ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Multi-User Authorization on Versionized Document Repository in Cloud Environment

G. Michael[1], G.Kavitha [2]

Assistant Professor, Department of Computer Science Engineering, Bharath University, Chennai, Tamil Nadu, India[1]

Assistant Professor, Department of Computer Science Engineering, Bharath University, Chennai, Tamil Nadu, India[2]

ABSTRACT: Traditional IT has its defects intrinsic resource sharing and low maintenance, so it was replaced by Cloud Computing. Cloud computing is a pay-per-use model which provides enhanced accessibility, convenient, and on-demand network access to a shared pool of configurable computing resources. By using Protection Affirmation Markup Language, the user can be authenticated to cloud. Document version maintenance and log maintenance mechanisms provide data availability and effective data recovery strategies for the user to access the shared data in the cloud environment. The strategy provides the way to the organize data among the multi-user dynamic environment while, maintaining the security and privacy of data as well as users.

KEYWORDS: Cloud computing, document versioning, security, privacy,PAML (Protection Affirmation Markup Language).

I. INTRODUCTION

Cloud computing has great potential of providing robust computational resources to the society at low maintenance and cost. It enables the customers to enjoy the massive computational power, storage and even software which can be shared in a pay-per-use manner. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By relocating the local data management systems into cloud servers, users can enjoy high-quality services and saves significant investments on their local infrastructures. One of the most fundamental services offered by cloud providers are data storage. With cloud storage service, the members of an organization can share data with other members easily by uploading their data to the cloud. Since data operations in the cloud are not transparent to users, and security breaches or improper practices are common and inevitable, users still have a huge concern about the security of their data on the Cloud. The version number is unique in the document version series and is actually comprised of two properties—the major version number and the minor version number. A minor version always has some number other than zero as its minor number. Both 0.1 and 4.32 are examples of a minor version. Reservation versions are always assigned a minor number. A major version always has an integer other than zero as its major number, and always has a minor number equal to zero; for example, 5.0. It is important to have a clear picture of which personnel will have the rights to access the sensitive data and how they are going to do it.

II. PROPOSED SYSTEM

In the existing system, any user in the group can store and share the data with the others in the cloud. Access control guarantees that any member in a group can utilize the cloud resource. User revocation through novel revocation list is done by group manager. But it incurs following disadvantages namely,

- Algorithm for encryption is not more secure.
- No version and log based maintenance for the shared document.
- Real identities of the data owner can be revealed by the group manager when disputes occur[1].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Thus the proposed system provides authentication and secure encryption scheme for dynamic group access on versionized document repository in cloud environment. Authentication provides assurance that the communicating entity is the one that it claims to be. Log maintenance mechanism provides effective data recovery option for the shared data. Version maintenance mechanism provides effective data availability option for the shared data. Secure encryption algorithm and Support for dynamic group[2]. Archive options such as visible, invisible and downloadable are used by document owners in order to provide privilege among the groups. The objectives of the proposed system are:

- To provide secure and privacy preserving access to the shared data and allow dynamic group authorization and authentication in the cloud environment.

- To maintain the document under a cloud environment with an archive option based user access group under a data owner. It includes a strategy of defining individual user access grant/revoke option by the data owner.

- The concept of versioning has been formulated to maintain the document flexibly and provide the user with a strategy of dynamic document view in web browser.

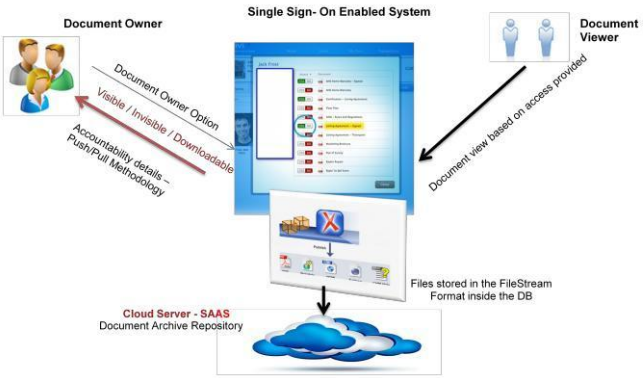

Fig 1 System Architecture

Document owner is responsible for providing access to the document stored in the cloud environment. Document viewer gain the access based on the access privilege provided by the owner on the single sign-on enabled system[3].

III. SYSTEM DESIGN

A. Group Access Policy Authorization

Document access mechanism will allow the user to specify the authorization information. Administrator will provide the constraint to allow the valid user access in the cloud environment. The group policy will provide the security level of permission based on the priority.

B. Document Upload /Object Access Specify

OPTIONS:

- Document read
- Document write
- Document downloadable

The documents will be categorized into visibility and invisible property.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

C. Group/User Access/Revoke

Group access mechanism allows the group members to access the shared documents in a secure manner. User access allows updating of document. Revoking mechanism is used for document revocation by group manager.

D. Document Version/View Module

The version of the document has been maintained on the basis of the user usage. Dynamic view of documents can be provided in the web browser after authenticating with the server[5]-[8].

E. Document Search

Document viewer and document owner can search the versionized document. Document owner is responsible for secure search of the versionized document.

F. Log Management

Log maintenance mechanisms provide data availability and effective data recovery strategies for the user to access the shared data in the cloud environment[9].

G. Accountability Information Retrieval

The methodology provides the better way to organize data among a dynamic multi-user environment, maintaining security and privacy of data as well as users.

IV. RELATED WORK

In [1], the files are divided into file groups and encrypting each file group with a unique file-block key, the data owner can share the file groups with others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file block keys. However it includes heavy key distribution overhead for large –scale file sharing file-block keys need to be updated and distributed for a revocation. In [2], files stored on the untrusted server include two parts: file Meta data and file data. The file metadata implies the access control information including a series of encrypted key blocks, each of which is encrypted under the key of authorized users. However it includes the size of the file metadata is proportional to the number of authorized users. User revocation is in-tractable issue for large-scale file sharing, since the file metadata needs to be needed. In [3] A scalable and fine-grained data access control scheme in cloud computing based on key policy attribute-based encryption (KP-ABE) technique. The data owner uses a random key to encrypt a file, where the random key is further encrypted with the set of attributes using KP-ABE. While it is not applicable for Single owner manner, since any member in the group should be allowed to store and share the data files in the cloud. In [4], a scheme based on group signature and ciphertext-policy attribute based encryption techniques. Each user obtains two keys after the registration namely a group signature key and attribute key. Any user in the group can be able to encrypt the data file using attribute based encryption and others can decrypt the file using attribute keys. User signs the encrypted data with the group signature key for privacy preserving and traceability. However user revocation is not supported.

V. TECHNIQUES AND ALGORITHM USED

A. DOCUMENT VERSIONING

Some computer file systems, such as the OpenVMS File system, also keep versions for files. Versioning amongst documents is relatively similar to the routine used with computers and software engineering, where with each small change in the structure, contents, or conditions, the version number is incremented by 1, or a smaller or larger value, again depending on the personal preference of the author and the size or importance of changes made[9].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

B. PROTECTION AFFIRMATION MARKUP LANGUAGE

Protection Affirmation Markup Language is an XML-based open standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. The single most important problem thatPAML addresses is the web browser single sign-on (SSO) problem. ThePAML specification defines three roles: the principal (typically a user), the identity provider (aka IdP), and the service provider (aka SP). The principal requests a service from the service provider. The service provider requests and obtains an identity assertion from the identity provider. On the basis of this assertion, the service provider can make an access control decision - in other words it can decide whether to perform some service for the connected principal[10].

C. TRIPLE DES

Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm[11].

VI. CONCLUSION

Thus it formalizes an approach to share and maintain the document under multiple document owner in a cloud environment. It includes the strong concepts of log based management and versioning to maintain the document in the cloud environment securely and efficiently. It also provides a privilege to the users in the group to view the document in the browser dynamically.

REFERENCES

1. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc.USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
2. Udayakumar R., Khanaa V., Kaliyamurthie K.P., "High data rate for coherent optical wired communication using DSP", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) 4772-4776.
3. E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius:Securing Remote Untrusted Storage," Proc. Network and DistributedSystems Security Symp. (NDSS), pp. 131-145, 2003.
4. Jaikumar S., Ramaswamy S., Asokan B.R., Mohan T., Gnanavel M., "Anti ulcer activity of methanolic extract of Jatropha curcas (Linn.) on Aspirin-induced gastric lesions in wistar strain rats", Research Journal of Pharmaceutical, Biological and Chemical Sciences, ISSN : 0975-8585, 1(4) (2010) PP.886-897.
5. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable,and Fine-Grained Data Access Control in Cloud Computing,"Proc. IEEE INFOCOM, pp. 534-542, 2010.
6. Udayakumar R., Khanaa V., Kaliyamurthie K.P., "Optical ring architecture performance evaluation using ordinary receiver", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4742-4747.
7. 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.
8. Kumar S.S., Rao M.R.K., Balasubramanian M.P., "Anticarcinogenic effects of indigofera aspalathoides on 20-methylcholanthrene induced fibrosarcoma in rats", Research Journal of Medicinal Plant, ISSN : 5(6) (2011) PP. 747-755.
9. 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, Apr. 2010.
10. Udayakumar R., Khanaa V., Kaliyamurthie K.P., "Performance analysis of resilient ftth architecture with protection mechanism", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4737-4741
11. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.
12. [12]P.JENNIFER, DR. A. MUTHU KUMARAVEL, Comparative Analysis of advanced Face Recognition Techniques, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801, pp 4917-4923 Vol. 2, Issue 7, July 2014
13. [13]Dr.R.Udayakumar, Computer Simulation of Polyamidoamine Dendrimers and Their Complexes with Cisplatin Molecules in Water Environment, International Journal of Innovative Research in Computer and Communication, ISSN(Online): 2320-9801,pp 3729,25-30, Vol. 2, Issue 4, April 2014
14. [14]DR.A.Muthu kumaravel, Mr. Kannan Subramanian, Collaborative Filtering Based On Search Engine Logs, International Journal of Innovative Research in Computer
15. and Communication Engineering, ISSN(Online): 2320-9801,pp 2432-2436, Vol. 2, Issue 1, January 2014
16. [15]Dr.A.Muthu Kumaravel, Mining User Profile Using Clustering FromSearch Engine Logs, International Journal of Innovative Research in Computerand Communication Engineering, ISSN(Online): 2320-9801,pp 4774-4778, Vol. 2, Issue 6, June 2014
17. [16]P.Kavitha, Web Data High Quality Search - No User
18. Profiling, International Journal of Innovative Research in Computerand Communication Engineering, ISSN(Online):
19. 2320-9801,pp 2025-2030, Volume 1, Issue 9, November 2013