ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Survey on Two Layer Encryption System

Uma B. Ajantiwale, Prof. Ranjana Badre

PG Scholar, Department of Computer Engineering, MIT Academy of Engineering, Alandi(D), Pune, India.

Associate Professor Department of Computer Engineering, MIT Academy of Engineering, Alandi(D), Pune, India.

ABSTRACT: Security and privacy are the major concern in the adoption of cloud technologies for the data storage purpose. To reduce these concerns one can use the encryption process. However, whereas encryption assures confidentiality of the data against the cloud, but encryption is not sufficient to support the enforcement of fine-grained organizational access control policies (ACPs). Under this approach, data owner can encrypt data before uploading on the cloud and re-encrypt it whenever user credentials are changed. Thus data owners have to pay high communication and computation cost. To overcome this issue, Two Layer Encryption (TLE) process is proposed to delegate the enforcement of fine-grained access control to the cloud. In this system, data owner performs a coarse-grained encryption and cloud performs fine-grained encryption. The TLE system is the NP-complete. This system assures the confidentiality of the data and preserves the privacy of users from the cloud.

KEYWORDS: Privacy, Identity, Cloud Computing, Policy Decomposition, Encryption, Access Control.

I. INTRODUCTION

In the recent era of digital world, various organizations produce a huge amount of sensitive data including Electronic Health Record (EHR), personal information, financial and other data. Such huge amount of data is difficult to handle, problematic and costly due to the requirements of high storage capacity and qualified personnel. Therefore, security and privacy represent the major concerns of cloud technologies for data storage. However, encryption assures the confidentiality of the data against the cloud, but encryption is not support the enforcement of fine-grained organizational access control polices (ACPs). Today many organization have used ACPs that regulating which users can access which data, these ACPs are often expressed in terms of the properties of the user, which is referred to as Identity Attributes using access control languages such as XACML [3]. Such an approach, called as a attribute based access control (ABAC), that supports fine-grained access control which is crucial for high assurance data security and privacy.

The rest of the paper is organized as follows:- Section A describes the Traditional methods, Section B describes the GKM and BGKM methods, Section C describes the SLE System, Section D describes the TLE system and Section 6 concludes the paper.

II. RELATED WORK

A. TRADITIONAL APPROACH

1. In traditional approach [1], [2], [3], [4]the encryption has been proposed for fine-grained access control [9] over encrypted data. As shown in fig.(1), those group data items which are based on ACPs and that will encrypt each group with different symmetric key. Then users have 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 approach however have several limitations:

1. The data owner does not keep a copy of the data, whenever user dynamics changes, the data owner needs to download and decrypt the data and then the re-encrypt it with the new keys, and upload the encrypted data.
2. In order to issue the new keys to the users, the data owner needs to establish private communication channels with the user.
3. The privacy of the identity attributes of the users are not taken into account. Therefore, the cloud can learn sensitive information about the users and their organization.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

4. They are not able or sufficient in fine-grained ABAC polices.

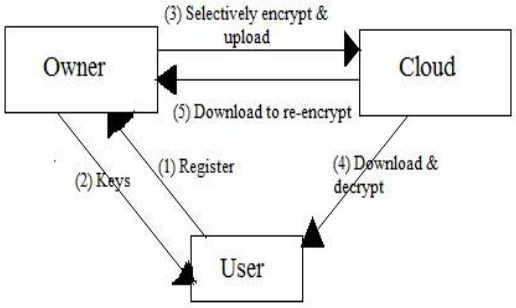

Fig. 1. Traditional Approach

2. An approach which support to the fine-grained selective attribute based access control before uploading the content to the cloud i.e. to encrypt each content portion to which the same access controls policy or set of policies they satisfy. It is to use a hybrid solution where the keys are encrypted using public key cryptosystem such as attribute based encryption (ABE)/ or proxy re-encryption (PRE) [1], [2]. However such approach consists of several weakness as follows:

1. It is unable to handle adding/revoking users or identity attributes and policy changes.
2. It is required to keep multiple encrypted copies of the same key.
3. It incurs high computational cost. Therefore, a different approach is required.

B. BGKM SCHEMES

TheGroup Key Management (GKM) [6] is widely used to securely distribute a message to a group of users using confidentially as a key. In the GKM, users in the group uses or sharesa symmetric key K, called as a Group Key. Whenever they want to communicate with each other, the message is encrypted with key K and broadcast to all users present in the group. K is only known to the users in the group and only they can decrypt that message and obtain it. When dynamically changes happen in the group, i.e. a new user join or existing user leaves the group; key must be generated or redistributed securely to the entire current user present in the group. So that the new member of the group cannot access any future communication in the group, which is called as a Backward Secrecy and a user who left the group cannot access any future communication in the group, which is used as a Forward Secrecy. This both process is called as a rekeying method. A traditional GKM schemes all requires to setup private communication channel for regularly updating the group key. Such an approach is not suitable if there are frequently leaved or joined the users in the group. The Broadcast Group Key Management (BGKM) [6], [7], [10], [11], [12] overcomes these issues.

A key advantage of BGKM scheme is that adding user/leaving users or updating access control policies can be performed efficiently and only requires updating the updating the public information. BGKM schemes satisfies the requirements of minimal trust, key in distinguishability, key independence, forward secrecy, backward secrecy and collusion resistance with minimal computational, space and communication cost.

Using BGKM scheme develop an attribute based access control mechanism therefore a user is able to decrypt the contents if and only if its identity attributes satisfy the content provider and the cloud learn nothing about user's identity attributes. The mechanism is fine-grained in that different policies can be associated with different content portions. A user can derive only the encryption keys associate with the user is entitled to access.

C. SINGLE LAYER ENCRYPTION(SLE)

Broadcast Key Management schemes [1], [5], [6], [7] also known as a Single Layer Encryption. The SLE overcomes the limitations of traditional approach. As shown in fig. (2), the SLE scheme consists of four entities Owner, User, Idp and Cloud. They play different following role.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

1. *Owner–*
   The data owner defines the ACPs and uploads encrypted data to the cloud and provides cloud storage services.
2. *Cloud–*
   It stores encrypted data of the owner.
3. *Idp–*
   Idp stands for Identity Provider. It acts as a trusted third party. It issues identity tokens to user, based on the attribute that users have. An identity token is a signed Pedersen commitment that binds the identity attribute value to a user while hiding it from other. There can be one or more certified Idps.
4. *User –*
   The user uses one or more identity tokens to gain access to the encrypted data hosted in the cloud.

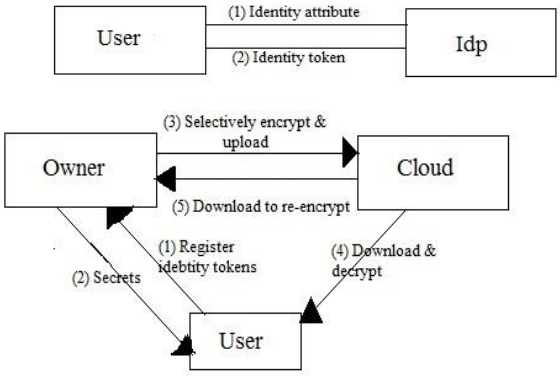

Fig 2. Single Layer Encryption Approach

The SLE approach based on 3 main phases:-

1. *Identity token issuance***:**
   Idps issues identity token for certified identity attributes to users. An identity tokens is used to identity users through specified electronic format in which the involved identity attribute value is represented by semantically secure cryptographic commitment. Identity tokens are used by users during registration process.

2. *Identity token registration***:**
   Firstly, user has to register at the owner then they are able to decrypt the document that will be downloaded from the cloud. While registering, user should have its identity tokens and he receives a set of secrets for each identity attribute from owner which is based on the SecGen algorithm of the Access Control Vector-Broadcast Group Key Management (ACV-BGKM) [7], [13]. The set Secrets are further used by user to drive its key and decrypt the subdocument and for this they must satisfy the access control policy using the Key Decryption algorithm of the ACV-BGKM Scheme. The owner delivers the secret to the users using a privacy preserving approach based on the OCBE protocol with the user.

3. *Document Management***:**
   The owner group uses the ACPs into policy configuration (PCs). The documents are divided into subdocument based on the PCs. The owner generates the keys based on the ACPs in each BGKM schemes, and selectively encrypts the subdocuments. This encrypted subdocument uploaded on the cloud and if users require any document then it will be downloaded from the cloud. According to user secrets, user can generate their key K for each PC using KeyGen algorithm of the ACV-BGKM scheme in an efficient and secure manner.

With this scheme, the SLE approach efficiently handles new users and revocations to provide forward and backward secrecy. However, this scheme also consists of several limitations as follows:-

1. The SLE scheme still requires the data owner to enforce all the ACPs by fine-grained encryption.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

2. In this, all these encryption activities have been performed by the owner that thus incurs high communication and computation cost.
3. For example:- If a user is revoked, the owner must download from the cloud the data affected by this change, generate a new encryption key, re-encrypt the downloaded data with the new key and then uploaded the re-encrypted data to the cloud.

III. PROPOSED SYSTEM

A. TWO LAYER ENCRYPTION SCHEME (TLE)

In the TLE [1], [2], [7], [14], [15] data can be encrypted by two times. Firstly, the data owner can encrypt the data which is called as Coarse-grained encryption and secondly the cloud can re-encrypt the encrypted data which is called as Fine-grained encryption. The two layer encryption is not new but the performance of Coarse-grained and fine-grained are best and provide better solution than existing solution. A challenging issue in the TLE is how to decompose ACPs so that fine-grained ABAC enforcement can be delegated to the cloud. Using Policy Decomposition [1], [2], the ACPs can be divided into sub ACPs. Such that the conjunctions of two sub ACPs result the original ACPs. In this process, the data owner first encrypt the data based on one set of sub ACPs and the cloud re-encrypt the encrypted data using other set of sub ACPs. For two encryptions, the user should perform two decryption processes to access the original data. The TLE process overcomes the above all limitations.

Like the SLE system described in Section 4, the TLE system consists of four entities Owner, User, Idp and cloud as shown in fig (3). Unlike the SLE, the owner and the cloud collectively enforce ACPs by performing two encryptions on each data items. This two layer enforcement allows one to reduce the owner load and delegates as much access control enforcement duties as possible to cloud. Specifically TLE provides a better way to handle data updates, and user dynamics change. The TLE system goes through one additional phase compared to SLE system. The phases are as below:

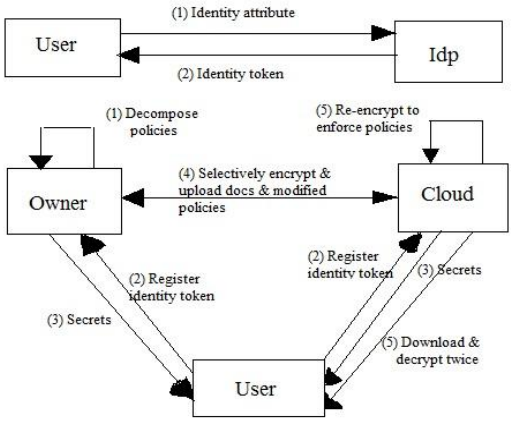

Fig 3. Two Layer Encryption Approach

1. *Identity token issuance*:-

Idps are trusted third parties that issues identity tokens to user based on their identity attributes. It should be noted that Idps need not be online after they issue identity tokens.

2. *Policy Decomposition*:-

Using the Policy decomposition, the owner decomposes each ACPs into two sub ACPs. Such that the owner enforces the minimum number of attributes to assure confidentiality of data from the cloud. The two sub ACPs are noted as $ACPB_{owner}$is used by owner to enforce the confidentiality and the $ACPB_{cloud}$is used by the cloud.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

3. *Identity token registration*:
User register their identity tokens in order to obtain secrets to decrypt the data. Users only register those tokens which are related to owner's sub ACPs and remaining identity tokens related to cloud.
4. *Data encryption and uploading:*
Firstly, owner can encrypt the data based on owner sub ACPs and then that data uploaded on the cloud along with the public information which is generated by the Attribute Based-Group Key Management : KeyGen (AB-GKM::KeyGen) algorithm and remaining sub ACPs used on the cloud.

5. *Data downloading and decryption*:
Users download encrypted data from the cloud and decrypt the data using the derived Key. Users can decrypt two times encrypted data, first to remove the encryption layer added by the cloud and then the encryption layer added by the owner.

6. *Encryption evolution management*:
Regularly users credential may change. Further, already encrypted data may go through various changes or updates. In such situation, already encrypted data must be re-encrypted with a new key.

V. CONCLUSION

In the fine-grained organizational access control polices, data owner can encrypt data before uploading on the cloud and re-encrypt it whenever user credentials are changed. Thus data owner have to pay high communication and computation cost. To overcome this issue, the Two Layer Encryption system is proposed to delegate the enforcement of fine-grained access control to the cloud. The key problem is how to decompose ACPs so that the owner has to handle a minimum number of attribute conditions while hiding the content from the cloud. The TLE system protects the privacy of user while enforcing attribute based ACPs and it is NP-Complete problem.

REFERENCES

1. M. Nabeel and E. Bertino, "Privacy Preserving delegated access control on Public Clouds", IEEE Transactions on Knowledge and Data Engineering, 2013
2. M. Nabeel and E. Bertino, "Privacy preserving delegated access control in the storage as a service model," in EEEInternational Conference on Information Reuse and Integration(IRI), 2012.
3. Bertino and E. Ferrari,"Secure and selective dissemination of XML documents," ACM Transaction Inf. Syst. Secure., vol. 5, no. 3, pp. 290–331, 2002
4. Miklau and D. Suciu, "Controlling access to published data using cryptography," Proceedings of the29th international conference on Very large data bases. VLDB Endowment, pp. 898–909, 2003.
5. N. Shang, M. Nabeel, F. Paci, and E. Bertino, "A privacy preserving approach to policy-based content dissemination," Proceedings of the IEEE 26th InternationalConference on Data Engineering, 2010.
6. 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 CollaborativeComputing: Networking, Applications and Worksharing, ser. CollaborateCom. 11 pp. 172–180,2011.
7. M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Transactionson Knowledge and Data Engineering, 2012.
8. S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in Proceedings of the33rd International Conference on Very Large Data Bases, VLDB Endowment, pp. 123–134, 2007.
9. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proceedings of the 13th ACM conference on Computerand communications security. New York, NY, USA: ACM, pp. 89–98, 2006.
10. Y. Challal and H. Seba. "Group key management protocol : A novel taxonomy". International Journal of Information Technology, 2(2):105-118, 2006.
11. Chiou and W. Chen "Secure Broadcasting using the secure lock". Software Engineering IEEE Transaction on, 15(8):929-934, Aug 1989.
12. X. Zou, Y. Dai and E. Bertino. "A practical and flexible key management mechanism for trusted collaborative computing". INFOCOM the 27th Conference on Computer Communication IEEE, pages 538-546, April 2008.
13. N. Shang, M. Nabeel, F. Paci and E. Bertino, "A privacy-preserving approach to policy-based content dissemination". In ICDE Proceedings of the IEEE 26th International Conference on Data Engineering 2010.
14. A .Reddy, GudivadaLokesh and N. Vikram "Privacy Preserving Delegated Access Control in Public Clouds", International Journal of Computer Science Trends and Tech (IJCST)- Vol. 2 Issue 4, July Aug 2014.