International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-3, March 2015

Privacy Preservation in Private Cloud

Vishal M. Pund, Prashant P. Pathak, Kapil P. Nilekar, Dipak V. Nikam

***Abstract*— Current approaches to enforce access control on privacy & confidentiality of data hosted in private cloud. Are based mostly on SLE under such approaches, data owners are in charge of encrypting data & decrypting it which involves huge burden in terms of computation & communication costs. A better approach by taken key management. Thus minimizes load of data owner & ensuring more secured system. In this paper we proposed a system which uses 2 layer encryption & 2 layer decryption for enhancing security & privacy using policy cover & policy decomposition algorithm along with AES in private cloud.**

Our system assures the confidentiality of the data and preserves the privacy of users from the cloud while delegating most of the access control enforcement to the cloud.

***Index Terms*— Security, Data owner-burden, ACP (Access Control Policy).**

I. INTRODUCTION

The cloud computing paradigm has achieved widespread adoption in recent years. Its success is due largely to customer's ability to use services on demand with a pay as you go pricing model, which has proved conve- nient in many respects. Low costs and high flexibility make migrating to the cloud computing. Despites it's obvious advantages, however, many companies hesitate to "move to the cloud", mainly because of concerns like security, privacy, confidentialityetc. In this project we introduce an efficient group key management scheme that supports expressive ACPs. Thus, system assures the confidentiality of the data and preserves the privacy of users from the cloud while delegating most of the access control enforcement to the cloud. 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 so it is through this project that we make use of cloud technology in a more secured & confidential way. This project aims at maintaining privacy & security for applications in private clouds. In this project we enhance encryption technique & reduced the workload of data owner. For this purpose we use ACPs i.e. Access Control Policies, Policy decomposition algorithm, Attribute based encryption etc to resolve the major concerns in security & privacy while handling data in private cloud based environment.

Manuscript received March 24, 2015.

Vishal M. Pund, U.G. Students, Department Of Computer Engineering, SRESCOE, Kopargaon

Prashant P. Pathak, U.G. Students, Department Of Computer Engineering, SRESCOE, Kopargaon

Kapil P. Nilekar, U.G. Students, Department Of Computer Engineering, SRESCOE, Kopargaon

Dipak V. Nikam, U.G. Students, Department Of Computer Engineering, SRESCOE, Kopargaon

II. RELATED WORK

In the Fine-grained Access Control (FGAC) it allows one to enforce selective access to the content based on expressive policy specifications. In FGAC they are use two models push based and pull based models. Our work focuses on the pull based model.

In push based model approach [4] each subdocument encrypted with different keys and those keys are provided at the time of user registration phase. Then all encrypted subdocument send to all users. However such approaches require distributing the keys in advance during user registration phase. [4] Hence it is difficult and insecure to forward and backward the keys at the time of registration of user so we can use the Two Layer encryption technique to provide security and to reduce the burden from data owner.

In pull based model content publisher is required to be online in order to provide access to the content. There are many approaches [5] of privacy preserving access control system using multiple levels of encryption of the same document which is inefficient. In all approaches require the data owner to handle encryption so the burden on data owner will be increased so to reduce the burden from data owner we will developed the our system. [5] In this we are using the attribute based policies.

Attribute Based Encryption:

The Initial attribute based encryption based only to threshold policies in which there are at least k out of n attributes common between the attributes used to encrypt the plaintext and the attributes user possess. [6]

III. METHODOLOGY

Two Layer Encryption:

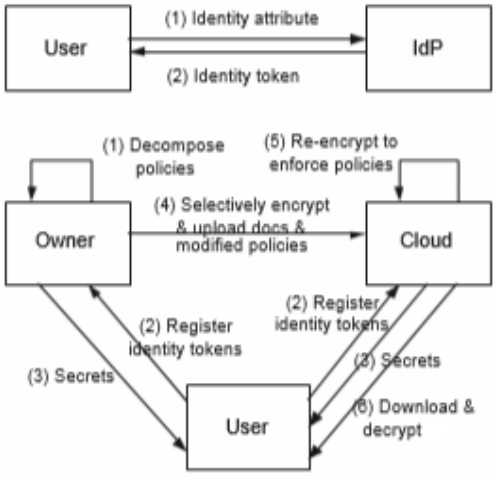

Fig1. Two layer Encryption approach

1.Registration:

In registration module the user will register . After the registration the data is send to the data owner then data will be verified by the data owner. If data is correct then data is stored in the database othervice registration will be fail.

2.Token Generation:

After successful registration the token generation module generate the two tokens are generated based on the registration attribute. Out of two token one token is goes towerds cloud and one to data owner. Usrs register their identity tokens in order to obtain secrets to decrypt the data that they are allowed to access. Usrs register only those identity tokens related to the Owner's sub ACPs and register the remaining identity tokens with the Cloud in a privacy preserving manner. It should be noted that the Cloud does not learn the identity attributes of Usrs during this phase.

3.ACP Generation:

ACP Generation module generate the two ACP's . As that of the token the ACP's are distributed to the cloud and the data owner. The Owner decomposes each ACP into at most two sub ACPs such that the Owner enforces the minimum number of attributes to assure confidentiality of data from the Cloud. It is important to make sure that the decomposed ACPs are consistent so that the sub ACPs together enforce the original ACPs. The Owner enforces the confidentiality related sub ACPs and the Cloud enforces the remaining sub ACPs.

3.1 Policy Cover :

We define the policy cover problem as the the opti- mization problem of finding the minimum number of attribute conditions that "covers" all the ACPs in the ACPB. We say that a set of attribute conditions covers the ACPB if in order to satisfy any ACP in the ACPB, it is necessary that at least one of the attribute conditions in the set is satisfied. We call such a set of attribute conditions as the attribute condition cover. For example, if ACPB consists of the three simple ACPs { "role = doc" ∧ "ip = 2-out-4", "role = doc" ∧ "yos ≥ 2", "role = nur" }, the minimum set of attributes that covers ACPB is {"role = doc", "role = nur"}. "role = doc" should be satisfied in order to satisfy the first two ACPs. Notice that satisfying "role = doc" is not sufficient to satisfy the ACPs. The set is minimum since the set obtained by removing either "role = doc" or "role = nur" does not satisfy the cover relationship. While one can compute the minimum cover for simple examples such as the above one, below we show that it is a hard problem in general and there is no polynomial time algorithm to do.

3.2 Policy Decomposition

The Owner manages only those attribute conditions in ACC. The Cloud handles the remaining set of attribute conditions, ACB/ACC. The Owner re-writes its ACPs such that they cover ACC. In other words, the Owner enforces the parts of the ACPs related to the ACs inACC and Cloud enforces the remaining parts of the policies along with some ACs in ACC.

The POLICY- DECOMPOSITION algorithm 3 shows how the ACPs are decomposed into two sub ACPs based on the attribute conditions in ACC.

3.3 Algorithm:

POLICY – DECOMPOSITION:

1: ACPBOwner = φ
2: ACPBCloud = φ
3: **for** Each ACPi in ACPB **do**
4: Convert ACPi to DNF
5: ACPi(owner) = φ
6: ACPi(cloud) = φ
7: **if** Only one conjunctive term **then**
8: Decompose the conjunctive term c into c1 and c2 such that ACs in c1 ∈ ACC, ACs in c2 _∈ ACC and c = c1 ∧ c2
9: ACPi(owner) = c1
10: ACPi(cloud) = c2
11: **else if** At most one term has more than one AC **then**
12: **for** Each single AC term c of ACP_ i **do**
13: ACPi(owner) ∨= c
14: ACPi(cloud) ∨= c
15: **end for**
16: Decompose the multi AC term c into c1 and c2 such that ACs in c1 ∈ ACC, ACs in c2 _∈ ACC and c = c1 ∧ c2
17: ACPi(owner) ∨= c1
18: ACPi(cloud) ∨= c2
19: **else**
20: **for** Each conjunctive term c of ACP_ i **do**
21: Decompose c into c1 and c2 such that ACs in c1 ∈ ACC, ACs in c2 _∈ ACC and c = c1 ∧ c2
22: ACPi(owner) ∨ = c1
23: **end for**
24: ACPi(cloud) = ACP_ i
25: **end if**
26: Add ACPi(owner) to ACPBOwner
27: Add ACPi(cloud) to ACPBCloud
28: **end for**
29: Return ACPBOwner and ACPBCloud

4.File Upload:

User will send the request to the data owner to upload the file. After receiving the request the data owner will encrypt the data and that encrypted data will be send to the cloud then cloud again reencrypt the data and then file will be uploaded into the cloud.

5.File Download:

To download the file the user will directly send the request to the cloud instead the request is send to the user then it passes to the cloud. After receiving the request cloud will decrypt the data and the file will downloaded on the user PC.

IV. EXPERIMENTAL RESULTS:

Our Project input given is any form of file. After giving input we performed the encryption two time on the data and store it on the cloud. At the time of downloading the ACP must be required and then decrypt the file. In this way we are providing the privacy and security for data in cloud.

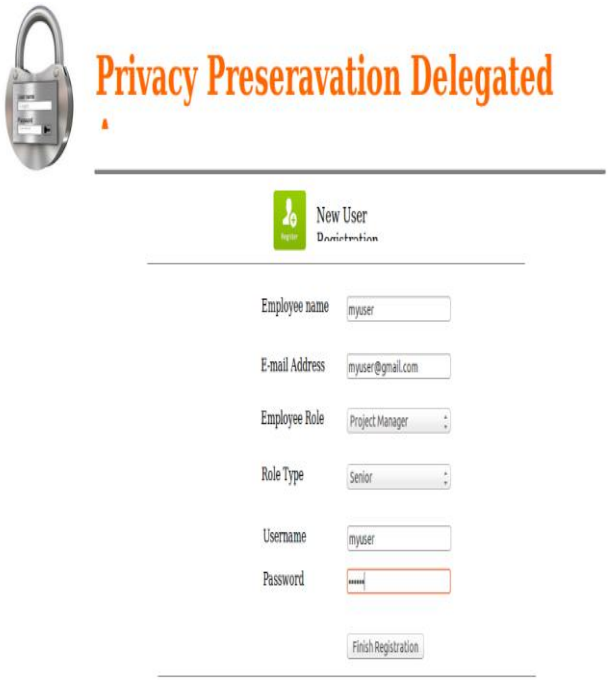

Fig2. User registration

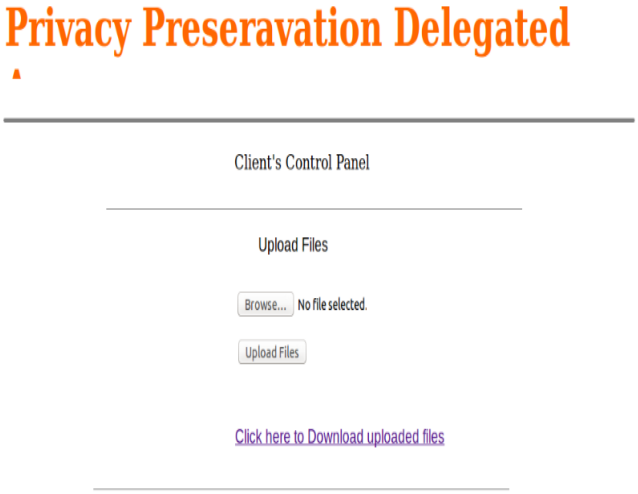

Fig3. File upload and download

V. FUTURE SCOPE:

In this paper we shown that ACP & use of two layer encryption reduces the burden of dataowner.As future work we can reduce the computational costs by exploiting the partial relationships among ACPs.

VI. CONCLUSION :

In this project we focuses on a two layer encryption and two layer decryption based approach to solve the problem by delegating as much of the access control enforcement responsibilities as possible to private cloud by minimizing the information exposure risk. 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, this way requires high communication & computational costs besides huge load of data.Based on novel approach to privacy preserving fine-grained delegated access control to data in private clouds. Our approach is based on a privacy preserving attribute based key management scheme that protects the privacy of users while enforcing attribute based ACPs.The proposed system also proves that decomposing the ACPs & utilizing two layer of encryption to reduce overhead at the owner.

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] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Transactions on Knowledge and Data Engineering, 2012.
[3] M. Nabeel and E. Bertino, "Towards attribute based group key management," in Proceedings of the 18th ACM conference on Computer and ommunications security, Chicago, Illinois, USA, 2011.
[4] 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 Endowment, 2003, pp. 898–909.
[5] M. Nabeel, E. Bertino, M. Kantarcioglu, and B. M. Thurais- ingham, "Towards privacy preserving access control in the cloud," in Proceedings of the 7th International Conference on Col- laborative Computing: Networking, Applications and Worksharing, ser. CollaborateCom '11, 2011, pp. 172–180.
[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Eurocrypt 2005, LNCS 3494. Springer-Verlag, 2005, pp. 457– 473.