



# INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS

ISSN 2320-7345

## DATA SECURITY AND LOAD BALANCING IN CLOUD

Ramya P<sup>1</sup>, Jayapradha J<sup>2</sup>

<sup>1</sup>M.E in KRISHNASAMY COLLEGE OF ENGINEERING & TECHNOLOGY, Cuddalore , Tamil Nadu  
Email-id: ramyafeb35@gmail.com

<sup>2</sup> ASSISTANT PROFESSOR in KRISHNASAMY COLLEGE OF ENGINEERING & TECHNOLOGY,  
Cuddalore, Tamil Nadu  
Email-id: jpanandhi@gmail.com

**Abstract:** - Cloud computing has emerged it maximum but still the security and its performance to be considered a lot. First scenario is how to handle user request multiple at time and how server respond to the situation .Second one is security issues because in cloud data are reside in outside the organization. So users have no control over their data. In existing system server and proxy server is present once server get enormous request load balancer automatically redirects to the proxy server. Once load limit exceed the proxy server limit their user not server still load decreases to overcome this server virtualization be done to manage the load. Using server virtualization technique files are dynamically created, deleted, and updated. Distributed load rebalancing algorithm is presented to cope with the load imbalance. To enhance security identity-based proxy re-encryption techniques are used to protect the authorization in cloud. user data is cryptographically protected and authorization techniques are used. It protects data from the cloud service provider. In this system multiple user send request to server it provide proper response.

**Keywords:** Identity based Proxy re encryption, server virtualization, and cloud server.

### 1. INTRODUCTION

In cloud computing, the users are increased day by day so to ensure security and performance is difficult for cloud service provider. Cloud computing provides three types of services. There are software as a service (SAAS), platform as a service (PAAS), infrastructure as a service (IAAS).we provide the service as software as a service to users. Users are not able to trust the cloud service provider. They easily use user's data and provide it to the third party. So we protect data from the cloud service provider. In existing system use rule based approach. We propose role based approach using identity based proxy re encryption [2]. This paper provides solution based on the self protected data to the cloud .To increase the performance of server because it is difficult to accommodate large number of files and accessing to that files in a particular time that is peak time. So we introduce virtualization technique to balance the load in cloud server. We are interested to review the load balancing problem in distributed file systems intended for large-scale, dynamic and data-intensive servers. Such a large-scale cloud has hundreds or

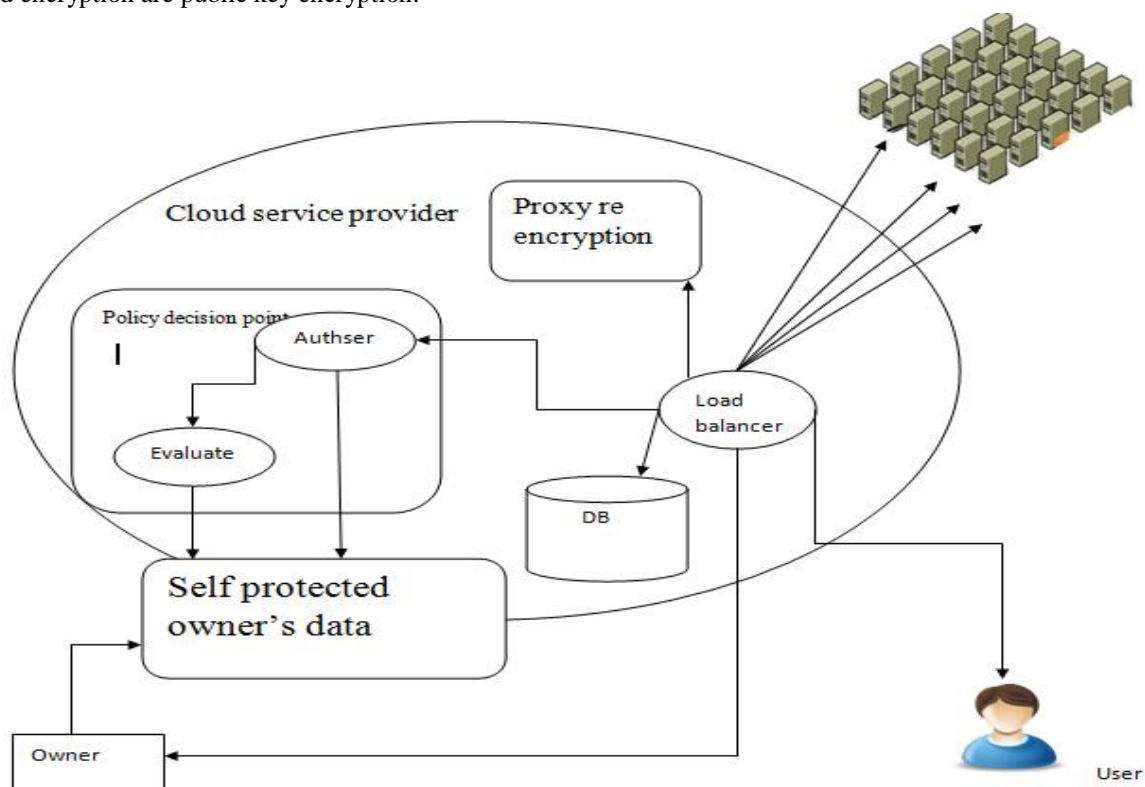
thousands of nodes. Our objective is to allocate the servers of files as uniformly as possible among the users such that server manages an excessive number of users. In virtualization the server provide the on demand service to the user without delay in network. In load balancing of several servers and one of the server failed then the service to user are not denied or waited ,the load balancer divert the processing into another user[6].

It improves the security for data owner from cloud service provider.

- It minimizes the administrative work and customer support.
- It reduces the power wastage by using dynamic server virtualization.

## 2. IDENTITY BASED PROXY RE ENCRYPTION

There are many encryption techniques and algorithms are used in cloud computing to provide security. Identity based proxy re encryption is the combined algorithm of identity based encryption and proxy re encryption. Identity based encryption are public key encryption.



**Fig: 1 system architecture**

Key pairs are generated based on the identity of owner [4]. Proxy re encryption is a modern cryptographic technique the provides proxy as a third party to re encrypt data from one key to another.

In identity based proxy re encryption allows a proxy to re encrypt encrypted data under owner's identity into another user's identity. It uses the key generation function to generate re encryption key [3]. The identity based proxy re encryption provides the solution to the data owner from cloud service provider.

Owner must register to get the access rights once, then the registered owner will get a unique Id. Owner can upload file and send to users with an encrypted key and send the data. At receiver end user need to provide the key to download the files else user can't access the files. Registered user can login to access they received files. If they need to download the received file they need to provide key which is provided by the owner for decryption.

Secondly proxy decryption is will done after trust third party key verification. Members access the cloud file upload and download.

### 3. VIRTUALIZATION

Virtualization provides a platform multiple operating systems run on a single physical server. It will maintain the status of the server, like how many users access the server. If the user limits gets exceeded or the bandwidth drops then the load balancer will create a virtual server and allocates the user to access the files without any interruption [5]. Load balancing ensure optimization by resource use, increase throughput, decrease response time, and prevent overloading there sources. Once server bandwidth rises automatically virtual server will be deleted. Similar n no virtual servers can be created.

Load balancer is used to improve the reliability and performance. If user limits get exceed load balancer will create a virtual server on demand

If user request for access

Check status

//status= bandwidth utilizing by other resource.

If (status< max bandwidth)

Allow user to access the server

Else

Create virtual server and move file

Allow member to access to virtual server

// after resource utilization

Check status of server

If (status< max bandwidth)

Delete virtual sever and update server.

### 4. CONCLUSION

For security and performance related issues there are many algorithms are existed. This paper provides the security to the data owner from cloud service providers using data centric approach. For representation and evaluation it uses the semantic web technologies. It proposed a fully identity based proxy re encryption algorithm based to provide the feasible result to cloud users. It provides the role based solution to the authorization mode [8]l. Modern cryptographic techniques are applied to protect the authorization model. In our software as service software is provided to the A effective load balancing technique gives the beneficial to the cloud users. It provides proper throughput and response time to the data requesters. [6] A server virtualization is the load balancing technique used to improve the performance of cloud application. It avoids bad load balancing by forwards traffic to the ideal server. It provides the zero downtime to the cloud user.

### REFERENCES

- [1] Cloud Security Alliance, 2003 “Security guidance for critical areas of focus in cloud computing v3.0,” CSA, Tech. Rep.
- [2] Y. Zhang, J. Chen, R. Du, L. Deng, Y. Xiang, and Q. Zhou, 2014, Feacs: A flexible and efficient access control scheme for cloud computing , in IEEE 13th International Conference on, pp. 310–319.
- [3] B. Waters, 2011Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Public Key Cryptography - PKC 2011, vol. 6571, pp. 53–70.
- [4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, 2006,Attribute-based encryption for fine-grained access control of encrypted data, in Proceedings of the 13th ACM Conference on Computer and Communications Security, ser. CCS '06, New York, NY, USA, pp. 89–98

- [5] Dharmesh Kashyap, Jaydeep Viradiya, 2014, A Survey of Various Load Balancing Algorithms in Cloud Computing” in international journal of scientific & technology research volume 3, pp.36-40
- [6] Ankush P. Deshmukh, Prof. Kumarswamy Pamu,2012,Applying Load Balancing: A Dynamic Approach, in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 6, pp 20-25
- [7] B. B and V. P, 2014, Extensive survey on usage of attribute based encryption in cloud, in processing of Journal Emerging Technologies in Web Intelligence, vol. 6, no. 3.
- [8] V Bozovic, D Socek, R Steinwandt, and V. I. Vil-lanyi, 2012,Multiauthority attribute-based encryption with honest-but-curious central authority in International Journal of Computer Mathematics, vol. 89,pp. 3.

#### AUTHOR’S PROFILE

**P. RAMYA** is presently pursuing her M.E degree in computer science and engineering at Krishnasamy College of Engineering and Technology, Tamilnadu, India. She has received her B.TECH degree in I.T from Info institute of engineering, Tamilnadu, India. Her research interests are in the areas of Mobile computing, Networking.

**J. JAYAPRADHA** received B.E CSE degree from Dr.Pauls Engineering College and M.E CSE degree from Hindustan College of Engineering and Technology. She is working as Assistant Professor in the department of computer science at Krishnasamy College of Engineering and Technology, Cuddalore, Tamilnadu, India. Her research interests are in the areas of Operating system, Compiler design, and Distributed system.