ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 427- 430 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

An Empirical Model of Secure Data Sharing between Multi Data Owners

[1]**Padmashree,** [2]**V. Vidya Sagar**
[1]Final M.Tech Student, [2]Associate Professor
[1,2]Dept of Computer Science and Engineering
[1,2]Pydah College of Engineering, Visakhapatnam, AP, India

Abstract: Cloud computing is one of the interesting research issue now days of recent technology, due to its services , features ,low -maintenance and high quality on demand service to cloud users. Multiple data owners can share the data component securely with authentication. In this paper we are proposed the concept digital certificate for user authentication and key establishment. By providing security of data in the cloud we are using Triple Des for encryption and decryption of data. So that by using those techniques we can provide more security and low maintenance of characteristics.

INTRODUCTION

Cloud is a resource area, it can be used either software as service, database or storage area as service or virtual system as service and infrastructure as service ,everything is possible with cloud in pay and use manner, so many service providers available to provide services to cloud users such as Amazon with data centers[1].

End user can easily avail the services and resources which are provided the data owner. Data owner uploads data components to cloud server. Third party auditor monitors data components which are uploaded by respective data owners, end user consumes the service or data which are provided by the data owner through cloud service provider [2].

Cloud provides on demand services in efficient and simple manner, additional hardware or software infrastructure not required to avail the services of cloud, an entire organization can share the resources provided by the cloud with maintaining additional infrastructure in client systems. Cloud is simply a cost effective service and need not to maintain the data in local servers or systems but this situation may takes to confidentiality issue because our data available or stored at third party server. Cloud provides services to data owners and end users in an efficient manner with remote and secure accession demand high quality service or applications, infrastructure to many systems[3][4].

Cloud maintains reliability, integrity and maintainability and confidentiality. In day to day challenges cloud enhances their services in all aspects, sometimes multiple data owners shares a common data component, there service provides authentication parameters to access authorized users only, by generating an secure session key for encryption and decryption.

Policies between data owners to maintain data confidentiality. Even though auditor monitors the data components which are uploaded, but there is a chance to leak our confidential information to other parties, to resolve these issue some researches provided various auditing protocols for secure auditing service between data owner, Auditor and cloud service provider [5].

RELATED WORK

Cloud Computing is new class of network based totally computing that takes place over the internet. It is recognized as an alternate to ancient data technology due to its intrinsic resource-sharing and low-maintenance characteristics. Cloud Computing uses the online for communication and provides varied services to cloud users with the help of powerful datacenters. By migrating the native information management systems into cloud servers, users can relish high-quality services and save necessary investments on their native infrastructures. One altogether the essential services offered by cloud suppliers is data storage. Specially, the cloud servers managed by cloud suppliers don't seem to be completely trustworthy by user whereas the knowledge files keep inside the cloud might even be sensitive and confidential, like business plans. To preserve data confidential and privacy, a basic resolution is to jot down data files, thus transfer the encrypted data into the cloud. Sadly, turning out with associate economical and secure information sharing theme for groups inside the cloud is not a straightforward task due to the following troublesome issues. Identify privacy is one altogether the foremost necessary obstacles for the wide activity of cloud computing. Whereas the guarantee of identity is not privacy, users might even be unwilling to hitch in cloud computing systems as results of their real identities could be merely disclosed to cloud suppliers and attackers.

It is extraordinarily prompt that any member in a passing cluster needs to be ready to completely get pleasure from the knowledge storing and sharing services provided by the cloud, that's printed as a result of the multiple-owner manner. In the single-owner manner, where solely the cluster manager can store and modify information inside the cloud, the multiple-owner manner could be a heap of versatile in smart applications.

Various group key authentication mechanisms provided by cloud service providers to authenticated communication between the data users with generation of secure key between data owners and updates session key if a new user added or removed from the session.

PROPOSED SYSTEM

The proposed system is a more efficient and low cost for maintained data in cloud. In this paper we are emphasizing on user authentication, key establishment and security of shared data. The authentication user and key establishment we are using the digital certificate technique.

Secure transmission can be provided by triple DES, by using Triple Des, encrypt and decrypt sharing data. The encrypted data store into cloud and that data can be decrypt by any other users by using shared key.

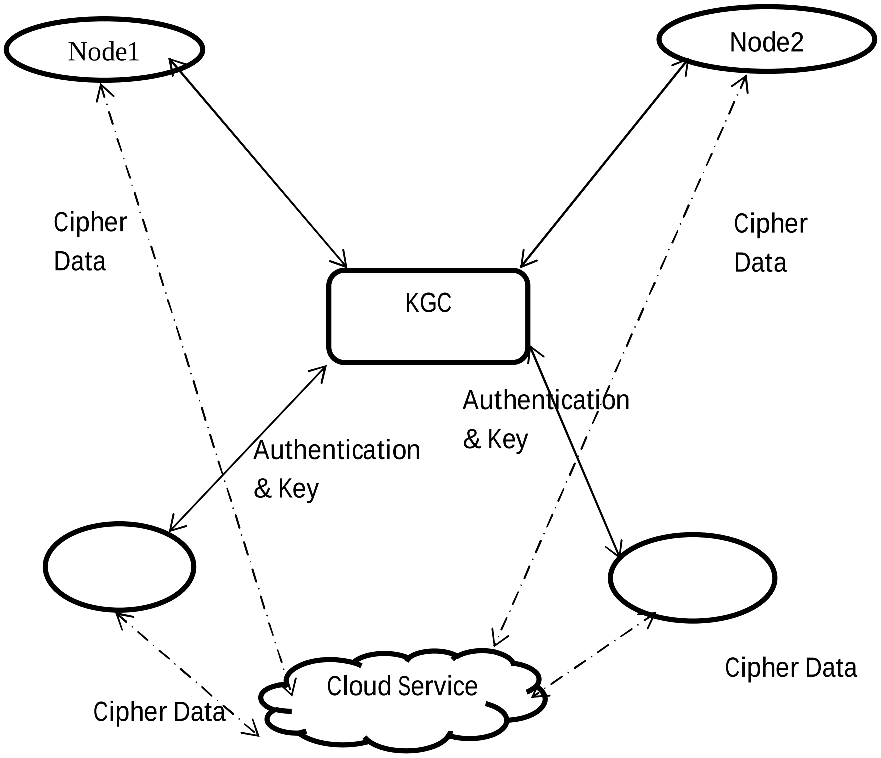

Fig1: Proposed Architecture

In this module every end user will generate signature and sent to KGC. The DSA signature provides authentication verification for all end users. The KGC will perform authentication users by using signatures comparison. In this paper, the generation signature we are using digital signature algorithm. By using this algorithm each user will generate signature and sent to KGC. The KGC will check he/she authenticate users or not.

In this module the KGC will generate secret key for encryption and decryption of shared data. Before performing the encryption and decryption of shared data the KGC generate secret key and sent to individual users. Before sent the secret key the KGC will perform the authentication users. If they are authenticated users the key will sent only that users. The generation of secret key we are using Shamir secret share for the purpose of data encryption and decryption.

In this module each and every user will encrypt and decrypt shared data. The encrypted shared data will be stored in to cloud service. If any user wants to retrieve the shared data, it can be decrypted by secret key. The encryption and decryption of shared data we are using triple DES algorithm. By using this algorithm we can provide more security and flexible of shared data.

DSA algorithm

1. End User choose a large prime number p with 2L-1 < p < 2L where L= 512 to 1024 bits and is a multiple of 64
2. End User choose q with 2159 < q < 2160 such that q is a 160 bit prime divisor of (p-1)
3. End user choose g = h(p-1)/q where 1<h<p-1 and h(p-1)/q mod p > 1

Users choose private & compute public key:

4. End user choose x<q
5. End user compute y = gx mod p

Signature creation:

6. End user calculate r = (gk mod p)mod q
7. End user generate signature s = [k-1(H(M)+ xr)] mod q and send to trusted party.

Signature verification done by trusted party:

1. Trusted party will calculate w = s-1 mod q
2. Trusted party will calculate u1= [H(M)w]mod q and u2= (rw)mod q
3. v = [(g(pow)(u1) y(pow)(u2))mod p]mod q

After successfully verification of user the trusted party will generate secret key and send to all users in cloud. The secret key generated by Shamir's secret-sharing scheme.

Mathematical definition

The goal is to divide secret (e.g., a safe combination) into pieces of data D1,D2 ....Dn in such a way that
1. Knowledge of any or more Di pieces makes easily computable.
2. Knowledge of any k-1 or fewer Di pieces leaves' s that completely undetermined (in the sense that all its possible values are equally likely).

This scheme is called (k,n) threshold scheme. If k=n then all participants are required to reconstruct the secret.

Shamir secret Sharing scheme
The essential idea of Adi Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4points to define a cubic curve and so forth. That is, it takes points to define a polynomial of degree k-1.

Suppose we want to use a(k,n) threshold scheme to share our secret , without loss of generality assumed to be an element in a finite field Fof size P where 0<k<=n<P;S<P and P is a prime number.

Choose at random k-1 positive integers a1,.....,ak-1 with ai<P, and let a0=S. Build the polynomial f(x)=a_0+a_1x+a_2x^2+a_3x^3+.......+a_{k-1}x^{k-1}. Let us construct any n points out of it, for instance set i=1....n to
retrieve (i,f(i)). Every participant is given a point (an integer input to the polynomial, and the corresponding integer output). Given any subset
of k of these pairs, we can find the coefficients of the polynomial using interpolation. The secret is the constant term a_0.

Key Generation Process

Let us consider a secret key S=1234

- Consider number of points n=6 and k=3 and obtain any random integers a_1=166 and a_2=94*$f(x)=1234+166x+94x^2$*
- Secret share points D0(1,1494),D_1=(2,1942)D_3=(3,2598)D_4=(4,3402)D_5=(5,4414)D_6=(6,5614)

We give each participant a different single point (both x and f(x)). Because we use D_{x-1} instead of D_x the points start from (1, f(1)) and not (0, f(0)). This is necessary because if one would have (0, f(0)) he would also know the secret (S=f(0))

Re-construction:

- In order to reconstruct the secret any 3 points will be enough
- Let us consider

$(x_0,y_0)=(2,1924),(x_1,y_1)=(4,3402),(x_2,y_2)=(5,4414)$

Using lagrangeous polynomials

$L_0=(x-x_1/x_0-x_{1)}*(x-x_2/x_0-x_{2)}=(x-4/2-4)*(x-5/2-5)=(1/6)x^2-(3/2)x+10/3$
$L_{1=(}x-x_0/x_1-x_{0)}*(x-x_2/x_1-x_{2)}=(x-2/4-2)*(x-5/4-5)=-(1/2)x^2-(7/2)x-5$
$L_2=(x-x_0/x_2-x_{0)}*(x-x_1/x_2-x_{1)}=(x-2/5-2)*(x-4/5-4)=(1/3)x^2-2x+8/3$

$f(x)=\sum_{j=0}^{2} y_{j*} l_j(x) =1942((1/6)x^2-(3/2)x+10/3)+3402(-(1/2)x^2-(7/2)x-)+4414((1/3)x^2-2x+8/3)$

$f(x)=1234+166x+94x^2$

Recall that the secret is the free coefficient, which means that S=1234.

After generation of points the trusted party will send the all user and the user will generate secret key using these points. So that the user will use these secreat key to encrypt the store data. As well the user also retrieve the data with cipher and decrypt using these secreat key. The encryption and decryption process can be done by using Triple DES alogorithm. The details decryption Triple DES as follows.

After storing data into cloud if any user wants read the data from cloud in form of cipher text. After retrieving the user can decrypt the data set and getting required data set.

CONCLUSION

The cloud computing shares the data to more than one user securely. So that provide security of data we are using different type of public key cryptography techniques. In this paper we are proposed concepts of authentication of users, generation of group key and security of data. For the purpose of authentication we are using digital signature algorithm. Using this concept we are find out given user is authenticated user or not. After completion of authentication the KGC will generate secret key and sent to each and every user. The generation of secret key we are using Shamir secret share. After generating secret key each user will encrypt the data by using Triple DES algorithm using the secret key. If any user want the that data it will decrypt by using the secret key. By proposing those concepts we can provide more flexible and security of data.

REFERENCES

1. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53,no. 4, pp. 50-58, Apr. 2010.
2. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc.USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
3. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: TheEssential of Bread and Butter of Data Forensics in CloudComputing," Proc. ACM Symp. Information, Computer and Comm.Security, pp. 282-292, 2010.
4. D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature,"Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO),pp. 41-55, 2004.
5. D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf.Theory and Applications of Cryptographic Techniques (EUROCRYPT),pp. 440-456, 2005
6. C. Delerablee, P. Paillier, and D. Pointcheval, "Fully CollusionSecure Dynamic Broadcast Encryption with Constant-Size Ciphertextsor Decryption Keys," Proc. First Int'l Conf. Pairing-BasedCryptography, pp. 39-59, 2007.
7. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-PreservingPublic Auditing for Data Storage Security in Cloud Computing,"Proc. IEEE INFOCOM, pp. 525-533, 2010.
8. D. Pointcheval and J. Stern, "Security Arguments for DigitalSignatures and Blind Signatures," J. Cryptology, vol. 13, no. 3,pp. 361-396, 2000.
9. .D. Boneh, B. Lynn, and H. Shacham, "Short Signature from theWeil Pairing," Proc. Int'l Conf. Theory and Application of Cryptologyand Information Security: Advances in Cryptology, pp. 514-532, 2001.