ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2, Issue 3 (July - Sept. 2014)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

Multi-Message Cipher Text Policy Attribute-Based Encryption

[I]G. Venkata Krishna, [II]K. Lavanya
[I]Student, [II]Assistant Professor
[I,II]Dept. of IT, LBRCE, JNTUK University, Mylavaram, Andhra Pradesh, India

Abstract
This paper presents a new Multi-message Cipher text Policy Attribute-Based Encryption technique, and employs the MCP-ABE to design an access control scheme for sharing scalable media based on data consumers' attributes rather than an explicit list of the consumers' names. The scheme is efficient and flexible because it allows a content provider to specify an access policy and encrypt multiple messages within one Ciphertext such that only the users whose attributes satisfy the access policy can decrypt the Ciphertext. Moreover, the paper shows how to support resource-limited mobile devices by offloading computational intensive operations to cloud servers while without compromising data privacy.

Keywords
Multi-message Cipher text, Attribute-Based Encryption, access policy, computational intensive operations, data privacy

I. Introduction

There is a trend for sensitive user data to be stored by third parties on the Internet. For example, personal email, data, and personal preferences are stored on web portal sites such as Google and Yahoo. The attack correlation center, dshield.org, presents aggregated views of attacks on the Internet, but stores intrusion reports individually submitted by users. Given the variety, amount, and importance of information stored at these sites, there is cause for concern that personal data will be compromised. This worry is escalated by the surge in recent attacks and legal pressure faced by such services. One method for alleviating some of these problems is to store data in encrypted form. Thus, if the storage is compromised the amount of information loss will be limited. One disadvantage of encrypting data is that it severely limits the ability of users to selectively share their encrypted data at a fine-grained level. Suppose a particular user wants to grant decryption access to a party to all of its Internet traffic logs for all entries on a particular range of dates that had a source IP address from a particular subnet. The user either needs to act as an intermediary and decrypt all relevant entries for the party or must give the party its private decryption key, and thus let it have access to *all* entries. However, it is challenging to design a suitable access control mechanism in content sharing services due to:

(1) any individual is able to freely produce any number and any kind of online media such as text, image, sound, video, and presentation;
(2) any individual is able to grand any access to his media to anyone, at any time;
(3) an individual may reveal a large number of attributes (e.g., name, age, address, friendship, classmate, fans, hobby, personal interest, gender, and mobility), and some of them can be very dynamics; and
(4) Individuals may share contents using various devices and bandwidth, and hence demand different access privileges for the same media.In this paper we present an access control scheme for scalable media.

The scheme has several benefits which make it esp ecially suitable for content delivery. For example, it is extremely scalable by allowing a data owner to grant data access privileges based on the data consumers' attributes (e.g., age, nationality, gender) rather than an explicit list of user names; and it ensures data privacy and exclusiveness of access of scalable media by employing attribute-based encryption. For this purpose, we introduce a novel Multi-message Ciphertext Policy Attribute-Based Encryption (MCP-ABE) technique. MCP-ABE encrypts multiple messages within one ciphertext so as to enforce flexible attribute-based access control on scalable media. Specifically, the scheme constructs a key graph which matches users' access privileges, encrypts media units with the corresponding keys, and then encrypts the key graph with MCPABE; only those data consumers with the required user attributes can de-crypt the encryption of the key (sub) graph and then decrypt the encrypted media units. To cater for resource-limited mo-bile devices, the scheme offloads computational intensive operations to cloud servers while without compromising user data privacy. Attribute based encryption schemes, such as CP-ABE and MCP-ABE, are designed to be secure against user collusion attacks. The present scheme is also secure against user collusion attacks due to use of attribute-based encryption. The experiments demonstrate that the present scheme is applicable on smart phone, especially when a cloud platform is available.

II. Related Work

A. Fine-grained Access Control

Fine-grained access control systems facilitate granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users. Several techniques are known for implementing fine grained access control.

Common to the existing techniques and the references there in is the fact that they employ a trusted server that stores the data in clear. Access control relies on software checks to ensure that a user can access a piece of data only if he is authorized to do so. This situation is not particularly appealing from a security standpoint. In the event of server compromise, for example, as a result of a software vulnerability exploit, the potential for information theft is immense. Furthermore, there is always a danger of "insider attacks" wherein a person having access to the server steals and leaks the information, for example, for economic gains. Some techniques (see, e.g., [2]) create user hierarchies and require the users to share a common secret key if they are in a common set in the hierarchy. The data is then classified according to the hierarchy and encrypted under the public key of the set it is meant for. Clearly, such methods have several limitations. If a third party must access the data for a set, a user of that set either needs to act as an intermediary and decrypt all relevant entries for the party or must give the party its private decryption key, and thus let it have access to all entries. In many cases, by using the user hierarchies it is not even possible to realize an access control equivalent to

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

monotone access trees.

Identity-Based Encryption: The concept of Attribute-Based Encryption was introduced by Sahai and Waters [34], who also presented a particular scheme that they called Fuzzy Identity-Based Encryption (FIBE). The Fuzzy-IBE scheme builds upon several ideas from Identity-Based Encryption. In FIBE, an identity is viewed as a set of attributes. FIBE allows for a private key for an identity, ω, to decrypt to a ciphertext encrypted with an identity, ω^0, if and only if the identities ω and ω^0 are close to each other as measured by the "set overlap" distance metric. In other words, if the message is encrypted with a set of attributes ω^0, a private key for a set of attributes ω enables decrypting that message, if and only if $|\omega \cap \omega^0| \geq d$, where d is fixed during the setup time. Thus, FIBE achieves error tolerance making it suitable for use with biometric identities. However, it has limited applicability to access control of data, our primary motivation for this work. Since the main goal in FIBE is error tolerance, the only access structure supported is a threshold gate whose threshold is fixed at the setup time.the underlying data contents by combining techniques of attribute-based encryption, proxy re-encryption, and lazy re-encryption.

Pirretti proposed an information management architecture using CP-ABE and optimized security enforcement efficiency. Furthermore, they employed the architecture and optimization method on two example applications: an HIPAA (Health Insurance Portability and Accountability Act) compliant distributed file system and a content delivery network.

B. Media Structure Oriented Access Control

The SSS (Secure Scalable Streaming) encryption method [7] for scalable video is a progressive encryption technique. As SSS encryption may result in decryption failures due to package loss [8], it should be integrated with error correction techniques in practice so as to overcome this problem.

By exploiting the JPEG2000 property of " *encode once, decode many ways* ", Wu *et al.* [9] designed an access control scheme which is efficient and secure. More importantly, the scheme is extremely flexible as its **" encrypt once, decrypt many ways "** property is completely compatible with the feature of the JPEG 2000 image code-streams.

An MPEG4 [10] stream may have two types of quality scalabilities—either PSNR or bit rate scalability. Zhu *et al.* [11] proposed access control schemes for streams encoded by the MPEG- 4 Fine Granularity Scalability (FGS) standard so as to allow a single encrypted stream to support both types of scalabilities simultaneously.

III. Problem Statement

A. Existing System

A promising approach to access control in content sharing services is to empower users to enforce access controls on their data directly, rather than through a central administrator. However, this requires flexible and scalable cryptographic key management to support complex access control policies. A native access control solution is to assign one key for each user attribute, distribute the appropriate keys to users who have the corresponding attributes, and encrypt the media with the attribute keys repeatedly Another method is to classify users into different roles based on their attributes, assign role keys to users, and then encrypt the content using the role keys. However, this approach results in high complexity, i.e., the number of keys for each user and the number of cipher texts for one message are on the order of where is the number of all possible user attributes. Both of these solutions suffer from the rigid and inflexible definition of the underlying access control policies. A remedy to this problem is employing Ciphertext Policy Attribute-Based Encryption (CP-ABE). In CP-ABE, a Ciphertext is embedded with an access control policy, or access policy for short, associated with user attributes. A recipient of the ciphertext is able to decrypt the ciphertext only if her attributes satisfy the access policy in the ciphertext. CP-ABE can be viewed as a one-to-many public key encryption scheme and hence enables a data owner to grant access to an unknown set of users. Nonetheless, existing CP-ABE schemes merely deliver one encrypted message per ciphertext to all authorized users and are not optimal for efficient sharing of scalable media.

Disadvantages

- In an existing system solution is flexible, but it is vulnerable to collusion attack.
- The existing method is to classify users into different roles based on their attributes, assign role keys to users, and then encrypt the content using the role keys. However, this approach results in high complexity.
- Existing CP-ABE schemes merely deliver one encrypted message per ciphertext to all authorized users and are not optimal for efficient sharing of scalable media.

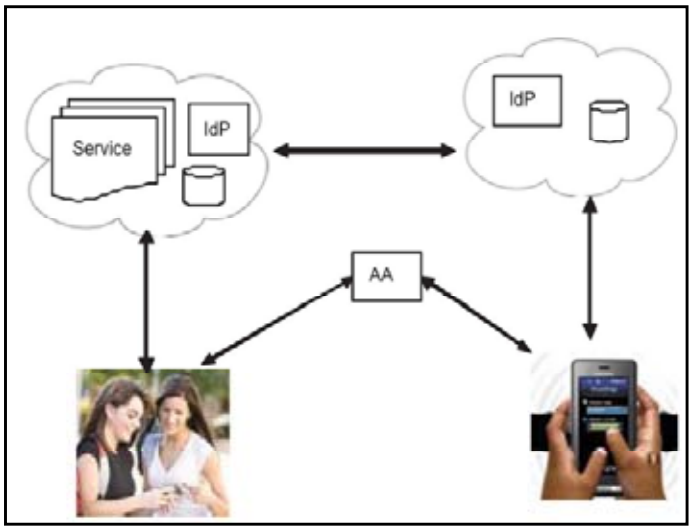
B. Proposed System

In this paper we present an access control scheme for scalable media. The scheme has several benefits which make it especially suitable for content delivery. For example, it is extremely scalable by allowing a data owner to grant data access privileges based on the data consumers' attributes (e.g., age, nationality, gender) rather than an explicit list of user names; and it ensures data privacy and exclusiveness of access of scalable media by employing attribute-based encryption. For this purpose, we introduce a novel Multi-message Ciphertext Policy AttributeBased Encryption (MCP-ABE) technique. MCP-ABE encrypts multiple messages within one ciphertext so as to enforceflexible attribute-based access control on scalable media. Specifically, the scheme constructs a key graph which matches users' access privileges, encrypts media units with the corresponding keys, and then encrypts the key graph with MCP-ABE; only those data consumers with the required user attributes can decrypt the encryption of the key (sub) graph and then decrypt the encrypted media units. To cater for resource-limited mobile devices, the scheme offloads computational intensive operations to cloud servers while without compromising user data privacy.

Advantages

- The present scheme is also secure against user collusion attacks due to use of attribute-based encryption.
- The experiments demonstrate that the present scheme is applicable on smartphone, especially when a cloud platform is available.
- We present an access control scheme for scalable media. The scheme has several benefits which make it especially suitable for content delivery.

4. System Architecture



Architecture of a cloud -assisted network, where IdP (Identity Provider) is used to authenticate users to the media provider.

V. Modules

Module Description

A. Registration

In this module normal registration for the multiple users. There are multiple owners, multiple AAs, and multiple users. The attribute hierarchy of files – leaf nodes is atomic file categories while internal nodes are compound categories. Dark boxes are the categories that a PSD's data reader has access to.

- PUD - public domains
- PSD -personal domains
- AA -attribute authority
- MA-ABE - multi-authority ABE
- KP-ABE - Key Policy Attribute based Encryption
- MCP-ABE - Multi-message Cipher-text Policy Attribute-Based Encryption

B. Attribute oriented access control

In this Module, supports ï¬ ne-grained access control policies and dynamic group membership6by using CP-ABE scheme. In addition, is able to revoke a user without issuing new keys to other users or re-encrypting existing cipher-texts by using a proxy.

KP-ABE (Key Policy Attribute based Encryption) to enforce access policies based on data attributes. Their scheme allows data owners to delegate most of the computation tasks involved in ï¬ ne-grained data access control to untrusted cloud servers without disclosing the underlying data contents by combining techniques of attribute-based encryption, proxy re-encryption, and lazy re-encryption an information management architecture using CP-ABE and optimized security.

C. One-way hash function

In this Module, usually for security or data management purposes. The "one way" means that it's nearly impossible to derive the original text from the string. A one-way hash function is used to create digital signatures, which in turn identify and authenticate the sender and message of a digitally distributed message.

D. Cipher-text policy attribute-based encryption

In this Module, every user's personal secret key is associated with a set of attributes while every ciphertextis associated with an access policy. A user successfully decrypts a ciphertext only if her set of attributes satisï¬ es the access policy speciï¬ ed in the ciphertext. We brieï¬,y describe the CP-ABE.

VI. Experimental Results

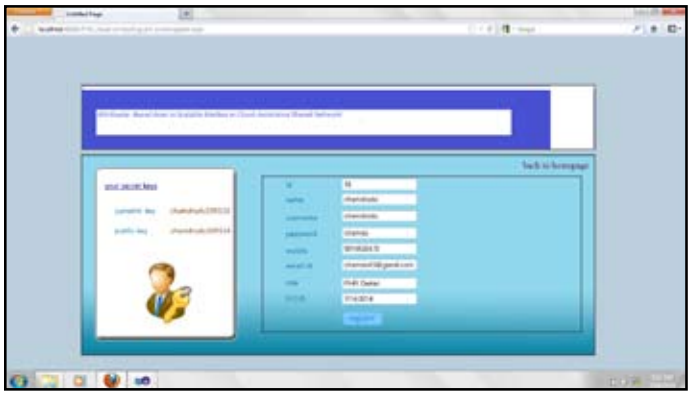


Fig: Key generation

Fig: File upload

VII. Conclusion

CP-ABE primarily based access management permits a data owner to enforce access management supported attributes of data customers while not explicitly naming the particular information customers. However, CP-ABE supports just one privilege level and therefore isn't suitable for access management to ascendable media. In this paper we presented a basic development of the CP-ABE and how the access structure is built in the CP-ABE. Cloud computing is the highly adaptive technology and mobile devices are becoming widespread the above presented CPABE access control helps to free from the computational demanding operations on the cloud server. The experimental results show that the CP-ABE is flexible, scalable, user, accountability, collision, resistant, user revocation. With the assistance of the cloud the acceleration of the decryption increased but it is still slow in some lowend devices because a Integrated exponentiation operation is required.

References

[1] *E. Messmer, "Are security issues delaying adoption of cloud computing?," Network World, Apr. 2009 [Online]. Available http://www.networkworld.com/news/2009/042 709-burning-secu-rity-cloud-computing.html*

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

[2] *E. Messmer, "Security of virtualization, cloud computing divides IT and security pros," Networkworld.com, Feb. 2010 [Online].Available:http://www.networkworld.com/news/2010/022210-virtual-ization-cloud-securitydebate.html*

[3] *X. Zhang, M. Nakae, M. J. Covington, and R. Sandhu, "Toward a usage-based security framework for collaborative computing systems," ACM Trans. Inf. Syst. Security, vol.11, no. 1, pp. 1–36, 2008.*

[4] *S. Jahid, P.Mittal, and N. Borisov, "EASiER: Encryption-based access control in social networks with efficient revocation," in Proc. ACM Symp. Inf. Computer Commun. Security, Mar. 2011, pp. 411– 415.*

[5] *S.Yu, C.Wang,K.Ren, andW. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE Int. Conf. Comput. Commun., 2010, pp. 1–9.*

[6] *V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attribute based encryption for fine-grained access conrol of encrypted data," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.*

[7] *S.J. Wee and J. G. Apostolopoulos, "Secure scalable streaming enabling transcoding without decryption," in Proc. IEEE Int. Conf. Image, 2001, pp. 437–440.*

[8] *V. Gergely and G. Feher, "Enhancing progressive encryption for scalable video streams," in Proc. EUNICE, Open European Summer School and IFIP TC6.6 Workshop on The Internet of the Future, 2009, vol. 5733, Lecture Notes in Computer Science, pp. 51–58.*

[9] *Y. Wu, D. Ma, and R. H. Deng, "Flexible access control to JPEG2000 image code-streams," IEEE Trans. Multimedia, vol. 9, no. 6, pp. 1314–1324, Oct. 2007.*

[10] *ISO/IEC 14496-2, Coding of Audio-Visual Objects Part 2: Visual.*

[11] *B. B. Zhu,C.Yuan, Y. Wang, and S. Li, "Scalable protection for MPEG-4 fine granularity scalability," IEEE Trans. Multimedia, vol. 7, no. 2, pp. 222–233, Apr. 2005.*

Authors Profile

G venkata krishn pursuing M.Tech Degree in Software Engineering from Lakireddy Bali Reddy College of Engineering, Vijayawada, AP, INDIA. Her research Interests include Software Engineering, Image Processing and Biometrics.

K Lavanya is an assistant professor of Information Technology at Lakireddy Bali Reddy College of engineering. She obtained her M.Tech from JNTUK. Her research interests include Artificial intelligence, Neural Networks, Data Mining and Information security.