ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 1 January 2015, Page No. 10140-10143

Data Privacy in Multi Cloud Environment using Third Party Key Providence in Public Clouds

S.V Satish Kumar Reddy[1], *K.Narayana*[2].

[1]PG Scholar, Dept of CSE, Seshachala Institute of Technology, Puttur-517583. Mail id: challasatishv@gmail.com

[2]ASSISTANT PROF, Head of the Department, Seshachala Institute of Technology, Puttur-517583, qualification: MS(IS),M.Tech , Mail id: karnatham.narayana@gmail.com, M.Phil pursuing S.V.Univrsity, Tirupati.

Abstract: Cloud computing provides the data to the users remotely on different services. The Encryption plays major role in securing the data in cloud. We can access the data using encryption with key for more privacy reasons. Now-a-days the public cloud needs more privacy because of the increment of number of users everyday. The multi cloud technique performs load balancing when there is huge transactions of the data. The key is used to arrange more security for accessing the data by the owner, but to have secure communication better to have a support of the third party for key issuing. In this paper we provide third party for key providing in multi cloud environment. The encryption algorithm provides basic security for the data.

Keywords: Privacy, Multi cloud, Third party, Encryption.

I. INTRODUCTION

Cloud computing has the property of transparency in the communication process between user and the cloud. It is emerging because of its scalability and elasticity property. The virtualization makes data availability for all users using build and deployment in platform, software and infrastructure services. The huge data in cloud is stored and handled by various cloud service providers. The security is major aspect in cloud, so we can have third party which can handle all the key providence to keep both cloud and the users secure.

With out privacy policy data collector may provide data to all users, the privacy policy makes data provider to whom it can give data. The access of data to authorized users should go through privacy policy. Third party follows many encryption techniques to provide the key to both the users and cloud uniquely for accessing the data. The cloud makes the privacy policy accessing to be followed for data access.

The data accessing has two layer of encryption for the privacy where coarse grained and fine grained encryption is performed on the data. The cloud, data owner, user and third party is combined to form a total package of communication. The burden on a cloud is decreased by multi cloud and the third party.

II. EXISTING SYSTEM

Several factors based on encryption and key providence have been proposed for access control over the data in cloud. Users will be issued keys for the data's which are accessible by owner. The secure communication between user and the data owner will be doubtful. The single cloud may be in risk for satisfying the request of user and data owner. 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.

III. PROPOSED SYSTEM

In this paper, we are using two-layer encryption and third party key providence for data access in multi cloud environment rather than a single public cloud. This two layer enforcement helps one to reduce the load on the Owner and delegate’s access control enforcement over the third party. Especially, it provides a better way for security of data and various updates, user locations, and modifications of the data. The system goes through one additional step 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.

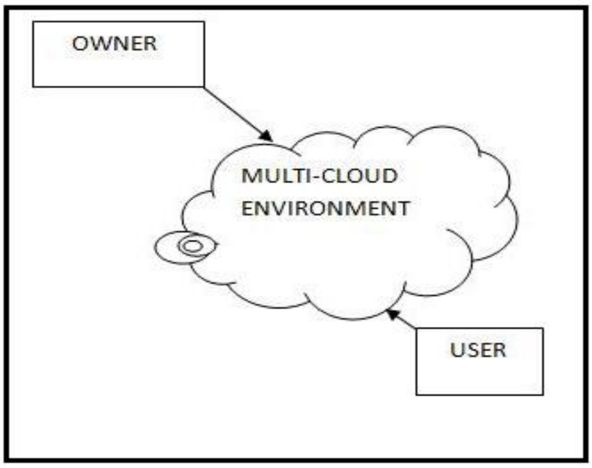


Fig 1: Multi-cloud storage

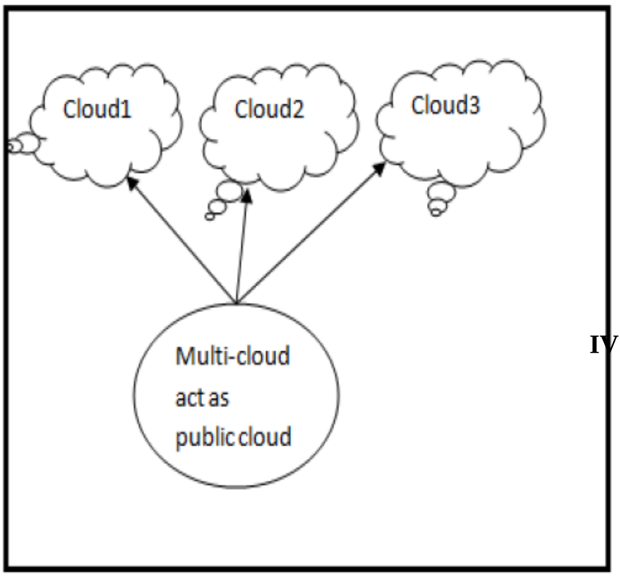


Fig 2: Multi-cloud splitting

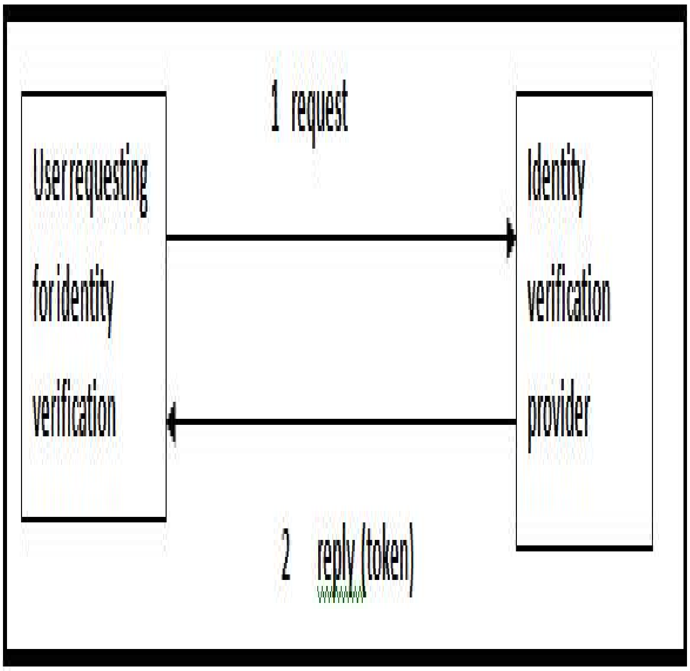

1 request
User requesting for identity verification
Identity verification provider
2 reply (token)

Fig 3: Two layer encryption in multi-cloud environment

IV. TWO LAYER ENCRYPTION METHOD WITH THIRD PARTY TOKEN PROVIDENCE

Steps:

1)The Identity Token is provided to users based on their identity attributes. The policy which is used for privacy is decomposed so that the original is obtained when rollback. The decomposed access control policies are consistent so that sub access control policies together moves to original Access Control Policies.

2).The User register the identity token in order to start the accessing of data both at data owner and the cloud, the user information in available at cloud and data owner. After the registration the users are allowed to have secrets for decryption for privacy preserving.

3)The keys are requested from the third party in order to have access for the data. The third party has more encryption technologies for key providence.

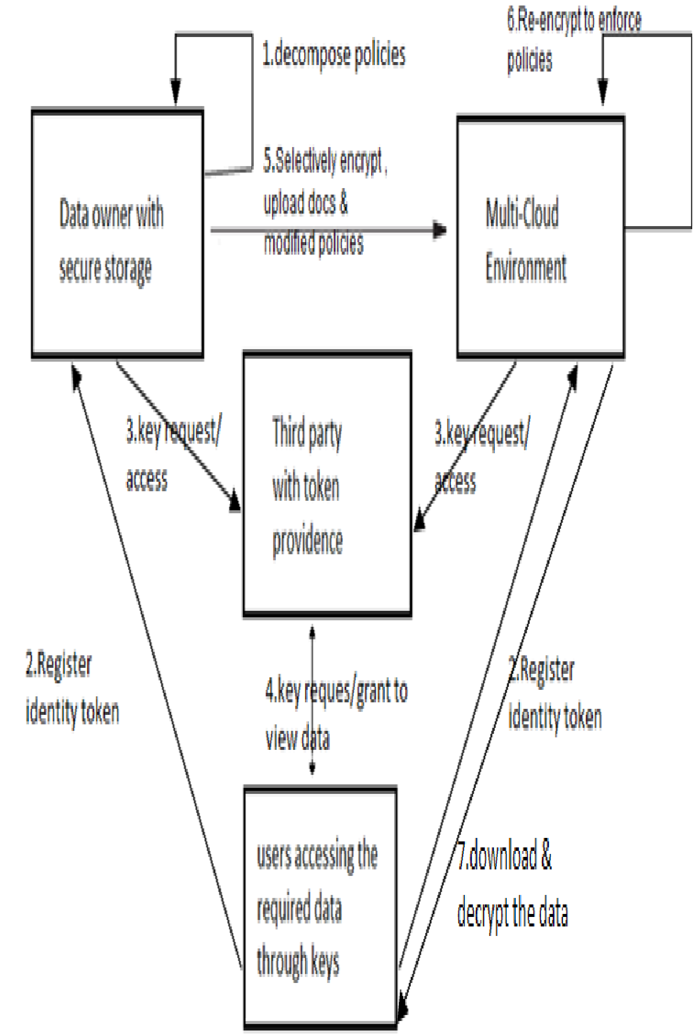
4)User request the key from third party then using the key the data can be accessed. The authorization can be monitored by the third party which has more encryption and data keys, the matching of the key denotes the file is ready to be accessed. Encryption algorithms helps third party to handle with random keys.

5)The owner encrypts the data as coarse grained encryption in order to hide the content from the cloud. The data is now uploaded to the cloud where policies are applied. Task of owner is reduced by additional phase which provides the keys.

6)The cloud again encrypts data using policies as fine grained encryption. It is the outer layer encryption the cloud will not provide the keys it is shifted to third party.

7)Data downloading and decryption can be done using keys by the third party. The encrypted data is downloaded from cloud and decrypted twice.

8)).The User register the identity token in order to start the accessing of data both at data owner and the cloud, the user information in available at cloud and data owner. After the registration the users are allowed to have secrets for decryption for privacy preserving.


1.decompose policies
6.Re-encrypt to enforce policies
5.Selectively encrypt , upload docs & modified policies
Data owner with secure storage
Multi-Cloud Environment
3.key request/ access
Third party with token providence
3.key request/ access
2.Register identity token
4.key reques/grant to view data
2.Register identity token
users accessing the required data through keys
7.download & decrypt the data

V. CONCLUSION AND FUTURE WORK

In this paper, we present a unique method for data privacy with third party key providence in multi-cloud environment, which reduces the burden of the cloud. It also provides several advancements in cloud computing due to its technical capabilities.

Fig. 1 Example of an unacceptable low-resolution image

The future 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 data privacy using third party key providence in multi-cloud delivers the critical capabilities required for a robust, cost-effective, and secure cloud security implementation.

The heading of the Acknowledgment section and the References section must not be numbered.

Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template. To see the list of contributors, please refer to the top of file IEEETran.cls in the IEEE LaTeX distribution.

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 Endownment 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 envi- ronments,” 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.

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

[12]“OpenSSL the open source toolkit for SSL/TLS,”http://www.openssl.org/.