International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

Increasing Security in Cloud Based Services

Sandeep B. Gholap
Computer Engineering AISSMS COE PUNE
Pune, India

Sunil K. Sonawane
Computer Engineering AISSMS COE PUNE
Pune, India

Abhishek R. Golande
Computer Engineering AISSMS COE PUNE
Pune, India

V. S. Vairale
Computer Engineering AISSMS COE PUNE
Pune, India

***Abstract*—A cloud computing is one of hottest research due to its ability to reduce costs associated with computing while increasing scalability and flexibility for computing services .Cloud Computing is a term which involve virtualization ,distributed computing networking ,software and web services .A cloud consist of several element such as client, datacenter and distributed server. It consist of fault tolerance, high availability ,scalability, flexibility on demand on service etc. Security of information is challenging task. In this paper high level of security provided to cloud based services by using some standard encryption decryption algorithm. The primary goal is to create system to secure all type of information by using some standard algorithm. In this system we are providing web services are data upload and retrieval**

Keywords:Encryption,Decryption,Cloudcomputing,SHA,Integrity ,Confidentiality,Cloud Security

I. INTRODUCTION

In recent year new term call "cloud" has been evolved which is provided by different provides. A cloud is nothing but facility or services of different resources or component like hardware ,platform, storage's ,software etc. and it is gaining importance because it frees user from maintainance perspective on investment of some money for the use of some services provided by cloud service providers. Now provide such service to the client naturally the provider's must have and rather can have access to resource which are used by the peoples/clients. Among the reason these access are greatly required are for maintenance perspective. And definitely since billions of clients will be thinking to use the services, the infrastructure thought to be capable enough to support them, and these resources thought to be shared between billions of clients. Service avaibility, data synchronization between different devices avaibility of a data via any devices which include browser facility make cloud more attractive. Now since the information gets shared or stored in providers area, the client get worried about privacy of its data although there are several agreement for secure data and SLA which are agreed by cloud provider and clients. . Now although client have a platform to generally share the info, the expense of securing his/her data or in a nutshell making its data private gets costlier .

The cloud term is of interest not just to the patient clients but to organizations as well. With organization as a consumer the concern of data security becomes multifold. Consider a typical example of small scale business that has different departments like HR, Finance, etc. We will focus on finance department since finance details of any business/ company/organization is considered to be very sensitive and must be confidential. Therefore if the little scale company thinks of using the cloud services like storage. Storing all account/finance related information in cloud stored makes it prone to leakage of sensitive information tells un-authorized users. Therefore securing this finance data is vital before it gets uploaded to the storage cloud, and just in case the data stored in cloud storage gets tampered there should be a method to verify the integrity of the data, moving further specific band of people should have access to this data which may be folks from finance department of client company or special auditors. Simply speaking the client must have the ability to store the data securely, verify the integrity of the data, share the data securely with specific band of people.

II. RELATED WORK

According to the 3 dimensional security in cloud computing by Parikshit Prasad, Badrinath Ojha, Rajeev Ranjan shahi, Ratan Lal ,Abhishek Vaish, Utkarsh Goel [2]they are focus on the problem of data leakage and process framework in two phase . First phase is known as data classification is done by client before storing the data. During this phase data is characterized on the basis of CIA (Confidentiality, Integrity,Avability).The client wants to give the value for C,I,A.The value of C is based on the basis of secrecy it prevent unauthorized disclosure, value of I is based on how munch assurance of accuracy is provided reliability of information and unauthorized modification is required and value of A is based on how frequently it is accessible. By using proposed formula priority rating is calculated. Data

having higher priority is critical and is recommended for 3D security.

After completion of the first phase data is send to storage uses 3 dimensional security. Now if there is third entity i.e another customer wants to access the data he wants to register first to the organization. He need authenticate before access to the data.as show below in fig 1

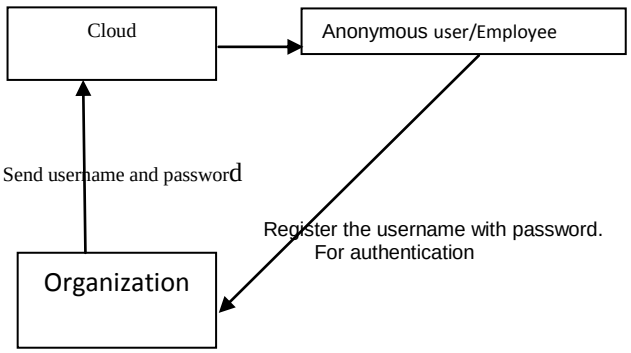

Fig1.General Framework

According to our proposed system if client wants to secure the data then he wants to register first.The data/information which he/she want to secure can upload .Then two keys are calculated i.e public and private keys.Then keys are stored on the encryption server and encrypted data are stored on the store on the storage server.There is no need for client to give value for confidentiality,integrity and avability.Two keys i.e public key and private key are stored on the encrypted server threfore there is need to remember the keys . Storage server store the data in encrypted format so admin can not access the data.

III. WORKING OF PRAPOSED SYSTEM

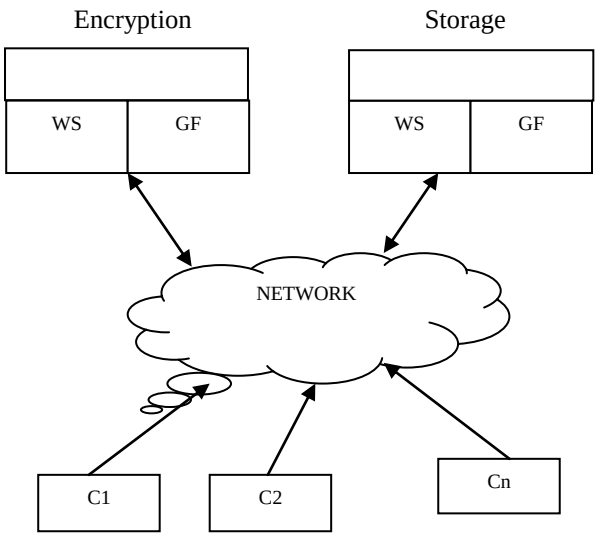

Fig2.Block Diagram

The proposed system consist of encryption-decryption server, storage server and clients as shown in fig 1The system provides hash, access list, encryption and decryption service trusted by third party client ie TCP. Over the network which can provide Saas i,e Software as aService.The third party i.e. the TCP provide service security and does not store data at its ends. The third party client can store the master key for the purpose of encryption and decryption. The third party client can secure data by using standard RSA algorithm .The RSA[1] algorithm can secure the data store by client using public key and private key. The encryption can be done by using public key and decryption can be done by using private key. The system also provides functionality where other users from small scale Business Company will be able to access data which is stored in cloud storage. The sessions between client and security server is secured using RSA[1] as the encryption algorithm. SHA1 is used for calculating the hash of the data, and RSA is used encryption/decryption algorithm for computing cipher at security server end.

A. Upload Service.

The system provide upload service i.e. the client can upload the data in any formats like docs,jpg etc .For the uploading purpose client can sign in with its unique username and password .If the client cannot registered then sign up service is also provided .For the upload purpose client must have to connect first with the third party client i.e the encryption server. The encryption server can encrypt the data by using RSA algorithm. The encryption can be done by using public key.The third party client can store the keys not the actual data. The encrypted data can send back to the client .Then client must have connect to the storage server which can actually store the data. The storage server can store the encrypted the data.

B. Download Service

The system can also provide download service where client can choose the file from the retrieval list. For the downloading i.e retrieving file the client first have to connect to the storage server. The storage server can send encrypted data send back to the client .The data send by storage server to the client is not in proper format i.e encrypted format.For the proper format data client must have to connect to the encryption decryption server .The encryption decryption server can decrypt the data by using digital signature extraction .The decryption can be done by using private key.The decrypted data i.e data in proper format can be send back to the client.

IV. CONCLUSION

We have seen how delegation of responsibility trusted 3rd party which provides security services secures user data. It reliefs the client from maintaining any kind of key information and allowing the client for using any browser enabled device to access the cloud services. It allows the client to verify the integrity of the data stored on download or retrieval of its own stored data in cloud. The client can

share the data securely with specific band of people without any overhead of key distribution..

ACKNOWLEDGMENT

We would like to thank all the professors of Computer Engineering Department of AISSMS College Of Engineering, Pune -01. We are indebted to Ms. V.S.Vairale our project guide who was very generous in providing us with technical-support, material and otherwise. Her invaluable suggestion and time have helped in making this project possible. Nonetheless we would like to thank her constant help and support.

REFERENCES

[1] Ron Rivest, Adi Shamir, and Leonard Adleman fire published in 1977 " RSA algorithm"

[2] Parikshit Prasad, Badrinath Ojha, Rajeev Ranjan shahi, Ratan Lal *Abhishek Vaish, *Utkarsh GoelIndian Institute of Information Te chnology, Allahabad U.P India "3 dimensional security in cloud computing" 2011

[3] Balachandran reddy Cloud computing security issues and challenges, et al, 2009

[4] Weinshall, D. "*Cognitive Authentication Schemes Safe Against Spyware* (Short Paper)". IEEE Symposium on Security and Privacy, 2006."

[5] Jing-Jang Hwang, Hung-Kai Chuang,Yi-Chang Hsu, Chien-Hsing Wu, "A BusinessModel for Cloud Computing Based on a Separate Encryption and Decryption Ser-vice," Proceedings of the 2011 International Conference on Information Science andApplication, April 2011.

[6] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. Atanu Rakshit, "CloudSecurity Issues", IEEE International Conference on Services Computing, pp. 517-520, September 2009.

[7] Ling Li, Lin Xu, Jing Li, Changchun Zhang,"Study on the Third-party Audit in Cloud Storage Service", 2011 International Conference on Cloud and Service Com-Putting

[8] A. Parakh and S. Kak, "Online data storage using implicit security", Information Sciences, vol. 179, issue 19, pp. 3323-3333 ,September 2009.

[9] William Stallings, "Cryptography and Network Security", 2009. Peter Mell, Timothy Grance, "The NIST De_nition of Cloud Computing", NISTSpecial Publication 800-145C.

[10] Heiser j Nicolett M. Assessing the security risk of cloud computing http://www.gartner.com/displaydocument? Id=685308, 2008

[11] Ensuring Data Storage security in cloud computing, Cong Wang, etal 2010

[12] Inforamtion security risk management framework for cloud computing environments, Xuan Zhang etal, 2010