Securing Data in Cloud Using Session Key

Miss. Dolly Patel
Department of CSE, BE Students, Sandip foundation, Nashik, 422001, India
3211maahi@gmail.com

Miss. Farheen Khan
Department of CSE, BE Students, Sandip foundation, Nashik, 422001, India
farheenk07@gmail.com

Miss. Ashwini Malode
Department of CSE, BE Students, Sandip foundation, Nashik, 422001, India
ash.malode@gmail.com

Miss. Komal Bhatia
Department of CSE, BE Students, Sandip foundation, Nashik, 422001, India
kmbhatia13@gmail.com

Prof. Sujit A. Ahirrao
Department of CSE, BE Students, Sandip foundation, Nashik, 422001, India

Abstract— Cloud computing provides quick delivery of services and it provides benefits from low-cost and pay-by-use model. Cloud computing is very flexible it poses great threat to security of user data as user user fully trust o cloud services and data is transparent to the user. So there are many existing systems which provides security to the cloud and user data but there is no security mechanism for the data transmission or the data path. Therefore our system is focusing on the data transition path in which user can safely access and update the data on cloud. So our project provides session key for securing data transition path. The user will autonomously interact with the cloud without the external interface .We pay more attention on synchronizing and access rights to the user

Index Terms—Cloud computing,Security,Session Key.

I. INTRODUCTION

Now a days cloud computing is popular among users because it allow the centralize data storage and get access to the services. It is used for sharing of the data between different users and organizations. The cloud stores a large amount of sensitive data,so there can be possibility of hacking or cracking the data.

Cloud computing is used to provide services on the internet. These services consist of three categories such as:

1.Infrastructure as service (IaaS)
2.Software as service (SaaS)
3.Platform as service (PaaS).

1. Infrastructure as service (IaaS):
It is used to provide infrastructure services. For Example operational hardware, networking devices,servers,storage space etc. This service provider provides his own equipment to the user or customer for use.

2. Software as service (SaaS):
In this service,service provider provides his or her own application to the user or the customer on internet. It mainly works on the principle of ASP (Application Service Provider).It is compatible as it provides same copy to all users.

3. Platform as service (PaaS):
It provides services like operating system. The features of operating system can be changed and updated frequently. The advantage of this is, by using the internet we can access this services from anywhere. So it helps to reduce the overall cost of hardware and software.
In the cloud environments, a reasonable security protocol should achieve the following requirements.

1) Authentication: A authorized user can access its own data files, only the authorized partial or entire data fields can be identified by the legal user, and any illegal user cannot access it.
2) Data anonymity: any irrelevant entity cannot recognize the exchanged data and communication state even it intercepts the exchanged messages via an open channel.
3) User privacy: any irrelevant entity cannot know or guess a user's access desire. If any user represents a his or her interest in another user's authorized data fields then he or she can access the data if and only if the both users have mutual understanding in each other. The cloud server will inform both the users to permit the access permission of data sharing.
4) Forward security: Any adversary cannot correlate two communication sessions to derive the prior interrogations according to the currently captured messages.

II. LITERATURE REVIEW

Hong Liu,[1] In existing systems,there is mainly focus on the cloud security and authentication of user. But there is no security for the transition of data between the authorized user and cloud. Public key was used in previous system to secure data on cloud which was insufficient for securing data.
Larry A. Dunning,[2] the purpose of this paper is to avoid the collision which occurs in communication between different users of cloud. In this paper,an anonymous ID assignment based data sharing algorithm (AIDA) is used for an anonymous id assignment. It uses Newton's identities and Strum's theorem for developing this algorithm. It reduces the overhead of communication. This algorithm is used for sharing private data among N parties. The anonymous id is arranged from 1 to N.
Xuefeng Liu,[3] this paper uses multiowner data sharing secure scheme(Mona),in cloud for dynamic groups. In this the user can share the data by using public cloud. This

sharing is done between only authorized user in one to one manner. The authorized user can decrypt data without knowing the owner and also secret key is not updated. The dynamic groups can use the cloud resources and the data owner ids are used by the group manager only. The advantage is to reduce the storage overhead and encryption cost.

Slawomir Grzonkowski,[4] the goal of this paper is to share the data in the trusted network i.e. in home network. It is based on Zero knowledge Proof(ZKP) only for social home network. Zero knowledge Proof(ZKP) is authentication scheme for sharing cloud services. Data sharing is done only between trusted users via TCP/IP.

III. EXISTING SYSTEM

Hong Liu [1], As cloud is used to store the data in the large amout. So existing system was used to prevent the unauthorized accessed to the users own account and access rights. At the time of accessing the data from cloud the users were supposed to be in a relationship like one to one etc and this due to this the data sharing become beneficial. The existing system focuses on authentication that is given to the user at the time of data sharing but forget about the privacy issues.

This system uses Shared Authority based Privacy preserving authentication protocol(SAPA) which is mainly for authentication and authorization. It will does not loss the user's private data . The main focus on the following:

Gives authentication protocol for access request privacy and also authority is achieved for the shared access mechanism.

Provide encryption decryption policy that gives a user can access it's own data and accept the proxy by re-encrypting among the multiple users

Fig 1. shows architecture of existing system which include the three main important component i.e. User's,Trusted third party and Cloud Server.

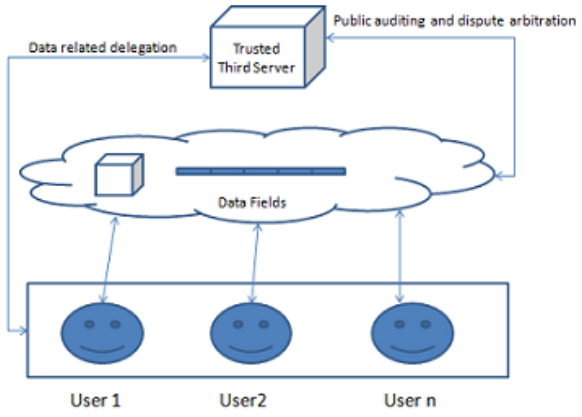

Fig 1 :Existing Architecture

The user will store the data on cloud via online by using various software that can be work on distributed or parallel mechanism. At the time of accessing the data user will interact with cloud sever by some data field that is assign at the time of uploading. It will make sure that the user private information can not be taken by the intruders .Here their can be group of the user also .

So the authentication will be provided to the user at the time of bi-directional shearing of data. Th most important thing is to care about that the user data field can not get exposed to the outsiders.

Thus the role of trusted third party is to perform public auditing of data on behalf of user . The cloud sever will provide the cloud services or application.

IV. DISCUSSION AND PROBLEMS

We know that no single technique or technology is the "magic bullet" to guarantee protection against current or future attacks. In order to robustly protect enterprise and government networks against the complete spectrum of threats and vulnerabilities, all methodologies of security must be employed.

As we have seen various existing system in the literature survey that are used to provide security to the user on cloud but those system have some disadvantages like:

1. As first system is used to provide security like authentication and sharing of data with the help of public key. So this system uses public key for sharing data or content,it has the drawback of getting the public key hacked easily.

2. In the second system, anonymous id is used secure and share the data in private network. But it helps only sharing data in private network. So the information cannot be accessed from outside the private network.

3. In the third system, Mona architecture is used to share the data between dynamic groups and only authorized users in one to one manner. But in this system data sharing is not possible in one to many and many to many manners.

4. In the last system, Zero Knowledge Proof(ZKP) authentication scheme is used only for home network security. It shares data between trusted users only. This system uses simple user id and password for authentication. So there are greater chances of hacking the home network security.

So the previous systems are used to secure only cloud and user data by using various techniques as mentioned above.

In summarized way, the objective of the proposed work is:

Our system mainly focuses on the transmission path of data where the security is not yet considered. So we are using the technique of session key to provide the security for the transmission path.

V. PROPOSED SYSTEM MODEL

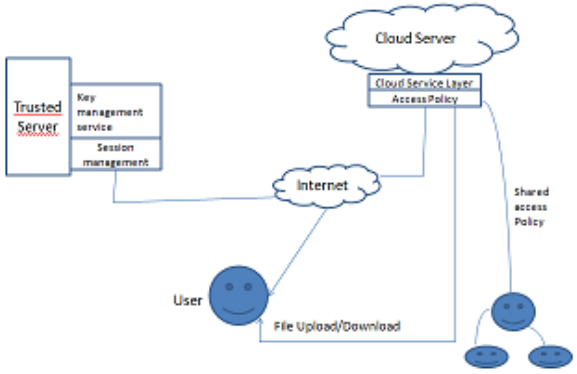

Fig 2: System Model

The Proposed Architecture as shown in the above Fig 2. consists of major modules explained below.

Trusted Server (TS):

The TS is responsible for managing the user session and key generation. Every user of the system is registered to the server. On successful registration the TS issues a Session Key which unique for the entire user. This Session Key along with Login should be used by the user when entered into the cloud server. On successful Authentication a pool of Session Key (SK)is maintain by the Trusted Server. The SK is used for every transaction the user performs on the System. The Transaction here in the system is uploading files. That means every time the user uploads a file a new transaction is created and every transaction the TS issues a key to the user and to the cloud. The Cloud service should authentication the transaction using the key issued for that transaction by the Trusted Server. On authentication the cloud allows the transaction to be complete and stores the files in the user account.

Whenever the user performs any Write Transaction such as Upload or creating a Shared Policy the TS issues a unique session key. The data being shared between the User and the cloud is encrypted using a Key.

For Key Generation the TS makes use of Quantum Protocol

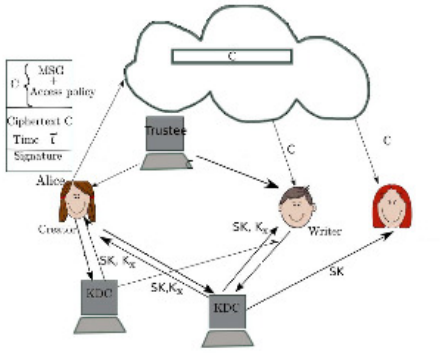

Fig 3: Key Generation

Session Key Generation Prototype Algorithm:

It is shared secret key which is used to for encryption and decryption. The size of session key is 8 bits. This session key is generated from pseudo random prime number and exponential value of random number.

Qubit Generation:

1) Generate Random String S
2) Convert S into HEXCODE H
3) Convert H into Binary Values B
4) Find Least of two Binary Values and get the quantum bit of 0 and 1.

Quantum Key Generation:

The generation of the quantum key using the qubit and session key depends on qubit combinations, such as:

1)If the value is 0 and 0, then 1/0.707(p[0]+p[1])
2)If the value is 1 and 0, then 1/0.707(p[0]-p[1])
3)If the value is 0 and 1, then p[0]
4)If the value is 1 and 1, then p[1]

Key Distribution:

It distributes the original session key and qubit to the User for encryption and the same is given to the Cloud for Authentication of the Transaction.

VI. CONCLUSION

In this paper a variety of security technique are discussed which consist of Anonymous ID Assignment, multiowner data sharing secure scheme(Mona),ZeroKnowledgeProof(ZKP)authentication scheme.

For each of the security detailed discussion consist of the working of the security techniques which are used to provide security for cloud storage and user data. From this detailed survey we discussed the advantages and shortcomings of all security techniques. When we come across the security of transmission path of data there is no such mechanism. This technique is design in such manner we can able to avoid the security attack on the path. This system works for mainly securing transmission path between cloud and user. Overall study tells that all technique trying to provide better result in terms of security of data.

VII. REFERENCES

[1] Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing Hong Liu, Student Member,

IEEE, Huansheng Ning, Senior Member, IEEE, Qingxu Xiong, Member, IEEE, and Laurence T. Yang, Member, IEEE.

[2] L.A.Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp. 402-413, 2013.

[3] X. Liu,Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Mulch-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6374615, 2012.

[4] S. Grzonkowski and P. M. Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking," IEEE Transactions on Consumer Electronics, vol. 57, no. 3, pp.1424-1432, 2011.