Dynamic Data and Mutual Trust For Cloud Computing Storage System

Vaishali B. Kolate
M.E. student Computer Engg
PVPIT ,Pune, India.
Vaishali.bkolate@gmail.com

Abstract : **Many organizations are producing a large amount of data which they need to store But storing such a large data is somewhat problematic at a local storage area. So this system provide storage as a service facility and cloud service provider. This system allow the different organizations to store data at remote site by paying some amount as per the usage. Thus it minimizes the overhead of storing a large data at local storage.**

Keywords-Storage as a service , cloud service provider.

I: INTRODUCTION

Cloud computing has important advantages including: cost effectiveness, low management overhead, immediate access to a wide range of applications, flexibility to scale up and down information technology (IT) capacity, and mobility where customers can access information wherever they are, rather than having to remain at their desks. It is a distributed model over a large pool of shared-virtualized computing resources. Cloud service providers offer different classes of services Storage-as-a-Service , Application-as-a-Service, and Platform-as-a-Service that allow organizations to concentrate on their core business .

Currently different organizations produces different information like personal , electronic health data, financial transactional information. Digital data amount is also increasing so rapidly . This data needs to be get distributed over a wide area as local management of such huge amount of data is problematic and costly. Storage-as a service offered by this cloud service provider is used to avoid maintenance cost of different business and provide high storage facility. CSP provide this storage facility for customers in exchange of fees measured in GB/month. Because of this storage system different owners store their data on remote server instead of local storage area . CSP provide the recovery system for stored data for this facility it store different duplicate copies of data on different sites. Because of this storage facility different authorized users can access their data remotely from any location. As owners store their sensitive data to CSP storage they want confidentiality, integrity, and access control of their data. Data confidentiality is very important issue. For example, in e-Health applications the data should have privacy and it should follow some policies so that is should not display any personal information to unauthorized users.

II : PROPOSED SYSTEM

It includes file splitting process, which means storing of data into multiple servers. We propose the system with the data stored in the cloud may not only accessed but also be frequently updated by the users. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. In this work, we propose a scheme that addresses important issues related to outsourcing the storage of data, namely *dynamic data*, *newness*, *mutual trust*, and *access control*. The remotely stored data can be not only accessed by authorized users, but also updated and scaled by the owner. After updating, authorized users should receive the latest version of the data (newness property), i.e., a technique is required to detect whether the received data is stale. Mutual trust between the data owner and the CSP is another imperative issue, which is addressed in the proposed scheme. A mechanism is introduced to determine the dishonest party, i.e., misbehavior from any side is detected and the responsible party is identified. Last but not least, the access control is considered, which allows the owner to grant or revoke access rights to the outsourced data.

System architecture:

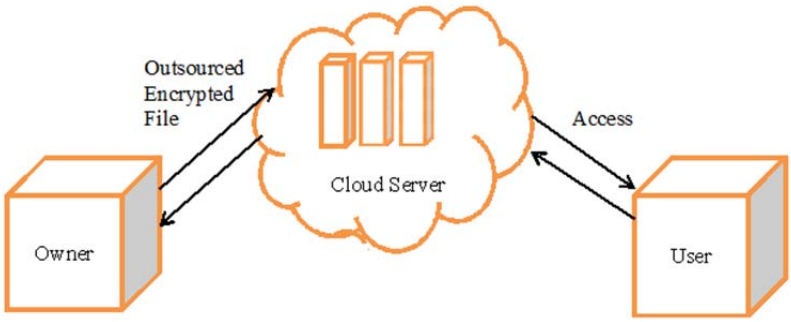


Fig 1:Proposed system architecture diagram.

System Modules:

(i)Data Owner Management

(ii) Secure Cloud Storage

(iii)User Controls Management

(iv)TTP Monitoring

(v)CSP File Verification

Module Descriptions

(i)Data Owner Management

(i)The Data Owner Management is important role in cloud storage to check the confidentiality.

(ii)In this module, the data storage must be authenticated for the data provider since the data provider can be a intruder or can misuse others data of the providers.

(iii)First the data owner will login by using their authenticated user name and password.

(iv)If their user name and password gets matched then they can login to store the cloud user data in the cloud storage.

(v)If it does not match then they have to go for the new registration to register by self.

(vi)In the new registration, they have to give the basic information about themselves and then will give the course details and number of sessions they need to store on the cloud.

(ii)Secure Cloud Storage

(i)The Cloud Storage is available to multiple users in public. So the storage must be in a very secure manner to avoid hacking by anyone who is unauthorized.

(ii)In this module, the cloud storage will be secured using the cryptographic algorithm.

(iii)the Data Owner files will be created from their requirements.

(iv)Once they created multiple folders to store the data they will go for the data storage.

(v)The data which are going to be stored in the particular folders will be first encrypted using a private key of the data owner.

(vi)Then the encrypted form will be stored in the given path for data usage by the data user.

(iii)User Controls Management

(i)The user authentication is the mail drawback of the cloud storage since the multiple users have rights to access the data in the legal manner.

(ii)To avoid the misusing of the data, the data accessing users must be first validated before they access the cloud storage.

(iii)In this module, the user must login in using the authorized user name and password.

(iv)If their given username and the password get matched then they will be allowed to proceed in further performances.

(v)Else they will not get any access right to read any of the contents from the cloud storage.

(vi)Once they are validated they can update their payment for the particular sessions and know their remaining amount needs to be paid.

(vii)They can view the cloud storage data as much they paid for their particular sessions and remaining data can be viewed in the encrypted form as per their access rights given by the data owner.

(iv)TTP Monitoring

(i)The TTP is the trusted third party who perform the key matching and file validation before the data accessing by the data user.

(ii)In this module TTP gets the hash code for the data owner file from the data owner.

(iii)The hash code of individual file will be stored in TTP data base which can be reused for the future hash code matching.

(iv)Once it gets the request for a data owner file form the Cloud Service Provider it retrieve the particular files hash code to perform the hash code matching validations.

(v)If the hash code generated by both the data owner and the provider gets matched they inform the data provider that the file is unmodified and there is no mismatching in the hash codes.

(vi)If they do not match it says something gets modified in the owner data to the data provider.

(v)CSP File Verification

(i)CSP stands for the Cloud Storage Provider is the one who provides the cloud storage data for the paid users.

(ii)CSP can get the file request from the data user to provide the requested file for the data user.

(iii)Once it gets the request it will make a request to the TTP to perform the file verification.

(iv)If the reply from the TTP is positive then it provides the requested file from the data owner and delivers it to the requested data user.

(v)Else it stops the accessing of the file for the particular data user.

Mathematical Model :

Definition 1 : Two integers a and b are relatively prime if their greatest common divisor is 1.

That is , gcd(a,b) = 1.

Definition 2: Euler's totient function $\varphi(N)$ is difined as :

If N is prime,

$\Phi(N) = N-1$;

If $N = N_1 N_2 \ldots N_k$ and

i, j : [1..k].N_i and Nj are relatively prime,

$\varphi(N) = \varphi(N_1) \varphi(N_2) \ldots \varphi(N_k)$.

Definition 3: A key K is a pair<e,N> , where n is a product of distinct primes and e is relatively prime to $\varphi(N)$;e

is the exponent and N is the base of key K.

Definition 4 : The encryption of a message m with key K = <e,N> denoted as [m.K], is defined as

$[m,<e,N>]= m^{e \bmod N}$.

Definition 5 : the matching key K = <e,N>,denoted as K^{-1}, is a pair <d,N>, satisfying ed=1mod φ(N) where "=" is the congruence modulo relation. K can decrypt the message encrypted using K^{-1}, and vice versa. That is, $[[m,K,K^{-1}] = [[m,K^{-1}],K] = m$.

In the RSA cryptosystem a pair of matching keys is called a public/private key pair.

Definition 6: Two keys $K_1 = <e_1,N_1>$ and $K_2=<e_2,N_2>$ are compatible if $e_1=e_2$ and N1 and N2 are relatively prime.

Definition 7 If two keys K1 = <e,N1> and K2 = <e,N2> are compatible , then the product key , K1*K1, is defined as <e,N1,N2>. Compatible keys. For any message m such that m <= Ni,

$[[m,K1\times K2\times\ldots\times Kn],k^{\wedge-1}] = m$,

Where $K^{\wedge-1}$ is matching key of key K^ and

$K' = K_{x1} \times K_{x2} \times \ldots. \times K_{xp}$ such that

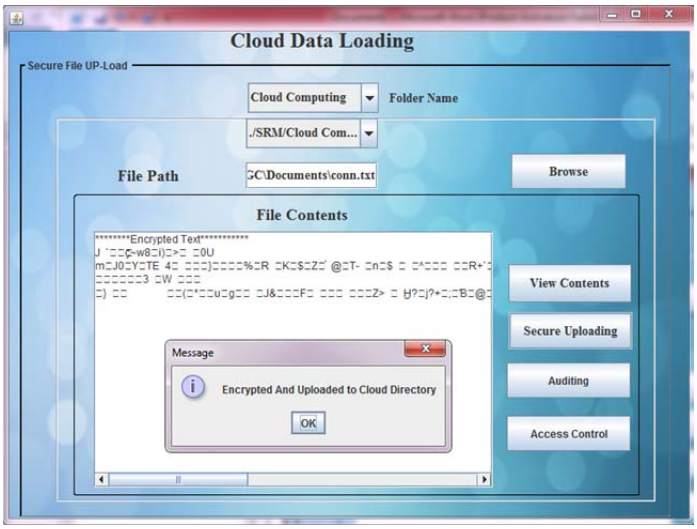
$1 \le xi \le n$,$1 \le i \le p$ and $x_i \neq x_j$ if $i \neq j$.

In Theorem 1 , K^ is key that is formed by the subset of keys in the set $K_1, K_2 \ldots K_n$. Theorem 1 states that is message is encrypted using product key that is formed with all the keys in $K_1, K_2 \ldots K_n$, then the matching key of K^ , i.e, $K^{\wedge-1}$, can be used to decrypt the encrypted message for example assume that K_1 , K_2 and K_3 are compatible keys , a message encrypted with product key $K_1 \times K_2 \times K_3$ can be decrypted using any of the keys in the set

$\{K_1^{-1}, K_2^{-1}, K_3^{-1}, (K_1 \times K_2)^{-1}, (K_1 \times K_3)^{-1}, (K_2 \times K_3)^{-1}, (K_1 \times K_2 \times K_3)^{-1}\}$

IV: RESULT

By using this proposed system remote users can store their files on remote servers. The remotely stored data can be not only accessed by authorized users, but also updated and scaled by the owner.



Above screen shows that file get stored at remote site in an encrypted format. When we calculate the computation overhead of system in response to number of customers following graph occure.

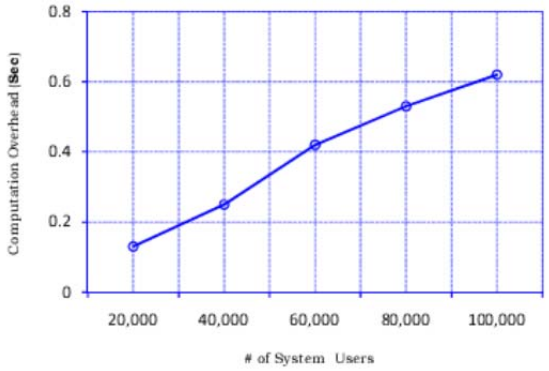


Fig 2:owner's average computation overhead due to dynamic operation

V : CONCLUSION

In this we proposed the cloud based storage system which provide the facility to store the large amount of data from different owners dynamically on different remote sites. This also provide facility to perform different operations on the file data block like modify , add, delete files. In this we have implements different cryptographic technique like lazy revocation, broadcast encryption, digital signature for providing the different security features to the data block.

ACKNOWLEDGEMENT

I have worked with full support of my guide Prof. Y. B. Gurav . great spirit, very patiently with full interest on making high performance computing based project and eventually after a long research throughout, have made a project report entitled "Dynamic data and Mutual Trust for Cloud Computing Storage Systems"

REFERENCES

[1] A. Singh and L. Liu, "Sharoes: A data sharing platform for outsourced enterprise storage environments," in Proceedings of the 24th International Conference on Data Engineering, ICDE. IEEE, 2008.
[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. Provable data possession at untrusted stores. Cryptology ePrint archive, May 2007.
[3] F. Sebe, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," Knowledge and Data Engineering, IEEE Transactions on, vol. 20, pp. 1034 –1038, aug. 2008.
[4] Z. Hao and N. Yu, "A multiple-replica remote data possession checking protocol with public verifiability," in Data, Privacy, and E-Commerce, September 2010.
[5] Venkata Pallavi , E.Padma "Authentication based remote data possession in multi-cloud storage" International Journal of Science, Technology & Management Volume No 04, Special Issue No. 01, March 2015.
[6] Vaishnavi V R , Senduru Srinivasulu , Divya C "Data veracity verification and cryptography algorithm for health care systems using cloud technologies" International Journal Of Pharmacy & Technology Vol. 8 , Issue No.1 March-2016.
[7] Khaba M.V , M.Santhanalakshmi "Remote Data Integrity Checking in Cloud Computing" International Journal on Recent and Innovation Trends in Computing and Communication ISSN 2321 – 8169 Volume: 1 Issue: 6 553 – 557 JUNE 2013.
[8] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "SiRiUS: securing remote untrusted storage," in NDSS, 2003.
[9] F. Brick, "Are you ready to outsource your storage?" *Computer Technology Review*, June 2003.
[10] Amazon Storage Service., *http://aws.amazon.com/s3*.