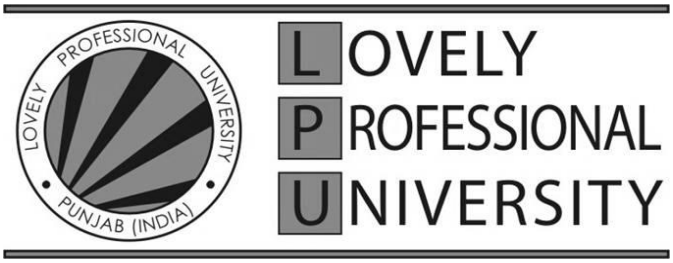

OBJECT BASED ACCOUNTABILITY FRAMEWORK FOR INFORMATION SHARING IN CLOUD COMPUTING

A Dissertation Proposal
Submitted By

Pradeep Singh

(11012016)

To

Department of Computer Science & Engineering

In partial fulfilment of the Requirement for the
Award of Degree of

Master of Technology in Information Technology
Under the guidance of

Mr. PARMINDER SINGH
Assistant Professor, LPU

(April 2015)

PAC FORM

LOVELY PROFESSIONAL UNIVERSITY
Transforming Education Transforming India

School of: LFTS

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Pradeep Singh
Registration No: 11012016
Batch: 2010-15
Roll No. K2308B17
Session: 2014-15
Parent Section: K2308
Details of Supervisor:
Designation: Asst. Prof.
Name: Parminder Singh
Qualification: MTech CSE
U.ID: 16479
Research Experience: 8 yrs

SPECIALIZATION AREA: Network and Security (pick from list of provided specialization areas by DAA)

PROPOSED TOPICS

1. Authentication Model for PaaS Security
2. Novel Middleware for cloud computing security in Web Applications
3. Security in PaaS

Signature of Supervisor

PAC Remarks:

Topic No '2' may be pursued.

APPROVAL OF PAC CHAIRPERSON: Signature: Date: 19/9/14

*Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)
*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.
*One copy to be submitted to Supervisor.

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 rising technology that is employed for providing numerous computing and storage services over the web. Within the cloud computing, the web 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. Now a days, nobody have a full trust over cloud means nobody wants to use the cloud services because of security issues. Also the user always have a doubt that the service provided is fake or illegitimate. To remove this problem on the cloud, the accountability along with the security is provided in the cloud. The accountability means that the user will get the information about his data usage. If any if his private data is used by someone else on the cloud or if the service provider send his data to another service provider, the user will be informed. The user will also know why his data is used. To do that a new framework is developed that works in the form of an object. It is developed on the middleware. As like the service broker splits the requests into small jobs and send the service to the cloud service provider. All this history of information transactions is saved into a log file which is used to get the accountability. Using this framework, the existing problem of accountability can be removed. Also with comparing object based accountability framework with the previous framework, Object based accountability framework give a better in terms of accountability as compared to previous framework. And it can be used to build the user trust on the cloud

CERTIFICATE

This is to certify that **Pradeep Singh** has completed M.Tech dissertation proposal titled **"OBJECT BASED ACCOUNTABILITY FRAMEWORK FOR INFORMATION SHARING IN CLOUD COMPUTING"** under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

The dissertation proposal is fit for the submission and the partial fulfilment of the conditions for the award of M.Tech Computer Science &Engineering.

Date: _____ Signature of Advisor

ACKNOWLEDGMENT

I would like to express my sincere gratitude to my advisor **Mr. Parminder Singh** for the continuous support of my thesis study, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my M.Tech study.

Pradeep Singh

DECLARATION

I hereby declare that the dissertation proposal entitled, **"OBJECT BASED ACCOUNTABILITY FRAMEWORK FOR INFORMATION SHARING IN CLOUD COMPUTING"** submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: _____

Investigator

Reg. No. 11012016

TABLE OF CONTENTS

ABSTRACT ..... **ii**
CERTIFICATE ..... **iii**
ACKNOWLEDGMENT ..... **iv**
TABLE OF CONTENTS ..... **vi**
LIST OF TABLE ..... **viii**
LIST OF FIGURES ..... **ix**
CHAPTER 1 INTRODUCTION **1**
1.1 Cloud computing 1
1.2 Service model of cloud computing 3
1.3 Deployment model of cloud computing 4
1.4 Virtualization in cloud computing 5
1.5 Major Concerns of Cloud Computing 6
1.5.1 Benefits of cloud computing 6
1.6 The Accountable Cloud 7
1.7 Components of Secure Cloud 10
1.8 Challenges of Cloud computing 10
1.9 Cloud Computing Using the Communications Services 11
1.10 Accessing through Web APIs 11
1.11 Cloud Computing Trends for 2014 12
1.13 Advantages of cloud computing 16
1.14 Disadvantages of Cloud Computing 17
CHAPTER 2 REVIEW OF LITERATURE **19**
CHAPTER 3 PRESENT WORK **29**
3.1 Problem Formulation 29
3.1.1 Major Drawback of Existing System 31
3.2 Objectives of the study 32
3.3 Proposed Methodology 33
3.3.1 The Cloud Accountability Life Cycle 33
3.3.2 The Object Based Accountability Framework 34
CHAPTER 4 RESULTS AND DISCUSSIONS **38**
CHAPTER 5 CONCLUSION AND FUTURE SCOPE **43**

REFERENCES.....**44**
APPENDIX.....**47**

LIST OF TABLE

Table 1: Literature Survey Table 19

LIST OF FIGURES

Figure 1: Cloud computing in the form of internet 1
Figure 2: cloud computing components 2
Figure 3: Service Models of Cloud Computing 4
Figure 4: Cloud computing scenario 7
Figure 5: Web 2.0 Interfaces to the Cloud 12
Figure 6: cloud computing threats 15
Figure 7: Abstraction Layers of Accountability in Cloud Computing 22
Figure 8: Main e-DSA lifecycle phases 27
Figure 9: JAR Based Accountability Framework 24
Figure 10: Encrypted Logging Based Framework 25
Figure 11: Data sharing with web application 30
Figure 12: The Cloud Accountability Life Cycle (CALC) 34
Figure 13: The Object Based Accountability Framework 36
Figure 14: Mat lab running on Windows 38
Figure 15: User Logging and Accept the security policy 39
Figure 16: Data Process in Log file 40
Figure 17: Reply Message to user 41
Figure 18: Performance of OBAF 42

CHAPTER 1

INTRODUCTION

1.1 Cloud computing

Cloud is one of the most new and one of the emerging technology in the internet world. Cloud computing provides the user with different types of services on the basis of pay as you basis which helps in mitigating the cost and effort of buying and installation of different software or platforms that are needed for different applications and storage needs [1]. Now, with the advent of new technologies, the computing devices are becoming smaller and smaller while the capability or the storage capacity of these computing devices are increasing day by day.

In such environment, the cloud computing provides different services such as PaaS (Platform as a service), IaaS (Infrastructure as a service), SaaS (Software as a service) [2]. In all the services cases, the user made the use of the cloud service for their applications or data storage or as per the requirements of individual or an organization. So, the network have gotten more faster than previously and cloud computing and other server based application are executed on specific systems.

Anyone can store data over the cloud and it makes the data ubiquitous. Also you can run your application on the cloud environment which might contain some powerful tool which is useful with your software [1]. Also, it mitigates the user requirement of installation of the required software's for running their application.

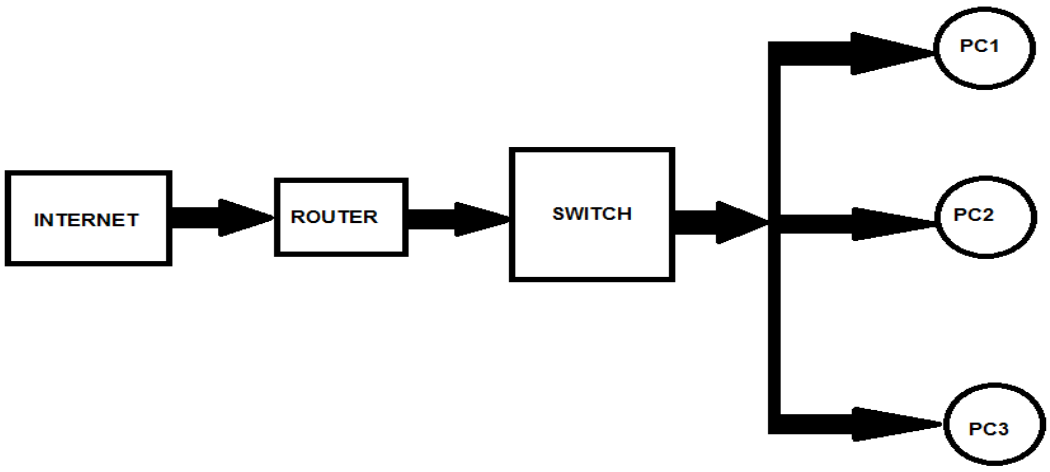

Figure 1: Cloud computing in the form of internet

The cloud computing is very much flexible and this is due to the resources which are allocated on the request of authority [3]. The cloud computing is a new and robust emerging technology that can provide different computing and other storage services to the user over the internet.

The cloud computing usually integrates three things: infrastructure, platform, and software as services [4]. The users can use the services provided by the class as per needed and have to pay only for the services they acquire from the cloud environment. As if they were servicing through a super computer that is using cloud computing.

Anyone can store data over the cloud and it makes the data ubiquitous. Also you can run your application on the cloud environment which might contain some powerful tool which is useful with your software [3]. Also, it mitigates the user requirement of installation of the required software's for running their application. They can use the cloud environment to use the right software for their application running and remove the burden of extra installation.

Cloud computing consists of three main components. These components are:

- Clients
- Datacenter
- Distributed servers.

Each component in cloud computing plays a particular role

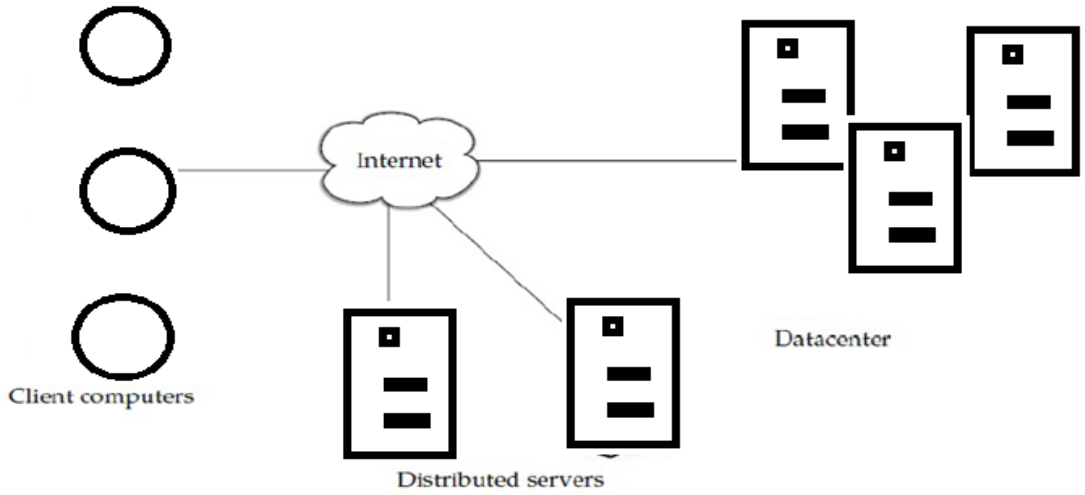

Figure 2: cloud computing components

- **Clients**

In the cloud computing, the knowledge is managed by users. They {are doing} interaction with the shoppers to manage the knowledge that are required for the cloud surroundings [4]. The shopper's area unit divided into 3 totally different categories:

➢ **Mobile Client:** he clients can be mobile in nature. It includes windows Smartphone's or like, blackberry and iPhone.

➢ **Thin:** These clients don't do computational work. They specifically used to display information. These clients don't have the internal memory; the servers do all the work for the clients.

➢ **Thick:** These shoppers use completely different browsers to attach the net cloud. These browsers embrace web soul, Mozilla Firefox or chrome to attach to the cloud setting.

- **Datacenter**

Datacenter is nothing but a collection of servers; these servers host the various applications. A user connects to the datacenter application to use different applications. The datacenter may exists at large distances [3]. Now, the virtualization concept is used to install an s/w that allows us to create multiple instances of server application.

- **Distributed Servers**

Distributed servers are servers that are present throughout the different distant location throughout the internet in a cloud computing environment [3]. These sever hosts the various applications.

1.2 Service model of cloud computing

Once a cloud is developed, it is disagree from its needs [3]. There's varied models use in cloud computing.

These models are:

Software as a Service (SaaS)

In this, the users acquire the ability to use any application or the services that are there in the cloud environment.

Platform as a Service (PaaS)

In this, the user has acquired or purchased the access which allows them to deploy their software or any application in the cloud environment [4]. There are some explicit constraints like operating system and network access which is in the hands of the user and it might limit the applications that can be deployed.

Infrastructure as a Service (IaaS)

In this, the user has no inheritable or purchased the access to regulate and manage the OS, network access, or storage. The physical infrastructure of the cloud setting is employed to produce computing, storage, and networking as a service mitigating the expense and wish for a special dedicated system.

Figure 3: Service Models of Cloud Computing

1.3 Deployment model of cloud computing

Deployment of the cloud computing is depends au fait the various needs, therefore it's disagree from one another [3]. As for deploying a cloud laptop, four preparation models is used. Every model has its specific characteristics.

- **Private Cloud**

The private cloud is used for the personal work, as the private cloud can be operated and maintenance is done by some organization. The operations can be by yourself or some third party.

- **Community Cloud**:

In this, the cloud is shared by different organizations which share the same requirements. This can help them in reducing the total expense that they might have to pay for the establishment because now the same cost is shared by various organizations that will be using that cloud.

- **Public Cloud**

In this, the cloud environment infrastructure is made available to everyone on a commercial basis by the service provider. This enables the user to develop and deploy a service with the in cur of a very little cost.

- **Hybrid Cloud**:

In this, the cloud environment infrastructure consists of different clouds of dissimilar types and they allow the applications or data to be moved from one cloud to another because they have ability to allow through interface. They can be a mixture of private and public cloud.

1.4 Virtualization in cloud computing

The clouds are of 3 types: Public Clouds, non-public Clouds and therefore the Hybrid Cloud. Virtualization means that one thing that's notional or not real [4]. Virtualization may be a software system implementation of pc. It helps to hold the execution of varied programs love it is occurring on a true machine. It relates with cloud's computing as a result of virtualization is employed by finish users and therefore the finish users use the various services of a cloud [3]. The various classes of virtualization are listed below:

- Full Virtualization
- Partial Virtualization

1.5 Major Concerns of Cloud Computing

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. Also, in corporate area, the people are afraid that some key information might not get leaked in this process [2].

Privacy concern is also one of the major concerns. Because a user can log on to the cloud environment from any location and can access the data, so it is possible that the user may be compromised [3]. There are some alternatives to these problems like authentication. Providing username and passwords and also by limiting the access to the user on the specification of their job requirements.

1.5.1 Benefits of cloud computing

There are many benefits of the cloud computing, these benefits are based upon the services and applications of the cloud computing.

- **Scalability:** The cloud computers are scalable in nature. The companies can start with a small deployment and grow to a large deployment according to the needs of the companies. The companies can scale back to its initial state if necessary.
- **Flexibility:** The flexibility of cloud computing allows the companies to use the various resources, whenever the customer demands the additional features. To satisfy a customer the flexibility of the resources is needed.
- C**ost Savings:** cloud computing helps the organization to reduce their capital expenditures.
- **Reliability:** cloud computing is more reliable because the services used in this having multiple redundant sites. These sites support the business continuity.
- **Maintenance:** The cloud system provides the maintenance. It does not requires the application installation on the PC, the access of the system done through APIs directly.
- **Mobile Accessible:** These systems are accessible in any infrastructure. Hence cloud system help to increase the productivity of the system.

1.6 The Accountable Cloud

Cloud computing requires the companies and individuals to provide some or all of control to all the resources to service provides in the cloud i.e. Cloud Service providers (CSPs) [5]. Such process naturally poses a threat to the companies or the individual and concerns the companies' decision makers.

In 2010, there was a survey conducted by Fujistu Research Institute on cloud environment. During the survey, some major outcomes came into light. Firstly, they found that 88% of data access in the cloud environment has no accountability. So there is no way to tell who is accessing that data [5]. The second thing that came into light is that most of the data in the cloud is stored in which physical server; there is no knowledge of that. So lack of accountability in the cloud and what its importance was a major outcome of this survey.

But all the security risks can be prevented by using some preventive control measures. These measures are responsible for privacy and security [6]. Also it should provide transparency, governance and the accountability of the cloud service provider.

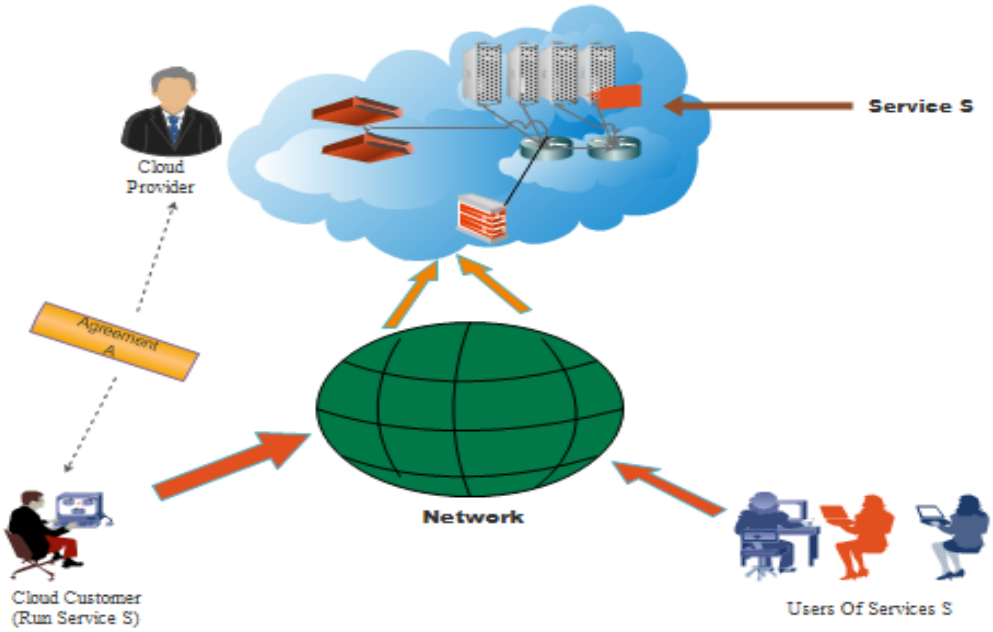

Figure 4: Cloud computing scenario

However, from the shopper purpose of read, the utilization of cloud surroundings is somewhat risky as a result of he must relinquish some or all management of his computing resources to the cloud service supplier [6]. within the typical model, wherever the computation runs on a server on the customer's location, the client has access to the machines, he will directly observe their standing, and he will himself or have that managed by individuals he trusts. But, within the new model, the computation method works on virtual machine within the cloud, and therefore the client don't have any management or observation power over that [7]. The physical server area unit managed by the service suppliers and therefore the client gets controls of virtual machines solely which may be managed remotely from anyplace. The loss of management just in case of one thing gone wrong is problematic [6]. Let's say this time, yield through little choice of potential problems:

- The machines used in the cloud environment can be misconfigured or may be defective. This will consequently corrupt the user's data or cause the computation to return incorrect results.
- The cloud service provider may sometime accidentally allocate insufficient resources to the user which will affect the performance of the user's services and cause the user's to miss the SLAs.
- The attackers can use a bug in the user's software to gain access to some valuable data, or to take the control of user's machines for spam purposes or DoS attacks. [6]
- The customer might lose control of data because the data on the cloud might be unavailable at an inconvenient time or because the cloud loses it.

Some of the on top of mentioned issues, such of not correct allocation of resources, area unit cloud-specific and this may not happen on an infatuated platform, whereas issues like, information loss or broken hardware, area unit vulnerable and long used systems whose severity simply enhanced by victimization it in cloud [6]. For instance, systems will be defective or become defective once use of someday whether or not it's utilized by client, or a cloud, however if it's an infatuated platform, then the user will perform regular upgrades and may mitigate the danger by hiring system directors [8]. If the user is victimization the cloud, then he must trust the service supplier to perform all this things diligently.

Since, within the cloud, the management responsibilities area unit divided among each the client and therefore the service supplier, neither of them is in a very sensible position to

handle of those problems diligently [6]. Even the detection of drawback are significantly difficult: with the supplier, the matter is that, the supplier doesn't grasp what to seem for or what the computation is meant to do; and on the opposite hand, the purchasers have access to the cloud solely remotely, therefore the data out there is extremely restricted [8]. Moreover, once a tangle is found, the confusion is formed whether or not it's the service supplier or the client United Nations agency is accountable for it- and it's quite natural for the service supplier to suspect as there's one thing wrong with the customer's software package and vice-versa [6]. And in such cases, if this confusion isn't resolved amicably, then it's not possible for them to 3rd party (like Associate in Nursing intermediary or a judge) that the opposite is accountable [7].In general, they can say that a system is accountable if

a) Faults can be easily detected

b) Each detected fault can be linked to the responsible faulty node.

Apart from that, they consider systems as accountable that have these following features:

• **Identities**: Every Action performed by the machine should be linked to the machine that performed it.

• **Secure record**: The system should have record of what action which machine has performed so that machines cannot falsify, or tamper with its entries;

• **Auditing**: The records should be monitored and inspected for faults.

• **Evidence**: Whenever a fault is detected, the information to identify and resolve that fault by a third party acts as evidence [6]. That evidence of the fault that can be verified independently by a third party.

Accountability may be a promising approach to the higher than mentioned issues within the cloud surroundings. Associate in nursing responsible cloud system may offer its customers to watch WHO has access to his information and the way. And conjointly that data user has no physical access to the client information and cloud is playacting as in agreement [7]. If a tangle happens, the client and also the supplier will use the data to make a decision what the reason behind that's and WHO is accountable, and will gift the proof to 3rd party just in case of dispute [8]. However existing answerableness techniques disappoint of the wants for cloud computing in many ways that. Since the clouds are used

largely normally now-a-days by the client, the supplier ought to supply answerableness for negative service that the client requests [6]. This may rule out the requirement of specific application specific techniques like CATS or Repeat and Compare. These techniques are deployed to examine for correctness of execution and that they cannot be wont to monitor alternative properties of interest in cloud, like SLA agreement, information protection, service convenience, and information sturdiness then on.

1.7 Components of Secure Cloud

To best mitigate barriers to confidence, they'd like to know the most elements moving secure cloud [5]:

Security completely different Mechanisms will be deployed (e.g. encryption) which might give security measures that create it extraordinarily tough for associate degree unauthorized or intruded person to access any reasonably data [5]. This builds a trust among the client that his knowledge is prevented with sensible security procedures.

Privacy as mentioned above, different protective measures to prevent potential privacy threats in the cloud could be mitigated. The protection of privacy is one the major concerns of customers [5]**.** The privacy of data means restrictions of illegal use of customer's data by any unwanted person or entity.

Accountability The irresponsibleness is outlined as "the obligation and/ or temperament to demonstrate and take responsibility for performance in lightweight of agreed-upon expectations" [5]. However the irresponsibleness doesn't limit to it solely [9]. It holds accountable any organization or person in control of their actions [10]. Irresponsibleness' has been established in steerage by organizations like OECD, APEC, and PIPDA as inserting a burden [9]. The organizations uses in person peaceable info (PII) to confirm that shrunk partners to whom it provides the PII area unit compliant to privacy pointers, where within the world they'll be.

Auditability The auditing of any system keeps the records of what has to be upgraded or what's the system records state [11]. Poor auditability means the system has poorly-maintained (or non-existent) records and systems that alter economical auditing of processes among the cloud [5]. It is check if the action taken is compliant against the policy outlined or not [11]. And if not, it will hold the person or organization that area unit liable for that action.

1.8 Challenges of Cloud computing

There are many challenges that are associated with cloud computing.

- **Security and Privacy:**

In the cloud computing data storage and data security is important aspects. The cloud [3] computing can be monitor by the service providers.

- **Lack of Standards:**

In the cloud computing, clouds have documented interfaces. Hence there are no standards associated with the cloud computing. To resolve these issues open cloud computing interface is comes into picture, it helps to resolve many issues [18].

- **Continuously Evolving:**

The requirements of the user are continuously evolving, hence requirements for interfaces, networking and storage is increased and decreased according to the need of person. This means that a cloud behave dynamically.

- **Compliance Concerns:**

Cloud computing has many issues regarding its data protection. Its main concern is about the affecting factors of cloud computing. These factors based on the type of data and application for which the cloud is being used.

1.9 Cloud Computing Using the Communications Services

In a cloud the communications services will extend their capabilities. It conjointly helps to provides new interactive capabilities to current services. These services modify businesses to implant communications capabilities into business applications. The services of the cloud computing are often accessed from any location and coupled into current services to increase their capabilities, also as standalone as service offerings.

1.10 Accessing through Web APIs

Accessing communications capabilities in an exceedingly cloud-based atmosphere is achieved through genus Apes. It permits the applying development outside the cloud to require advantage of the communication infrastructure inside it. An API defines functionalities that area unit freelance of their individual implementations, that permits definitions and implementations to vary while not compromising one another. A decent API makes it easier to develop a program by providing all the building blocks. A coder then puts the blocks along.

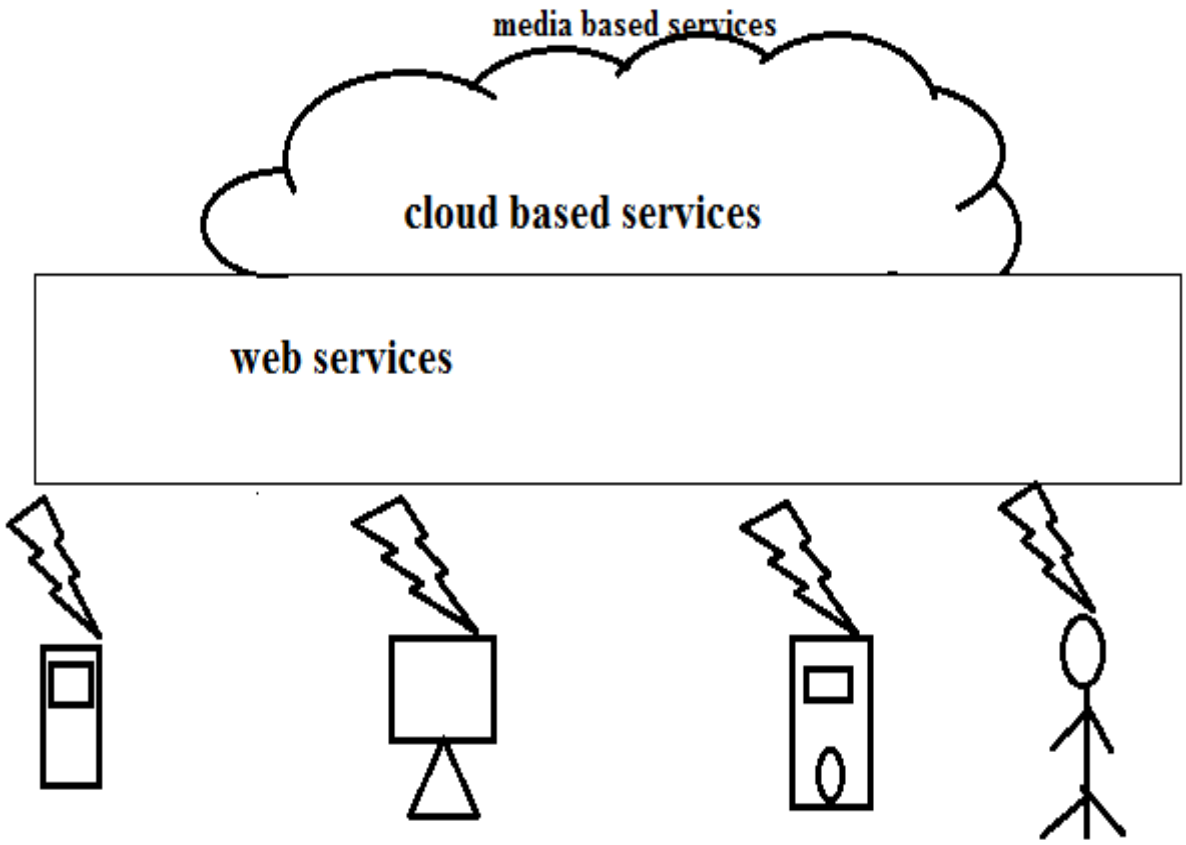

Figure 5: Web 2.0 Interfaces to the Cloud

1.11 Cloud Computing Trends for 2014

Cloud enables agility and business innovation

Now days, every business is a digital business. The world is changing, due to the increasing need of IT. Cloud computing supports the rapid experiments and innovation, hence is recognized as facilitating speed to market. The cloud solutions are used to help business to understand the customer unique challenges. [18]

Security, Addressing security & privacy is key to building trust in cloud computing

The cloud performance is depends upon its security. Everyone, who want to do work in cloud, he or she must check the security of cloud. There are many security issues in cloud computing, as:

Physical Security and Data Location

- Network Security
- Backup & Recovery

- Operational Compliance
- Confidentiality & Integrity
- Data Portability
- Location of Data

System of Engagement - Common User Experience across delivery models, cloud as a wrapper

Cloud solutions are highly agile wrapper around different systems, different behavior. They help in bringing all together in an engagement cycle. Cloud computing helps in changing way of interaction between the peoples and technology. It may lead in enabling new forms of consumer applications.

Cloud as the innovation platform – Mobile, Social, and Big Data

Mobile is the mega trend of our century. It has become a commodity. Social has permeated through our personal and business networks. Big Data, the volume of data available for organizations to mine for business value is staggering. Cloud technology provides a standard platform for Mobile, Social and massive knowledge applications to cross fecundate likewise as enhance and extend existing investments.

Social: Collaboration in a business context

The Collaboration between generations of staff got to be transactional in addition as give business context for a winning information transfer. The collaboration is embedded into the business method. Progressively business processes can have several cloud bit points, creating a case for cloud based mostly collaboration.

Big Data – Actionable data

Big Data has become the catch, all phrase for the volume of data businesses generate today. Without appropriate action, the collection and analysis of the data is worthless. Cloud technology makes the collection, analysis and dissemination of results and actions that much easier due to its flexibility.

Real time and Predictive

Now a day, the real time is no longer enough, the real time also needs to be predictive. It is not about the advance analytics.
A cloud platform and solutions will provide the base for such innovation and agility.

Networks - The business network effect

The Complex effect lone highs in if you are exposed and you measure fast. It is simple, more users make a network more attractive and intensify the benefit for all.

Platform

You need to have a PaaS to succeed with cloud solutions. A critical factor will be the ability of this platform to drive innovation as well as provide integration to your existing landscape.

Hybrid cloud

You cannot move everything to the cloud. You may not even want to.

1.12 Cloud Security threats

Cloud computing has many security threats. The files in the cloud computing is share by many users. Hence the confidentiality becomes the major issue in this case [20]. There are many security threats in cloud computing, as:

Data Breaches

The data breach biggest issue in case of cloud security. At the target the data breaches result in the loss of personal and credit card information of many users. If the database of cloud computing is not properly designed then there may be chances of attacker to attack the data. This may harmful to our whole system.

Data Loss

In a cloud computing, knowledge loss is occur. The info is lost in several conditions, such as: once a hard drive dies while not its owner having created a backup. The info loss might occur deliberately within the event of a malicious attack.

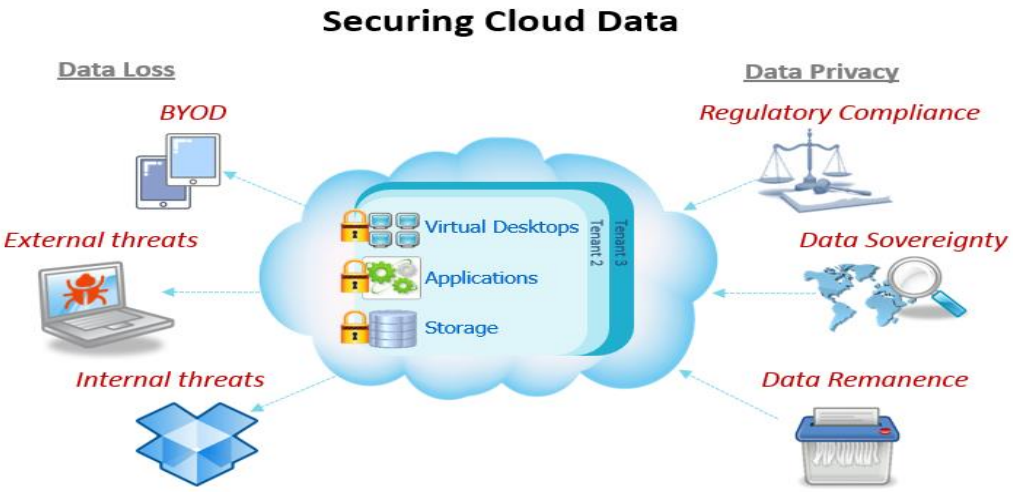

Figure 6: cloud computing threats *[20]*

- **Service Traffic Hijacking**

The service hijacking is the biggest issue in cloud computing. Phishing, exploitation of software vulnerabilities and credentials can all lead to the loss of control over a user account.

- **Insecure APIs**

The application programming interface, (API), defines however a 3rd party connects Associate in Nursing application to the service and providing verification that the third party manufacturing the applying.

- **Denial Of Service**

Denial of service attack is a previous disrupter of on-line operations, however they continue to be a threat. The assault by many thousands of machine-controlled requests for service should be detected and screened out before it ties up operations, however attackers have temporary progressively subtle and distributed ways that of conducting the assault, creating it more durable to discover that components of the incoming traffic square measure the dangerous actors versus legitimate users.

- **Malicious Insiders**

Inside an oversized cloud organization, the hazards square measure enlarged. One maneuvers cloud customers ought to use to safeguard themselves is to stay their cryptography keys on their own premises, not within the cloud.

- **Abuse Of Cloud Services**

Cloud computing brings massive scale, elastic services to enterprise users and hackers alike. It would take assailant years to crack a secret writing key victimization his own restricted hardware.

- **Insufficient Due Diligence**

There are a unit several enterprises jump into the cloud while not understanding the complete scope of the endeavor. While not Associate in nursing understanding of the service providers' atmosphere and protections, customers do not know what to expect within the manner of incident response, secret writing use, and security observance. Enterprises might push applications that have internal on-premises network security controls into the cloud, wherever those network security controls do not work.

- **Shared Technology**

In a multi-tenant setting, the compromise of one element exposes quite simply the compromised client. The cloud is regarding shared infrastructure, and a miss-configured OS. During a shared infrastructure, the CSA advocate Associate in nursing in-depth defensive strategy. Defenses ought to apply to the utilization of cipher, storage, networking, applications, and user access.

1.13 Advantages of cloud computing

- **Scalability**

Cloud computing is scalable. Whenever user would like additional resources, the user will add it to anytime. That's Cloud computing is infinite pool of resources [23].

- **Environment friendly**

Cloud computing makes economical use of hardware that helps to scale back energy price.

- **Cost efficient**

Cloud Cloud computing is price economical. They've got to pay that abundant quantity that it tend to used similar to electricity bill.

- **Up to date**

They need not to stress concerning the updates to the software's and hardware's that we tend to square measure mistreatment within the cloud. The supplier is accountable for the update method of all the elements [2].

- **Improved performance**

Whenever we need not to stress concerning the updates to the software's and hardware's that we tend to square measure mistreatment within the cloud. The supplier is accountable for the update method of all the elements [2].

- **Availability**

The cloud service is distributed over multiple servers. The cloud systems will transfer the hosted applications close to instantly between this infrastructures. Therefore even though a server fails, the supply are nearly uninjured.

- **Coping with large load variations**

There are a unit multiple servers and datacenters of the cloud computing. If the applications of the cloud computing become extremely popular, the cloud infrastructure will not fall to its knees.

- **Timely and consistent updates**

The cloud infrastructure is must be absolutely according to one another. There are running many shoppers applications, a failure owing to a patch isn't one thing the cloud service can settle for. Therefore all servers are going to be terribly quickly and systematically updated

- **Extremely fast scaling out**

If your application includes a sustained high visit rate, it wants additional servers to run on. This is often terribly simple to implement during a multi-server, multi-site atmosphere of a cloud service.

1.14 Disadvantages of Cloud Computing

- **Custom platform**

The cloud service provider designs the cloud service setting with its specifics, like underlying OS, databases, [1] application server and development platform. These unit of measurement mounted across the total cloud platform.

- **Lock in**

Once the entire application is accommodates run on the cloud service atmosphere, it should be tough to maneuver it to a different cloud service supplier. Here the user has got to readjust everything to run on the new cloud service.

- **Isolation breach**

A breach between the isolation controls of various customers will cause access to proprietary information.

- **Data protection**

In the cloud computing, knowledge is incredibly vital. Generally knowledge is incredibly confidential in nature. Since all this knowledge is managed by the service supplier, incidents of information loss, knowledge leaks and security breaches will all happen.

- **Cost**

The cloud service suppliers have lots of innovative evaluation mechanisms, like evaluation per I/O, Bandwidth, or any combination of these. Thus whereas potency and convenience will certainly increase, thus could the prices is additionally inflated [24].

CHAPTER 2
REVIEW OF LITERATURE

Table 1: Literature Survey Table

S. No	Author Name	Title	Year
1	Santos, Nuno, et al.	Towards trusted cloud computing	2009
2	Haeberlen, Andreas	A case for the accountable cloud	2010
3	Chen, Shiping, and Chen Wang.	Accountability as a Service for the Cloud: From Concept to Implementation with BPEL	2010
4	Shuai Han, et.al,	Ensuring data storage security through a novel third party auditor scheme in cloud computing	2011
5	Jen-Sheng Wang, et.al,	How to manage information security in cloud computing"	2011
6	G. Jai Arul Jose1, C. Sajeev2, Dr. C. Suyambulingom	Ensuring data storage security through a novel third party auditor scheme in cloud computing	2011
7	Ko, Ryan KL, et al	Trust Cloud: A Framework for Accountability and Trust in Cloud Computing	2011
8	Prashant Srivastava et.al,	An architecture based on proactive model for security in cloud computing	2011
9	Parsi Kalpana, Sudha Singaraju	Data security in cloud computing using RSA algorithm	2012
10	Epuru Madhavarao, M Parimala, Chikkala JayaRaju	Data sharing in the cloud using Distributing accountability	2013
11	Pankaj Kumar Singh, Ajit Kumar, R.Karthikeyan	Ensuring Distributed Accountability for Data Sharing in the Cloud	2013
12	Casassa-Mont, Marco	Towards safer information sharing	2014

		in the cloud	
13	Sinjilawi, Yousef K., Mohammad Q. AL-Nabhan, et al	Addressing Security and Privacy Issues in Cloud Computing	2014
14	Akram, Raja Naeem, and Ryan KL Ko.	Digital Trust-Trusted Computing and Beyond: A Position Paper	2014

Santos, Nuno, et al. (2009) "Towards trusted cloud computing" The main focus center of discussion is the reliable cloud environment [12]. The organization uses the cloud to reduce the cost of offloading the data and for the cloud services. The cloud has provided the encryption services to reduce the confidentiality violations. It is an effective and very secure way of storing data to the service provider [12]. The companies reduce their incurring costs using the cloud services. The cloud services provide outsourcing computation-on-demand. In this paper, a new proposed design platform approached is discussed called TCCP [13]. The TCCP allows IaaS service providers to give a closed box environment to its customers which will ensure confidentiality of the customer [12].

Haeberlen, Andreas (2010) "A case for the accountable cloud" Haeberlen et al. were one in all the researchers that highlighted the requirement of Associate in nursing responsible cloud system [6]. It assumptions was to a have a primitive Audit, alongside the thought of agreement, service and timestamps. However this AUDIT doesn't have the clear clarification of scope, scale, phases and layers of abstraction of irresponsibleness [5]. They additionally projected the thought of responsible virtual machines.

Chen, Shiping, and Chen Wang. (2010) "Accountability as a Service for the Cloud: From Concept to Implementation with BPEL" HyTrust, a new recent start up, is mainly focuses on cloud accountability and auditing [14]. It released a tool named HyTrust Appliance consolidated hypervisor log report and policy enforcement for accountability management of virtual machines in clouds [5]. This tool tracks the accountability of system layer in cloud. Despite that, the most address of this tool was on virtual layers. Also, it monitors work for responsibility from system perspective and not file-centric perspective [15]. Chen and Wang of CISRO had presently a team watching "accountability as a service" for the cloud. They conferred a model that enforces responsibility suppliers whose services square measure deployed within the cloud [15].

This model works by creating the service suppliers answerable for any faults within the services and the way to permit identification of the reason for faults.

Shuai Han, et.al, [(2011) Ensuring data storage security through a novel third party auditor scheme in cloud computing, Cloud environment is one of the rapidly growing concept which is providing computing, storage and other services. The cloud is the IT next generation architecture [16]. The internet is considered as cloud in a cloud environment which provides various services. It save the extra incurring cost by providing a platform for the development and deployment of user software or application. But, also it has some security concerns like privacy of data in the cloud environment. These are some major concerns of the user's. This discussion proposes a brand new theme known as third party auditor. It helps in providing the unsuspecting authentication to user.

Jen-Sheng Wang, et.al, (2011) "How to manage information security in cloud computing" The main focus of this discussion is data security in the cloud environment. As in the cloud environment, all the data storage is done at web servers [17]. The cloud computing divides the application into two scenarios: Back-end and Front-end. But every system in the cloud may not have the same interface because every system has its own operating system. The cloud uses middleware which is a combination of protocols and different software's. The cloud stores all of its user's information on some physical storage devices on some location. That information is required to for giving access to the user to the data. Cloud computing allows to share distributed resources and software's which gives user access to resources at pay-per-use basis. The internet is used as a communication medium by the cloud computing. This paper proposes a model which integrates cloud computing with cluster load balancing.

G. Jai Arul Jose1, C. Sajeev2, Dr. C. Suyambulingom, (2011) "Ensuring data storage security through a novel third party auditor scheme in cloud computing" The main issue disussed in this paper is data secuirty and privacy concerns. Many organizations are now using cloud environment for their sevices and application and implementing the measusres for data secuirty and privacy protection in the cloud environment [18]. The cloud computing helps in gaining efficiency and it provides

platform for development and deployment which saves the extra incurring cost of the organization. But the user's are not happy with the secuirty and privacy issues which are addressed in the cloud computing. Also, in the corportae world, the key reason of afraid of user's is the privacy of the information. The information might get leaked from the cloud environment due to the lack of proper secuirty measures. The information might be accessed by some unwnated person or organization for their benefit. This paper provides precise and all round analyis of privacy and security issues of cloud environment.

Ko, Ryan KL, et al (2011) "Trust Cloud: A Framework for Accountability and Trust in Cloud Computing". In the "Trust in Cloud Computing" the data is divided into two parts: Private and Sensitive. In this data, the logging and log files provide the accountability. In this paper, a accountability life cycle is discussed which takes some components as inputs like Policy, Sense and Trace, Logging, safe keeping of logs, Reporting and replaying, auditing, optimizing and rectifying. Using these components, they can get accountability and auditing to the client side [5]. But here the accountability provided will only for the stored data and not for real time data. So here the, the customer is provided a cloud with accountability and trust.

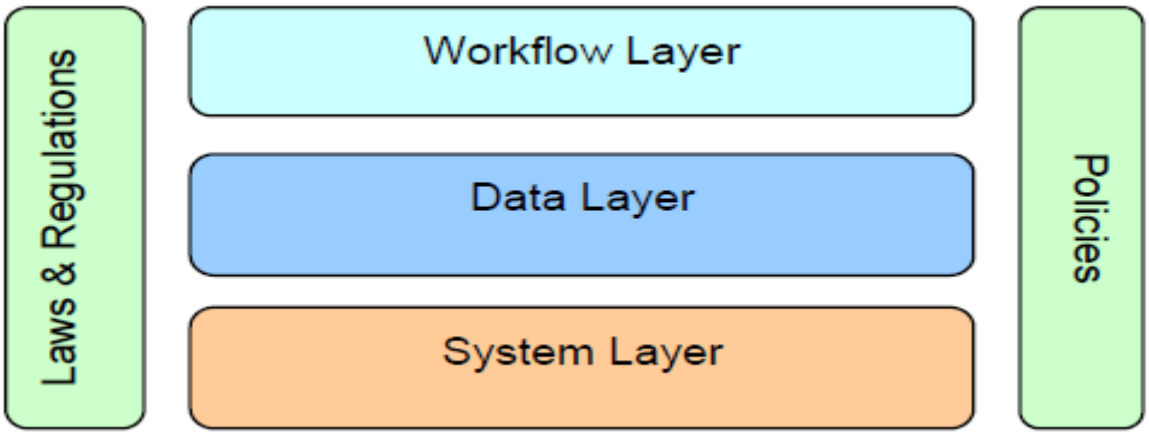

Figure 7: Abstraction Layers of Accountability in Cloud Computing *[19]*

Also, the cloud remains secured of the unauthorized users. If any action on the data is performed by some unauthorized user, the service provider will be informed that someone is intruding without proper authentication in the cloud. But using this existing framework, they can make the cloud a trusted cloud environment but user will not get the accountability because as this framework works at five different layer i.e. workflow layer, data layer, system layer, policy layer and law layer. This all layers work on the local

system layer and not on the networking OSI layer. Keeping in mind, all these drawbacks, I created a new framework which will provide accountability to the service providers as well as the users in the cloud [19]. In this framework, the data is divided into three types, private, protected and public which is totally based on the user requirements. In this existing framework the main layer basically depends on the local system which is not required in any cloud environment to run this framework because it is using the stored data and not real time generated data that is required to request from the internet or the cloud environment.

Prashant Srivastava et.al, (2011]) "An architecture based on proactive model for security in cloud computing" in this paper, author discuss a proactive model for the protection of cloud computing. Cloud computing is outlined as a model for facultative convenient, on demand network access to a shared pool of configurable [10] computing resources that may be apace provisioned and free with marginal management effort or service supplier interaction. The cloud technology may be a growing trend. Cloud Computing paradigm has one evident problem: security, as a result of the cloud may be a new paradigm, it involves careful coming up with and execution. During this paper, they have a tendency to analyze the protection landscape intimately and propose design supported a proactive model that tackles this progressively tough drawback in an exceedingly comprehensive manner. A Security Cloud actively monitors the Cloud Service supplier for policy violations.

Parsi Kalpana, Sudha Singaraju (2012) "Data security in cloud computing using RSA algorithm" This discussion revolves around the private cloud that is used for the disaster recovery. It proposes a framework for disaster recovery [20]. This framework is based on the IaaS architecture. The construction of this prototype is carried by several cloud computing fabrics. A distributed storage system is used in building the private cloud fabric. The distributed storage system is used to store the large file systems. This distributed storage allows to keep running a file system when some private cloud fabric does not working because of some problem.

Epuru Madhavarao, M Parimala, Chikkala JayaRaju (2013) "Data sharing in the cloud using Distributing accountability" Many peoples are doing research on Cloud computing. Similarly, Mr. Epuru Madhavarao, in his paper has talked about the accountability in the cloud [21]. In this paper, he talked about an accountability framework which treat user in the cloud as an object and user is provided and this approach is named as Object cantered approach.

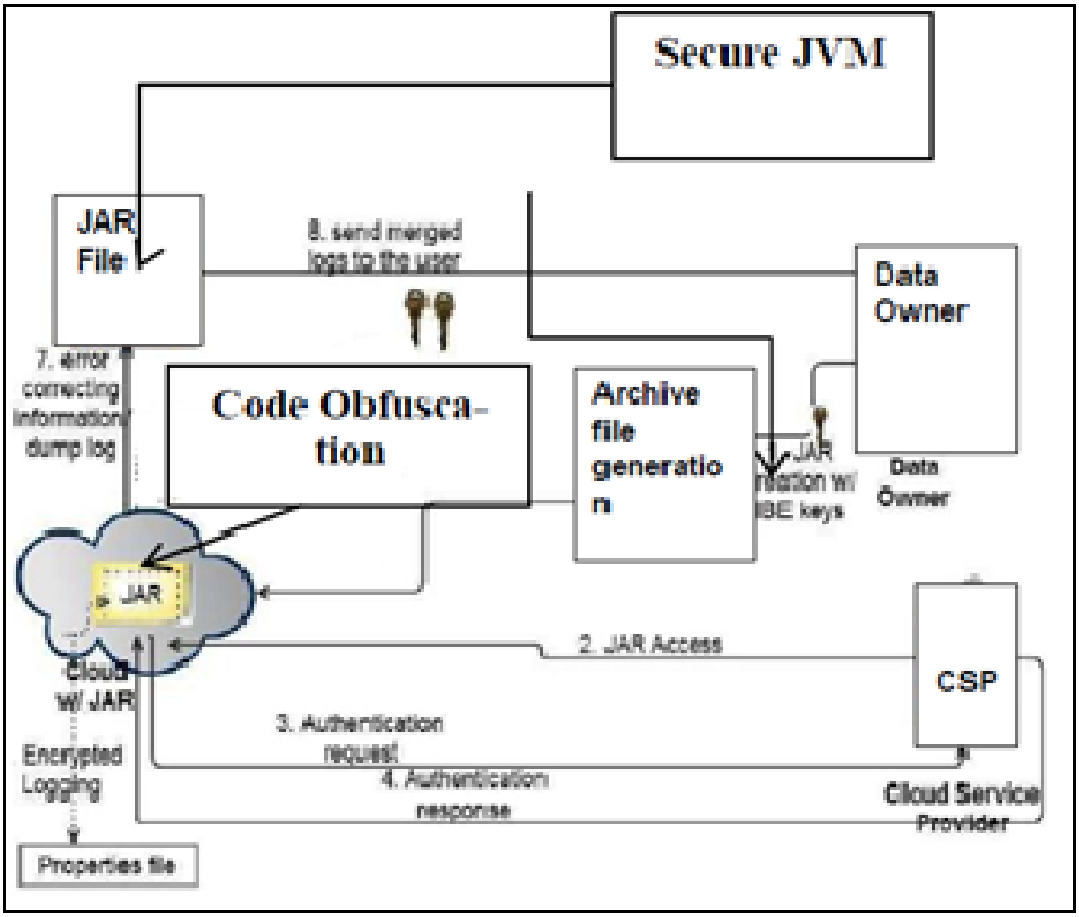

Figure 8: JAR Based Accountability Framework *[21]*

In this mechanism, the user is provided with automatic logging mechanism and policy mechanism. In both this mechanism, user is provided with the accountability checks and the transparent use of data by the user, and if the user broke any policy mechanism or not. This all is checked simultaneously if user found violating these policies, then the user is blocked from the cloud. And the automatic logging mechanism discussed in this paper

uses a JAR programming which improves privacy and security. By using this, if any user is added to the cloud, then he has to go through the distributed auditing mechanism. In this way, they can provide a better security and privacy to the user in the cloud. And to improve the accountability in the cloud, a JAR file is created in which the user logging information is saved [21]. To achieve this approach, an algorithm is used named as Lo Retrieval for push and pull mode which works on user logging user session which reduces a lot number of attacks, for e.g., Man-In-The-Middle attacks and so on.

Pankaj Kumar Singh, Ajit Kumar, R.Karthikeyan (2013) "Ensuring Distributed Accountability for Data Sharing in the Cloud" Now a days, the security and the accountability are two major concerns in the cloud. Keeping in mind, all of these, Mr. Pankaj Kumar Singh published this paper in which the problem of accountability has been resolved. In this, there are two main components, the logger and the second is harmonizer [22]. This both works on the JAR file which stores the log file. The log file contains the cloud session information which can be used to check the integrity of the JRE.

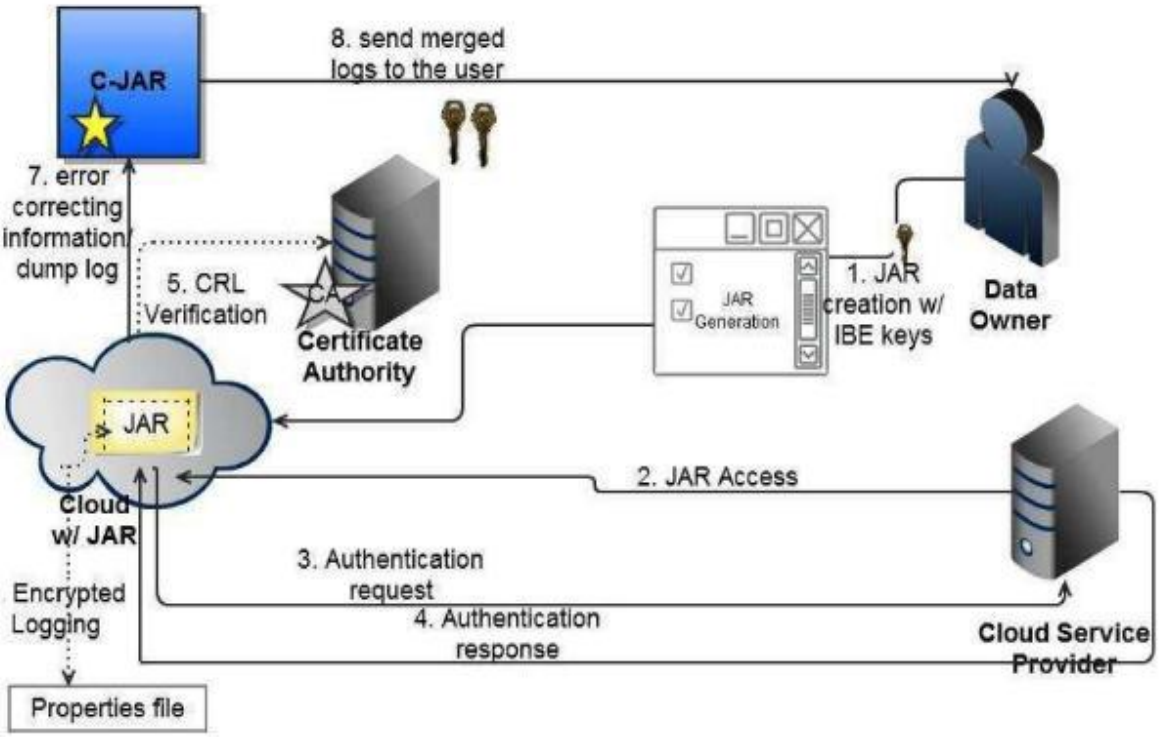

Figure 9: Encrypted Logging Based Framework *[22]*

The approach discussed in this paper is completed in 8 steps which creates a jar in the cloud. And on the client side, it matches with the data owner key. If there is any error in the match of the key, then the JAR file logging is failed and the user will not be able to logging in the cloud as he doesn't have the real key. In this also, Log retrieval algorithm is used which pull & pushes the data or the Jar file logging with session. This approach allows the data owner to audit the data content but also provides strong back-end protection when required [22]. Also, they have enclosed PDP methodology to improve the integrity of owner's data. Also, they are planning to improve our approach to verify the integrity of JRE. To do so, they are looking into whether it is possible to use secure JVM being developed by IBM and they will enhance the PDP architecture from user end which allows the user to check data remotely in better manner in multi cloud environment [22].

Casassa-Mont, Marco, (2014) "Towards safer information sharing in the cloud" It is an e-commerce world where online transactions and cloud sharing are highly used. The main objective was to automate the manual transactions by using the online way [23]. Using the online way, they can share data or can do online transactions of any type. But there is a problem with these kind of apporaches, the user's have always doubt of what will happen to the information that is shared by the user. The data can be misused or can be used by someone for spamming or fraud transactions [13]. So, there is no assurance to online data sharing doubts. Here, the disussion is about the possible reasons that led the user's to avoid data sharing in the cloud environment [23]. As discussed in manual transaction, the similar is provided in the online transaction by the use of E-DSA (Electronic Data sharing Agreement) [13]. The E-DSA is a human-readable and machine-process able contract which monitors how a transaction between two parties or data sharing between organizations or individuals among themselves. The E-DSA automates the process of verification and validation and it enforces some policies through a manageable and consistent lifecycle.

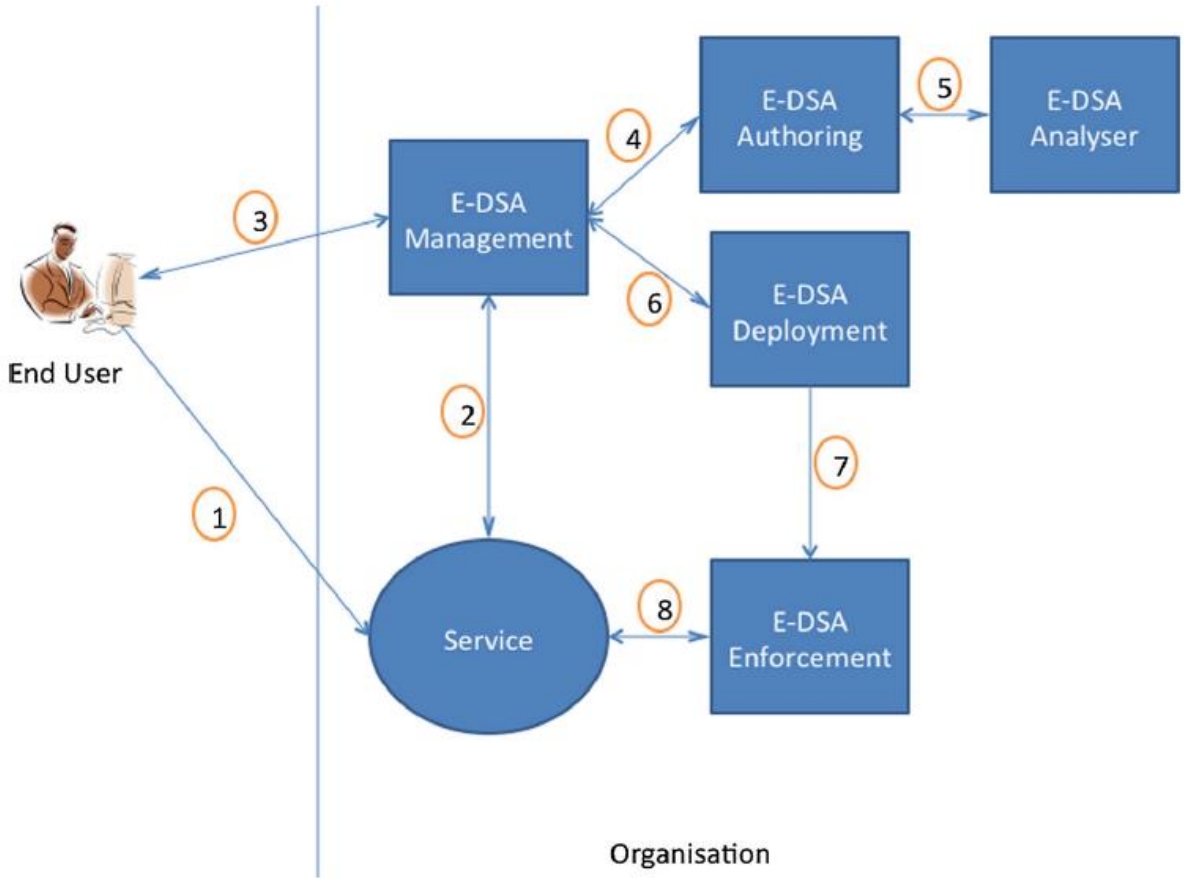

Figure 10: Main e-DSA lifecycle phases *[24]*

In the manual transactions, the user's kind of have conceptual agreement referring to certain rules and constraints that had obeyed by both the parties between which the transaction is happening. Here, the disussion is about the possible reasons that led the user's to avoid data sharing in the cloud environment [23]. As discussed in manual transaction, the similar is provided in the online transaction by the use of E-DSA (Electronic Data sharing Agreement) [13]. The E-DSA is a human-readable and machine-process able contract which monitors how a transaction between two parties or data sharing between organizations or individuals among themselves. The E-DSA automates the process of verification and validation and it enforces some policies through a manageable and consistent lifecycle. The policies monitor the flow of data among organizations or individuals that are involved in the transaction. The violations in the transactions can be tracked back to policies statements mentioned in E-DSA [23].

Sinjilawi, Yousef K., Mohammad Q. AL-Nabhan, et al (2014)"Addressing Security and Privacy Issues in Cloud Computing " The focus of this paper revolves around

security concerns related to the data storage in the cloud environment [13]. As you know, the cloud is an internet based development process which provides high bandwidth network and flexible network connections [25]. This makes it more suitable for the users to use the cloud services. Cloud provides a platform for development and deployment and in a more productive way because of its flexible services and support [25]. Cloud was firstly treated as an data warehouse but it is not just that because the data is updated time to time. Cloud computing provides large datacentres which allows to move our application and databases but this may not be trustworthy. The data can be accessed by some unauthorized person which may not be trustworthy for an user or an organization [13]. This paper discuss an effective and flexible distributed system for correctness and security of user data in the cloud environment.

Akram, Raja Naeem, and Ryan KL Ko. (2014) "Digital Trust-Trusted Computing and Beyond: A Position Paper " This reasearch discussed various way of providing security in the cloud computing. Cloud computing allows the user to use a service or software prior to owing it [26]. Also, if need that service for some one time use dervice only, they can use pay for use services of the cloud means they only pay for the service they need, they don't need to own or buy that service. The secuirty in a cloud is abig issue. The data transparency, access of data, and lack of data availability are some issues related to the cloud [26]. The main purpose of this paper is to find out different secuirty and privacy concerns in the cloud environment and find a scheme to overcome these problem or to provide a way around them. In such cases, data centric apporach is used which helps in secuirty and privacy of data in the cloud environment [13]. Pearson and Mow bray, in their research paper, have provided information about technical and procedural methods for promoting cloud privacy [10]. Their papers focused on higher level accountability layers in cloud [10]. Pearson and KO lee, together in 2011, established the paper which concerns cases and scenarios that predicts high level concerns of accountability in a cloud system.

CHAPTER 3

PRESENT WORK

3.1 Problem Formulation

A chain of Accountability permits the members of a cloud system to make sure that obligations to shield information area unit discovered by all United Nations agency method the information, regardless of wherever that process happens. Now, regardless of the work is completed as [5] Mr. Ryan K L blow builder a trust cloud framework that divides the info properly. The one is the private data and the other is sensitive data and this data used by anyone in this model is providing only the client side accountability which is applying to the logging means that whenever a user a user is logging in , log is generated at the user side. In other words, they can say that whenever from the client side, a user is logged into the cloud, his information is stored in to a log file is sent to the cloud. By this, the cloud service provider know at which time which user has logged on and from where he had logged on and what the user is using the cloud data. Because of this, the user and the cloud accountability are maintained as well as the user security and privacy. Also, the cloud remains secured of the unauthorized users. If any action on the data is performed by some unauthorized user, the service provider will be informed that someone is intruding without proper authentication in the cloud. But using this existing framework, they can make the cloud a trusted cloud environment but user will not get the accountability because as this framework works at five different layer i.e. workflow layer, data layer, system layer, policy layer and law layer. This all layers work on the local system layer and not on the networking OSI layer. Keeping in mind, all these drawbacks, I created a new framework which will provide accountability to the service providers as well as the users in the cloud. In this framework, the data is divided into three types, private, protected and public which is totally based on the user requirements. In this existing framework the main layer basically depends on the local system which is not required in any cloud environment to run this framework because it is using the stored data and not real time generated data that is required to request from the internet or the cloud environment. This framework is working logging on the client side and the other approach is to provide accountability using detective and preventive approach. They have many discussions that the migration of concerns from system health and performance to

the integrity and accountability of data stored in the cloud environment [5]. This requires a file-centric approach, on the top of general system-centric approach for logging.

Another researcher Mr. Casassa-Mont in 2014 has worked a new way of accountability in which the local service provider can provide the accountability to the user [23]. 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 [13]. 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 [13].

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.

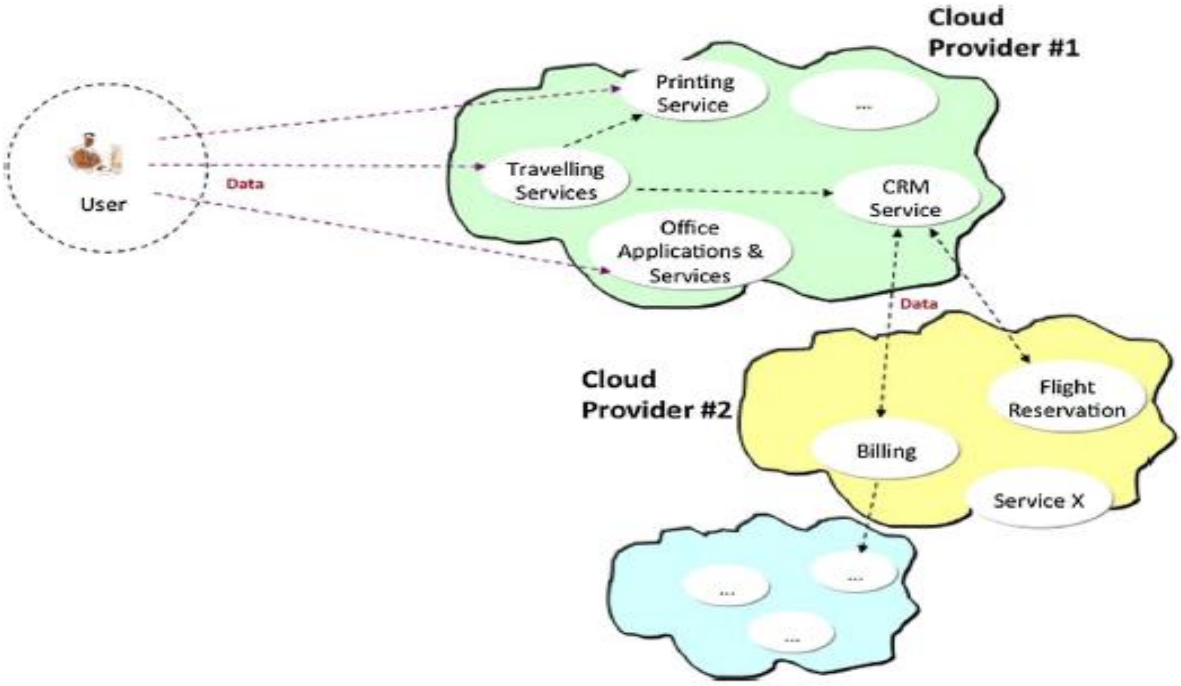

Figure 11: Data sharing with web application *[24]*

But security is one in every of vital the key the foremost} considerations in cloud atmosphere and whereas exploitation net applications on cloud computing it play an awfully important role as a result of it helps to stay our secret info 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.

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.

3.1.1 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 they can use service brokers which a better and reliable option as compared to local service providers Cloud computing is used as for the purpose of computation, as a platform and as a services also. It is a surroundings wherever the user doesn't would like his/her own infrastructure and that they will use the cloud services on pay per use basis. however security is one among the main the key the foremost} considerations in cloud surroundings and whereas mistreatment net applications on cloud computing it play an awfully important role as a result of it helps to stay our secret info confidential. In previous work the work is completed on the idea of agreement, suggests that once user desires to share his info with any service supplier it'll be agreement in between user and repair supplier that service supplier won't share his info with the other person. Currently the work is essentially supported trust approach. owing to agreement user will depend on service supplier however some attacks square measure attainable like men in middle attack they will retrieve info from the trail whereas sharing agreement. therefore to reinforce the work and to scale back the chance they tend to square measure aiming to add some a lot of techniques like encoding , steganography etc. in order that it transmit our knowledge a lot of firmly and may create the employment of net applications with a lot of liableness and security.

3.2 Objectives of the study

When it deal with the web applications of cloud computing the much security is obligatory because in web applications like online payment they need a high security because we have to share our important credentials like account number and password

etc. so while looking at appropriate security schema the objectives of our work are as following:

- To study and analyze the security of web applications in cloud computing.
- To develop new framework that can met with accountability issues in cloud computing security.
- To implement new framework in heterogeneous environment and compare with existing framework.

3.3 Proposed Methodology

Security of internet application in cloud computing could be a terribly difficult task. If they have a tendency to point out the protection of internet application like on-line payment application the protection is extremely needed as a result of here we've to exchange our import data like act. Number etc. that is extremely confidential. To shield our counsel we'd like to produce security on each channels, suggests that from internet application to bank verification and from we have a tendency to application to payment receiver.

3.3.1 The Cloud Accountability Life Cycle

Using this Cloud Accountability lifecycle, we can improve the accountability and provide more secure cloud environment. Providing accountability to the user in the cloud is very difficult but using this lifecycle, it can do provide the accountability to the user easily. It can classify this CALC (Cloud Accountability Life Cycle) into five phases, and using these phases it can mitigate the problem of accountability from the cloud. The five phases are:

Logging The file perspective logging is the logging of user in both the virtual and the physical layer of cloud. Whenever the user logins to an application in the cloud environment, a log file is created where the location of the user and the server storage location which the user access are both logged. It is done for all the users who logged on to the cloud applications. The user's private data is kept private in this log and is not shared with anyone [5].

Policy planning in this phase, the data is divided according to the policy. Using this policy, the service provider's stores and shares data among themselves or with others service providers. In this, all the roles are defined and if the user needs to gain the

accountability, he needs to accept the policy terms mentioned. Also, this is one of the most important phase in the CALC lifecycle.

Safe Keeping of logs once, the logging phase is done, we need to protect the integrity of the logs and to prevent unauthorized access. The logs contains the private data of user who had accessed the cloud application and we need to ensure that they are tamper-free. Encryption or other preventive measures can be applied to protect the logs. There should also be mechanisms to ensure proper backing up of logs and prevent loss or corruption of logs.

Figure 12: The Cloud Accountability Life Cycle (CALC) *[19]*

Reporting and Replaying Reporting tools square measure accustomed generate summaries and audits of all the files within the cloud [5]. The news keeps a record history of the file life cycle within the cloud system and that we once required will access them as file-centric summaries and reports of the audit trails. It conjointly helps in police work any irregularities if gift and that they square measure flagged to the end-user. Reports scope might vary from scope to scope, for instance recording virtual and physical server histories among the cloud; from OS-level read/write operations of sensitive information, or high-level advancement audit trails.

In Auditing, Logs tools square measure accustomed generate summaries and audits of all the files within the cloud [5]. The news keeps a record history of the file life cycle within

the cloud system and that they once required have access them as file-centric summaries and reports of the audit trails. It conjointly helps in police work any irregularities if gift and that they square measure flagged to the end-user. Reports scope might vary from scope to scope, for instance recording virtual and physical server histories among the cloud; from OS-level read/write operations of sensitive information, or high-level advancement audit trails.

3.3.2 The Object Based Accountability Framework

The first thing is that providing security in the cloud is very difficult. The more problematic is to provide accountability in the cloud environment. Before implementing the cloud services, the first thing is consider is to how to provide security to the cloud environment. So, that we can make the cloud fully secure and provide the accountability in that. The accountability factor in the cloud is very important as it will assure the access log of user's data and provide more security to the user data. In this way, the user can use cloud computing for their data and can trust it that their data will secured in the cloud environment. For example, if a user buy anything online, he has to provide his information prior to buying that information to the other party which can be risk full if the not trustworthy party. For Example, his bank details can be used for fraud transactions or his bank details could be stolen and shared by someone [13]. To remove such kind of problem, the accountability factors is implemented in the cloud environment. Some people have done research on this very matter and they divided the data in two parts but we divided the data in three parts: private, public and protected that is used in the new framework and can be used to improve accountability in the cloud environment which is explained in the below section.

The design of Object based accountability framework

This framework is divided into several parts and keeping in mind, working of each is explained here.

User As you know, the user or any human being request any resource from the internet or the cloud environment where the secured or unsecured data is processed through an interface provided by the cloud where data needs to be entered by the user whenever he request for any services from the cloud. We provides the user with our new framework policy which divide the data into public, private and protected and send data and policy to the cloud service provider.

Service broker Firstly what is service broker, service broker main task is that whenever he gets a request from the user, he divides the request into small parts. These small parts are called jobs and later the jobs are distributed to different service providers. Service providers play an important role in the cloud. The service providers process the requests.

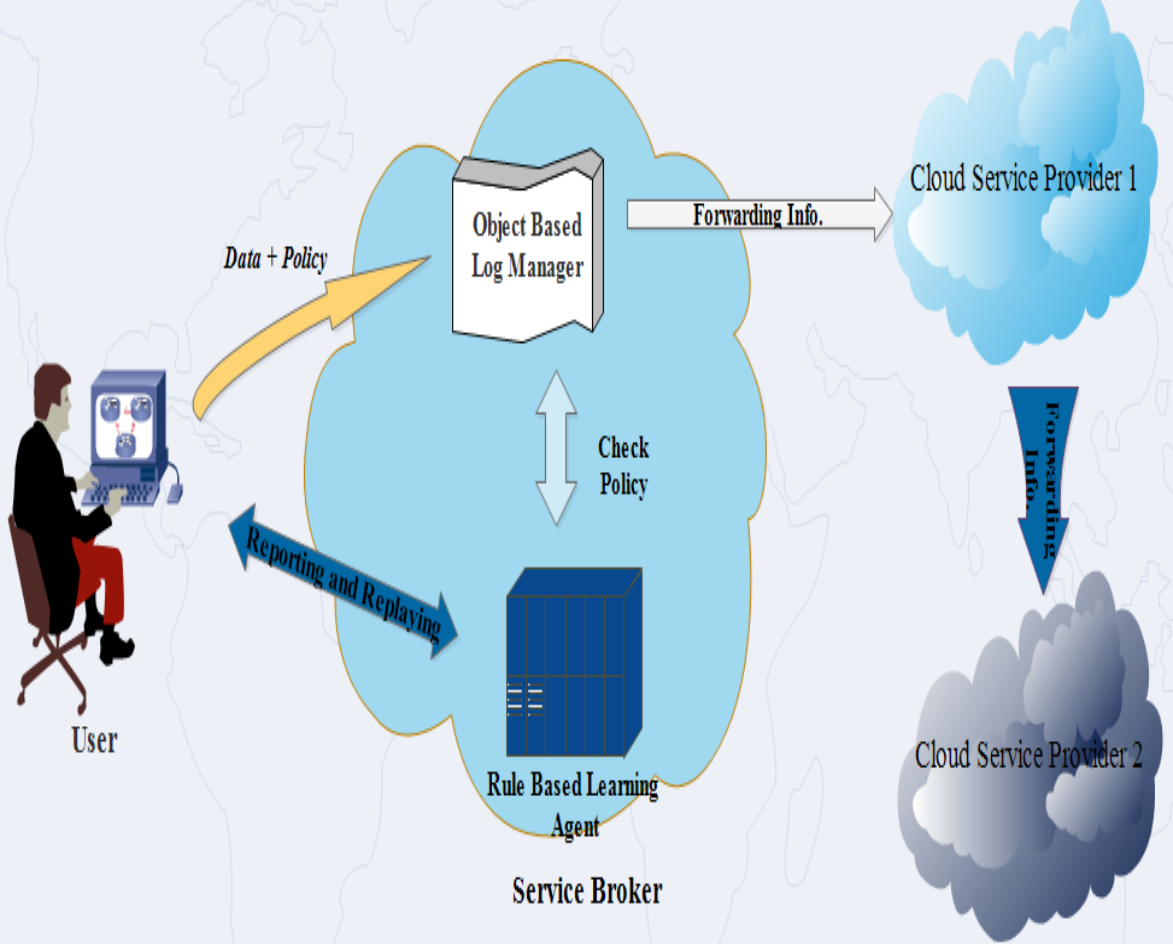

Figure 13: The Object Based Accountability Framework

Basically, in the new framework, we are deploying at service broker so that we can get real time data accountability. The service provider can be divided into two parts which are discussed later.

Object based log manager The first thing is that you all know very well what is the purpose of an object and that log means to capture every entry in the log from horizontal format in the XML file format [13]. To store a log based file, firstly it is checked against its rule based learning agent to check if the data is private, protected or public and while sharing that data on cloud with the service provider may not sharing with anyone else and

if it does, then it is checked with RBLA and then sends a message informing him. Same thing happens for protected and public data.

Rule Based Learning Agent The main purpose of RBLA that it defines the rules according to the policy and send a message to the user that his data is being used by someone and where. In this number of rules are defined according to which you can store your data privately on the cloud and if someone tries to perform any action on that data without your concern, then a message is sent to the user that his data is being used CS1 and CSP2 for the given time. If the data of user is public, then also the user is informed of such actions performed on his data. Same is done for protected type of data [13].

Cloud Service provider there are variety of issues that must be evaluated for your service suppliers within the cloud surroundings [27]. The value can supported pay-per-use based mostly model however there are variety of variables to contemplate. Like, the physical location of the server is massive variable and is major issue for sensitive information. Trust or irresponsibleness is extremely vital if your information should be acceptable. A typical cloud SLA have predefined service levels alongside the resources or compensation that is entitled to the user if the supplier fails to produce the service as in agreement. However, each fine print within the agreement ought to be created important as a result of generally, the suppliers create discount of ten min of outages however now might have an effect on massive loss for the user [27]. Security is another main factor to contemplate here. Cloud Security Alliance provides certification to the qualified service suppliers [27]. The CSA's sure Cloud Initiative program was created to assist cloud service suppliers develop industry-recommended, secure and practical identity, access and compliance management configurations and practices.

CHAPTER 4

RESULTS AND DISCUSSIONS

In this chapter, we have discussed the results of the proposed system. This research used MATLAB for implementation purpose. MAT laboratory can be a source language and interactive setting for numerical computation, image, and programming. Practice MATLAB, you may analyze data, develop algorithms, and create models and applications. The language, tools, and per se science functions alter you to explore multiple approaches and reach a solution faster than with spreadsheets or ancient programming languages, like C/C++ or Java. You. MATLAB is spread of applications, at the side of signal method and communications, image and video method, management systems, take a glance at and measure, procedure finance, and procedure biology. Quite 1,000,000 engineers and scientists in business and domain use MATLAB, the language of technical computing.

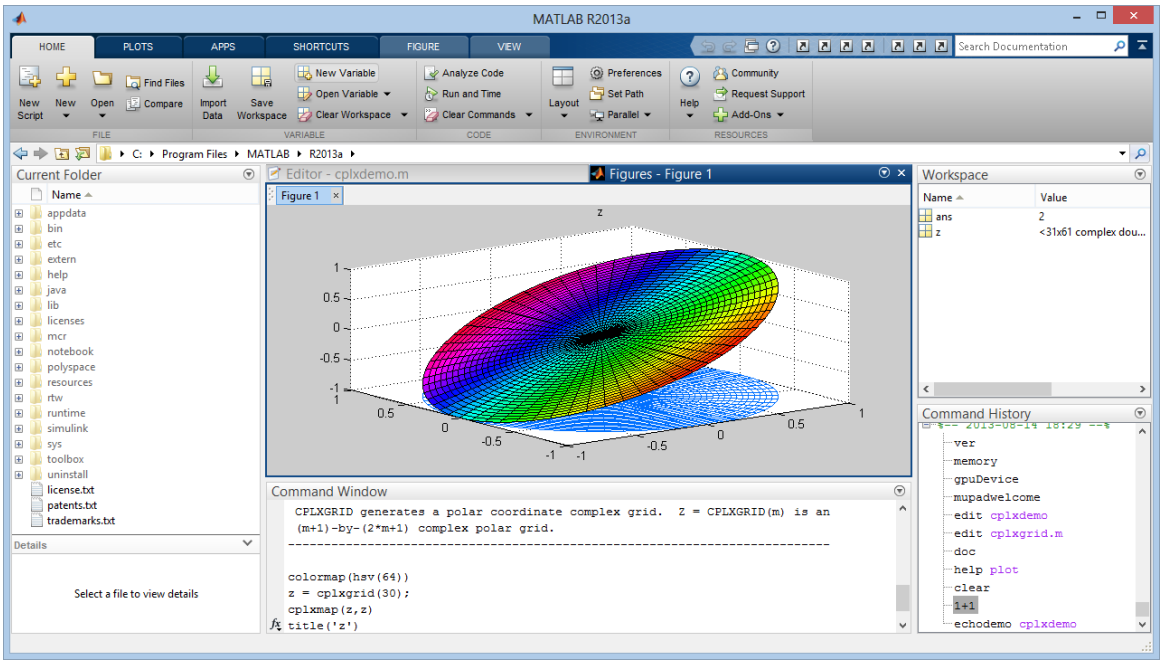

Figure 14: Mat lab running on Windows *[28]*

Although MATLAB is supposed primarily for numerical computing, degree no mandatory toolbox uses the MuPAD symbolic engine, allowing access to symbolic computing capabilities [28]. An additional package, Simulink, adds graphical multi-domain simulation and Model-Based vogue for dynamic and embedded systems.

In 2004, MATLAB had around 1,000,000 users across trade and world. MATLAB users come from various backgrounds of engineering, science, and science [28]. MATLAB is wide used in tutorial and analysis institutions nevertheless as industrial enterprises.

In this section, it is described that in the new system, we can provide accountability to the user in the cloud environment. Therefore when the user is logging, whether he is inputting is data or he is connecting to the cloud through internet for the request. Along with request he demands, he also agrees to the policy demands to whether he wants to keep the data private or public or protected. This all depends on the user on how he wants to store his data as it is shown in the below diagram.

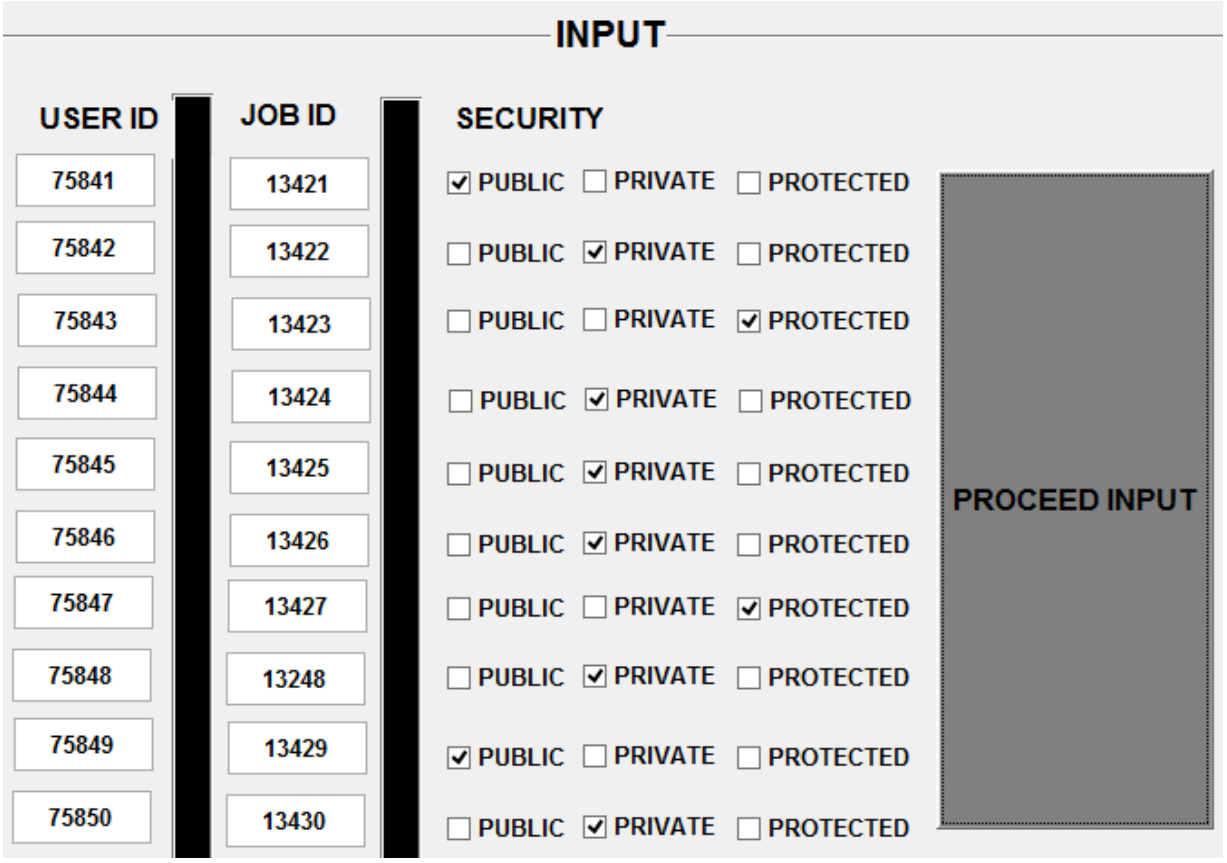

Figure 15: User Logging and Accept the security policy

After that, when the user accepts the security policy, then the data is sent to the service broker where it is divided into smaller jobs. But before splitting it into jobs, it is stored in the log file format where all the adequate information for each job is entered and

maintained. It contains all job information like when the job they arrived, how much time did it take or when the job done, or what's the status of the job whether it is completed or not. After that, it is calculated that which resource got the job and the job id, which user gets the job and what is the policy for that job whether private, public or protected. After that, all this is checked by the job learning manager and then sent to the service providers for processing. In below figure, the same is configured.

After figure 13 processes the data is transferred to as shown in figure 14 to job learning manager. The job learning manager checks each and every job against its security policy and then sends it to the service providers. Then, it is checked if any of the cloud service provider is breaking any policy or not and if it does, then the request are checked by the object manager against the log if the data is private which is shared by the service provider.

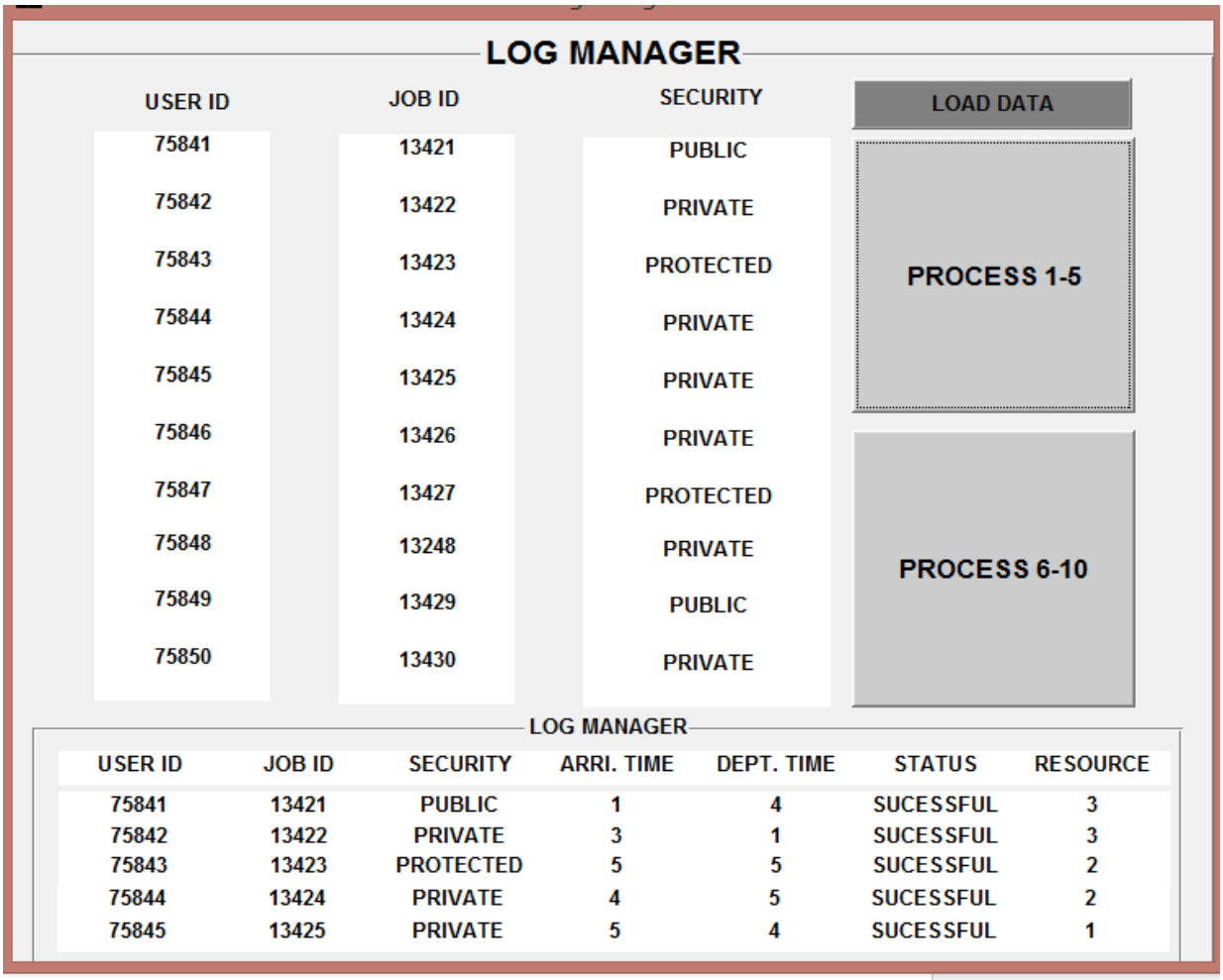

Figure 16: Data Process in Log file

If the private information of the user is shared with another service provider and if any modification is done to the data, the user is informed that his data is shared with another CSP or modified by another CSP. This all is shown in the figure 16. And in this processes, each user in a cloud gets the accountability using this new framework. This is the best framework for storing data in cloud and real time data access. Using this new framework, data classification can be improved and data can be securely shared in the cloud without any problem because we divide the data into three parts which led to easier data analysis due to which we can easily analysis online data and can provide user with better services. This is reason why this framework is better than the previous framework.

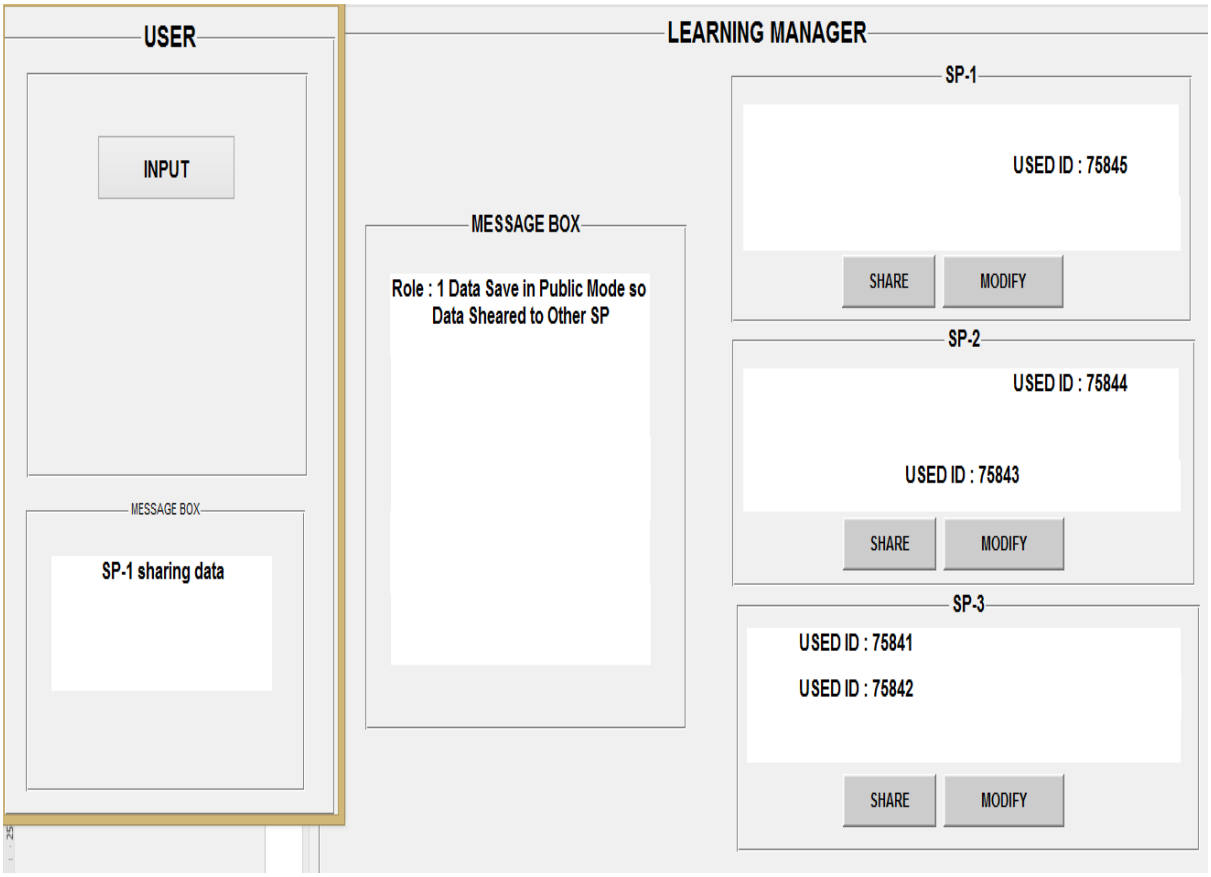

Figure 17: Reply Message to user

In figure 17, the main system performance is displayed. There are two axis where one represents execution and the second one represents the successful alert or message which the cloud sends to the user if his data is secured or not. Performance is basically very important part in security and accountability.

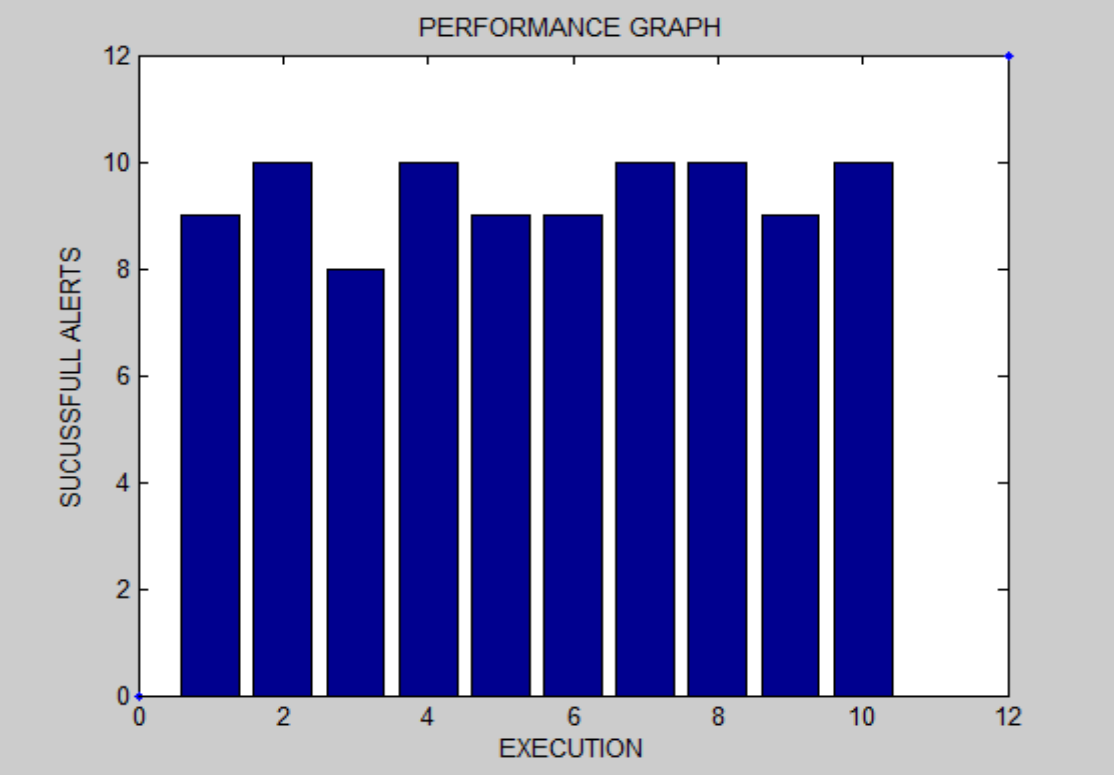

Figure 18: Performance of OBAF

If the system maintenance is not good, then it is not acceptable to the user in the cloud or for the application. We have, in the new object based accountability have maintained performance by managing the requests that comes on the cloud environment and dividing them into smaller jobs so that they can be easily performed. The job is securely analyzed and it is evaluated that what is the data mode and how is the processing of the job is going.

If the user keeps his data is public, then the data is send forward and the user is informed that his data is forwarded by one cloud service provider to another. We have analyzed this whole process situation to get how many jobs the user has sent to the cloud and how many of them are successfully executed by sing successful alert message to the user. In fig. 17 we have introduced new OBAF (Object based accountability framework) has a success rate of about 89% job execution and about 87-89% of successful alert messages to the user. In this new framework, we are providing 88% of the accountability to the user. Using the current framework, we can provide around 80% of accountability and 79% security to the cloud. So if we compare this statistics, our framework is a better option from providing security and accountability.

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

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 web is viewed as a cloud. The users use the services provided by the cloud atmosphere as per their demand on pay per use basis. The cloud provides the service of storing knowledge on the cloud rather than our own devices that makes it present. 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. Cloud computing is a very new area where a large number of applications runs. To run an application, we need new resources and a platform to run that application. The cloud provides these resources and the platform for an application to run. It is true that security in the cloud environment is a big issue but along with that, the accountability is also an important term that needs to be addressed. To remove this kind of problems from the cloud, we need to improve the accountability of cloud computing. We can do so by using object based accountability framework. The service provider who is providing service to the user along with the accountability allows the user to know when and where his data is accessed and by whom. And at which time, his data is located where, to another user or not. This all information will be provided to the user through implementing this new framework. This new framework is deployed at the service broker and in this every job data is analyzed. We have developed a protocol to improve this framework process. This protocol will work at different layer which will also analysis data packets. This will improve the process of data analysis as well as improve the accountability. Because, in this new framework, after analyzing the job we are providing the accountability to the user but by using this protocol, we can improve the accountability more as this protocol works with the data packet. The use of this protocol in different layers for job analysis will be doing in the future which will better the performance and will provide

REFERENCES

[1] j. Woo, "Introduction to Cloud Computing," 10th KOCSEA 2009 Symposium, UNLV, pp. 18-19, 2009.

[2] V. Alangar, "Cloud computing security and encryption," International Journal of Advance Research in Computer Science and Management Studies, 2013.

[3] A. F. Michael Armbrust, "A Berkeley View of Cloud," Electrical Engineering and Computer Sciences, 2009.

[4] T. J. R. E. Anthony T.Velte, Cloud Computing A Practical Approach, TATA McGRAW-HILL, 2010.

[5] P. J. M. M. S. P. M. K. Q. Ryan K L Ko, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," in IEEE Cloud Forum for Practitioners, Washington DC,, 2011.

[6] A. Haeberlen, "A case for the accountable cloud," in ACM SIGOPS Operating Systems Review 44.2, 2010.

[7] A. R. Y. a. J. S. Chase., "Trust but verify: Accountability for internet services.," in ACM SIGOPS European Workshop, 2004.

[8] P. K. a. P. D. Andreas Haeberlen, "Practical accountability for distributed systems," in ACM SIGOPS Operating Systems Review. Vol. 41. No. 6. ACM, 2007.

[9] N. J. a. V. T. R. King, "Protecting the privacy and security of sensitive customer data in the cloud," in Computer Law & Security Review 28, no. 3, 2012.

[10] S. a. A. C. Pearson, "Accountability as a way forward for privacy protection in the cloud," Springer Berlin Heidelberg, pp. 131-144, 2009.

[11] D. a. G. H. Catteddu, " Cloud computing risk assessment," in European Network and Information Security Agency (ENISA) , 2009.

[12] N. K. P. G. a. R. R. Santos, "Towards trusted cloud computing," in In Proceedings of the 2009 conference on Hot topics in cloud computing, pp. 3-3., 2009.

[13] P. S. A. K. Pradeep Singh, "Object based Accountability Framework for Information Sharing in Cloud Computing," International Journal of Computer Applications 115(19):28-32, vol. 115, pp. 28-32, 2015.

[14] HyTrust, ", “HyTrust Appliance," http://www.hytrust.com/product/overview/., 2010.

[15] S. a. C. W. Chen, "Accountability as a Service for the Cloud: From Concept to Implementation with BPEL.," in In Services (SERVICES-1), 2010 6th World Congress on, pp. 91-98. IEEE, 2010.

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

[17] J.-S. C.-H. L. a. G. T. L. Wang, "How to manage information security in cloud computing," in " Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on, 2011., 2011.

[18] S. a. 0J. c. X. Han, "Ensuring data storage security through a novel third party auditor scheme in cloud computing," in Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on, 2011. , 2011.

[19] 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.

[20] P. a. S. S. Kalpana, " Data security in cloud computing using RSA algorithm," in IJRCCT, 2012.

[21] M. P. C. J. Epuru Madhavarao, "DATA SHARING IN THE CLOUD USING DISTRIBUTED ACCOUNTABILITY," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 3, no. 6, 2013.

[22] A. k. Pankaj Kumar Singh, "Ensuring Distributed Accountability for Data Sharing in the Cloud," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 3, pp. 765-760, 2013.

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

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

[25] Y. K. M. Q. A.-N. a. E. A. A.-S. Sinjilawi, "Addressing Security and Privacy Issues in Cloud Computing," Journal of Emerging Technologies in Web Intelligence 6,, vol. 2, pp. 192-199, 2014.

[26] R. N. a. R. K. K. Akram, "Digital Trust-Trusted Computing and Beyond: A Position Paper," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on. IEEE, 2014., 2014.

[27] searchcloudprovider.techtarget.com, "cloud service provider," http://searchcloudprovider.techtarget.com/definition/cloud-provider, 2015.

[28] "Matlab," [Online]. Available: http://en.wikipedia.org/wiki/MATLAB. [Accessed 29 4 2015].

[29] P. a. S. S. Kalpana, "Data security in cloud computing using RSA algorithm," IJRCCT, pp. 143-146, 2012.

[30] 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.

[31] J.-S. C.-H. L. a. G. T. L. Wang, "How to manage information security in cloud computing," Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on, 2011.

[32] 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.

[33] S. S. a. H. G. A. Yau, "Software engineering meets services and cloud computing," Computer 44.10, pp. 47-53, 2011.

[34] 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.

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

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

List of Abbreviations

Abbreviations	Meaning
MCC	Mobile-cloud-computing
REAL	Rubbing Encryption Algorithm
VPN	Virtual Private Network
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
MSS	Managed Security Service
OTP	One Time Password
2FA	2 factor Authentication
XMPP	Extensible Messaging and Presence Protocol
VM	Virtual Machine
OBAF	Object based accountability framework
CALC	Cloud accountability life cycle
CSP	Cloud service provider