INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 4, Issue 4 AUG 2015

SECURING SENSITIVE DATA IN PUBLIC CLOUD STORAGE SYSTEMS

[1]K.RAMESHWARAIAH, [2]ANGIDI VEERABABU

[1]Professor, Department of CSE,Sreyas Institute of Engineering & Technology, Thatti Annaramvillage, Hayathnagar Mandal, Ranga reddy District, A.P, India.

[2]M.Tech Student, Department of CSE, Sreyas Institute of Engineering & Technology, Thatti Annaramvillage, Hayathnagar Mandal, Ranga reddy District, A.P, India.

Abstract— Current approaches to enforce fine-grained access management on confidential information hosted within the cloud area unit predicated on fine-grained cryptography of the info. Below such approaches, information homeowner's area unit answerable of encrypting the info afore uploading them on the cloud and re-encrypting the info whenever utilizer credentials amendment. Information homeowners so incur high communication and computation prices. A lot of overriding approach ought to delegate the {enforcement social management} offine-grained access control to the cloud, therefore to reduce the overhead at the info homeowners, whereas reassuring information confidentiality from the cloud. We have a tendency to propose associate degree approach, predicated on 2 layers of cryptography that addresses such requisite. Below our approach, the info owner performs a coarse-grained cryptography, whereas the cloud performs afine-grained cryptography on prime of the owner encrypted information. A difficult issue is the way to decompose access management policies (ACPs) specified the 2 layer cryptography is performed. We have a tendency to show that this quandary is NP-consummate and propose novel optimization algorithms. We have a tendency to utilize associate degree economical cluster key management theme that fortifies communicatory ACPs. Our system Assures the confidentiality of the info and preserves the privacy of users from the cloud whereas deputation most of the access management social control to the cloud.

Index Terms—about four key words or phrases in alphabetical order, separated by commas

I. INTRODUCTION

In typical access control models, the set of access rights auser gets is determined. Predetermining a user's access rights is equivalent to anticipating possible usages of the system by that user. However, users may need new access rights due to the dynamic nature of their work. There are two ways to assign access rights. First, a system administrator acts every time a user needs an access right. Secondly, a user gets the right from a different user who already possesses it. The later approach is called delegation.

The proposed scheme is "two layer encryption" And it is extended from the previous scheme of mcl-pke. Mcl-pke scheme works on certificate-less encryption and User is not certified by any authorized entity but

in my scheme There will be certification for user, certification of the user also Provides security to the information in the cloud, due to this Only authorized person can use the data. The double Encryption approach (dea) means two layer encryption Approach addressesthe shortcomings of the mcl-pkeScheme. In dea approach user will have to first register to the Owner to get the secret key for decryption of the encrypted Documents. The basic scheme is, owner encrypts the Documents and sends these encrypted documents to the

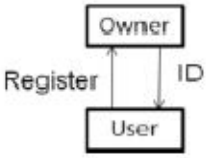


Fig 1.certification of user

Cloud, now cloud decrypts the outer-layer of the encrypted Contents and sends these documents to the requested users,now user fully decrypts the encrypted contents means innerlayer of the encryption by the secret keys. In this approachthere are three main entities (1) Owner, (2) Cloud and (3) User, Cloud has three sub parts that are (1) Encryptedstorage,(2) Decryption center, (3) Key GenerationCenter(KGC).

II. BASIC APPROACHES TO PRIVACY-PRESERVINGABAC

Using our ab-bgkm scheme, we have developed an abac mechanism whereby a user is able to decrypt theData if and only if its identity attributes satisfy the data owner's policies, whereas the data owner and the cloud learn nothing about user's identity attributes. The mechanism is fine-grained in that different policies can beassociated with different sets of data items. A user can derive only the encryption keys associated with the sets of data items the user is entitled to access.

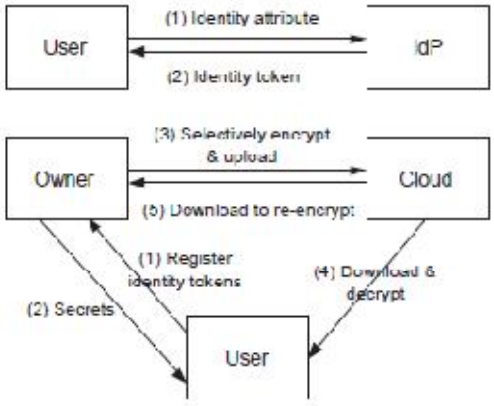


Fig 2.*Overall system architecture*

We now give an overview of the overall scheme. As shown in figure 2, our scheme for policy based content sharing in the cloud involves four main entities: the data owner (owner), the users (users), the identityProviders (idps), and the cloud storage service (cloud). Our approach is based on three main phases: identityToken issuance, identity token registration, and data management.

A. Identity token issuance

Idps issue identity tokens for certified identity attributes to users. An identity token is ausr's identity encoded In aspecified electronic format in which the involved identity attribute value is represented by a semantically Secure cryptographic commitment[2].We use the Pedersen commitment scheme [8]. Identity tokens are used by Users during the identity token registration phase.

B. Identity token registration

In order to be able to decrypt the data to be downloaded from the cloud, users have to register at the owner.During the registration, each user presents its identity tokens and receives from the owner a set

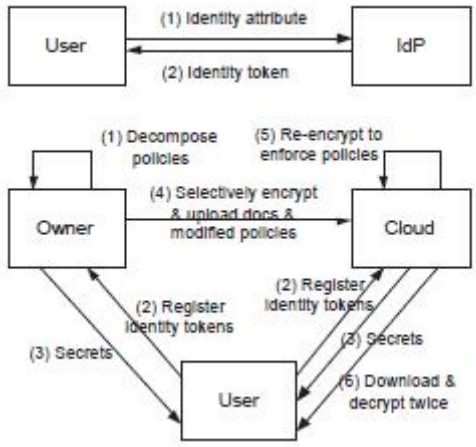
of secrets for each identity attribute based on the sec-gen algorithm of the ab-gkm scheme. These secrets are later used by Users to derive the keys to decrypt the sets of data items for which they satisfy the access control policy usingthe keyed algorithm of the ab-gkm scheme. The owner delivers the secrets to the users using a privacypreserving approach based on the ocbe protocols [4]. The ocbe protocols ensure that a user can obtain theSecrets if and only if the user's committed identity attribute value (within user's identity token) satisfies theMatching condition in the owner's access control policy, while the owner learns nothing about the identityAttribute value. Note that not only the owner does not learn anything about the actual value of users' identityAttributes but it also does not learn which policy conditions are verified by which users, thus the owner cannotInfer the values of users' identity attributes.

C. Data management

The owner groups the access control policies into policy configurations. The data items are partitioned into sets of data items based on the access control policies. The owner generates the keys based on the access controlPolicies in each policy configuration using the keygen algorithm of the ab-gkm scheme and selectivelyEncrypts the different data item sets. These encrypted data item sets are then uploaded to the cloud. Users Download encrypted data item sets from the cloud. The keyed algorithm of the ab-gkm scheme allows users to derive the key k for a given policy configuration using their secrets in an efficient and secure manner.With this scheme, our approach efficiently handles new users and revocations to provide forward and backwardSecrecy. The system design also ensures that access control policies can be flexibly updated and enforced by theOwner without changing any information given to users.

III. PROPOSED SYSTEM

In this paper, we propose an incipient approach to address this shortcoming. The approach is predicated on two layers of encryption applied to each data item uploaded to the cloud. Under this approach, referred to as two layer encryption (TLE), the data owner performs a coarse grained encryption over the data in order to assure the confidentiality of the data from the cloud. Then the cloud performs fine grained encryption over the encrypted data provided by the data owner predicated on the ACPs provided by the data owner.



It should be noted that the conception of two layer encryption is not incipient. However, the way we perform coarse and fine grained encryption is novel and provides a more preponderant solution than subsisting solutions predicated on two layers of encryption. We elaborate in details on the differences between our approach and subsisting solutions in the cognate work section. Our incitation issue in the two layer encryption approach is how to decompose the ACPs so that subdued ABAC enforcement can be delegated to the cloud while at the same time the

privacy of the identity attributes of the users and confidentiality of the data are satiated. In order to delegate as much access control enforcement as possible to the cloud, one needs to decompose the ACPs such that the data owner manages minimum number of attribute conditions in those ACPs that assures the confidentiality of data from the cloud. Each ACP should be decomposed to two sub ACPs such that the conjunction of the two sub ACPs result in the pristine ACP. The two layer encryption should be performed such that the data owner first encrypts the data predicated on one set of sub ACPs and the cloud re-encrypts the encrypted data utilizing the other set of ACPs. The two encryptions together enforce the ACP as users should perform two decryptions to access the data.

IV. SYSTEM DESIGN

Modules Description:

The system is proposed to have the following modules along with functional requirements.

1. Identity token issuance
2. Identity token registration
3. Data encryption and uploading
4. Data downloading and decryption
5. Encryption evolution management

i) Identity token issuance:

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

ii) Identity token registration:

Users register their token to obtain secrets in order to later decrypt the data they are allowed to access. Users register their tokens related to the attribute conditions in ACC with the Owner, and the rest of the identity tokens related to the attribute conditions in ACB/ACC with the Cloud. When Users register with the Owner, the Owner issues them two set of secrets for the attribute conditions in ACC that are also present in the sub ACPs in ACPB Cloud. The Owner keeps one set and gives the other set to the Cloud. Two different sets are used in order to prevent the Cloud from decrypting the Owner encrypted data.

iii) Data encryption and uploading:

The Owner first encrypts the data based on the Owner's sub ACPs in order to hide the content from the Cloud and then uploads them along with the public information generated by the AB-GKM: KeyGen algorithm and the remaining sub ACPs to the Cloud. The Cloud in turn encrypts the data based on the keys generated using its own AB-GKM:KeyGen algorithm. Note that the AB-GKM:KeyGen at the Cloud takes the secrets issued to Users and the sub ACPs given by the Owner into consideration to generate keys.

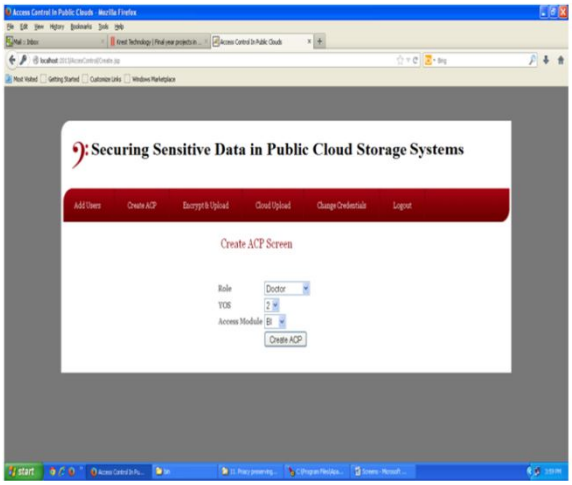
iv) Data downloading and Decryption:

Users download encrypted data from the Cloud and decrypt twice to access the data. First, the

Cloud generated public information tuple is used to derive the OLE key and then the Owner generated public information tuple is used to derive the ILE key using the AB-GKM::KeyDer algorithm. These two keys allow a User to decrypt a data item only if the User satisfies the original ACP applied to the data item.

v) Encryption Evolution Management:

Over time, either ACPs or user credentials may change. Further, already encrypted data may go through frequent updates. In such situations, data already encrypted must be re-encrypted with a new key. As the Cloud performs the access control enforcing encryption, it simply re-encrypts the affected data without the intervention of the Owner.



V. CONCLUSION

We presented a two-level access control scheme enabling data sharing in outsourced storage, like the cloud environment. Our present approach is to expect access control policies on utilize selective data first of all encryption is require constitution to manage keys, encryptions and upload the encrypted data to the remote storage. Whenever we integrate any details the encryption is required for that data, these method acquires immense communication and computation cost to manage keys. Predicated on the decomposed ACPs, we proposed a novel approach to privacy preserving fine-grained delegated access control to data in public clouds. Our project is predicated on preserving attribute predicated key management scheme that forefends the privacy of users while enforcing attributes predicated ACPs.

REFERENCES

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

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

[3] J. Li and N. Li, "OACerts: Oblivious attribute certificates," IEEE Transactions on Dependable and Secure Computing,vol.3, no. 4, pp. 340–352, 2006.

[4] T. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," inCRYPTO '91: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology. London, UK: Springer-Verlag, 1992, pp. 129–140.

[5] M. Nabeel and E. Bertino, "Attribute based group key management,"IEEE Transactions on Dependable and Secure Computing, 2012.

[6] ateniese, g., burns, r., curtmola, r., herring, j.,khan, O., kissner, l., ... & song, d. 2011. Remote data Checking using provable data possession. Acm Transactions on information and system security (tissec), 14(1), 12

[7] mohammed, a., alsudiari, t., &vasista, t. G. K. 2012. Cloud computing and privacy regulations: anExploratory study on issues and implications. Advanced Computing: an international journal (acij), 3 (2), 159-169...

[8] Yang tang, patrick p.c. lee, member, ieee, john c.s. lui, fellow, Ieee, and radiaperlman, fellow, ieee "secure overlay cloud storage With access control and assured deletion" november/december 2012.

[9] wang, q., wang, c., ren, k., lou, w., &li, j. 2011.Enabling public auditability and data dynamics for Storage security in cloud computing. Parallel and Distributed systems, ieee trans. On, 22(5), 847-859.