Security and Load Balancing In Cloud Computing

Tejashri Khandve
UG Student
Dr. D.Y.Patil School of Engineering and Technology
Savitribai Phule Pune University

Megha Talekar
UG Student
Dr. D.Y.Patil School of Engineering and Technology
Savitribai Phule Pune University

SheetalDhiwar
UG Student
Dr. D.Y.Patil School of Engineering and Technology
Savitribai Phule Pune University

Madhuri Patil
Assistant Professor
Dr. D.Y.Patil School of Engineering and Tech
Savitribai Phule Pune University

Abstract

The Attribute based accessto extensible media in cloud to help sharing the contents to the network.The data encryption standard cipher text policy algorithm is use. It's a important to protect the data from unauthorized access. Media contents such as images, audio, video, and text etc..These contents are protected by this security method. . All the storage is done on cloud so the security of data is threatened. So there is need to secure the data on the cloudThe public cloud services are sent to the client by internet. The load balancing technic is use in cloud computing.Cloud Load Balancing simply means doing load balancing, i.e. allocate workload across different servers, network channel, CPU, disk drives, on the cloud, i.e. inside the Internet itself. This method is use helps to obtain , as other load balancing methods, helps to achieve optimal system utilization**,** maximumthroughput**,** minimum response time**,** and prevent overload of system.

General Terms

Access control, cloud computing,load balancing, scalable media, data security, encryption and decryption.

Keywords

C.2.0.Security and protection, D.4.6.Access controls,D.4.6.Cryptographic controls, C.2.0.Data*Encryption,*H.5.1.Multimedia *Information System*

I. Introduction

Now days all the storage is done on cloud so the security of data is threatened. so there is need to secure the data on the cloud.Content sharing network are very effective in terms of online users, storage requirement, network bandwidth etc.so it is not easy for a service earner.

The attribute base access control is a authorization model that provides dynamic, situation-wise and risk-intelligent access control. It helps achieve efficient administrative conformity, effective cloud services, diminished time-to-market for new applications, and a top-down way to governance through transparency in method administration.

Yet, it is challenging to design a correct access control system in content sharingworks due to:

1) Any singular is capable to produce any kind of online multimedia. And multimedia includes text, audio, video, animation contents.2) any singular is capable to several access to his media to everybody, at any time.3) Any singular can publish a maximum number of attributes (e.g. name, age, address, hobby, personal interest, gender, etc.4) Individuals can share contents using different devices and bandwidth. So use different access advantages for the same media**.**

A promising way to access control in sharing the content services. In this services is the entrust users to apply access rules on their data straightly, through administrator. However, access control policies are complicated because this requires soft and extensible cryptographic key management that's why

support for access control method is complicated. In Cipher text ABEcipher text is fixedwith an access control procedure. For the encryption and decryption technic we use data encryption standard algorithm. The cipher text attribute base encryptioncan be seen asone to severalpublic key encryptionplans; thereforea data owneris supportto grant access tostrangeset of users.

Cloud computing is the use of hardware and software computing resources via internet.

Load balancing technic is the process of improving performance in cloud computing. In load balancing distribution of loads among the processors. As the importance of or use of web increases every day, so there is need to increase the requirements of load balancing. . Cloud Load Balancing simply means doing load balancing, i.e. allocate workload across different servers, network channel, CPU, disk drives, on the cloud, i.e. inside the Internet itself. This method is use helps to obtain , as other load balancing methods, helps to achieve optimal system utilization**,** maximum throughput**,** minimum response time**,** and prevent overload of system. In this system we are use skewness algorithm for load balancing technics and binary encryption technic is use for encryption and decryption.

I. RELATED WORK

Control model is the concept of attributes , that attached user as well as resources. The content sharing works dynamically for mapping identity and resources of users. This method's work in to two categories

A. User Attribute Oriented Access Control

Easier is one of the technology which can be used for user attribute access control policy and dynamic control policy using CP-ABE scheme. It assign new keys. In CP-ABE it assign the keys to authorized user by using the attributes of user and particular file.

The keys will be provided only on the mail_id of authorized user so the file will be secured.

The methods like attribute based encryption , Proxy re_encryption, and Lexy Encryption are used in CP-ABE.

General Encryption method's used number of keys it is very difficult to manage such a large number of keys. So the our method we are going to assign a access based attribute and so the management of keys will be minimize to some extend

B. Media Structure Oriented Access Control

SSS is one of the encryption method for videos and it may result in failures while description and lead to packet losses and information inconsistency and so the error correction apply to techniques is needed to apply to SSS.

JPEG2000 is one of the technique efficient and sequence and it is follows the flexible scheme that the "Encrypt once , Decrypt more than one ways ".

In this media structure only assign the key and do not deal with the assign user to access privilege so there must be a media structure that knows how to assign user attribute to access privilege.

C. CP-ABE

A Security model for Cipher text -Policy Attribute Based Encryption technic. An every user's personal secret key is associated with a set of attributes while every Cipher text with an access format and the private keys with aspects. A user successfully decrypts a Cipher text- Policy only if her of aspects satisfy the access rule specified in the Cipher text.

This scheme has four different algorithms: Setup, Encrypt KeyGen, And Decrypt.

We will extend this CP-ABE scheme to MCP-ABE scheme and use the latter in our access control scheme

- *AB-Setup*

This algorithm takes no input other than the implicit security parameter as input a security and gain a public key PK and a master secret key.

- *AB-KeyGen*

  This methodtakes as inputMK and the set of attributes A of the user, and gains a private keySK, for each user.

- *AB-Encrypt*

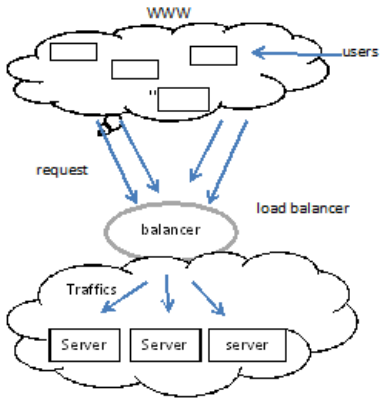
  This method takes as input the public parameters PK. Data ownerto encrypt a message according.

- *AB-Decrypt*

  Data consumer in possession of a group of aspects A and the private key SK in order to decrypt the cipher-text CT with an access method.

C. Load Balancing

Load Balancing is aapproach of allocate workload beyond multiple computing resources such as collection of computers, network channel.



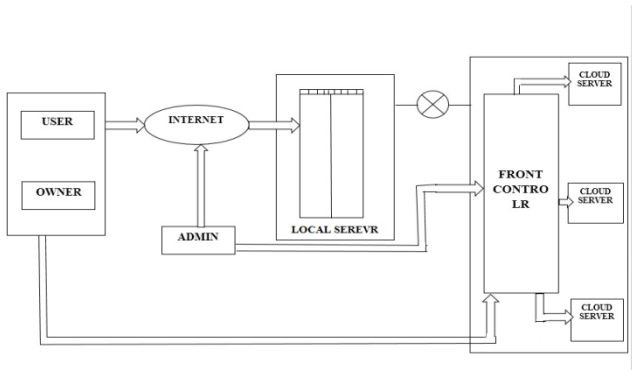
Cloud hosting enviroment

The Objectives of load balancing are:

1. Performance
2. Throughput
3. Fault tolerance
4. Migration
5. Response time
6. Scalability

III.RELATED WORK

i. System architecture



ii. System Architecture:-

1) **Backend Server**:-Backend server is framework of the cloud computing platform. Cloud Computing is defined as type of computing that released on sharing computing resources rather than having local server or personal devices to handle for Example- Network, application, Services , Servers. It can be assumed that it has sufficient storage capacity and computation power. Hence, from the direction of network services provider cloud computing significantly decreases the traffic and storage requirements incurred by their application.

2) Foreground Server:-

In this server the service provided to only those applicants how are always online. This server is usually operated by Cloud Services Provider (CSP). Sometimes a user is also able to run his/her own service on the cloud platform. Web Service , Database Service, Media maker service, Media de-coding service are the service of foreground server

3) Attribute Authority:-

It is a reliable third party which groups up the system guideline of Attribute Based Encryption system checks every users attribute and issue personal secret key parallel to the set of attribute of the user. Practically there cloud multiple. AAs in a system Ex- A corporate may run an AA and a user may act as an AA for his/her extended family**.**

4) Data Owner or User Modules:-

Customer may be a data owner or data consumer or both . A data owner produces media content and uploads the media content to cloud server to have accesscontrol to his dataowner assigns access privileges to data users whom the data owner may or may not a user module download media content of his/ her interest from cloud server and gets content based on attribute and the access policy of the data owner. The user module must get a personal secret key bound to her of attribute from AA at end.

IV. Future Scope

Easier is one of the technology which can be used for user attribute access control policy and dynamic control policy using CO-ABE scheme. It assign new keys. In CP-ABE it assign the keys to authorized user by using the attributes of user and particular file.

The keys will be provided only on the email_id of authorized user so the file will be secured.

The methods like attribute based encryption , Proxy re_encryption, and Lexis Encryption are used in CP-ABE.

General Encryption method's used number of keys it is very difficult to manage such a large number of keys. So the our method we are going to assign a access based attribute

and so the management of keys will be minimize to some extend

V. Conclusion

In order to share media content in a controllable manner, a suitable access control mechanism should be deployed. CP-ABE based access control allows a data owner to enforce access control based on attributes of data consumers without explicitly naming the specific data consumers. However, CP-ABE supports only one privilege level and hence isnot useful for access control to scalable publishing. In this paper we extended CP-ABE to a novel MCP-ABE. As cloud computing is increasingly being adopted and control scheme allows a mobile user to offload computational intensive MCP-ABEoperations to cloud servers during without compromising user's privacy. The experimental results indicated that the proposed access control scheme is efficient for securely and flexibly managing media content in large, loosely-coupled, distributed systems. With the assistance of the cloud server, the decryption operation is accelerated significantly at the consumer side. However, the decryption may be still slow for low-end devices because a modular exponentiation operation is requiredThe load balancing in cloud has imported collision on the performance. Good load balancing makes more efficient and improve user fulfillment in cloud computing**.** Thus, one future work is how to speed-up the decryption operation at low-end devices.

VI. ACKNOWLEDGMENTS

We would like to thanks those people who have guided us for doing this serveyof Various Load Balancing Techniques.

VII. References:

[1] E. Mesmer, "Are security issues delaying adoption of cloud computing?," *Network World*, Apr. 2009 [Online]. Available: http://www.networkworld.com/news/2009/042709-burning-security-
cloud-computing.html

[2] http://en.wikipedia.org/wiki/Load_balancing_(computing)

[3] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attributebased encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.

[4] *National Inst. Standards and Technol., Secure Hash Standard (SHS)*, FIPS Publication 180-1, 1995.

[5] P. Mell and T. Grance, "The NIST Definition of Cloud Computing,"NIST Special Publication 800-145, 2011.

[6] M. D. Soete, "Attribute certificate," in *Encyclopedia of Cryptography and Security*, H. C. A. Van Tilborg and S. Jajodia, Eds., 2nd ed. Berlin, Germany: Springer, 2011, p. 51.

[7] B. Carbunar, Y. Yu, W. Shi, M. Pearce, and V. Vasudevan, "Query privace in wireless sensor networks," *ACM Trans. Sensor Networks*, vol. 6, no. 2, 2010, Art. ID 14.

[8] X. Zhang, M. Nakae, M. J. Covington, and R. Sandhu, "Toward a usage-based security framework for collaborative computing systems," *ACM Trans. Inf. Syst. Security*, vol. 11, no. 1, pp. 1–36, 2008.

[9] S. Jahid, P.Mittal, and N. Borisov, "EASiER: Encryption-based access control in social networks with efficient revocation," in *Proc. ACM Symp. Inf. Computer Commun. Security*, Mar. 2011, pp. 411–415.

[10] S.Yu, C. Wang,K. Ren, andW. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE Int. Conf. Comput.Commun.*, 2010, pp. 1–9.

