International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 2, Issue 7, July 2015

Two Layer Approach to Enhance Data Security in Cloud

[1] Sameer Ahmed , [2] Romit Kumar, [3] Sultan Baig, [4] Neeraj Jain And [5] Vaidehi.M
[1,2,3,4]Under Graduate Students Department of Information Science and Engineering Dayananda Sagar College of Engineering, India
[5]Associate Professor Department of Information Science and Engineering Dayananda Sagar College of Engineering, India
[1] sameer.ahmed7799@gmail .com [2] romitkumar78@gmail.com [3] sultanbaig93@gmail.com
[4] neerajjain1993@gmail.com [5] dm.vaidehi@gmail.com

Abstract: **Fine grained encryption of data is essential to enforce fine grained access control on confidential data. In the Cloud operational model, security is a critical issue. In such scenarios, the data owner should be able to encrypt the data prior to submitting to Cloud and be able to re-encrypt whenever user permissions or authorization policies changes. This may lead to computation cost. This paper presents a fine grained access control to minimize operating cost at the data owners end and also ensuring data confidentiality at the Cloud service provider end. The proposed approach is based on two layers of encryption. Here the data owner performs a coarse-grained encryption and the cloud service provider performs a fine grained encryption on the data encrypted by the data owner. The proposed system assures confidentiality of data and also retains the privacy of users from the cloud.**

I.INTRODUCTION

Data security and privacy are the two important factors that should be ensured by the cloud service provider to its clients. One approach to ensure data security is by using efficient data encryption technique. The conventional encryption approach is in sufficient to support the enforcement of fine-grained organizational access control policies (ACPs)[1]

Many organizations have today ACPs regulating which users can access which data, these ACPs are often expressed in terms of the properties of the users, referred to as identity attributes, using access control languages such as XACML[1]. Such an approach, referred to as attribute-based access control (ABAC), supports fine-grained access control which is crucial for high-assurance data security and privacy. Supporting ABAC over encrypted data is a critical requirement in order to utilize cloud storage services for selective data sharing among different users. Notice that often user identity attributes encode private information and should be strongly protected from the cloud, very much as the data themselves.

II. EXISTING SYSTEM

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 encryption. However, whereas encryption assures the confidentiality of the data against the cloud, the use of conventional encryption approaches is not sufficient to support the enforcement of fine-grained organizational access control policies (ACPs) [1] [2] [3]. Many organizations have today ACPs regulating which users can access which data; these ACPs are often expressed in terms of the properties of the users, referred to as identity attributes, using access control languages such as XACML. Such an approach, referred to as attribute-based access control (ABAC), supports fine-grained access control which is crucial for high-assurance data security and privacy. Supporting ABAC over encrypted data is a critical requirement in order to utilize cloud storage services for selective data sharing among different users. Notice that often user identity attributes encode private information and should thus is strongly protected from the cloud, very much as the data themselves. Approaches based on encryption have been proposed for fine-grained access control over encrypted data. As showninFigure1, those approaches group data items based on ACPs and encrypt each group with a different symmetric key. Users then are given only the keys for the data items they are allowed 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 however have several limitations:

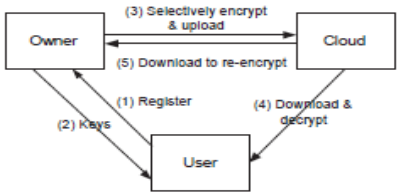

Fig. 1: Traditional approach

DISADVANTAGES OF EXISTING SYSTEM

As the data owner does not keep a copy of the data, whenever the user dynamics or ACPs change, the data owner needs to download and decrypt the data, re-encrypt it with the new keys, and upload the encrypted data. Notice also that this process must be applied to all the data items encrypted with the same key. This is inefficient when the data set to be re-encrypted is large. In order to issue the new keys to the users, the data owner needs to establish private communication channels with the users.

The privacy of the identity attributes of the users is not taken into account. Therefore the cloud can learn sensitive information about the users and their organization.

They are either unable or in efficient in supporting fine-grained ABAC policies.

III. Proposed system

The Two Layer Encryption (TLE) approach has many advantages. When the policy or user dynamics changes, only the outer layer of the encryption needs to be updated. Since the outer layer encryption is performed at the cloud, no data transmission is required between the data owner and the cloud. Further, both the data owner and the cloud service utilize a broadcast key management whereby the actual keys do not need to be distributed to the users. Instead, users are given one or more secrets which allow them to derive the actual symmetric keys for decrypting the data. This two layer enforcement allows one to reduce the load on the Owner and delegates as much access control enforcement duties as possible to the Cloud. Specifically, it provides a better way to handle data updates, user dynamics, and policy changes. The system diagram of the TLE approach. The system goes through one additional phase compared to the Single Layer Encryption (SLE) approach. We give an overview of the six phases below:

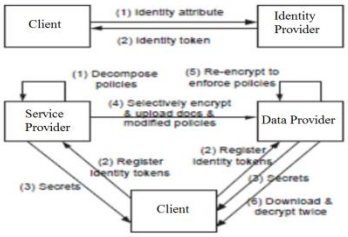

Fig 2:Two Layer Encryption Approach

ADVANTAGES OF PROPOSED SYSTEM

- More security as data is encrypted twice(AES+RNS)
- Access Control Policy is implemented by the cloud; so data owner burden is reduced.
- User privacy is preserved.

IV. MODULE DESCRIPTION

ADMIN

- Admin is a super user who creates the Data Owner and maintains the cloud servers' configurations. He has the right to Add, Edit or Delete the Data Owners.
- Once the Domain Authority logged in,he has following functions.
- Cloud Server (Add, Edit, Delete)
- Data Owner (Add, Edit, Delete)
- Domain
- Sub-Domain
- Change Password

Data owner

Data Owner is a person who will upload the files in cloud which in turn accessed by the authorized Data Users. Whenever the file is uploaded it will be encrypted by the system using Data Owners Encryption Key (Two Layer Encryption). Data Owner has to specify the Access Policy for each and every file. Access policies are set using Domain Attribute and Sub-Domain Attribute.

Once the Data Owner logged in he has following functions.

- User Details (View, Delete)
- View & Send Secret File
- View All Request
- Verify Identity Token

- Send Secret File to requested User

✓ Get RNS Key& AES Key
✓ Get user Domain & Sub Domain Details
✓ Concatenate Keys + Domain Details + Expiry Date
✓ Encrypt the above string using AES algorithm
✓ Send the Secret file to Requested User Email ID

- **File Upload**
- File Selection
- Encrypting using RNS
- Cloud Selection
- Move to cloud
- Transfer the Encrypted file to selected cloud
- Encrypting RNS output using AES
- Uploaded File Details (View, Delete)
- File Access Control Setting
- File Access Control Details (View, Delete)
- Transaction Details
- Change Password

V Data user

Data User can register themselves and he will receive the Identity Token through email.

Data Consumer will receive their access key (Attributed based Decryption Key) from respective data owner through email. With the help of the access key User can download the files for which they have access, remember access control is set by data owner.

Suppose the data user wants to download any file, first he has to select the file from the list and the system ask for the access key, After system getting the access key it will separate the Attribute Set from the key and check for the access rights, if the user has the access he can download the encrypted file which in turn decrypted using the decryption key and download to the data consumer local system.

Once the Data Consumer logged in he has following functions:

- User Registration – (Data Consumer)
- Fill the user details
- Provide Domain and Sub Domain Details
✓ Payment Gateway [Optional]
- Generate a Identity Token
- Email Identity Token to the user
- Login
- Identity Token Verification
- Request for Secret File

-
- Enter User ID
- Display User Details
- Upload Identity Token
- File Details (View)
- File Download
- Select the file from the list
- Select the Secret Identity file from the local system
- Send secret Identity file and Selected file to cloud
- Decrypt the Secret identity file
- Get the Domain Values
- Check the Access Control using Domain values
- If Access Control pass download the file or deny the file access
- Enter the transaction record in the table
- File Decrypt
- Select the file to be decrypted
- Select the Secret file
- Decrypt the file
✓ AES
✓ RNS

- Transaction
- View the transaction of logged user

VI. EXPERIMENTAL RESULTS

Security of the AES encryption is calculated as follow:
Faster supercomputer: 10.51 Pentaflops = 10.51 x 10^{15} Flops [Flops = Floating point operations per second]
No. of Flops required per combination check: 1000 (very optimistic but just assume for now)
No. of combination checks per second = (10.51 x 10^{15}) / 1000 = 10.51 x 10^{12}
No. of seconds in one Year = 365 x 24 x 60 x 60 = 31536000

No. of Years to crack AES with 128-bit Key = (3.4 x 1038) / [(10.51 x 1012) x 31536000]

= (0.323 x 1026)/31536000
= 1.02 x 1018
= 1 billion billion years

As shown above, even with a supercomputer, it would take 1 billion billion years to crack the 128-bit AES key using brute force attack. This is more than the age of the universe (13.75 billion years). If one were to assume that a computing system existed that could recover a DES key in a second, it would still take that same machine approximately 149 trillion years to crack a 128-bit AES key.

VII. CONCLUSION

Current approaches to enforce ACPs on outsourced data using selective encryption require organizations to manage all keys and encryptions and upload the encrypted data to the remote storage. Such approaches incur high communication and computation cost to manage keys and encryptions whenever user credentials or organizational authorization policies/data change. In this paper, we proposed a two layer encryption based approach to solve this problem by delegating as much of the access control enforcement responsibilities as possible to the Cloud while minimizing the information exposure risksdue to colluding Usrs and Cloud.

VIII. References

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

2. "Secure and selective dissemination of XML documents," E. Bertino and E. errari, ACM Trans.Inf. Syst. Secur., vol. 5, no. 3, pp. 290–331, 2002.

3."Controlling access to published data using cryptography,"G. Miklau and D. Suciu,inVLDB '2003: Proceedings of the 29th international conference on Very large data bases.VLDB Endowment, 2003, pp. 898–909.

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

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

6."Privacy preserving policy based content sharing in public clouds," M.Nabeel,N.Shang,andE.Bertino, IEEE Transactions on Knowledge and Data Engineering, 2012.

7."Over-encryption: Management of access control evolution on outsourced data," S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, in Proceedings of the 33rd International Conference on VeryL arge Data Bases, ser.VLDB '07. VLDB Endowment,2007, pp. 123–134.

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

9."*Broadcast encryption*," A. Fiat and M. Naor, in Proceedings of the 13th Annual International Cryptology Conference on Advances inCryptology,ser.CRYPTO '93. London, UK:Springer-Verlag, 1994, pp. 480–491.

10."Revocation and tracing schemes for *stateless receivers*," D. Naor, M. Naor, and J. B. Lotspiech, in Proceedings of the 21st Annual International Conference on Advances in Cryptology, ser. CRYPTO '01. London, UK: Springer-Verlag, 2001, pp. 41–62.