Coorperation Framework of e-Learning Envirment for Disaster Recovery," in IEEE International Conference on System, Man and Cybernetics, 2013.

[9] "Cloud Computing principles," System and Applications NICK Antonopoulos, 2015.

[10] D. P. A. R. I. S. a. M. Z. Lee, " Above the clouds: A Berkeley view of cloud computing.," in EECS Dept., Univ. California, Berkeley, No. UCB/EECS-2009-28, California,, 2009.

[11] S. S. a. G. M. V. B. Michael Vrable, "A Cloud-Backed File System for the Enterprise, Google.," in IEEE, New York, 2006.

[12] "File System," pp. 1-8, 15 3 2015.

[13] "Cloud computing basics," p. 1, 11 3 2015.

[14] "CLOUD COMPUTING BASICS FOR BEGINNERS AND NON-EXPERTS," pp. 1-10, 8 3 2015.