ISSN:0975-9646

DACD: Delegated Access Control of Data in Cloud computing environment

Dhanamjay.K[1], Krishna Sagar.B [2]

[1]M.Tech Student , [2]Assistant Professor in Computer Science and Engineering

Abstract-Cloud computing provides a service based on internet for several shared resources and system software across various environment. For secure cloud storage the process of encryption of the data to the users for various needs has been brought by the delegated access control method. Generally storage in public cloud requires high communication, heavy load due to maximum storage and high computational costs. In this paper, we are implementing multi-cloud environment for secure storage where it acts as a public cloud and provides low costs, also it involves two- layer encryption over the data stored in the cloud. We are using an efficient AES algorithm which provides higher confidentiality and privacy for several users in the cloud and stores the data in multi-clouds where the users can retrieve with the keys later while delegating it through access control from the cloud. Securities as well as expenses are the peak issues in this field of research and they vary significantly, depending on the vendor.

Keywords:Privacy, Cloud computing, Delegation, Encryption, Access control

1. INTRODUCTION

1.1 Cloud computing

Cloud computing is everywhere because the locality of physical resources and devices has been accessed in general are not known to the end user. It also provides services for users to build, deploy and manage their applications on the cloud. It involves virtualization of resources that maintains and manages by itself. It is a tool for providing simple, needed network access to a shared resources of configurable computing environment (network, storage etc) which can be swiftly provisioned and released with negligible management effort otherwise service provider interaction. Today most of the companies have to process huge amounts of data in a cost- reducing manner. Classic users are operators of Internet search engines such as Google, Yahoo, or Microsoft. The vast amount of data they have to deal with every day has made database solutions more expensive.

1.2 Privacy and Security

Security is mainly necessary for strong privacy in all online computing factors, but security alone is not enough. Security and cost are the pinnacle issues in this area of research and they vary greatly, depending on the vendor one choose. Despite the first success and recognition of the cloud computing model and the extensive availability of providers and tools, a number of challenges and risks are innate to this new model of computing

1.3 Delegation

Data collector may share data with unknown parties if they do not follow the privacy policy. In the proposed model, delegation follows privacy policy which allows only legitimate parties accessing the data. It also sets the data usage guidelines for them. Between two parties as inter-visibility delegation. The party or visibility which shares data is called source visibility while the visibility that receives data is called destination visibility. In addition, we study intra-visibility delegation where two users within a party share the access rights with each other. Users who delegate the rights are called delegators while users who receive the rights are called delegates

2. SYSTEM OVERVIEW

2.1 Existing System

Several factors based on encryption have been proposed for access control over encrypted group with a different symmetric key. Users will be issued keys for the data's which are accessible. Links to minimize the amount of keys that are to be distributed to the users who exploit them hierarchical and other relations among data items. Such approach has several limitations. As the data owner doesn't handle a copy of the data, whenever the user dynamics change, the owner needs to download the data for decryption, and re-encrypt it with the new keys for uploading. This progression must be practical applied to all the encrypted data items with the similar key. It is bungling when the data set to be re-encrypted is huge. To issue new keys, the owner wants to set up private communication channels by means of the users. The privacy and the identity of users are not taken into account. Therefore it can learn sensitive information about the organization and their users.

It requires the owner to enforce all the ACPs by encryption, both initially and subsequently after users are added or revoked. All these encryption activities have to be performed at the owner that thus incurs high communication and computation cost.

3.PROPOSED ARCHITECTURE

3.1.Proposed System

In this paper, we are using two-layer encryption for storage of data across multi-clouds rather than a single public cloud. This two layer enforcement helps one to reduce the load on the Owner and delegates access control enforcement over the cloud. Especially, it provides a better way for various updates, user locations, and modifications of the data. The system goes through one additional phase compared to the existing system. Also, it provides several functions based on the decomposition or splitting of data to store across various clouds, which are finally retrieved by the user with the help of keys

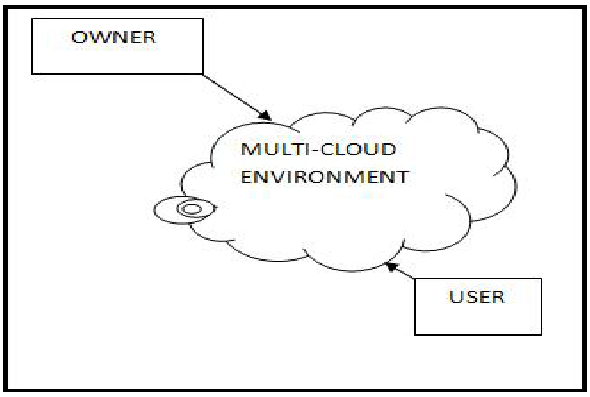


Fig 1: Multi-cloud storage

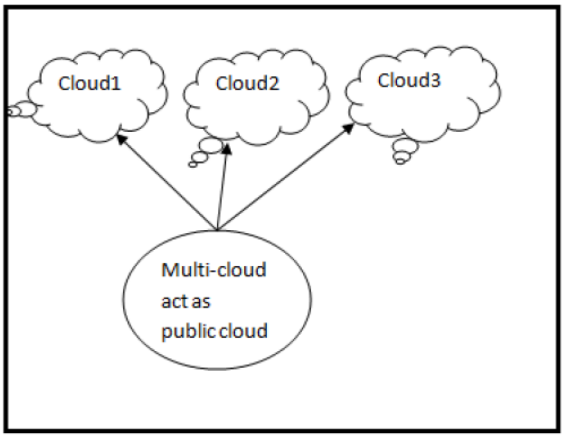


Fig 2 : Multi-cloud splitting

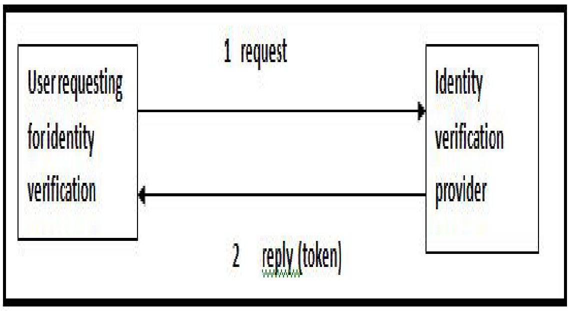

User requesting for identity verification
1 request
2 reply (token)
Identity verification provider

Fig 3: Two layer encryption in multi-cloud Environment

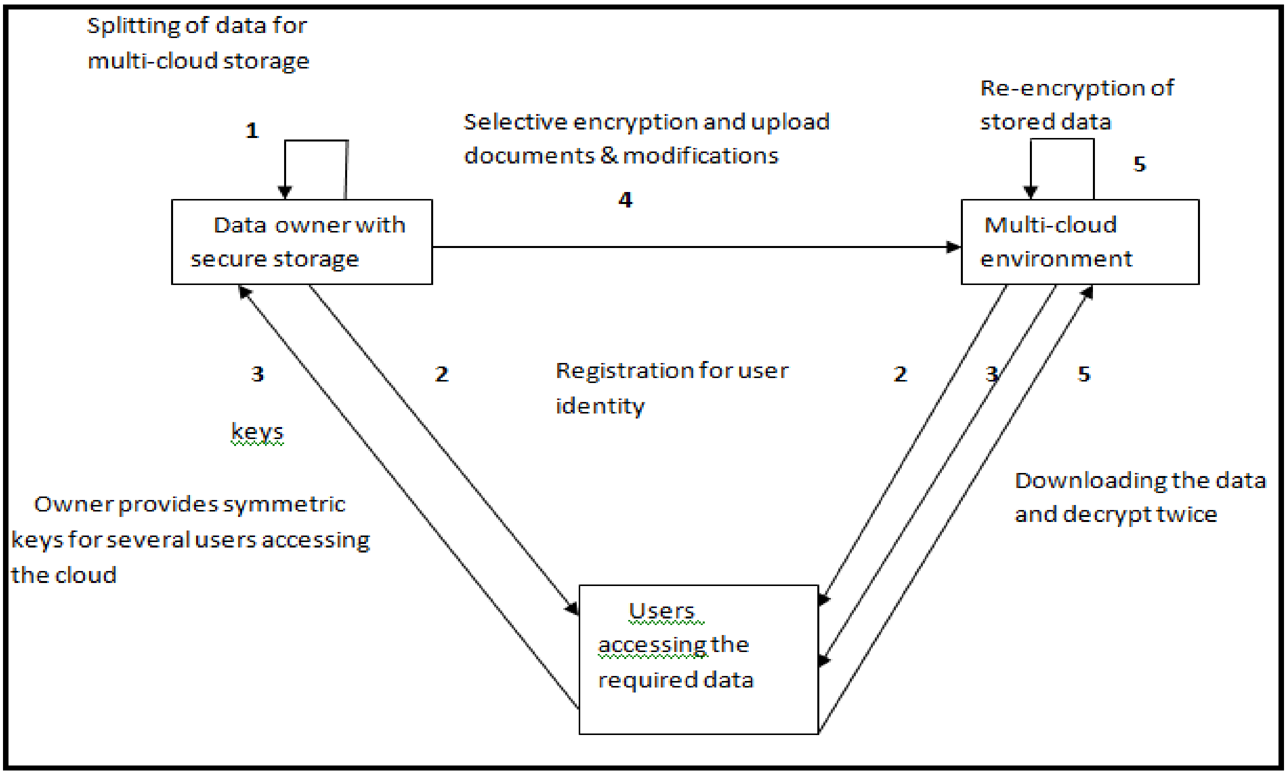
4. Two Layer Encryption Method

4.1 Identity token providence:

IdP's issue identity tokens to Users based on their identity attributes.

4.2 Policy decomposition:

The Owner decomposes each ACP into at most two sub ACPs such that the Owner enforces the minimum number of attributes to assure confidentiality of data from the Cloud. It is important to make sure that the decomposed ACPs are consistent so that the sub ACPs together moves the original ACP's The Owner enforces the confidentiality related sub ACPs and the Cloud enforces the remaining sub ACPs.


Splitting of data for multi-cloud storage
1
Selective encryption and upload documents & modifications
4
Re-encryption of stored data
5
Data owner with secure storage
Multi-cloud environment
3
2
Registration for user identity
2
3
5
keys
Owner provides symmetric keys for several users accessing the cloud
Downloading the data and decrypt twice
Users accessing the required data

4.3 Identity token registration:

Users register their identity tokens in order to obtain secrets to decrypt the data that they are allowed to access. Users register only those identity tokens related to the Owner's sub ACPs and register the remaining identity tokens with the Cloud in a privacy preserving manner. It should be noted that the Cloud does not learn the identity attributes of Users during this phase.

4.4 Data encryption and uploading:

The Owner encrypts the data based on the Owner's sub ACPs in order to hide the content from the Cloud and then uploads them along with the public information generated by the keygen algorithm and the remaining sub ACPs to the Cloud. It in turn allows data encryption based on the keys generated using its own algorithm. Note that the Keys at the Cloud takes the secrets issued to Users and the sub ACPs given by the Owner into consideration to generate keys.

4.5 Data downloading and decryption:

Users download encrypted data from the Cloud and decrypt the data using the derived keys. The users decrypt the data twice.

5. Conclusion

In this paper, we present a unique method for privacy preserving of data storage in multi-cloud environment. It also provides several advancements in cloud computing due to its technical capabilities. The feature work may also involves load-balancing in multi-cloud environment for maximum storage and accuracy for various users. Cloud computing is a growing paradigm as an enabling technology to deliver on-demand and elastic storage and computing capabilities, while removing the ownership need for hardware. But several privacy and security act demand strong protection of the cloud users, which in turn increases the complexity to develop privacy-preserving cloud services. The privacy preserving using delegated access control in multi-cloud delivers the critical capabilities required for a robust, cost-effective, and secure cloud security implementation.

References

[1] M. Nabeel and E. Bertino, “Privacy preserving delegated access control in the storage as a service model,” in EEE International Conference on Information Reuse and Integration (IRI), 2012.

[2] Rakshit, A. , et. Al, “Cloud Security Issues”, 2009, IEEE International Conference on Services Computing

[3] M.S.B. Pridviraju et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (5) , 2012,5206 – 5209

[4] E. Bertino and E. Ferrari, “Secure and selective dissemination of XML documents,” ACM Trans. Inf. Syst. Secur., vol. 5, no. 3, pp. 290–331, 2002.

[5] G. Miklau and D. Suciu, “Controlling access to published data using cryptography,” in VLDB ’2003: Proceedings of the 29th international conference on Very large data bases. VLDB Endowment, 2003, pp. 898–909.

[6] N. Shang, M. Nabeel, F. Paci, and E. Bertino, “A privacy- preserving approach to policy-based content dissemination,” in ICDE ’10: Proceedings of the 2010 IEEE 26th International Conference on Data Engineering, 2010.

[7] X. Liang, Z. Cao, H. Lin, and J. Shao, “Attribute based proxy re-encryption with delegating capabilities,” in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, ser. ASIACCS ’09. New York, NY, USA: ACM, 2009, pp. 276–286.

[8] C.-K. Chu, J. Weng, S. Chow, J. Zhou, and R. Deng, “Con- ditional proxy broadcast re-encryption,” in Proceedings of the 14th Australasian Conference on Information Security and Privacy, 2009, pp. 327–342.

[9] J.-M. Do, Y.-J. Song, and N. Park, “Attribute based proxy re-encryption for data confidentiality in cloud computing environments,” in Proceedings of the 1st International Conference on Computers, Networks, Systems and Industrial Engineering. Los Alamitos, CA, USA: IEEE Computer Society, 2011, pp. 248–251.

[10] L. Bussard, G. Neven and F.S. Preiss, “Downstream Usage Control,” In proceedings of 2010 IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY), 22-29, 2010