ISSN: 2277-9655
Impact Factor: 4.116

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SECURE DATA AUTHENTICATION IN CLOUD USINGTRUSTED THIRD PARTY MODULE

Mr.K.S.Pawar(M.E Student), Prof.S.A.Kahate(Asst.Professor)
Computer Engineering,Sharad Pawar Engineering collge,Otur,Pune,India

DOI:

ABSTRACT

Now a days Information sharing is not an easy task if the information is sensitive part of the cloud and if it has the role based access permission required.If particular document is uploaded by the data owner system module then data owner encrypt that file and give the attribute based security along with that file.This property is especially important to any large scale Information sharing system, as the single and multi user compromise the key then it will be problem to data owner to secure the data. In this paper provide for main purpose a concrete and efficient instantiation of scheme provided, prove its attribute based security and provide an implementation part to show its practicality. It has become more challenging part for data owner to share the data on cloud based System which is already existing use different technique to solves security problems.Solutions which are existing system to solve this issue are becoming very critical part to handle the key based data security and it sharing information.This paper will introduce the Trusted Third Party to authenticate user permission those who have the access to the data on cloud System.Trusted Third Party will use the Md-5 algorithm to generate the key and that key will get share to Athorise user as well as the owner. The Trusted Third Party 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 changeble operations and to determine the cheating party in the system cloud service Provider and data owner.Trusted Third Party send files F to Cloud Service Provider module to store on cloud.

KEYWORDS : Atribute Based Security; Trusted Third Party; Cloud Service Provider; Authentication Service; data sharing system;encrypt; privacy; cloud computing; authenticate;

INTRODUCTION

Past few years Cloud Computing System has a boomed in the IT Market.Local Server or computer consumer to much space required in a cloud, Cloud Computing introduced for Now a days. This means number of Organization have switched from local server to Cloud for storing purposed, processing and management of large data. Cloud Computing uses a remote servers users that are hosted on world wide web. While the users have access to more features like data transfer with other peers, remote file sharing, security of data. 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 system.

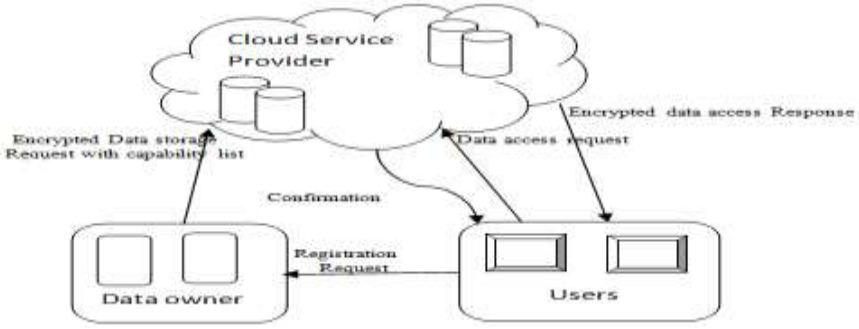

Fig 1.Basic Cloud Architecture

ISSN: 2277-9655
Impact Factor: 4.116

Cloud environment supports many features virtualization massive data traffic handling system, application security, distributed data processing and access control part. 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 authentication part, integrity and security of data, as services provided for Cloud computing must have complete control on it.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.

- **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.

- **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.

PROPOSED MODULE

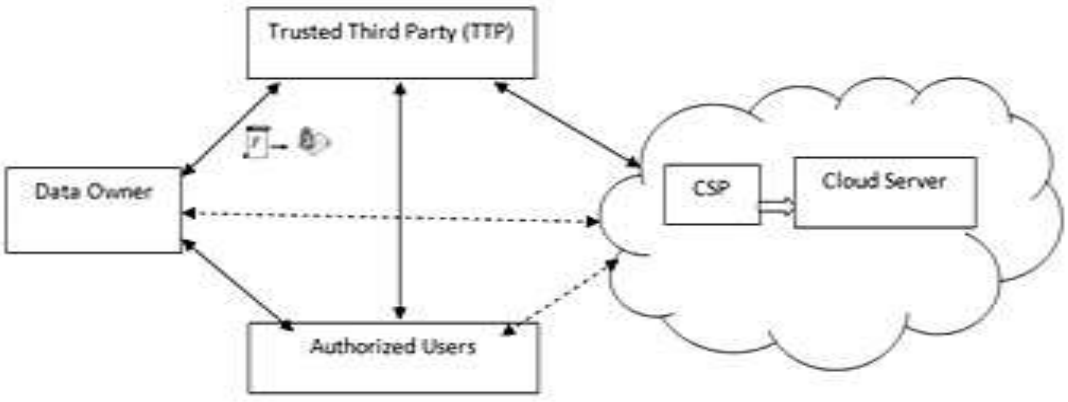

Fig. 2. System Architecture

- **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.

PROPOSED ALGORITHM

- **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 € 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 x€Zn*; 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)

- **MD-5 ALGORITHM**

MD5 digests have many uses. One such use is to take passwords and run MD5 to generate a digest version of the password. This is a one-way hash, meaning that it's easy to generate a digest, but we can't go backwards and find out the original String based on the digest. Thus, passwords are often stored in MD5 digest form so that the original password can't be figured out from the MD5 value.

```
package digest;
import java.security.MessageDigest;
public class MD5Digest {
        public static void main(String[] args) throws Exception {
                if (args.length != 1) {
                        System.err.println("String to MD5 digest should be first and only parameter");
                        return;
                }
                String original = args[0];
                MessageDigest md = MessageDigest.getInstance("MD5");
                md.update(original.getBytes());
                byte[] digest = md.digest();
                StringBuffer sb = new StringBuffer();
                for (byte b : digest) {
                        sb.append(String.format("%02x", b & 0xff));
                }
                System.out.println("original:" + original);
                System.out.println("digested(hex):" + sb.toString());
        }

    }
```

Console Output

```
original:secret
digested(hex):5ebe2294ecd0e0f08eab7690d2a6ee69
```

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	Intermediate Data: E(Z)= E1, E2, E3, E4	Output Data: O (Z) = O1, O2
I1=User Name, I2=Password, I3=File, I4=Key response.	E1=Authorized, E2=Encrypted, E3=Decrypted,E4=Attacker.	O1=Block Attacker, O2= Download File

Table 1.

SYSTEM DESIGN

- **UML DIAGRAM**

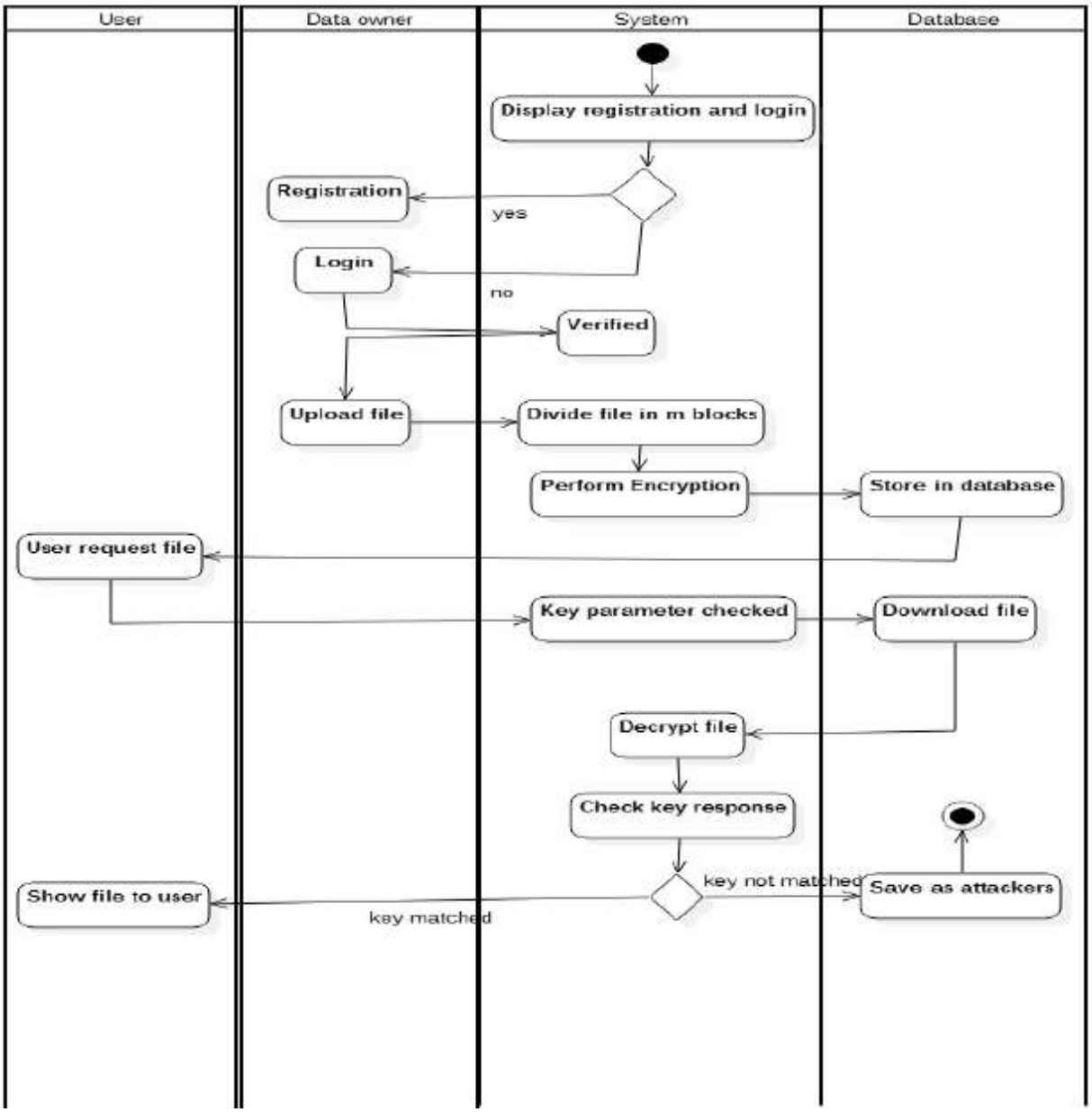

Fig 3. Activity flow diagram

CONCLUSION

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.

ACKNOWLEDGEMENTS

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):551563,2012.

[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 InformationTheory, 57(7):48334842,2011.

[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 166183.Springer, 2010.

[5] M. Abe, M. Ohkubo, and K. Suzuki, 1-out-of-n signatures from a variety of keys, in Proc. 8th Int. Conf. Theory Appl. Cryptol. Inform. Security: Adv. Cryptol., 2002, vol.2501, pp. 415432.

[6] R. Anderson, Two remarks on public-key cryptology, Manuscript, Sep. 2000. Relevant material presented by the author in an invited lecture at the Fourth ACM Conference on Computer and Communications Security, 1997.

[7] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Member, IEEE,Luigi Lo Iacono,and Ninja Marnau, Security and Privacy-Enhancing Multicloud Architectures, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO.4,JULY/AUGUST 2013.

[8] Ming Li Member, IEEE, Shucheng Yu, Member, IEEE, Yao Zheng, Student Member,IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE,Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption",IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL. XX, NO. XX, XX 2012.

[9] 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-Secure Digital Signature Scheme",Michael Wiener (Ed.): CRYPTO'99, LNCS 1666,pp. 431448, 1999.c Springer-Verlag Berlin Heidelberg 1999.

[10] 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.