IPASJ International Journal of Computer Science (IIJCS)

Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm

A Publisher for Research Motivation ....

Email:editoriijcs@ipasj.org

Volume 5, Issue 11, November 2017

ISSN 2321-5992

STATIC AND DYNAMIC ALLOCATION WITH PUBLIC AUDITING SCHEME IN CLOUD COMPUTING

RM. Iswarya[1], T. Nirmal Raj[2]

[1]M. Phil Research Scholar, SCSVMV University Enathur, Kanchipuram. TamilNadu , India –631561

[2]Assistant Professor, SCSVMV University Enathur, Kanchipuram. TamilNadu , India –631561

ABSTRACT

Security audit is a feature of important when it comes to cloud service environment and its customer. It's a certification process that audits the controls that is responsible to deliver the security requirements. These security audits are performed by qualified and trained staffs that belong to an independent external auditing firm. Security must be considered as a standard of security controls. Proper checks must be made to ensure that cloud users have a proper logging and reporting facilities in merge with the customer's system thereby ensuring appropriate operational and business flow of data through cloud service system. We propose a auditing system for cloud-based architecture that allows only trusted authority to efficiently store their secret data or file on the semi-trusted cloud service providers, and selectively share their secret data with huge number of data receivers and minimize key management complexity. The proposed system slightly differs from the previous cloud-based data system. Here the data owners can upload their secret data in cloud storage using both static and dynamic auditing scheme. Another specific characteristic of the proposed system is that if any data receiver wants a personal file to be downloaded then a request is sent to the authority from the data receiver. The authority owner will have control over the Access Control. If the Owner of the file wishes to share the original file with the data receiver, then he has to accept the data receiver request. Once the request is accepted, the data receiver can download the original file. This file will be uploaded with time and date and downloading time with date monitor by auditor. In addition de-duplication concept is also included. It helps to check for duplication of file or data to minimize the cloud memory space that is occupied. The files in this system are allocated using dynamic file allocation.

Keywords: - Cloud computing, Auditing, File allocation, Deduplication,.

1. INTRODUCTION

Cloud computing made us to realize the importance of information storage in a smart way. It changed the traditional thinking of running data and programs on individual desktop computer. It is the concept of having a number of computers and servers being accessed through the Internet. Cloud computing helps us to access all the applications and documents from anywhere around the world. It gives us the freedom from desktops and makes it easier for a group of members from different locations to work collaborate. Cloud computing has gained interest from a widespread of fields. Services like application hosting, resource renting and service outsourcing in cloud environment shows that the core concept of an on-demand service in the IT field is achievable. Various IT tycoons like Amazon's S3, Amazon'sEC2, Microsoft's Azure and Google App Engine etc are already making their presence in cloud computing. Cloud computing helps in easy computing capabilities, minimizes costs and capital, minimizes capital and costs expenditures and finally charges are based on the usage. Though cloud computing serves many benefits, there are still some unavoidable security challenges caused due the dynamicity in cloud computing environment. The open environment in the cloud platform and the high concentration of resources are also the reasons for these security threats. One of the important concerns is the security of user data. Security problems like privacy protection and data security in cloud computing are the serious obstacles that is not rightly answered. Security concerns involved in a distributed file system has been seen for the past few decades. Some of the concerns in a distributed shared system are how to make the control access and how to make a distributed file confidential. On considering the traditional users control mechanisms, it keeps the user authorities in an Access Control List (ACL) either in a group or in a hierarchical structure. Later it adds the access control attributes to a file through trusted server for authorization and authentication.

These traditional approaches completely depend on security of the access control list. Hence if the ACL is compromised then it impacts the access control service. In general, access control mechanisms use symmetric and public cryptographic schemes to secure the access control list. We propose a cloud-based secure data system to allow trusted authority to securely store their personal data in the semi-trusted environment and then selectively share the data to a wide range of data receivers. To minimize the complexity involved in key management the access is given to the file owners or the access owners. Another modification to the traditional approach is that the data receiver wants the personal file to be downloaded; the request from the data receiver is sent to the authority. The authority owner will have the Access Control. When the Owner wants to share the original file with the data receiver, then the keys are shared to the data receiver. After accepts request the data receiver download the secret key and use this key to download the original data. The cloud storage providers ensure that user privacy is still securely protected. Furthermore, the cloud server cannot decrypt any cipher text at any time. The security and efficiency analysis show that our system is not only secure but also practical. We present static and dynamic public auditing scheme for security purpose. This effectively eliminates the need to rely on the data storage server for preventing unauthorized data access and integrity. The performance measurements indicate that the proposed scheme is efficient to securely manage the data stored in the data storage servers and significantly reduces the computation time. In addition we include this algorithm for the data deduplication.

CLOUD SECURITY CHALLENGES

Authentication: The major disadvantage of storing data in cloud server is that it is available to all unauthorized people. Hence there is a demand for and efficient, interchangeability administration entity in certified user.

Access Control: It is important for cloud provider to have access control policies to enable only legalized users to access the information. This customized service must be scalable, adjustable and well planned all the time. The governor provision must work on Service Level Agreement (SLA).

Policy Integration: Some of the cloud providers like Google, Amazon, etc have minimum number of conflicts between their policies since they propose their own policies and approaches.

Service Management: In this case, the various cloud providers integrate together to form a new service in order to meet customer needs. In this stage there must be procure divider to have easiest localized services.

Trust Management: This should include trust negotiation factor among both the parties that is the user and the service provider. Example: for a user to release their services the provider must have trust on the user and the user must have trust on the provider.

In order to efficiently handle these cloud security issues, we must understand the compound security challenges in a unique way. To be precise we must: (i) to investigate on cloud security attributes that includes threats, vulnerabilities, risks and attack models; (ii) to identify the security requirements like integrity, confidentiality, transparency, availability, etc.; (iii) to identify the parties involved in the network like: service providers, clients, outsiders, insiders, etc and then understand their roles in the attack-defense cycle and (iv) to realize the impact of security concerns on several cloud deployment models like public, private, community, hybrid. The main proposal of this paper is to have a secure re-encryption scheme that helps in sharing encrypted data among the authorized users in cloud. Security is the underlying life of the entire cloud system as it serves the quality of the service.

DATA DEDUPLICATION

Data de-duplication is a technique used for data compression in order to eliminate duplicate copies of data or repeated data in the storage. This technique is used to enhance the storage usability and also applied on network data transfers to minimize the number of bytes that has to be sent. De-duplication eliminates multiple copies of same data and prevents redundant data in the storage. De-duplication can be implemented at the file level or at the block level. In case of file-level de-duplication it will remove duplicate copies of the same file. De- duplication can be implemented at the block level as well and in this case it removes duplicate blocks of data that happens in non-identical files.

AUDITING IS ESSENTIAL

Security audit is an important aspect or feature to be considered in cloud service customer. It is basically a certification process to audit the controls that deliver the security requirements. Security audits are conducted by trained and qualified staffs that belong to an independent auditing organization. Security audits must be carried as a standard of security controls.

Proper check to be made that the cloud user has a proper reporting and logging facilities with the customer's system and hence ensuring appropriate business and operational flow of data through cloud service.

AUDIT

Audit is the process to spy on the activities happening in the cloud system. This is placed as an additional layer in the virtual machine to monitor the activities on the system that are related to state change and other factors that influence the availability of the resource. Another aspect to be considered is that many countries have their own defined laws for cloud computing where the customer data should be kept confidential within the national boundary and this makes it necessary to have an audit in place.

2. RELATED WORK

Cong Wang et al [1] proposed an auditing system called as a flexible distributed storage integrity auditing mechanism. It uses homomorphic token and distributed erasure-coded data. This work allows cloud users to audit the storage using lightweight communication and with minimum computation cost. The result of this auditing ensures strong cloud storage, correctness, and also fast data error localization, i.e., to identify the misbehaving server. On the consideration that cloud data is dynamic, the proposed design can further support efficient and secure dynamic operations on the outsourced data that includes deletion, block modification and append. The analysis on this study shows that the proposed scheme is highly resilient and efficient against malicious data modification attack, Byzantine failure and colluding attacks.

Boyang Wang, et al [2] introduces the first privacy-preserving mechanism that can allow public auditing upon the shared data that are stored in cloud. In specific we use the ring signatures to manipulate the verification information that is required for the audit and integrity of the shared data. With this mechanism, the signer identity on each block in case of shared data is secured privately from the third party auditors (TPA), who can still be able to publicly verify the integrity of the shared data without even retrieving the entire file. The experimental results show that the efficiency and effectiveness of the proposed mechanism during auditing of shared data.

Sebastian Lins et al [3] introduces a conceptual CA architecture and also highlights the important processes and components to be implemented in this approach. Finally, the author discusses about the challenges and benefits that are to be tackled in order to incorporate the concept. of continuous cloud service auditing. We provide practical internal and third party auditing concepts for auditors and providers that are linked together in a conceptual architecture. We also provide the ground for future research for the implementation of CA in cloud service.

Cong Wang et al [4] proposes a secured cloud storage system to support privacy-preserving public auditing methods. The derived result is further extended to enable TPA perform audits for multiple users at the same time. In depth performance and security analysis was demonstrated to show that the proposed schemes are secure and efficient. The preliminary experiment that was conducted on Amazon EC2 demonstrated fast performance of the design.

Andreas Wolke et al [5] provides the results of an extensive experimental analysis performed on both capacity management approaches on a data center infrastructure. It is shown that the typical workloads of transactional business applications and dynamic resource allocation does not affect in increase of the energy efficiency over the static allocation of VMs to servers and can even come at a cost, since migrations lead to the overheads and service disruptions.

EXISTING SYSTEM

In cloud users need not physically possess their data. Hence to ensure integrity of their outsourced data is a challenge. In recent days proposed schemes like “proofs of retrievability” and “provable data possession” are designed exclusively address this problem. But they are designed to audit static archive data and hence lacks in data dynamics support. Also the threat models assumed in this prototype are honest data owner and focuses on detecting a dishonest cloud service provider despite the fact that clients may also misbehave inappropriately.

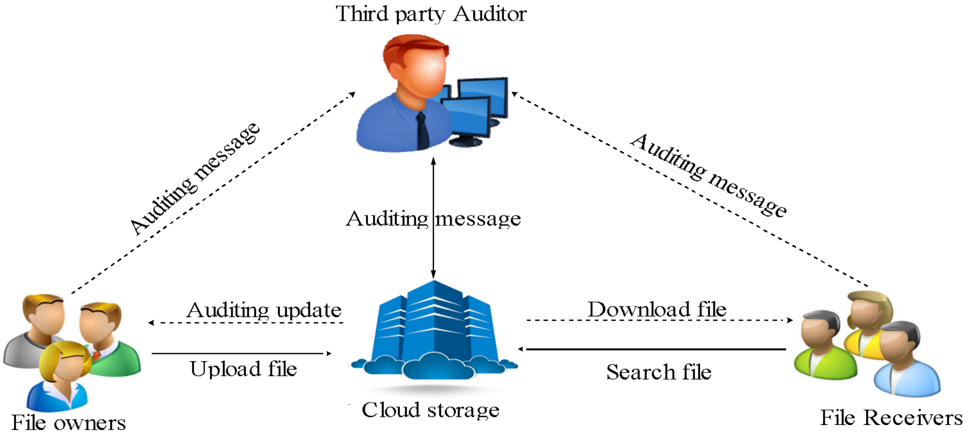

Figure.1 Architecture diagram of Existing system

EXISTING PROBLEMS

- Not efficiently secured.
- It occupies more memory space.
- Same files are uploaded into cloud.
- Data corruption.
- Recollection distribution problem.
- Over inscription of data.
- Failures happen in reduplication.
- Efficient to handle small amounts of data.
- Expensive
- Complex

3. OUR CONTRIBUTION

We propose a cloud-based secure data system that allows trusted authority to store their data securely on the semi-trusted cloud service providers, and also to selectively share their data to a wide range of data receiver. This approach is different from the traditional approach where in this case data owners upload their secret data into cloud either using static or dynamic auditing schemes. Another new specification in this method is that if any data receiver wants a personal file to be downloaded, the data receiver will send the request to the authority. The authority owner will have the Access Control. If the Owner wants to share the original file with the data receiver, accept data receiver request. After accepts request the data receiver download the original file and this file uploading time with date and downloading time with date monitor by auditor. In addition added de-duplication concept for reduce cloud memory space. And files are allocated using dynamic file allocation. So we change our file location and delete unwanted files from cloud storage list. Finally modify file location using static and dynamic file allocation. So files are allocated properly. And Auditing is the process to spy on the activities happening in the cloud system. This is placed as an additional layer in the virtual machine to monitor the activities on the system that are related to state change and other factors that influence the availability of the resource. Another aspect to be considered is that many countries have their own defined laws for cloud computing where the customer data should be kept confidential within the national boundary and this makes it necessary to have an audit in place.

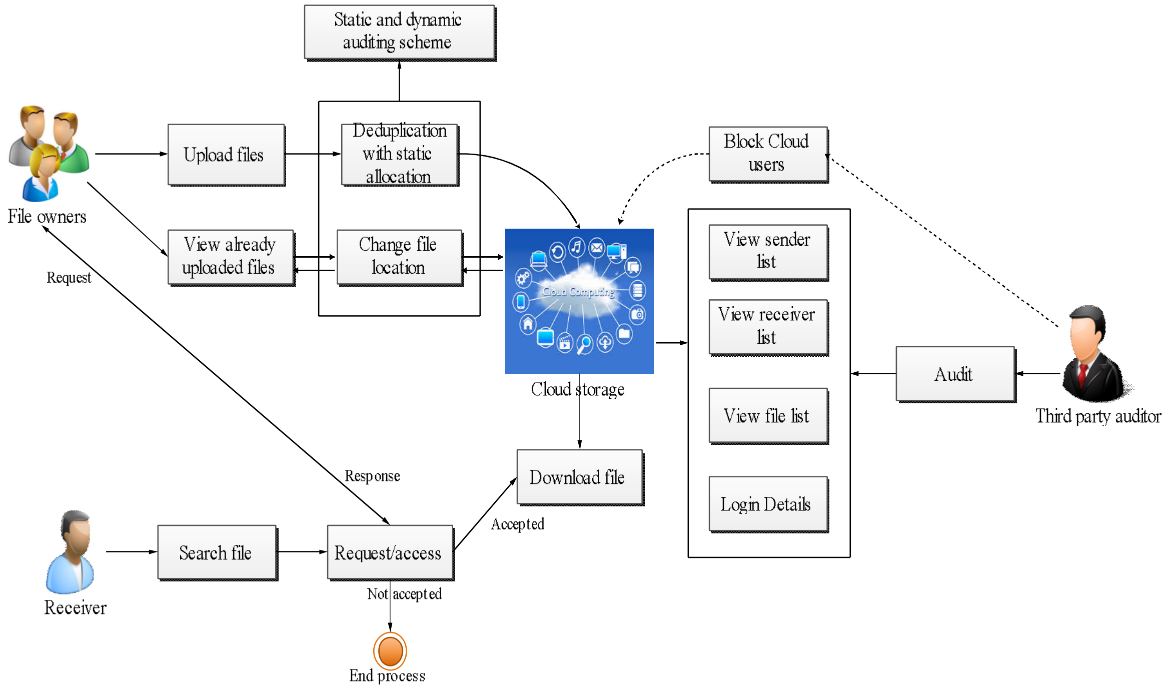

Figure.2 Architecture diagram of proposed system

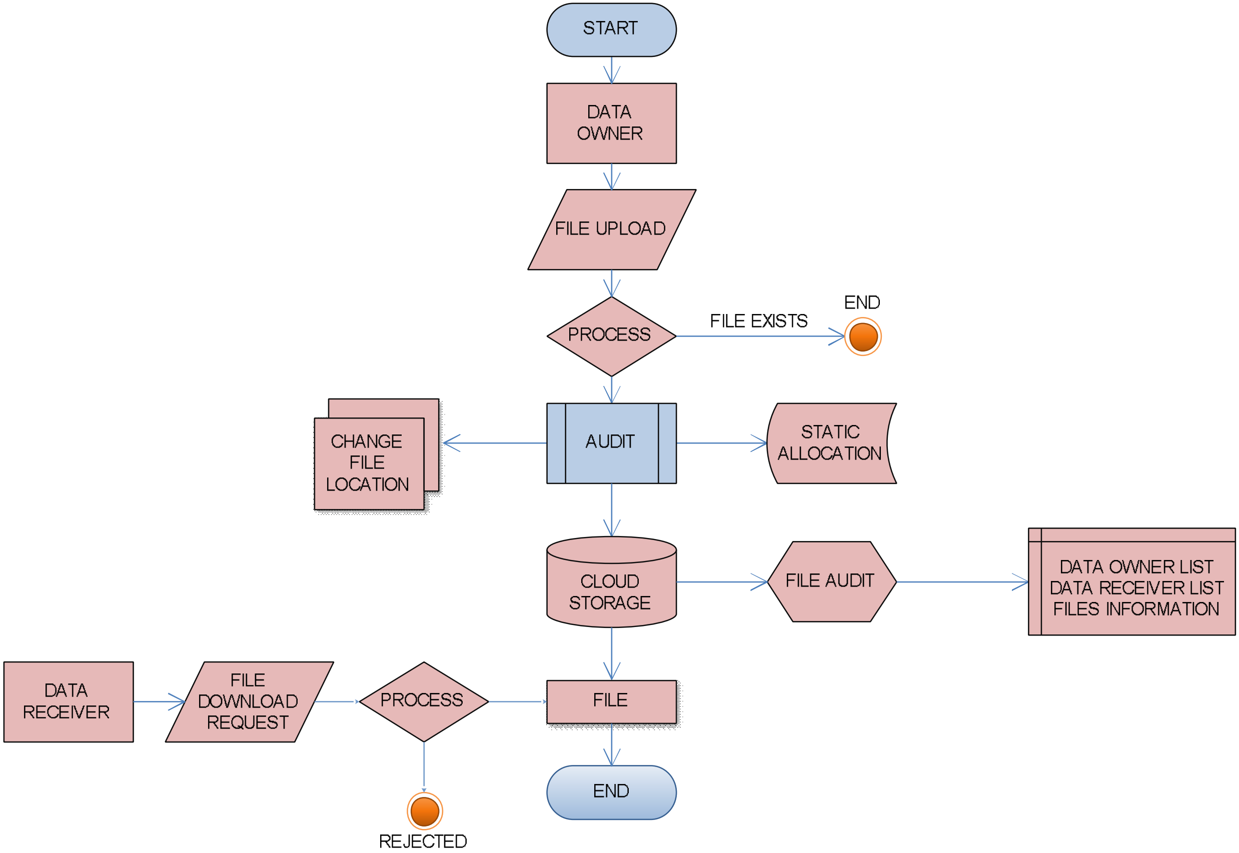

Figure. 3 Static And Dynamic Allocation With Public Auditing Scheme Flow Chart

STATIC AND DYNAMIC ALLOCATION SCHEME

STATIC ALLOCATION

Static Allocation schemes: This scheme is used to assign fixed resources present in the cloud system to the cloud user or to the applications. In this approach the cloud user must know the exact number of resources needed for the application, what type of resources and also must be capable to confirm the application’s peak load requests. The limitation attached to this approach is the under-utilization or over-utilization of the computing resources that is based on the normal workload of the application. This is not a cost-effective approach and it insufficiently uses resources during off-peak times.

DYNAMIC ALLOCATION

Dynamic Allocation schemes help cloud resources to be available on the fly. When a cloud user or an application is requested, in order to avoid over-utilization and under-utilization of resources dynamic allocation schemes are used. A possible drawback on implementing this method is that when needed resources are asked on the fly they not be accessible. Hence it is important that the service supplier allocates resources on various participating cloud data centers.Resource allocation strategy (RAS) is the process to assign scarce resources in the cloud system to be available at the point of demand.

ALGORITHM: Dynamic Allocation.

Require: job request J, datacenter's list DCi

```
Step 1:Block: B
        Step 2: launch J into resource r at $DC_i$
        Step 3:estimated B, i
        Step 4: for J in r do
        Step 5: Get current tag tag i
        Step 6: If J>B
        Step 7: Sort J in desc order with i
        Step 8:  Generate a sorted B request list J, sort J
        Step 9:  sort J
        Step10: end if
        Step 11: If J<B
        Step 12: Sort J in order
        Step 13: Generate a sorted B request list J, sort J
        Step 14: sort J
        Step 15: end if
        Step 16: Compute r at each DCi
        Step 17: laugh B based J and i
        .
```

```
    Step 18:  end for
```

Algorithm: General Fair Scheduler

```
    Require: when the slot s on the node n is available
    Step 1: sort jobs in increasing order of share
    Step 2: for j in jobs do
    Step 3: choose the best task t of job j
    Step 4:if t is good enough then
    Step 5: launch t, then exit
    Step 6:  end if
    Step 7: end for
```

MODELS FOR DYNAMIC (RA) IN CLOUD COMPUTING

In cloud computing the cost and quality of the services are decided based on their RA process. The resource provider will assign the resources in an optimal way to the clients. Still there are several RA techniques and models proposed for cloud computing. In this paper we are going to present some dynamic RA techniques and classify them based on the main strategy that is used for allocation of resources. The end result of an optimal RAS must consider specific parameters like throughput, latency and response time. We address some commonly used strategies like utility-based, service level agreement-based, priority-based and market-based strategies.

SLA based dynamic model

SLA Compliance Metamodel

SLA compliance formulation is a mixture of all the SLA models. The purpose of doing so is because to avoid violations in each individual SLA and also to have elasticity rules based on customers resource usage. Same service with same SLA can be offered to multiple customers. The Measured Metric stereotype replicates the value obtained from the monitoring system. The monitoring system collects information about the raw metrics like (e.g. service up/down time) and the SLA parameters proposed by the customers (e.g. availability of service) are not at the same level. In order to bridge this gap between measured values measures per service for each customer or per node of the system. If the SLA parameter of a service is not achieved then it indicates that the SLA has been violated. and the SLA parameters, we define OCL constraints as mapping rules. These attribute mapped Values replicates the value of the mapped measurements. A service can be a work combination of different service functionalities that can be measured or mapped similarly at the composite level. The attribute goal of the SLA parameter will decide the parameters optimization goal. For SLA parameters like availability the optimization goal is maximization and for other parameters like response time the goal is set to be minimization. The OCL constraints to avoid SLA violation is based upon these optimization goals. If a new SLA parameter is added then a new OCL constraint is not required as long as its optimization goal falls into the above mentioned categories.

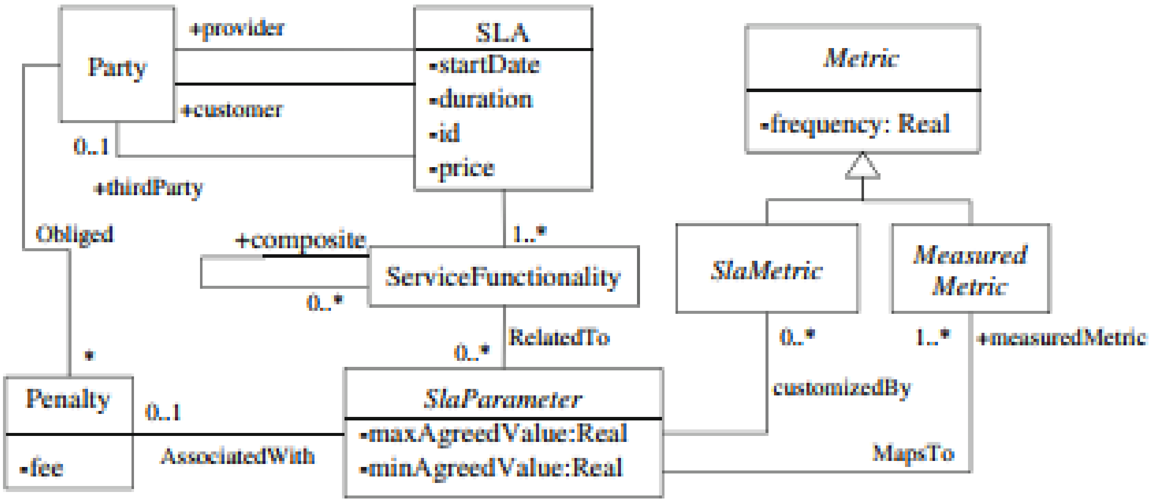

Figure.4 SLA Meta model

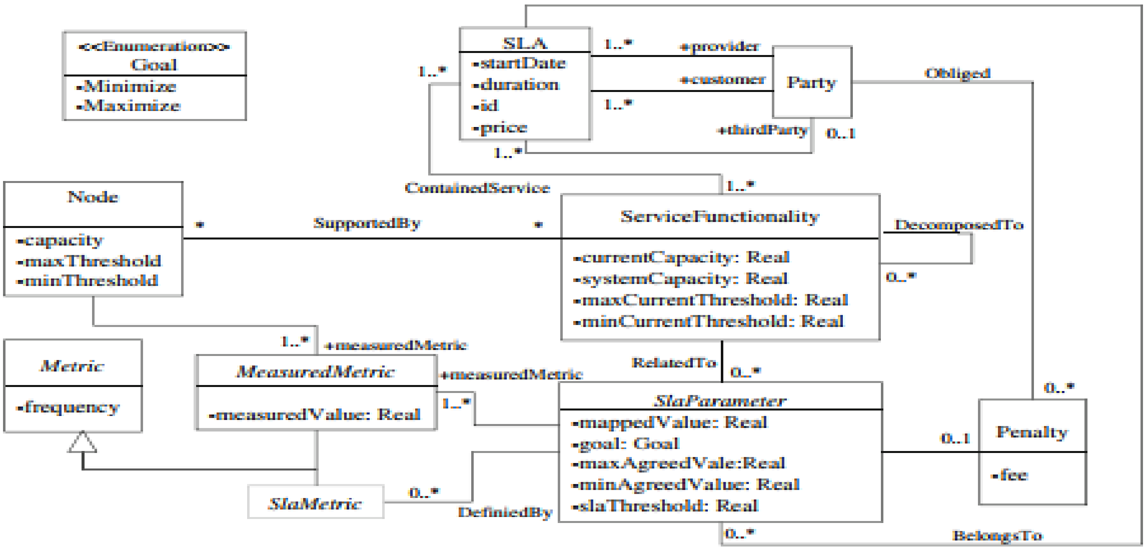

Figure.5 SLA Compliance Meta model

DATA PROTECTION

The data privacy is another important concern in Cloud computing. There must be a privacy steering committee set up to handle the decision makings that are concerned with data privacy. This will make sure that the organization is ready to face the demands that rise up in data privacy. In cloud system, data is usually distributed globally and hence it raises concerns on data exposure, jurisdiction and privacy. Organizations may have to stand for not complying with government policies if data protection is not rightly done. So for cloud vendors to expose sensitive information risk legal liability, the receiver request must be accepted by data owner and after which receiver can download original file.

RESOURCE ALLOCATION

Resource Allocation (RA) is an important field in the subject of cloud computing. It is considered in various sectors like operating systems, datacenter management, grid computing, etc. Resource Allocation means dividing the available resources between the applications and cloud users in an economic and effective way. It is a challenging task especially in cloud computing environment based on IaaS. RA for IaaS implemented in cloud computing has numerous benefits like: cost effective, hardware and software maintenance is reduced, flexible and allows users to access applications and data from any system across the world. No limitations proposed on the medium or site usage is another added advantage

4. CONCLUSION & FUTURE WORK

A cloud based system for secure data storage is proposed to entertain secure data storage in a semi-trusted environment like cloud system. In this approach the data owners can upload their private data through static allocation scheme. Data owners have the liberty to change their data location with the help of dynamic data allocation scheme. If the data receiver needs to download data then a request is sent to the authority. In this approach the authority owner has the Access Control. After this the data owner will share the secret data to the data receiver. First the request is received by the data owner and only then the receiver can download the original data. De-duplication concept is also included in this system to minimize memory space requirement.

In future there are opportunities for some extensions upon the current work. If in case the Auditor wants to modify a file that is already stored in cloud, then the file owner can perform the modification process. If Auditor needs to access data on a particular date, then it can show information about that particular date information.

REFERENCES

[1]Cong Wang, Qian Wang, “Toward Secure and Dependable Storage Services in Cloud Computing” VOL. 5, APRIL-JUNE 2012

[2]Boyang Wang, Baochun Liand Hui Li, “Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud”, IEEE Transactions on Cloud Computing, Volume: 2, Issue: 1, JAN.-MARCH 2014

[3]Sebastian Lins, Stephan Schneider, and Ali Sunyaev, “Trust is Good, Control is Better: Creating Secure Clouds by Continuous Auditing”, IEEE Transactions On Cloud Computing, TCC-2015-10-0378.

[4]CongWang, QianWang, “Privacy Preserving Public Auditing for Secure Cloud Storage”, IEEE transactions on computers, VOL. 62, NO. 2, FEBRUARY 2013

[5]Andreas Wolke, Martin Bichler, “Planning vs. dynamic control: Resource allocation in corporate clouds”, IEEE Transactions on Cloud Computing, 2013.

[6]Jianfeng Wang, Xiaofeng Chen, “Verifiable Auditing for Outsourced Database in Cloud Computing”, IEEE Transactions on Computers 2015.

[7]Jian Shen, Jun Shen, “An Efficient Public Auditing Protocol with Novel Dynamic Structure for Cloud Data” IEEE Transactions on Information Forensics and Security 2016

[8]Zhengwei Ren, Lina Wang, “Dynamic Proofs of Retrievability for Coded Cloud Storage Systems” IEEE Transactions on Services Computing 2015

[9]Xingwei Wang, Xueyi Wang, An Intelligent Economic Approach for Dynamic Resource Allocation in Cloud Services” IEEE Transactions on Cloud Computing 2015

[10]Thomas F. J.-M. Pasquier, Jatinder Singh, “ CamFlow: Managed Data-sharing for Cloud Services” IEEE Transactions on Cloud Computing 2015

[11]Gangyong Jia, Member, IEEE, Guangjie Han, “Coordinate Memory Deduplication and Partition for Improving Performance in Cloud Computing” IEEE Transactions on Cloud Computing 2015