PRIVACY PRESERVING ATTRIBUTE-BASED ACCESS CONTROL APPROACH FOR PUBLIC CLOUD

Prasad Tupkari, Bhushan Udawant, Sonali Vakale, Rohan Wagh

Dept. of Computer Engineering, SRES's College of Engineering,
Kopargaon.

Abstract

Security and privacy represent major concerns in the adoption of cloud technologies for data storage. An approach to mitigate these concerns is the use of Two Layer Encryption (TLE) which includes coarse-grained and fine grained access control encryption. But in this approach Data owners thus incur high communication and computation costs. To overcome this problem data owner performs a confidentiality related encryption; whereas the Trusted Third Party (TTP) performs a fine-grained re-encryption on top of the owner encrypted data which address this challenging issue using capability based access control with TTP to ensure valid users will access the outsourced data. In this paper, we proposed encryption method at TTP side to protect the privacy and integrity of outsourced data in cloud environment.

Keywords- coarse-grained, fine-grained, privacy, Trusted Third Party (TTP), Two Layer Encryption (TLE), security.

I. INTRODUCTION

Data storage on cloud is an important concern in security and privacy. In this approach these concerns are reduced by using encryption. The encryption on the data before uploading it to cloud assures confidentiality. In traditional approach fine-grained encryption is performed at owner side which is an overhead for owner and the encryption is performed depending on their identity attribute. The fine-grained access control assures data security and privacy. Also efficiently shares data among different users.

II. RELEATED WORK

Cloud:

The inspiration for the name cloud computing is from the symbol which represents internet in flow chart diagram. There are three distinct characteristic in cloud service which differs from traditional hosting.

1) Sold on demand or pay per use.
2) Elasticity, a user can have as much or as little of a service as they want at any given time.
3) The service management which will be taken care by provider. The requirement of the consumer is just a computer and Internet access.

Cloud computing offers significant innovations in virtualization and distributed computing, improves access to high-speed Internet as well and accelerated interest to a weak economy. Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) are the different service-oriented cloud computing models.

A cloud can be private or public. The public cloud consists of cloud service that can be sold to anyone on the Internet. Currently Amazon Web Services is the largest public cloud provider. The private cloud acts as a proprietary network or hosted services are supplied to limited people through Data Center. The ultimate goal of cloud computing is to provide scalable and easy access to cloud computing resources.

The security requirements in service-oriented cloud computing model are as follows:

• Data Security
The provider must ensure that their infrastructure is secure and that their client's data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.

• Privacy
The providers must ensure that all critical data are properly protected and that only authenticated users have access to its data.

• Data Confidentiality
The users of cloud should be satisfied that their data are confidential to unauthorized user, including cloud service provider.

• Fine-Grained Access Control
The provider grants differential access rights to a set of users and allow flexibility in specifying the access rights of individual users. This would be possible by encrypting the data by using certain access control possible.

Trusted Third Party (TTP):

In cryptography, a trusted third party facilitates interactions between two parties[8]. Here all critical transaction communication between parties occurs which is responsible for creating fraudulent digital content. The third party uses cryptography and other security measure to authenticate the identity of the sender and provide security during data transmission and to verify delivery to the intended user. TTP records and monitors the user database activities that are selected.

III. TRADITIONAL SYSTEM

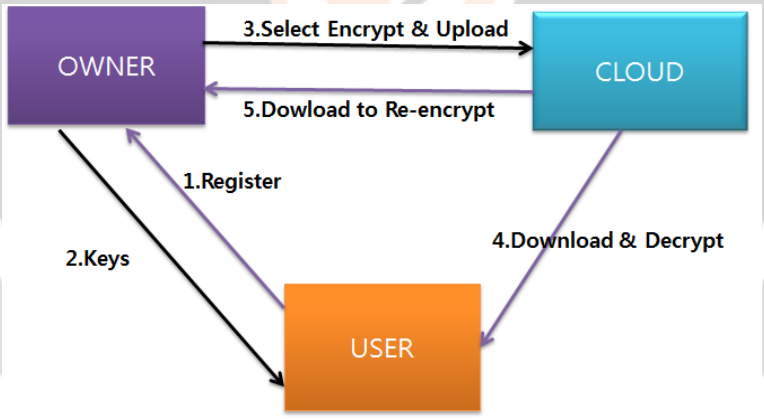

Fig-1 : Traditional Architecture

1) In traditional approach data owner does not keep a copy of data and whenever user dynamics or ACPs change the owner download and decrypt the data, re-encrypt it with new keys and then uploads encrypted data. This process is applied to all data items encrypted with same key. This is inefficient when the data set to be re-encrypted is too large.

2) The new keys are provided to authenticate users as the data owner needs to establish private communication channels with the users.

3) The identity attributes of the users is not taken into their account. Therefore cloud can learn information about the users and organizations.

4) Recent introduced approaches based on broadcast key management [3], [9], [10], which is referred to as single layer encryption. In this SLE approach data owner is required to perform fine-grained encryption for enforcing access control policies that assures privacy of the user unlike previous approach. Where owner enforces all ACPs initially and afterwards user dynamics or access control policies changes.

Issues in traditional system

1) Not a secure approach to store data and to maintain its privacy.

2) Inefficient when data set to be Re-encrypted is large.

3) In Traditional approach the data owner needs to enforce all the ACPs by fine-grained encryption which is overhead for owner.

IV. PROPOSED SYSTEM

To overcome the challenges on traditional system we introduce new approach named Two Layer Encryption (TLE).
Please, make a note that this approach is not new. In this approach challenging task is to re-encrypt encrypted data on public cloud. So we will use Trusted Third Party (TTP) as an intermediate between data uploader and public cloud.

The proposed system architecture is shown below,

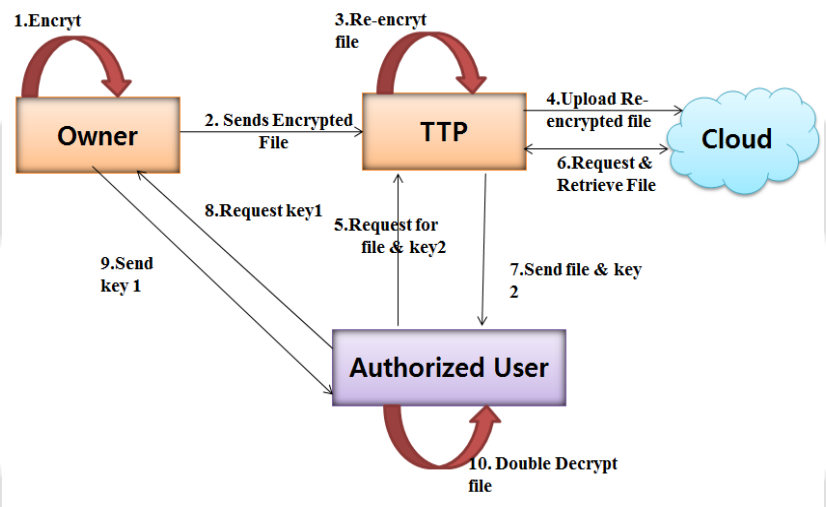

Fig-2 : Proposed Architecture

Initially data owner and respective authorized data users should register to the system with valid id and password. After successful registration and login the data owner encrypt the file to be uploaded and stores generated key 1 then it sends the encrypted file and public information to the intermediate TTP for re- encryption. The TTP re-encrypts the file and generates key 2 for decryption at user side and stores re-encrypted file on to the cloud. Whenever authorized user wants any file it will send request to TTP for file and key 2. TTP first verify the user if user is authorized then TTP retrieves requested file from cloud and send that file and key 2 to the user. Then user sends the request to data owner for key 1 of respective file. Owner sends key 1 of that file. After receiving both the keys user will double decrypt the file to get original file and by using proper algorithm it will verify integrity of file.

The modules in this system can be stated as follows:

Registration:
This module is used for registration of owner and user.

Login:
This module is used for login of owner, user and TTP.

File Encryption:
This module is used for performing encryption of user data at owner.

Re-encryption and Cloud Storage:
This module is used for performing re-encryption of file by TTP there by storing the file on cloud.

File and Key Request:
This module is used for processing file and key 2 request from TTP whereas key 1 request form owner.

File Receive and Double Decrypt:
In this module double decryption of data is performed for accessing the data by user.

V. CONCLUSION

Current technologies for uploading the encrypted data incurs high cost because it manages all keys. Whenever user dynamics and access control policies changes, the burden on the owner increases as owner has to manage all keys. To reduce the overhead of the data owner, we proposed a two layer encryption based approach to reduce the burden on the data owner and delegate access control to TTP in cloud environment. The Two Layer Encryption overcome this by making system more efficient to provide high level of security to user data and also maintains its privacy and confidentiality and also the intermediate TTP makes access control polices in such a way that only authorized user will have access to data which they deserved.

REFERENCES

[1] M. Nabeel and E. Bertino, "Privacy Preserving Delegated Access Control in Public Clouds," IEEE Trans. Knowledge and Data Eng., vol. 26, no. 9, pp. 2268-2280, Sept. 2014.
[2] G. Miklau and D. Suciu, "Controlling Access to Published Data Using Cryptography," Proc. 29th Int'l Conf. Very Large Data Bases (VLDB '03), pp. 898-909, 2003.
[3] M. Nabeel, N. Shang, and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," IEEE Trans. Knowledge and Data Eng., vol. 25, no. 11, pp. 2602-2614, Nov. 2013.
[4] S.D.C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over- Encryption: Management of Access Control Evolution on Outsourced Data," Proc. 33rd Int'l Conf. Very Large Data Bases (VLDB '07), pp. 123-134, 2007.
[5] A. Shamir, "How to Share a Secret," Comm. ACM, vol. 22, pp. 612-613, Nov. 1979.
[6] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure Attribute-Based Systems," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 99-112, 2006. Secure Cloud Data ," ISSN(E): 2321-8843; ISSN(P): 2347-4599 Vol. 2, Issue 6, Jun 2014, 203-210.
[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine- Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.
[8] R. S. Nejkar and G. A. Patil , "Trusted Third Party Service for Secure Cloud Data ," ISSN(E): 2321-8843; ISSN(P): 2347-4599 Vol. 2, Issue 6, Jun 2014, 203-210.
[9] N. Shang, M. Nabeel, F. Paci, and E. Bertino, "A Privacy-Preserving Approach to Policy-Based Content Dissemination," Proc. IEEE 26th Int'l Conf. Data Eng. (ICDE '10), 2010.
[10] M. Nabeel, E. Bertino, M. Kantarcioglu, and B.M. Thuraisingham, "Towards Privacy Preserving Access Control in the Cloud," Proc. Seventh Int'l Conf. Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom '11), pp. 172-180, 2011.

AUTHORS

1. Prasad R. Tupkari, BE in Computer Engineering, SRES's College of Engineering, Kopargaon.

2. Bhushan G. Udawant, BE in Computer Engineering, SRES's College of Engineering, Kopargaon.

3. Sonali R. Vakale, BE in Computer Engineering, SRES's College of Engineering, Kopargaon.

4. Rohan N. Wagh, BE in Computer Engineering, SRES's College of Engineering, Kopargaon.

CORRESPONDANCE AUTHOR

1. Prof A. V. Brahmane, Assistant Professor, SRES's College of Engineering, Kopargaon.