Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1346 – 1350

SURVEY ARTICLE

Survey on Access Control Delegation to Protect and Maintain Privacy of Cloud Data

Nicholaus Gati [1], Sudhakar G. [2]

[1]M.Tech Scholar, School of IT, JNTU Hyderabad, Tanzania

[2]Lecturer, School of IT, JNTU Hyderabad, India

[1] nicholausgati9@gmail.com ; [2] sudhakar4321@gmail.com

Abstract - Conventional access control models often assume that the entity enforcing access control policies is also the owner of the data. This assumption is no longer holds as it forces the data owner to do a lot of computations as the third party such as cloud only provide facilities for data storage, where the approaches to enforce fine grained access control on confidential data hosted in the cloud are based on fine grained encryption of data. Under these models the owner of data is force to perform the fine grained encryption of data before uploading on the cloud and once user dynamics or credentials change the data owner must re-encrypt the data. Data owners thus incur high computational and communication costs. We propose a better approach should delegate the enforcement of fine- grained access control to the cloud, so to minimize the overheads at the data owner, while assuring data confidentiality from the cloud. The proposed approach that can well delegate the enforcement of access control is based on two layer of encryption, where the data owner performs course-grained encryption and the clouds perform fine grained encryption on top of the owner encrypted data. The main challenging issue is how access control policies (ACPs) can be decomposed such that the two layers of encryption perform well as required. For this case some novel optimization algorithms are proposed to help solve such a problem. Also an efficient group key management scheme is utilized to support expressive access control policies. Our system assures confidentiality, integrity of data and preserves the privacy of the end user from the cloud while delegating most of the access control enforcement to the cloud.

Keywords— Protection; Delegation; Layer Interleaving; Policy breakdown; Data privacy; Access Control; DDoS

I. INTRODUCTION

Many benefits are provided by cloud data services, despite the benefits data privacy and security issues have been major concerns. Data stored in cloud often encode sensitive information and should be approach to address security and privacy is to encrypt the data before uploading them to the cloud. Encryption alone however is not enough as fine grained access control on the data can be enforced. Such control is often based on information such as role of data users in the organization, project on which users are working and so forth. Therefore an

important requirement is to support fine grained access control, based on policies specified in an expressive access control language, over encrypted data hosted in the cloud.

With the involvement of the third-party cloud services, a crucial issue is that the identity attributes in the access control policies may reveal privacy-sensitive information about users and organizations and leak confidential information about the content. The confidentiality of the content and the privacy of the users are thus not assured if the identity attributes are not protected. It is well-known that privacy, both individual as well as organizational, is considered a key requirement in all solutions, including cloud services, for digital identity management. Further, as insider threats are one of the major sources of data theft and privacy breaches, identity attributes must be strongly protected even from accesses within organizations. With initiatives such as cloud computing the scope of insider threats is no longer limited to the organizational perimeter.

However, while the existing approach addresses some limitations of previous approaches, it still requires the data owner to enforce all the Access control policies by fine-grained encryption, both initially and subsequently after users are added/ revoked or the Access control policies change. All these encryption activities have to be performed at the owner that thus incurs high communication and computation cost. For example, if an access control policy changes, the owner must download from the cloud the data covered by this access control policy, generate a new encryption key, re-encrypt the downloaded data with the new key, and then upload the re-encrypted data to the cloud. Such approaches however have several limitations:

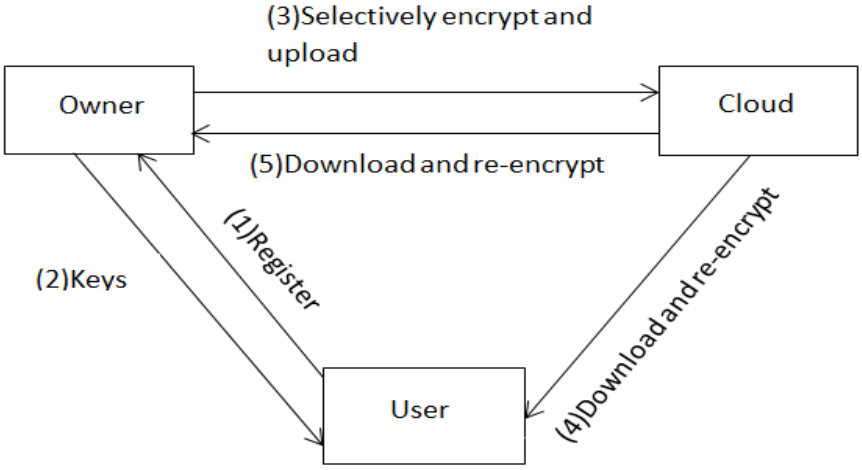

Fig 1: Traditional Approach

- 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.

Therefore, the better way to reduce the communication and computational cost, is to use the two layer encryption approach, where the fine grained encryption is enforced at the cloud and the data owner enforce the course grained encryption. Data privacy is defined as the accuracy and consistency of stored data, in absence of any alteration to the data between two updates of a file or record. Cloud services should ensure data integrity and provide trust to the user privacy. Hence, the system must have some sort of mechanism to ensure the data integrity. The current Cloud security model is based on the assumption that the user/customer should trust the provider. This is typically governed by a Service Level Agreement (SLA) that in general defines mutual provider and user expectations and obligations.

Proposed Architecture overview

In the new scheme we consider four basic roles: the data owner (owner), the data consumer (consumer), the Cloud provider (CP), and the access control provider (ACP). The goal of an owner is to store some data in a CP and allow authorized consumers to perform operations over this data. The data is protected using an access control policy. An access control policy is regarded as a function executed in an ACP. This function accepts as input a consumer's identification data and outputs either an error message if the user cannot be authorized, or an

integer number that denotes the access level of the consumer. The access level of a consumer indicates which operations she can perform over the data that is protected by the corresponding access control policy. Also the proposed system has provision to protect the cloud against Extensible Markup Language (XML)-based Denial of Service (X-DoS) and Hypertext Transfer Protocol (HTTP)- based Denial of Service (H-DoS) attacks. This is achieved using Cloud traceback and cloud protector mechanisms.

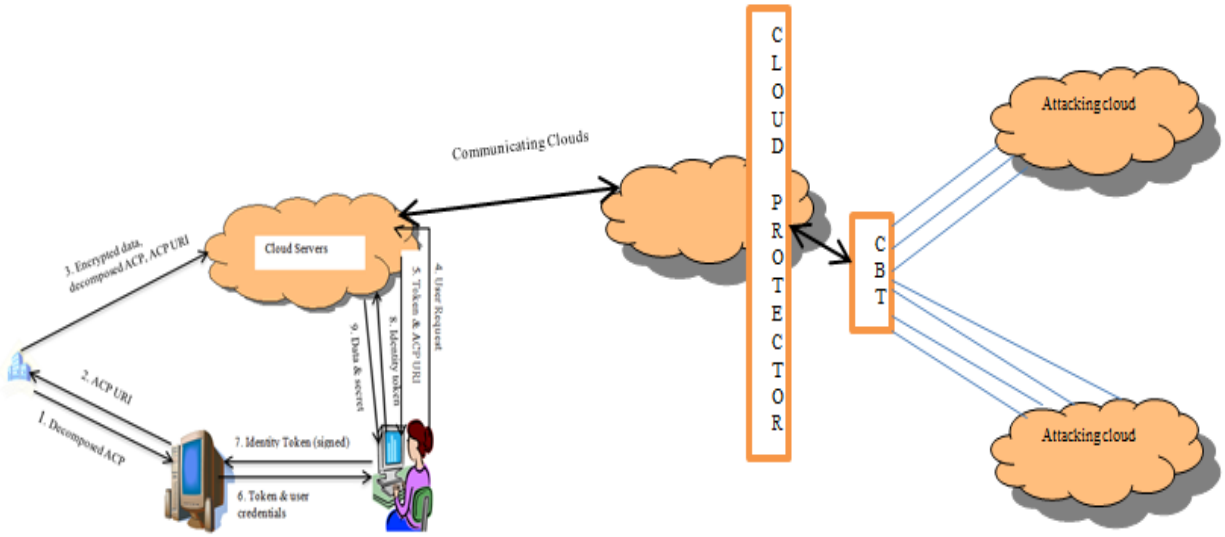

Figure 2: Proposed system architecture

II. SURVEY ON OVERALL DEVELOPMENT

As per E. Bertino and E. Ferrari

XML (eXtensible Markup Language) has emerged as a prevalent standard for document representation and exchange on the Web. It is often the case that XML documents contain information of different sensitivity degrees that must be selectively shared by (possibly large) user communities. There is thus the need for models and mechanisms enabling the specification and enforcement of access control policies for XML documents. Mechanisms are also required enabling a secure and selective dissemination of documents to users, according to the authorizations that these users have. In this article, we make several contributions to the problem of secure and selective dissemination of XML documents. First, we define a formal model of access control policies for XML documents. Policies that can be defined in our model take into account both user profiles, and document contents and structures. We also propose an approach, based on an extension of the CryptolopeTM approach, which essentially allows one to send the same document to all users, and yet to enforce the stated access control policies. Our approach consists of encrypting different portions of the same document according to different encryption keys, and selectively distributing these keys to the various users according to the access control policies.

As per Ayad F. Barsoum and M. Anwar Hasan

Currently, the amount of sensitive data produced by many organizations is outpacing their storage ability. The management of such huge amount of data is quite expensive due to the requirements of high storage capacity and qualified personnel. Storage-as-a-Service (SaaS) offered by cloud service providers (CSPs) is a paid facility that enables organizations to outsource their data to be stored on remote servers. Thus, SaaS reduces the maintenance cost and mitigates the burden of large local data storage at the organization's end. A data owner pays for a desired level of security and must get some compensation in case of any misbehavior committed by the CSP. On the other hand, the CSP needs a protection from any false accusation that may be claimed by the owner to get illegal compensations. In this paper, we propose a cloud-based storage scheme that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them. The proposed scheme has four important features: (i) it allows the owner to outsource sensitive data to a CSP, and perform full block-level dynamic operations on the outsourced data, i.e., block modification, insertion, deletion, and append, (ii) it ensures that authorized users (i.e., those who have the right to access the owner's file) receive the latest version of the outsourced data, (iii) it enables indirect mutual trust between the owner and the

CSP, and (iv) it allows the owner to grant or revoke access to the outsourced data. We discuss the security issues of the proposed scheme. Besides, we justify its performance through theoretical analysis and experimental evaluation of storage, communication, and computation overheads.

As per J. Li and N. Li

We propose Oblivious Attribute Certificates (OACerts), an attribute certificate scheme in which a certificate holder can select which attributes to use and how to use them. In particular, a user can use attribute values stored in an OACert obliviously, i.e., the user obtains a service if and only if the attribute values satisfy the policy of the service provider, yet the service provider learns nothing about these attribute values. This way, the service provider's access control policy is enforced in an oblivious fashion. To enable the oblivious access control using OACerts, we propose a new cryptographic primitive called Oblivious Commitment-Based Envelope (OCBE). In an OCBE scheme, Bob has an attribute value committed to Alice and Alice runs a protocol with Bob to send an envelope (encrypted message) to Bob such that: 1) Bob can open the envelope if and only if his committed attribute value satisfies a predicate chosen by Alice and 2) Alice learns nothing about Bob's attribute value. We develop provably secure and efficient OCBE protocols for the Pedersen commitment scheme and comparison predicates as well as logical combinations of them.

As per Padmanabhuni et al

A Denial of Service (DoS) is where an attacker attempts to deprive legitimate users of their resources. An X-DoS attack, according to Padmanabhuni et al. (2007) is where a network is flooded with XML messages instead of packets in order to prevent legitimate users to access network communications.

Further, if the attacker floods the web server with XML requests, it will affect the availability of these web services. Attackers can also manipulate the message content, in order to cause the web server to crash. To adapt X-DoS into a Distributed Denial of Service paradigm, called Distributed XML based Denial of Service (DX-DoS), the attacker uses multiple hosts to attack the victim with X-DoS attacks.

As per M. Nabeel and E. Bertino

It is very costly and cumbersome to manage database systems in-house especially for small or medium organizations. Data-as-a-Service (DaaS) hosted in the cloud provides an attractive solution, which is flexible, reliable, easy and economical to operate, for such organizations. However security and privacy issues concerning the storage of the data in the cloud and access

via the Internet have been major concerns for many organizations. The data and the human resources are the life blood of any organization. Hence, they should be strongly protected. In this paper, we identify the challenges in securing DaaS model and propose a system called Cloud Mask that lays the foundation for organizations to enjoy all the benefits of hosting their data in the cloud while at the same time supporting fine¬ grained and flexible access control for shared data hosted in the cloud.

Fine-grained Access Control: Fine-grained access control (FGAC) allows one to enforce selective access to the content based on expressive policy specifications. Research in FGAC can be categorized into two dissemination models: push based and pull-based models. In a push-based system, [10], [11] content publishers push the content to users either by broadcasting or making the content available in a public location. In a pull based system, every time users want to access some content, they login to the content provider and retrieve based on the access control policies. Our work focuses on the pull based model, but the techniques introduced can be used to construct push-based systems supporting FGAC. Under the push-based model, the database and security communities have carried out research concerning techniques for the selective dissemination of documents based on access control policies [3], [7]. In all such work, subdocuments are encrypted with different keys, which are provided to users at the registration phase, and broadcast the encrypted subdocuments to all users. However, such approaches require all [3] or some [7] keys be distributed in advance during user registration phase. This requirement makes it difficult to assure forward and backward key secrecy when user groups are dynamic with frequent join and leave operations. Further, the rekey process is not transparent, thus shifting the burden of acquiring new keys on existing users when others leave or join. In contrast, our approach makes rekey transparent to users by not distributing actual keys during the registration phase. Another distinction is that all these approaches focus on achieving confidentiality of the content and privacy of the users who access the content is not considered. In contrast, our goal is not only to provide confidentiality but also to preserve the privacy of users who access the documents. Under the pull-based model, the content publisher is required to be online in order to access the content. There has been some recent research efforts [6], [4] to construct privacy preserving access control systems by combining oblivious transfer [5], [1] and anonymous credentials [2]. The goal of such work is similar to ours but we identify the following limitations. Each transfer protocol allows one to access only one record from the database, whereas our approach does not have any limitation on the number of records that can be accessed at once since we separate the access control from the authorization. Another drawback is that the size of the encrypted database is not constant with respect to the original database size. Redundant encryption of the same record is required to support policies involving disjunctions. However, our approach encrypts each data item only once as we have made the encryption

independent of the policies. Further, such approaches are not designed to support privacy preserving content based access control.

CONCLUSION

Current trends in cloud computing and associated services are further pushing publishing functions to third-party providers to achieve flexibility and economies of scale. However, recent surveys have found that one of the key resistance factors for organizations to move to the cloud is represented by data privacy and security concerns. We believe that TLE is a promising solution to address privacy, security, communication and overheads at the owner concerns in the context of attribute based access control of organizational data over a cloud data service. Our approach is based on a privacy preserving attribute based key management scheme that protects the privacy of users while enforcing attribute based ACPs.

REFERENCES

[I]W. Aiello, Y. Ishai, and O. Reingold. Priced oblivious transfer: How to sell digital goods. In EUROCRYPT 'Oi: Proceedings of the International Conference on the The OlY and Application of Cryptographic Techniques, pages 1 19- 135, London, UK, 200 I. Springer-Verlag.

[2] M. H. Au, W. Susilo, and Y. Mu. Constant-size dynamic k-taa. In Security and Cryptography for Networks, LNCS vol. 4 i i 6, pages 1 1 1-125. Springer-Verlag, 2006.

[3]E. Bertino and E. Ferrari. Secure and selective dissemination of XML documents. ACM Trans. in! Syst. Secw: 5(3):290-331, 2002.

[4]J. Camenisch, M. Dubovitskaya, and G. Neven. Oblivious transfer with access control. In CCS '09: Proceedings of the i 6th ACM conference on Computer and communications security, pages 13 1- 140, New York, NY, USA, 2009. ACM.

[5]J. Camenisch, G. Neven, and A. Shelat. Simulatable adaptive oblivious transfer. In EUROCRYPT '07: Proceedings of the 26th annual international conference on Advances in Clyptology, pages 573-590, Berlin, Heidelberg, 2007. Springer-Verlag.

[6]S. Coull, M. Green, and S. Hohenberger. Controlling access to an oblivious database using stateful anonymous credentials. In Irvine: Proceedings of the 12th International Conference on Practice and TheolY in Public Key Clyptography, pages 501-520,B erlin,H eidelberg, 2009. Springer-Verlag.

[7]G. Miklau and D. Suciu. Controlling access to published data using cryptography. In VLDE '2003: Proceedings of the 29th international coriference on VelY large data bases, pages 898-909. VLDB Endowment, 2003.

[8]M. Nabeel and E. Bertino. Attribute based group key management. Technical Report CERIAS TR 2010, Purdue University 2010

[9]A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Euro crypt 2005, LNCS 3494. Springer-Verlag, 2005, pp. 457– 473

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

[11]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. 898–90

[12] G. Ateniese, K. Fu, M. Green, and S. Hohenberger,"Improved proxy re-encryption schemes with applications to secure distributed storage," ACM Transaction on Information System Security, vol. 9, pp. 1–30, February 2006.

Authors Bibliography

Nicholaus Gati Received BSc degree in Computer Engineering and Information Technology from the University of Dar Es Salaam, Tanzania. Pursuing M.Tech in Computer Networks and Information Security from School of Information Technology Jawaharlal Nehru Technological University, Hyderabad. His research interests include cloud computing security and storage, wireless network security, distributed systems and computing.

Sudhakar Gudlanarva received M.Tech degree in Software Engineering from School of Information Technology Jawaharlal Nehru Technological University Hyderabad 2006. Currently working as a lecturer at the School of Information Technology, Jawaharlal Nehru Technological University, Hyderabad. His research interests include cloud computing security and storage, distributed systems and Networks, wireless networks security

