International Journal of Innovative Research in Advanced Engineering (IJIRAE)
Volume 1 Issue 3 (May 2014) SPECIAL ISSUE

HEA WITH ACCESS CONTROL POLICIES IN PUBLIC CLOUD

Rahul Prasad
M.Tech student, Dept. Of CSE
Sri Venkateshwara College of Engineering, Bangalore
rahulprasad.svce@gmail.com

Sushma B
Asst. Prof, *Dept. Of CSE*
Sri Venkateshwara College of Engineering, Bangalore
sushma_b10@yahoo.com

ABSTRACT- ***In this paper two types of encryption schemes are discussed, in the primary schemes Data Owner will encrypt all records or data by using symmetric key algorithm before uploading to the cloud server and then secondary schemes carry out by cloud server, where cloud server perform complete access control policies related encryption on the top of the Data Owner encrypted records or data. This proposed scheme provides the confidentiality of the records or data and also protects the user's private information from the public cloud server.***

KEYWORDS—Hybrid Encryption Approach (HEA), AES-Encryption and Decryption, Access control policies, Cloud Computing and Confidentiality

I. INTRODUCTION

Security and confidentiality are important points to be considered while adopting cloud technologies for data storage. Security and confidentiality of records in cloud server can be performed with the help of encryption. The Traditional Encryption Approach is not sufficient for assure the confidentiality of records from the cloud server. Nowadays every organization perform access control polices (ACPs) means "*which users can access which data or records";* these access control policies can be expressed in the terms of user property, called as *identity attribute,* using access control language. Such an approach, called as Attribute Based Access Control (ABAC) [1], support fine-grained access control which is essential for high-assurance data security and confidentiality.

The problem statement in this paper is Traditional Encryption Approach (TEA) does not consider the metadata of encrypted records or data maintain in the Identity Provider i.e. third party whenever user's dynamic changes or when the access control policies are updated. The confidentiality of the user identity attributes of the users is not considered. Therefore the cloud can learn sensitive information about the users and their organization.

The main objective of this paper is to store the files in secure way along with flexible access control in public cloud and also minimize computation cost.

II. TRADITIONAL ENCRYPTION APPROACH

In this section**,** the existing system is briefly discussed. Fig. 1 show Traditional Encryption Approach (TEA), where records or data items are combined together is based on access control policies and using different symmetric key every combined records or data items are encrypted after that key send only to authorize users for records or data item which users can have the permission to access. Extensions to reduce the number of keys that need to be distributed to the users have been proposed exploiting hierarchical and other relationships among data items. Such approaches have various limitations:

1. In TEA, Data Owner does not maintain a copy of the records or data, whenever user's dynamics changes, the Data Owner needs to:
   a) Download and decrypt the data
   b) Re-encrypt the data with new keys
   c) Upload the encrypted data in the cloud.

This above step will apply to all encrypted records or data with same key but this process is inefficient when large data set to be encrypted.

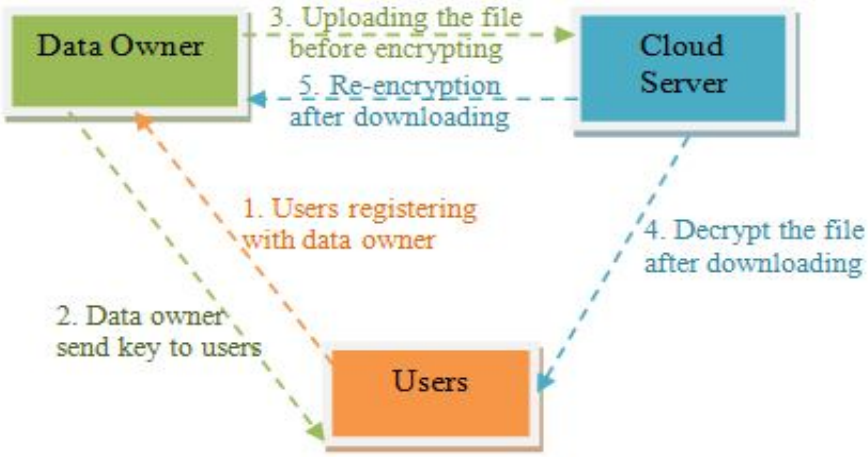

Fig. 1: Traditional Encryption Approach

2. Data owner needs to be establishing a private communication channels with the users for issuing new keys.
3. User's identity attributes confidentiality is not considered. So the cloud can learn user private information and their organization.
4. TEA does not support fine-grained ABAC policies.

TEA is based on broadcast key management scheme[2][3][4], addresses some of the above limitations, but it still require data owner to enforce all ACPs by fine-grained encryption whenever user dynamics changes due to all these encryption activities perform at Data Owner that needs high communication and computation expenditure. *For e.g.*, whenever user added or revoked in the system, the data owner need to download the affected data from the cloud, generate new encryption key, re-encrypt the downloaded data with new key, and then upload the re-encrypted data to the cloud server.

III. HYBRID ENCRYPTION APPROACH

In this section**,** the proposed system is briefly discussed. **Hybrid Encryption Approach (HEA),** by name itself says that there are two ways of encryption schemes, in the first way the Data Owner will encrypt all the records or data using symmetric key algorithm i.e. AES algorithm before uploading the encrypted records or data to the cloud sever in order to ensure the confidentiality of the records or data items from the cloud server and then second way carried out by cloud server, where cloud server performs the complete access control related encryption on the top of the data owner encrypted data or records. But challenging issue in this approach is how to decompose the ACPs so that it supports fine-grained ABAC policies while at same time the confidentiality of the identity attributes of users and records or data are assured [5]. However, performing two ways of encryption is new and provides a superior result than Traditional Encryption Approach. Fig. 2 show general ideas behind data under HEA, where initially data is encrypted by Data Owner and then again encrypted data is encrypted by Cloud server.

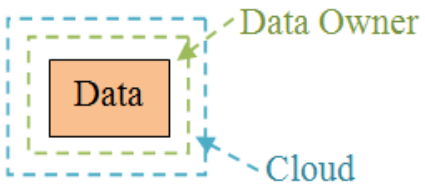

Fig. 2: Data under HEA

Consider the hospital example, where hospital acts as a Data Owner support access control on medical records and makes these records available to hospital employees acts as Users, and Users have different roles as an attribute such as receptionist (rec), cashier (cas), doctor (doc), nurse (nur), pharmacist (pha) and system administration (admin).

The main contributions of this paper are:

1. The proposed system is able to protect user's information from the cloud.
2. Efficient algorithm called KeyGen algorithm is used to generate key for proposed system.
3. The proposed system supports the fine grained ABAC policies.

The proposed system HEA has several advantages:

1. When user is revoked, only access control encryption needs to be updated.
2. No data transmission is required between data owner and cloud.
3. No need to establish private communication channel with users for issue new keys.
4. Assures the confidentially of the data and preserves the privacy of user from the cloud.
5. Minimize computation cost.
6. Supports fine-grained ABAC policies.

Fig. 3 shows a user registration, where user registers with username along with domain. After that IDP provide download permission to user for downloading file.

Fig. 3: User Registrations

Fig. 4 show an data owner registration, where data owner register with attribute like name, validity, space along with permission like upload file, account notification, audit logs and file deletion.

Fig. 4: Data Owner Registrations

Fig. 5 show **Hybrid Encryption Approach (HEA),** consist of the following phase:

1. Identity Provider: Identity Provider (IDP) Module maintained the metadata of encrypted data with details like filename, public key and secret key along with user privilege and attacker details also maintained in this system and IDP also deal with creating new data owner and users.

2. Data Owner Registration: Identity Provider will create new data owner by providing details like username, validity and file size allowed. According to the Data owner roles i.e. admin, doc etc the IDP will provides the permission like upload file, account notification, audit logs and file deletion.

3. File Encrypting and Uploading: Data Owner Module browse the file from the system and send the encrypted file to cloud server by providing username, filename and cloud IP address. For encrypting the file AES algorithm is used and combination of RSA and KeyGen algorithm is used for key distribution. After that data owner need to send metadata of particular file to the Identity Provider by providing filename and cloud IP address.

4. Cloud Server: Cloud Server Module maintain all data owner files with following details like filename, cloud IP address, public key and private key. Particular data owner file also can be seen by providing file name. Even cloud server module can have the permission to modify any particular data owner file. Blocked users information is also maintained in this system.

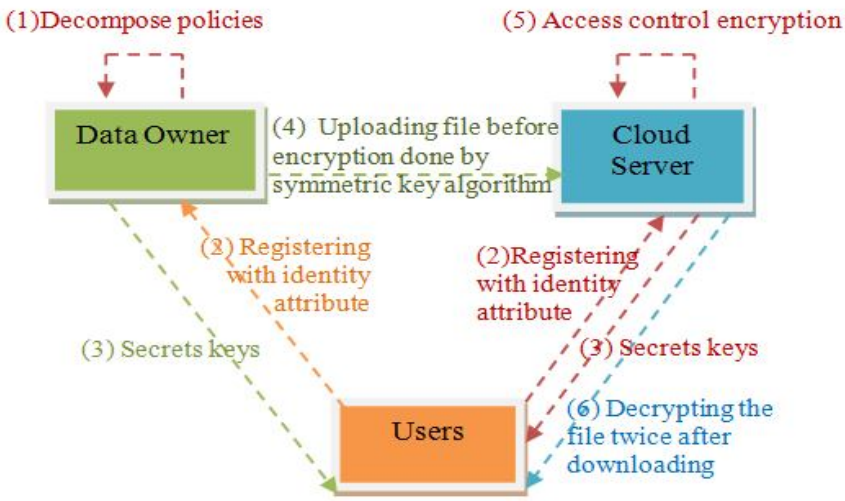

Fig. 5: Hybrid Encryption Approach

5. User Registration: Identity Provider will register users by providing details like username, download access permission along with suitable attribute i.e. doc.

6. File downloading and decrypting: User Module can download the particular file by providing username, filename, and secret key along with attribute at the time of registration. Here decrypting the file twice, first by providing attribute like doc, it decrypt the access control encryption i.e. outer layer encryption of the file and then again decrypt the file by AES algorithm i.e. inner layer encryption of the file. Suppose if user is trying to attack any file by giving wrong secret key, then particular user suddenly will be blocked and blocked list will update in Identity Provider as well as cloud server module.

IV. EXPERIMENTAL RESULTS

The experiments are performed on Windows XP with an AMD Athnol (tm) 64 X2 Dual core processor 5200+ 2.71 GHz, 960 MB of RAM. The proposed prototype system is implemented in java coding. In this AES-256 implementation is used for encryptions. Combination of RSA and KeyGen algorithm is used for key distribution to the user where key size is 16, the first 10 bit is used for public key and 6 bit is for private key.

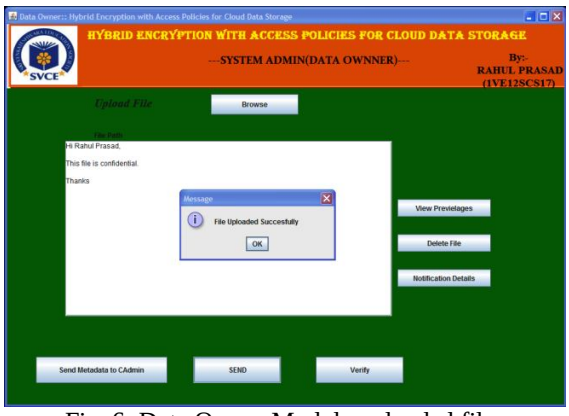

Fig. 6: Data Owner Module uploaded file

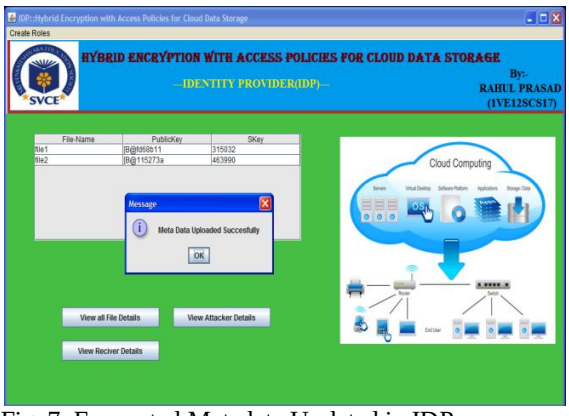

Fig. 7: Encrypted Metadata Updated in IDP

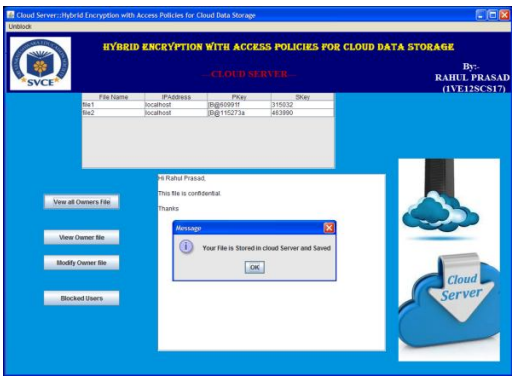

Fig. 8: File stored in Cloud Server Module

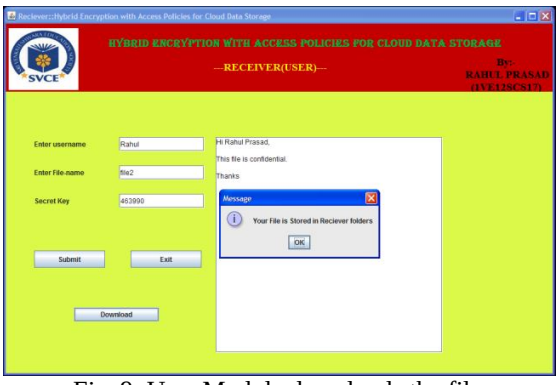

Fig. 9: User Module downloads the file

V. CONCLUSION

This paper describes a unique method for privacy preserving of data storage in cloud environment. Where two types of encryption approach is performed. This proposed system provide the confidentially of the file or records and protect the confidentiality of user information from the cloud server. As future works, investigate alternative choices for the HEA and will try to minimize computational cost.

REFERENCES

[1] M. Nabeel and E. Bertino, "Privacy preserving delegated access control in public cloud," in IEEE Transactions on Knowledge and Data Engineering, 2013.

[2] M. Nabeel and E. Bertino, "Privacy preserving policy based content sharing in public clouds, "In IEEE Transactions on Knowledge and Data Engineering, 2012.

[3] M. Nabeel, E. Bertino, M. Kantarcioglu, and B. M. Thuraisingham, "Towards privacy preserving access control in the cloud," in Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing, ser. CollaborateCom '11, 2011, pp. 172–180.

[4] 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.

[5] M. Nabeel and E. Bertino, "Towards attribute based group key management," in Proceedings of the 18th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2011.