Higher Protection in Cloud Using Efficient Anonymous Authentication Protocol

P. Yuvaraj[1], L. Sharmila[2]

[1]*P.G Student, M.E CSE,* [2]*Assistant professor, Dept. of M.E CSE, Alpha College of Engineering*

Abstract – Cloud computing is an effective data interactive paradigm to prove the data remotely stored in cloud server using online. That cloud services provide great flexibility for the users to enjoying the on-demand cloud applications without keeping the local infrastructure conditions. During the data access time, different users may be in a collaborative relationship, and thus data sharing becomes significant to achieve final overall benefits. The already existing security solutions majorly focus on the authentication alone, that means to realize that a user's confidential data cannot be illegally accessed without the authors or senders permission [3], but avoid a sub privacy issue during a user challenging the cloud server to request other users for the same data sharing. Shared Authority based Privacy-preserving Authentication protocol (SAPA) to identify above privacy issue for cloud storage. In this algorithm, shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations [14] (ex: user privacy, authentication, data anonymity, and forward security), attribute based access control is adopted to conform that the user can only access its own data fields.

Keywords: Cloud computing, SAPA, authentication, shared access, authority, data anonymity.

I. INTRODUCTION

Cloud computing provides highly computing services to be easily consumed over the Internet on a rent basis. A most important benefit of the cloud services is that user's data are usually processed remotely in unknown machines that users do not use. While enjoying the convenience brought by this technology, users get doubtful of missing data.

Cloud Service Providers (CSP) manages an infrastructure that offers a scalable, reliable and secure environment for users, at a much lower marginal cost due to the sharing property of available resources.

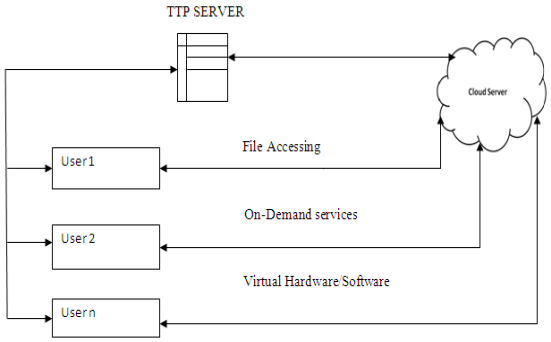
It is cycle for users to use cloud storage services to share data with others in a team, as data sharing becomes a standard feature in most cloud storage offerings, including drop box. The integrity of data in unsecured cloud can easily be lost or corrupted, due to human errors and hardware failures.

To protect the integrity of cloud data, it is best to perform public auditing by introducing a Third Party Auditor (TPA). The first Provable Data Possession (PDP) mechanism to perform public auditing is designed to check the correctness of data stored in an untrusted server, without getting the entire data.

Cloud computing has been visualise as the next-generation architecture of the Information Technology Field. Particularly, on-demand self-service, ubiquitous network access, location-independent resource pooling, resource elasticity, rent-based pricing.

II. CLOUD SYSTEM MODEL

The following fig shows how actually the cloud is working. And how the various processes have been done (i.e...) Storing, retrieving data's in cloud with secured manner, hardware and software virtualisation etc.



The number of services is unlimited in cloud and the users also in more numbers. Here the users are namely User1,2 till user n. That is all the users are connected in the cloud, whenever which user wants the particular service or the virtual product he/she can get the service/application with the minimum amount of time and high availability.

TTP server plays a major role here. Even though it was the optional one, the purpose of TTP is quiet important. This block performs public auditing on the data on the cloud.

III. PREVIOUS WORK

In the cloud storage based supply chain management, there are various interest groups (e.g., provider, carrier, and retailer) in the system. Each group owns its users which are permitted to access the authorized data fields, and various users have own relatively free access authorities. It means that any two users from various groups must access different data fields of the same file.

There into, a provider may want to access a carrier's data's, but it's not sure if the carrier will allow its access request.

If the carrier declines its request, the supplier's access desire will be revealed along with nothing obtained towards the desired data fields. Actually, the supplier may not send the access request or withdraw the unaccepted request in advance if it firmly knows that its request will be refused by the carrier. It is unreasonable to thoroughly disclose the supplier's private information without any privacy considerations.

The carrier also wants to access the supplier's data fields, and the cloud server should inform each other and transmit the shared access authority to the both users. The carrier has no interest on other user's data fields, therefore its authorized data fields should be properly protected, and meanwhile the supplier's access request will also be concealed.

The carrier may want to access the retailer's data fields, but it is not certain whether the retailer will accept its request or not.

IV.PROPOSED METHODOLOGY

Proposed technique is "Efficient Anonymous Authentication Protocol (EAAP)" to address a privacy issue for cloud storage. It indicates that the proposed protocol realizing privacy preserving data access authority sharing is attractive for multi-user collaborative cloud applications.

The security of the data to be uploaded in the website is amplified using the concept of One Time Password (OTP). This technique will used to know whether the authorized users can access the data or the data accessed by the unauthorized user. It will be a great task for the hackers to hack the system and steal the data.

1) EAAP is achieved by anonymous access request matching mechanism with security and privacy considerations (example: authentication, data anonymity, user privacy, and forward security); 2) Attribute based access control is adopted to realize that the user can only access its own data fields

3) Bit exchanging method encryption is applied by the cloud server to provide data sharing among the multiple users.

4) Towards the dynamic cloud data, the scheme supports dynamic outsourced data operations. It indicates that the scheme is resilient against Byzantine failure, malicious data modification attack, and server colluding attacks.

5) Proposed an object centered approach to enable enclosing the logging mechanism with the users' data and policies.

V.SYSTEM ARCHITECTURE

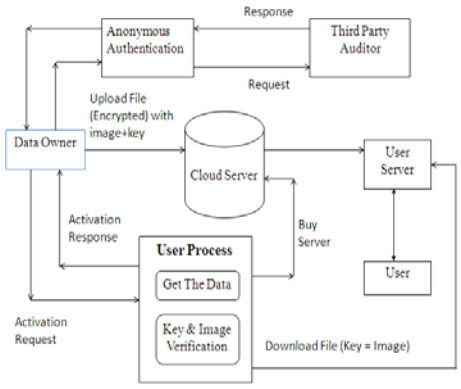


Fig.1: Architecture Diagram

System architecture is the overall model that defines the structure, behaviour, and over view of a system. An architecture description is a formal description and representation of a system, organized in a way that support reasoning about the structures and behaviour of the system. The architecture diagram shows the modules used in the project. The modules are listed and explained below.

Anonymous Authentication Process (AAP): This block contains two major sides namely data user side and data owner side. Data owner has to upload its files in a cloud server after the successful registration.

The data user side contains the process of downloading or viewing the content present in the cloud only after the registration process completes from data owner (who is actually upload the file) .

Trusted Third Party Implementation: User and owner register their details in cloud with the username and password. Third party auditor is verifying the data owners request and details. Then only TTP provides accessibility permission to the Data owner.

Then the data owner is sending the encrypted key to the user for reading the content of the file what already stored by that particular data owner. One data user may have subscribed more than one data owner (i.e.) one user having more number of subscriptions for the various data owners.

Cloud Service Provider: The cloud delivery model has provides software as a service, platform as a service, and infrastructure as a service. CSP should be responsible for the security of their customers data and it should be responsible for if any security

Access control development: Owner can permit access or deny accessing the data. So users can able to access his/her account by the corresponding data owner. It not permitted the user can't be view or download the data in the cloud storage.

For the increasing of the security level among all the data's, the encryption and decryption technique used namely called BEM_encrypt & BEM_decrypt method. The file owner has uploaded which has to be in encrypted form and decrypt it.

File authentication mechanism: This model used to register all users in the cloud. Authorized user can be access cloud with their username, password. Authorized user can access the file. by means of this security mechanism. Now a day the higher security level is also known as the password protection.

VI.CONCLUSION

In this work, we have identified a new privacy challenge during data accessing in the cloud computing to achieve privacy-preserving access authority sharing. Authentication is established to guarantee data confidentiality and data integrity. Data anonymity is achieved since the wrapped values are exchanged during transmission. User privacy is enhanced by anonymous access requests to privately inform the cloud server about the users' access desires. Forward security is realized by the session identifiers to prevent the session correlation. It indicates that the proposed scheme is possibly applied for enhanced privacy preservation in cloud applications

VII.FUTURE WORK

In privacy preserving public auditing for data storage, TTP should audit cloud file. To guarantee that the TTP would not learn any knowledge about the data content stored on the cloud server during auditing process. It's not eliminates the burden of cloud user from the tedious and possibly expensive auditing task. But it also alleviates the user's fear of their outsourced data leakage.

In the future implementation extend privacy preserving public auditing for multi user setting, where the TTP can perform multiple auditing tasks in batch manner for more efficiency.

VIII.REFERENCES

[1] A. Barsoum and A. Hasan, "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems," IEEE Trans. Parallel and Distributed Systems, vol. 24,no.12,pp.23752385,http://ieeexplore.ieee.org/stamp/stamp.jsptp=&arnumber=6392165, Dec. 2013.

[2] J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architecture for Cloud Computing," Computer, vol. 45, no. 7, pp. 73-78,2012.

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

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

[5] H.Y. Lin and W.G. Tzeng, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 6, pp. 995-1003, June 2012.

[6] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, http : // ieeexplore .ieee.org / stamp/stamp.jsp ?tp=&arnumber =6374615, June 2013.

[7] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," Nat'l Inst. of Standards and Technology, 2009.

[8] K. W. Park, J. Han, J. W. Chung, and K.H. Park, "THE MIS: A Mutually Verifiable Billing System for the Cloud Computing Environment," IEEE Trans. Services Computing, vol.6, no.3, pp. 300313, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6133267, July-Sept.2013.

[9] Y. Tang, P.C. Lee, J.C.S. Lui, and R. Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 6, pp. 903-916, Nov./Dec. 2012.

[10] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859-25, May 2011.

[11] C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[12] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, pr.-June 2012.

[13] Y. Xiao, C. Lin, Y. Jiang, X. Chu, and F. Liu, "An Efficient Privacy-Preserving Publish-Subscribe Service Scheme for Cloud Computing," Proc. IEEE GLOBECOM '10, Dec. 2010.