ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Survey of Delegated Access Control in Public Clouds

G.Surya Raj
M.Tech Student,
Department of CSE,
Sree Rama institute of Technology and Science,
Kuppenakuntla, Penuballi, Khammam,TS India.

B.R.M Reddy
Assistant Professor,
Department of CSE,
Sree Rama institute of Technology and Science,
Kuppenakuntla, Penuballi, Khammam,TS India.

ABSTRACT:

Current approaches to enforce fine-grained access control on confidential data hosted in the cloud are based on fine-grained encryption of the data. Under such approaches, data owners are in charge of encrypting the data before uploading them on the cloud and re-encrypting the data whenever user credentials change. Data owners thus incur high communication and computation costs. A better approach should delegate the enforcement of fine-grained access control to the cloud, so to minimize the overhead at the data owners, while assuring data confidentiality from the cloud. We propose an approach, based on two layers of encryption, that addresses such requirement. Under our approach, the data owner performs a coarse-grained encryption, whereas the cloud performs a fine-grained encryption on top of the owner encrypted data. A challenging issue is how to decompose access control policies (ACPs) such that the two layer encryption can be performed. We show that this problem is NP-complete and propose novel optimization algorithms. We utilize an efficient group key management scheme that supports expressive ACPs. 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:

Privacy, identity, cloud computing, policy decomposition, encryption, access control.

INTRODUCTION:

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). 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 (FGAC) 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 differentusers. Notice that often user identity attributes encode private information and should thus be 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 shown in Fig. 1, those approaches group data items based on ACP's and encrypt each groupwith 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.

Existing System:

In this section we first introduce broadcast encryption (BE) schemes and oblivious commitment based envelope (OCBE) protocols .

We present an abstract view of the main algorithms of those protocols and then describe how we use them to build our privacy-preserving attribute basedgroup key management (PP AB-GKM) scheme . We then present an overview of the SLE approach whichis used as the base model for comparison with the TLE approach proposed in this paper.

Broadcast Encryption:

Broadcast encryption was introduced to solve the problem of how to efficiently encrypt a message and broadcast it to a subset of the users in a system. The subset of users can change dynamically. In the broadcast encryption literature,these users are called privileged and the non-authorized users revoked. We denote the set of users by U, the set of revoked users R. The set of privileged users is thus UnR. We set N ¼ jUj and r ¼ jRj. While all users can get the encrypted message, only the privileged users can decrypt it. The most simplest broadcast encryption scheme simply consists of encrypting a message for each privileged user separately and then broadcasting all the encrypted messages. Obviously, this scheme is very inefficient as the message length is prohibitively large .

Oblivious Commitment Based Envelope Protocols:

The oblivious commitment based envelope protocols, proposed by Li and Li provide a mechanism to obliviously deliver a message to the users who satisfy certain conditions.There are three entities in these protocols, a server Svr, a user Usr, and a trusted third party, called the identity provider (IdP). IdP issues to Usr identity tokens, expressed as Pedersencommitments corresponding to the identity attributes of Usr.

Proposed System:

The BGKM schemes are a special type of GKM scheme where the rekey operation is performed with a single broadcast without requiring the use of private communication channels. Unlike conventional GKM schemes, the BGKM schemes do not give users the private keys. Instead users are given a secret which is combined with public information to obtain the actual private keys. Such schemes have the advantage of requiring a private communication only once for the initial secret sharing. The subsequent rekeying operations are performed using one broadcast message. Further, in such schemes achieving forward and backward security requires only to change the public information and does not affect the secret shares given to existing users. In general, a BGKM scheme consists of the following five algorithms: Setup, SecGen, KeyGen, KeyDer, and ReKey. Our overall construction is based on the AB-GKM cheme which is an expressive construct of the access control vectorBGKM (ACV-BGKM) scheme . A high-level description of the access tree is as follows. Each threshold gate in the tree is described by its child nodes and a threshold value. The threshold value tx of a node x specifies the number of child nodes that should be satisfied in order to satisfy the node. Each threshold gate is modeled as a Shamir secret sharingpolynomial [14] whose degree equals to one less than the threshold value. The root of the tree contains the group key and all the intermediate values are derived in a top down fashion. A user who satisfies the access tree derives the group key in a bottom-up fashion.

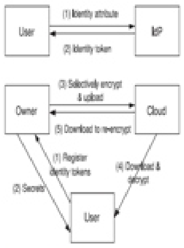


Fig. 2. Single layer encryption approach.

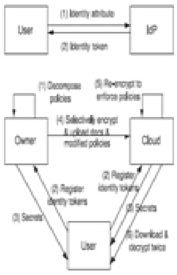

User
(1) Identity attribute
(2) Identity token
IdP
(1) Decompose policies
(5) Re-encrypt to enforce policies
Owner
(4) Selectively encrypt & upload docs & modified policies
Cloud
(2) Register identity tokens
(3) Secrets
(2) Register identity tokens
(3) Secrets
(6) Download & decrypt twice
User

Fig. 3. Two layer encryption approach.

OVERVIEW:

We now give an overview of our solution to the problem of delegated access control to outsourced data in the cloud. A detailed description is provided in Section 5. Like the SLE system described in Section 2.4, the TLE system consists of the four entities, Owner, Usr, IdP and cloud. However, unlike the SLE approach, the Owner and the cloud collectivelyenforce ACPs by performing two encryptions on each data item.

This two layer enforcement allows one toreduce 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, and user dynamics changes. Fig. 3 shows the system diagram of the TLE approach. The system goes through one additional phase compared to the SLE approach.

POLICY DECOMPOSITION:

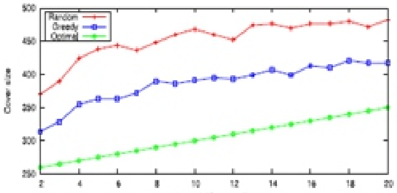
Recall that in the SLE approach, the Owner incurs a high communication and computation overhead since it has to manage all the authorizations when user dynamics change. If the access control related encryption is somehow delegated to the cloud, the Owner can be freed from the responsibility of managing authorizations through re-encryption and the overall performance would thus improve. Since the cloud is not trusted for the confidentiality of the outsourced data, the Owner has to initially encrypt the data and upload the encrypted data to the cloud. Therefore, in order for the cloud to allow to enforce authorization policies through encryption and avoid re-encryption by the Owner, the data may have to be encrypted again to have two encryption layers. We call the two encryption layers as inner encryptionlayer (IEL) and outer encryption later (OEL). IEL assures the confidentiality of the data with respect to the cloud and is generated by the Owner. The OEL is for fine-grained authorizationfor controlling accesses to the data by the users and is generated by the cloud.

TWO LAYER ENCRYPTION APPROACH:

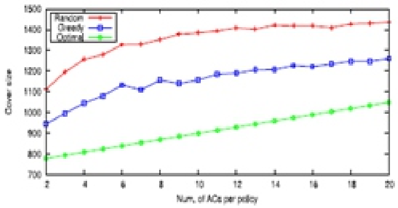
In this section, we provide a detailed description of the six phases of the TLE approach introduced in Section 3. The system consists of the four entities, Owner, Usr, IdP and cloud. Let the maximum number of users in the system be N, the current number of users be n (< N), and the numberof attribute conditions Na.

EXPERIMENTAL RESULTS:

In this section we first present experimental results concerning the policy decomposition algorithms. We then present an experimental comparison between the SLE and TLE approaches.



(a) 500 attributes



(b) 1500 attributes

Fig. 5. Size of ACCs for different number of ACs.

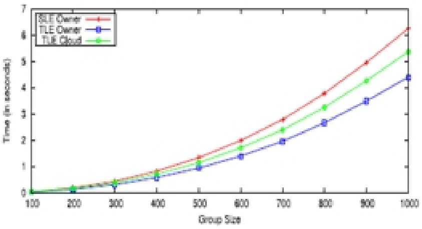


Fig. 7. Average time to generate keys for the two approaches.

ANALYSIS:

In this section, we first compare the SLE and the TLE approaches, and then give a high level analysis of the security and the privacy of both approaches.

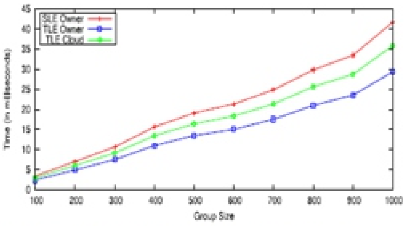


Fig. 8. Average time to derive keys for the two approaches.

CONCLUSIONS:

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 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 risks due to colluding Usrs and cloud. A key problem in this regard 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. We showed that the policy decomposition problem is NP-Complete and provided approximation algorithms.

Based on the decomposed ACPs, we proposed a novel approach to privacy preserving fine-grained delegated access control to data in public 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. As the experimental results show, decomposing the ACPs and utilizingthe two layer of encryption reduce the overhead at the Owner. As future work, we plan to investigate the alternative choices for the TLE approach further. We also plan to further reduce the computational cost by exploiting partial relationships among ACPs.

REFERENCES:

[1] M. Nabeel and E. Bertino, "Privacy Preserving Delegated AccessControl in the Storage as a Service Model," Proc. IEEE Int'l Conf.Information Reuse and Integration (IRI), 2012.

[2] E. Bertino and E. Ferrari, "Secure and Selective Dissemination ofXML Documents," ACM Trans. Information and System Security,vol. 5, no. 3, pp. 290-321, 2002.

[3] G. Miklau and D. Suciu, "Controlling Access to Published DataUsing Cryptography," Proc. 29th Int'l Conf. Very Large Data Bases(VLDB '03), pp. 898-909, 2003.

[4] N. Shang, M. Nabeel, F. Paci, and E. Bertino, "A Privacy-PreservingApproach to Policy-Based Content Dissemination," Proc. IEEE26th Int'l Conf. Data Eng. (ICDE '10), 2010.

[5] M.Nabeel, E. Bertino, M. Kantarcioglu, and B.M. Thuraisingham,"Towards Privacy Preserving Access Control in the Cloud," Proc.Seventh Int'l Conf. Collaborative Computing: Networking, Applicationsand Worksharing (CollaborateCom '11), pp. 172-180, 2011.

[6] M. Nabeel, N. Shang, and E. Bertino, "Privacy Preserving PolicyBased Content Sharing in Public Clouds," IEEE Trans. Knowledgeand Data Eng., vol. 25, no. 11, pp. 2602-2614, Nov. 2013.

[7] S.D.C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P.Samarati, "Over-Encryption: Management of Access Control Evolutionon Outsourced Data," Proc. 33rd Int'l Conf. Very Large DataBases (VLDB '07), pp. 123-134, 2007.

[8] M. Nabeel and E. Bertino, "Towards Attribute Based Group KeyManagement," Proc. 18th ACM Conf. Computer and Comm. Security,2011.

[9] A. Fiat and M. Naor, "Broadcast Encryption," Proc. 13th Ann. Int'lCryptology Conf. Advances in Cryptology (CRYPTO '93), pp. 480-491, 1994.

[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and TracingSchemes for Stateless Receivers," Proc. 21st Ann. Int'l CryptologyConf. Advances in Cryptology (CRYPTO '01), pp. 41-62, 2001.

[11] J. Li and N. Li, "OACerts: Oblivious Attribute Certificates," IEEETrans. Dependable and Secure Computing, vol. 3, no. 4, pp. 340-352,Oct.-Dec. 2006.

[12] T. Pedersen, "Non-Interactive and Information-Theoretic SecureVerifiable Secret Sharing," Proc. 11th Ann. Int'l Cryptology Conf.Advances in Cryptology (CRYPTO '91), pp. 129-140, 1992.

[13] M. Nabeel and E. Bertino, "Attribute Based Group Key Management,"to appear in Trans. Data Privacy, 2014.

[14] A. Shamir, "How to Share a Secret," Comm. ACM, vol. 22, pp. 612-613, Nov. 1979.

[15] V. Shoup, "NTL Library for Doing Number Theory," http://www.shoup.net/ntl/, 2014.

[16] "OpenSSL the Open Source Toolkit for SSL/TLS," http://www.openssl.org/, 2014.

[17] "boolstuff a Boolean Expression Tree Toolkit," http://sarrazip.com/dev/boolstuff.html, 2014.

[18] S. Coull, M. Green, and S. Hohenberger, "Controlling Access to anOblivious Database Using Stateful Anonymous Credentials,"Proc. 12th Int'l Conf. Practice and Theory in Public Key Cryptography,pp. 501-520, 2009.

[19] J. Camenisch, M. Dubovitskaya, and G. Neven, "Oblivious Transferwith Access Control," Proc. 16th ACM Conf. Computer andComm. Security (CCS '09), pp. 131-140, 2009.

[20] K.P.N. Puttaswamy, C. Kruegel, and B.Y. Zhao, "Silverline:Toward Data Confidentiality in Storage-Intensive CloudApplications," Proc. Second ACM Symp. Cloud Computing(SOCC '11), pp. 10:1-10:13, 2011.

[21] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc.24th Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques(Eurocrypt '05), pp. 457-473, 2005.

[22] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "SecureAttribute-Based Systems," Proc. 13th ACM Conf. Computer andComm. Security (CCS '06), pp. 99-112, 2006.

[23] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data,"Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06),pp. 89-98, 2006.

Author's:

G.Surya Raj is a student of Sree Rama Institute of Technology & Science, Kuppenakuntla,Penuballi, Khammam, TS,India.Presently he is Pursuing his M.Tech (CSE) from this collegeHis area of interests includes Information Security, Cloud Computing, Data Communication & Networks.

Mr. B.R.M.Redy is an efficient teacher, received M.Tech from JNTU Hyderabad is working as an Assistant Professor in Department of C.S.E, Sree Rama Institute of Technology & Science, Kuppenakuntla, Penuballi, Khammam, AP,India. He has published many papers in both National & International Journals. His area of Interest includes Data Communications & Networks, Information security, Database Management Systems, Computer Organization, C Programming and other advances in Computer Applications