Enhancing Data Privacy and Efficiency for Secure Cloud Storage Model

S.Simla Mercy[1], D.S.Delphin Hepsiba[2], G.Umarani Srikanth[3]

Abstract-**In cloud computing cloud service provider provides services to the cloud users from cloud server via internet. These services are referred as software as a service (SaaS). Information sharing is the key goal of cloud storage servers. Cloud allows storage of sensitive and large volume of data with limited cost and high access benefits. Cloud service providers have to provide proper security measures to protect the clients documents and to ensure that their cloud infrastructure is secure. Sharing the group resource among the group members via untrusted cloud results challengeable security issue because of group user membership change. In existing system security for group user document access is provided by dynamic broadcast encryption technique. Revocation of defined policies/ group is the obstacle of current system. In proposed system Security Assertion Markup Language and Triple Data Encryption Standard (DES) technique provides an effective security regarding authentication, recovery and for providing privilege. SAML is an XML based open standard data format for exchanging the data between client and server with authentication and authorization. DES algorithm is used to provide more assurance for data integrity. This methodology provides better way to organize data among a dynamic multi-user environment maintaining security and privacy of data as well as users.**

Index Terms-**Cloud Computing, Dynamic Group, Group Authorization, Document Sharing.**

I. INTRODUCTION

Cloud computing goal is to exploit large use of distributed resources by the customer to achieve high volume of throughput and to overcome large amount of computational problems. Cloud computing holds these entities: cloud server, cloud service provider, data owner, and data user. Cloud Server is the data center in which large collection of applications are hosted as services. Data center will be called as cloud. Cloud service provider deliver services or computing resources to the users from the cloud server over the internet through web browser interface. Cloud is maintained by the cloud service provider. Data owner is the owner of the document. Authorized Data user can access document from the cloud server.

Cloud services are provided to the users for pay per use. Cloud service frameworks are Software as a service, Platform as a service, and Infrastructure as a service. Cloud computing models the user to access the document from anywhere wherever network connection available. Characteristics of cloud computing are on demand self-service, broad network access, resource grouping, rapid elasticity and assessed service [11]. Cloud services are available as public cloud, private cloud, community cloud, hybrid cloud [11]. Public cloud is offered over the internet to the general public in pay as you go manner. Private cloud is operated for specific organization. Community cloud is available only to groups. Hybrid cloud is the combination of public cloud and community cloud.

Cloud document will be shared among the dynamic group. Dynamic group refers the changes of membership over the group. Outsourcing the document to the third party group causes the security and privacy issue. Because the members in the group are considered as dynamic. In a group each group member can read and modify the data of the file which is shared by the company. The changes of membership make secure data sharing extremely difficult. Any member in the group can store the data and share the services by the cloud which will be called as multiple owner models. In a single owner model group manager can only store and modify the data in the cloud. Security issue is the main problem of the development and widespread use of cloud computing. Cloud service provider should be trustworthy by providing trust and secure computing and data storage [11]. In the untrusted server data owner depot the encrypted data files and disseminate the comparable decryption keys only to authorized people. So that, unauthorized people and file servers cannot able to learn the content of the document.

II. PRELIMINARIES

A. Triple DES algorithm

Triple DES algorithm takes a fixed-length string of plaintext bits and transforms it through a series of

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET

complicated operations into another cipher text bit string of the same length. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks. Group members encrypt the data by using Triple DES algorithm so that only authorized user can decrypt the data. Triple DES algorithm allows the system administrator to dynamically include new members to the group and also conserves previously computed information. Triple DES is an excellent and reliable choice for the security needs of highly sensitive information while sharing the documents among the group members.

B. Secure Assertion Markup Language

SAML is the data format for exchanging the authentication and authorization data between user and cloud service provider. SAML description involved among group people, system administrator and cloud service provider. Group people calls for service from the cloud service provider. Cloud service provider requests and obtains an identity assertion from the service provider. Service Provider requests information such as user name and password from the user to authenticate. Cloud service provider makes access control decision and decides whether to perform service for the connected user.

C.Single Sign-On

In a single sign on system user logs in once and gains access to all systems without being prompted to log in again at each of them. In single sign on user enter one name and password to access multiple applications. The process certifies the user for all the applications. Single sign on focuses more on protection of the user credentials. In a single sign on system single action of user authentication and authorization permit a user to access all resources. The single sign on maintains a mapping between a user or group of users and the username and password needed to access a particular data source.

III. RELATED WORK

In [2] Lu et al proposed a scheme based on bilinear pairing techniques for secure provenance. Secure provenance furnishes confidentiality on sensible documents which is stored in cloud, secret authentication on user access, and provenance tracking on disputed documents. Each user acquires two keys after the registration: a group signature and an attribute key. Group people can encrypt the document using attribute based encryption and also group can decrypt the encrypted document using their attribute keys. Group people sign on the encrypted data with group signature key for confidentiality of the data. User revocation is not supported in secure provenance.

In [9] Ateniese et al proposed atomic proxy re-encryption technique in which partly trusted proxy converts a ciphertext without seeing the underlying plaintext. Unique and symmetric content keys used to encrypt the document which is again encrypted with master public key. Proxy re-encryption allows the centrally managed access control.

In [1] Kallahlla et al proposed a cryptographic storage system to reduce the numbers of cryptographic keys exchanged between users and achieves strong security. Filegroups divided as files and encrypted with distinctive fileblock key, data owner deliver the filegroups to group people with lockbox key. Fileblock keys encrypted with lockbox key. Accumulating keys into filegroups has the discernible advantage that it reduces the number of keys that users need to manage, distribute and receive. System brings heavy key distribution overhead for secure file sharing. System updates file block key and distribute for user revocation.

In [3] Wang et al proposed a System in that for constructing homomorphic authentication group signature is used. By doing this without retrieving the whole data third party auditor can verify the integrity of the data. The identity of the signer on each block in apportioned data is held private from the third party auditor. System supports expeditiously audit the correctness of the document, apportioned among large number of people. System feats homomorphic MACs to shorten the space utilized to depot such verification information.

To contribute the document with dynamic group, need to propose system with certain unique features: In a cloud any people in the group can store and contribute the document with group people. The complexity of encryption and ciphertext size are independent with the number of revoked users in the scheme.

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET

IV. PROPOSED SYSTEM

In the flow of the system, share confidential large volume of data in a cloud using various methodologies in secure manner. SaaS (Software as a Service) cloud has been used to store data in document repository. Document access mechanism will be authenticated to provide the user to specify the authorization. New user registers with the system administrator and get authorization in a group. System administrator issue the Triple DES key to group people to encrypt and decrypt the document. Administrator provides constrain to eradicate the valid user access for the policy making specification. In this flow, the Group policy will provide the security level of permission based on the user type.

By specifying Document read, Document write, Document downloadable options data owner upload the document in cloud server with encryption. The documents will be categorized into visibility and invisible property. In this proposed system, an user friendly option called dynamic document viewer in browser has been introduced, this in turn overcome the problems faced in the existing system. Dynamic view of documents provided in the web browser after authenticating with the server. Accessing the uploaded module specifies the privacy mechanism factor. Archive options such as visible, invisible and downloadable are used by document owners in order to provide privilege among the groups. System administrator can revoke the user when user leaves from the group. Group user can delete the file by sending request to the cloud server. Cloud server verifies the user details from the system administrator and deletes the file. User access will be furnished to update the document. Revoking the document is also specified for the user functionality.

Document search flow authorizes the group by revoking the User access. Revoking user document access provides security on the documents. The user can search the document thereby providing the search keyword. The versions of a document provide a history of the changes the document has undergone from the time it was initially created. Creating the document versions check a document in and out. Document information belonging to the Document class or one of the document subclasses is a version. It constitutes the document as it existed at a particular time in its history, and is individually saved and exerted in an object store. The different versions of a document become the version series for the document. In this flow, the version of the document has been maintained on the basis of the user usage. Maintenance such as log based maintenance to track ongoing transactions carried out as a part of security providing methodology to recover the data in-case of database crash. Log management will depict the maintenance of all the log history where the documents will be viewed and used up from the cloud. Document navigation will update the versioning feature. The information's are retrieved by passing the account information with request. Algorithm namely triple DES has been used to encrypt the data. Thus the proposed system provides an effective security regarding authentication, recovery and for providing privilege.

V. SYSTEM ARCHITECTURE

Cloud System Model explains that Group People may be a document owner or document viewer. Group people will register their user particulars with the system administrator and receive user name and password for authentication and get the services from the cloud. System Administrator will verify the user details and will contribute the encryption key.

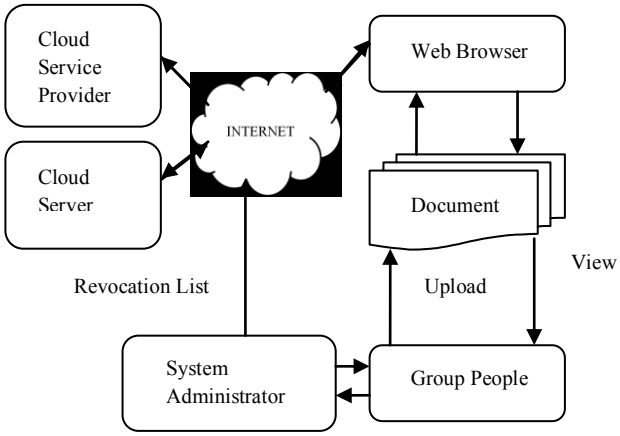

Fig. 1. Cloud System Architecture

By using the key data owner encrypt the document and upload it in the cloud server. CSP maintains the cloud server to store all the documents. CSP provide services to the authorized cloud user via internet. Authorized Group user can view the document by sending request to cloud service provider through web browser which is installed in their own system. CSP obtain the group user details from the system administrator and verify the user details and then contribute the services. System administrator places the revoked

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET

user details in the cloud server to restrict the services to the revoked user.

VI. CONCLUSION

The intention of the project is to provide secure document sharing among the group users. Here Data owner who is existing in the group store their own data on the cloud server in the encrypted format. For encrypting the document Triple Data Encryption Standard algorithm is used. Revocation of the user will be achieved by system administrator. System administrator will change the rights of the revoked user. Only authorized group people can only view the document. Cloud server often verifies the user details and provides the document access. In future sustainment, the version of the document has been maintained on the basis of the user usage. Dynamic view of the documents can be provided in the web browser after authenticating with the server. Log management will depict the maintenance of all the log history where the documents will be viewed and used up from the cloud. Document navigation will update the versioning feature. Information's are retrieved by passing the account information with request.

VII. REFERENCE PAPERS

[1] M.Kallahalla, A.Riedel, R.Swaminathan, Q.Wang, & K.Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage", Proc. USENIX Conf. File and Storage Technologies, pp. 29-42,2003.

[2] R.Lu, X.Lin, X.Liang, and X.Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing", Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[3] B.Wang, B.Li, and H.Li, "Knox: Privacy - Preserving Auditing for Shared Data with Large Groups in the Cloud", Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.

[4] M.Lori, "Data Security in The World of Cloud Computing", co-published by the IEEE computer and reliability societies, pp 61-64, 2009.

[5] Zhifeng Xiao & Yang Xaio, "Security and Privacy in Cloud Computing", IEEE communications survey and tutorials, vol. 15, No. 2, second quarter, 2013.

[6] 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, 2010.

[7] 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.

[8] B.Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization", Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography,pp.15-29, 2008.

[9] G.Ateniese, K..Fu, M.Green & S.Hohenberger, "Improved Proxy Re - Encryption Schemes with Applications to Secure Distributed Storage", Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[10]D.Naor, M.Naor, and J.B.Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers", Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

[11] Zhifeng Xiao and Yang Xiao, "Security and Privacy in cloud computing", IEEE Communications surveys & Tutorials, 2013.

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET