Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Information Security in a Cloud Using Trusted Third Party

K. S. Pawar, Prof. S. A. Kahate
Computer Engineering & Pune University, Pune,
Maharashtra, India

Abstract*— Data sharing is not an easy task if the data is sensitive and if it has the role based access. If particular information document is uploaded by the data owner then data owner encrypt that file and give the attribute along with that file. This property is especially important to any large scale data sharing system, as the single user compromise the key then it will be problem to data owner to secure the data. In this paper provide a concrete and efficient instantiation of scheme, prove its security and provide an implementation to show its practicality. It has become more challenging for data owner to share the data on cloud. System which is already existing use different technique to solves security problems. Solutions which are existing to solve this issue are becoming very critical to handle the key and it sharing. This paper will introduce the TTP to authenticate user those who have the access to the data on cloud.TTP will use the SHA algorithm to generate the key and that key will get share to user as well as the owner. The TTP module receives encrypted file F using RSA Algorithm from the data owner and computes hash value using MD-5 algorithm. It stores key in its database which will be used during the dynamic operations and to determine the cheating party in the system (CSP or Owner).TTP send files F to CSP module to store on cloud.

Keywords*— Trusted Third Party; Cloud Service Provider; Ring signature; Authentication; data sharing; privacy; cloud computing; forward security; smart grid.

I. INTRODUCTION

Over the past few years Cloud Computing has a boomed in the IT Market and its emerging Technology. Local Server or computer consume too much space, so as efficient alternative to it, Cloud Computing introduced. This means number of Organization have switched from local server to Cloud for Storing, processing and management of large data. Cloud Computing uses a remote servers that are hosted on Internet. While the customers have access to more features like data transfer with other peers, remote file sharing, security of data. A best example for today's Cloud Computing world is a Google Power Meter, was a software project of Google which guides consumer to track home electricity usage. This software was used to store the user's electricity usage on Cloud Computing in real time.

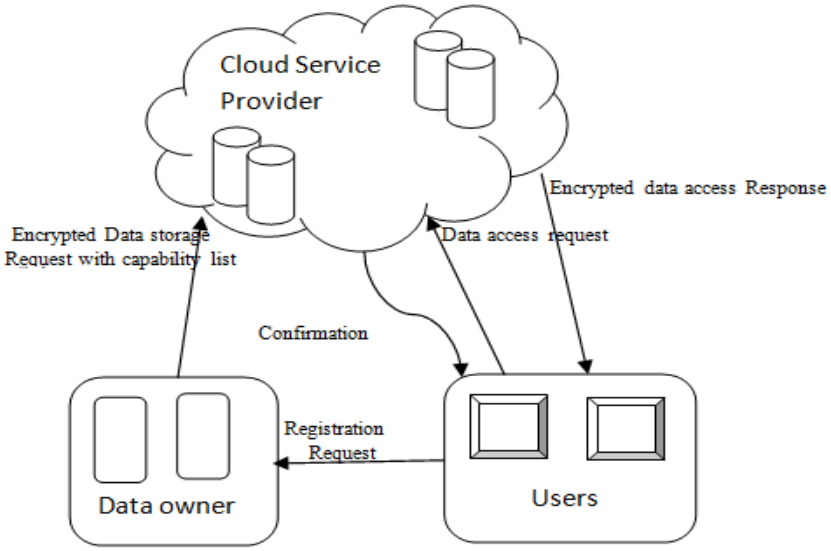

Fig 1. Cloud Structure

Cloud environment supports many features virtualization massive data traffic handling, application security, distributed data processing and access control. User can store data on external Cloud environment, which boost the demand and concerns of access control, data abstraction and encryption. Most important aspect of Cloud environment is confidentiality of data, integrity and security of data, as services provided for Cloud computing must have complete control on it. By Nature Cloud Computing is not secured, often seen that Cloud is intangible and visibility is less, inevitably produces a fake sense of security and anxiety about which is a correct secured and controlled cloud.

A. Secure and Confidential Data Sharing System

It's used for RSA and MD-5 Algorithm for using Confidentiality and security Purpose. The literature to have this feature for ECC based Algorithm is to be used in secure information to be store in cloud.

B. Attribute Based Accessed

To access the data, the authorized user sends a data access request to the Cloud Service Provider and Trusted Third Party, and receives the data file in an encrypted form F from Cloud Service Provider and hash value of encrypted file H(F) from Trusted Third Party.

II. PROPOSED SYSTEM

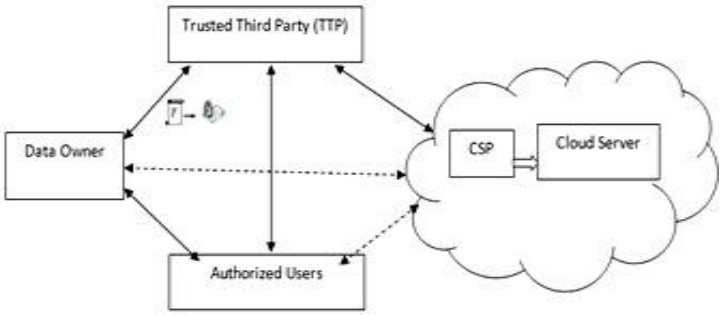

Fig. 2. System Architecture

Trusted Third Party / Auditor

Database auditing involves a database fields to not be unaware of the any type actions of the handling database users. Database administrators and consultants used to frequent set up auditing for the security purposes process.(E.g.to ensures that advice to be accessed by those without the permitted do not access it database fields.)Auditing is the monitoring and recording of user database related activities that are selected for Trusted Third party module. Data owner the user has more privileges and permissions than expected which can lead to reassessing user authorizations and an unauthorized user deleting or is manipulating information. Find issues with an authorization process or access control execution process.

Authorized User

Authorized User is a client of owner who has right to access the remote data and access cloud data permitted only this users are granted to access data remote cloud. This user is most important part of security purpose for using cloud data access control. It provides some privileges about for trusted third party module. Some authority to be provided by TTP module using attribute level based security.

Cloud Storage Service Provider (CSP)

Database is provided by cloud Storage Services Provider. It permits information owner to keep any kind of information and also able to make the user define database schema. It can be Non SQL / SQL form of database instance. According to user requirement CSP will allocated the space for the user instance.

III. RSA ALGORITHM

Let p and q are prime numbers, n=pq, P=C=Zn, and define

Step 1. K ={(*n, p, q, a,b*) : *n = pq* p and q are primes ,ab=1 (mod Φ (n)) }

Step 2. for K=(n,p,q,a,b) define $e_k(x)=x^0$ mod n and $d_k(y)=y^a$ mod n (x,y Є Zn) n and b are public, p,q,are secret.

Step 3. RSA crypto system is defined computations in Zn, where n is the product of two distinct odd primes p and q. This is Φ(n)=(p-1)(q-1) for value n.we have given formal definition of RSA crypto system above.

Now, Let's verify that encrypting and decrypting are inverse operations. Since,

Step 4. ab≡(mod Φ(n)) we have that

Step 5. ab=tΦ(n)+1 for some integers t≥1 Suppose that xЄZn*; then we have

Step 6. $(x^b)^a \equiv x^t\varphi^{(n)+1}$(mod n)= $(x^{\Phi(n)})^t$x (mod n)=1^tx (mod n)=x (mod n)

IV. MATHEMATICAL ASSUMPTION

RSA Problem: Let N = p*q, where p and q are two k-bit prime numbers such that p = 2p' + 1 and q = 2q' + 1 for some Primes p', q'. Let e be a prime 1 greater than 2 for some fixed parameters. An algorithm S solves the RSA problem if it receives an input the tuple (N; e; y) and outputs an element z such that ze = y mod N.

Input Data: I (Z) = I1, I2, I3, I4

I1=User Name, I2=Password, I3=File, I4=Key response.

Intermediate Data: E(Z)= E1, E2, E3, E4

E1=Authorized, E2=Encrypted, E3=Decrypted,E4=Attacker.

Output Data: O (Z) = O1, O2

O1=Block Attacker, O2= Download File

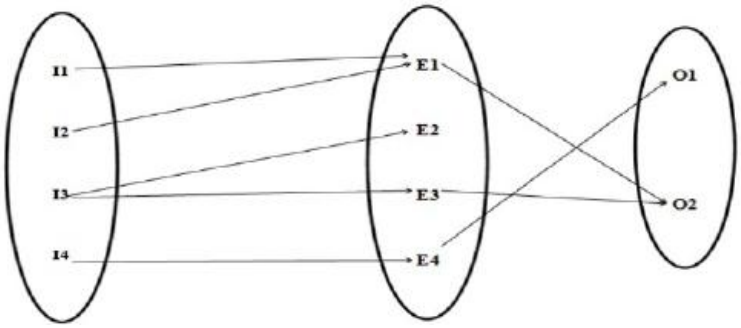

Fig 3. Mathematical Module.

V. SYSTEM DESIGN

A. Cloud Service Provider

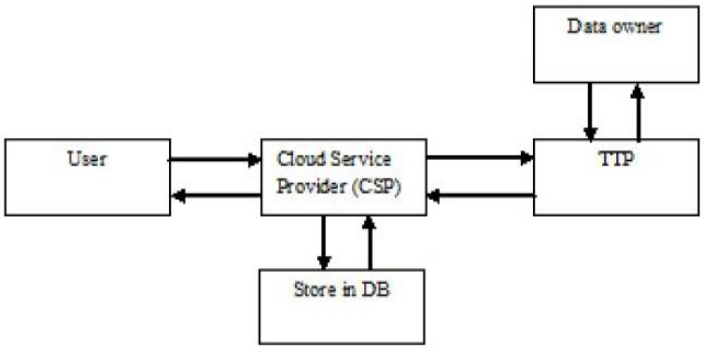

Fig 4.Cloud Service Provider

This System Provided for Services in cloud data owner and users and data store in Database .Cloud service provider mostly used in secure data store in system access.

B.Trusted Third Party Module

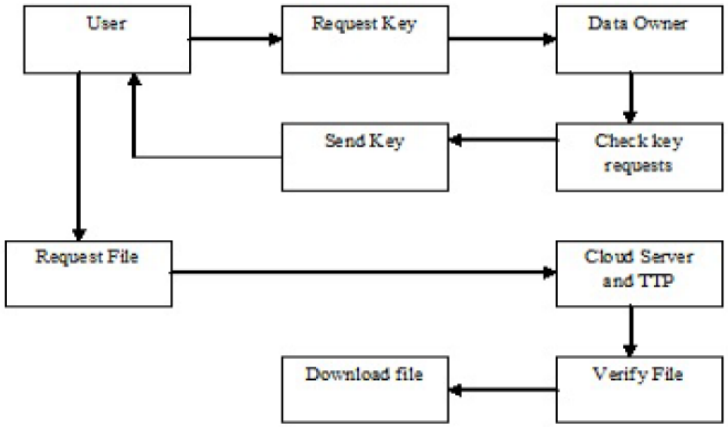

Fig 5 TTP Module.

This Third party Module is important work for access data from user and to check data owner key send key to user and TTP check this key and finally download data.

VI. CONCLUSION AND FUTURE WORK

Motivated by the practical needs in data sharing, we proposed a new notion called forward secure ID-based ring signature. It allows an ID-based ring signature scheme to have forward security. It is the first in the literature to have this feature for ring signature in ID-based setting. The size of user secret key is just one integer, while the key update process only requires an exponentiation. In a future to enhance the security more, a mechanism to secure the keys in security cloud can be a area of research. To reduce the overhead of network traffic can be another area of research. In this research uses TTP and RSA algorithm using cloud service Provider. Research Based Invention is best as Research in These security based selection RSA Algorithm.

ACKNOWLEDGMENT

For everything we achieved, the credit goes to all those who had really helped us to complete this work successfully. We are extremely thankful to P. G. Coordinator "Prof. S. A. Kahate for guidance and review of this paper. I would also like to thanks the all faculty members of "Sharadchandra Pawar College of Engineering".

REFERENCES

[1] Xinyi Huang, Joseph K. Liu+, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, Jianying Zhou, "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security", IEEE TRANSACTIONS ON COMPUTERS VOL: 64 NO: 6 YEAR 2015.

[2] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana. "Social cloud computing: A vision for socially motivated resource sharing". IEEE T. Services Computing, 5(4):551–563, 2012.

[3] C. A. Melchor, P.-L. Cayrel, P. Gaborit, and F. Laguillaumie. "A new efficient threshold ring signature scheme based on coding theory". IEEE Transactions on Information Theory, 57(7):4833–4842,2011.

[4] P. P. Tsang, M. H. Au, J. K. Liu, W. Susilo, and D. S. Wong." A suite of non-pairing id-based threshold ring signature schemes with different levels of anonymity (extended abstract)". In ProvSec, volume 6402 of Lecture Notes in Computer Science, pages 166– 183.Springer, 2010.

[5] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou. "Privacy preserving public auditing for secure cloud storage". IEEE Trans. Computers, 62(2):362–375, 2013.

[6] Joseph K. Liu1 and Duncan S. Wong2.Department of Computer Science, University of Bristol1 Woodland Road, Bristol, BS8 1UB, UK, Solutions to Key Exposure Problem in Ring Signature",International Journal of Network Security, Vol.6, No.2, PP.170180,Mar. 2008.

[7] A. Boldyreva, "Efficient threshold signature, multisignature and blind signature schemes based on the gap Diffie- Hellman group signature scheme," in Proc.6th Int. Workshop Theory Practice PublicKey Cryptography:Public Key Cryptography, vol. 567, pp. 31–46, 2003.

[8] Mihir Bellare and Sara K. Miner Dept. of Computer Science, Engineering University of California at San Diego, 9500 Gilman Drive La Jolla, CA 92093, USA, A Forward-SecureDigital Signature scheme",Michael Wiener (Ed.): CRYPTO'99, LNCS 1666,pp. 431448, 1999.

