International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 6 –NOVEMBER 2014.

CLOUD-ASSISTED CONTENT SHARING NETWORKS ON ATTRIBUTE-BASED ACCESS TO SCALABLE MEDIA

Nunna Saraawathi,S[*1] and Santhi Priya[#2]

[*]*Student, Dept of CSE, Chalapathi Institute of Technology, A.R.Nagar,Mothadaka, Guntur dist*

[#]*Asst Professor, Dept of CSE, Chalapathi Institute of Technology, A.R.Nagar,Mothadaka, Guntur dist*

Abstract— This paper presents a novel Multi-message Cipher text Policy Attribute-Based Encryption (MCP-ABE) technique, and employs the MCP-ABE to design an access control scheme for sharing scalable media based on data consumers' attributes (e.g., age, nationality, or gender)rather than an explicit list of the consumers' names. The scheme is efficient and flexible because MCP-ABE 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.

Index Terms—Access control, cloud computing, data security and privacy, scalable media content

I. INTRODUCTION

Content sharing environments such as social networking are very dynamic in terms of the number of on-line users, storage requirement, network bandwidth, computational capability, applications and platforms, thus it is not easy for a service provider to allocate resources following the traditional client-server model. As cloud computing offers application developers and users an abstract view of services that hides much of the system details and inner workings, it is more and more popular in content-sharing applications. However, the weak security provision of cloud computing services is delaying their adoption [1]. As a result, it is imperative for cloud computing based service providers, private or public, to build security functionalities into their services and manage

their services following prudent security practices [2]. Access control is the fundamental security mechanism to facilitate information sharing in a controllable manner. It exerts control over which user can access which resource based on a permission relationship between user attributes and resource attributes, where attributes can be any information deemed relevant for granting access, such as user's job function and resource quality, and permission is specified in terms of requirements on the attributes of resource and user. Any user with attributes that meet the requirements has access to that resource.

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. 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 naïve 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, e.g., the ciphertext is produced as to protect message with attribute key pair and cipher . This naïve solution is flexible, but it is vulnerable to collusion attack. Technically, a user having key for one attribute and another user having key for another attribute can collude to decrypt ciphertext to . In other words, two users having one attribute each are able to conspire to have the same capability as a user having those two attributes in the näive scheme. 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 ciphertexts 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) [3]. In CP-ABE, a ciphertexts 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 scheme merely deliver one encrypted message per ciphertext to all authorized users and are not optimal for efficient sharing of scalable media

II. RELATED WORK

Fundamental to usage control model [8] isthe concept of attributes attached to bothusers and resources. In content sharingapplications, as mapping between useridentity and resource is dynamic, accesscontrol methods related to our work can beclassified into two categories.A. User Attribute Oriented Access ControlEASiER [9] is an architecture thatsupports fine-grained access control policiesand dynamic group membership by usingCP-ABE scheme. In addition, EASiER isable to revoke a user without issuing newkeys to other users or re-encrypting existingciphertexts by using a proxy.Yu et al. [10] employed KP-ABE (KeyPolicy Attribute based Encryption [11]) toenforce access policies based on data attributes.Their scheme allows data owners todelegate most of the computation tasksinvolved in fine -grained data access controlto untrusted cloud servers without disclosingthe underlying data contents by combiningtechniques 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. Akinyele et al. [13] designed and implemented a self-protecting electronic medical records (EMRs) using both CPABE and KP-ABE. In order to protect individual items within an EMR, each item is encrypted independently with its own access control policy. Persona [14] enables access control by employing a combination of traditional public key cryptography and attribute-based encryption scheme. The combination of classical public- key schemes and ABE schemes has the drawback of increased key management complexity.

The above attribute- based access control methods enable flexible access policies for the users.However, they treated media content as a single monolithic object, ignoring the structure of the content. Hence, these schemes are not suitable for access control to scalable multimedia content. B. Media Structure Oriented Access ControlThe SSS (Secure Scalable Streaming) encryption method [15] for scalable video is a progressive encryption technique. As SSS encryption may result in decryption failures due to package loss [16], 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. [17] designed an access control schemewhich is efficient and secure. Moreimportantly, the scheme is extremelyflexible as its “ encrypt once, decrypt many ways ” property is completely compatiblewith the feature of the JPEG 2000 imagecode-streams.

An MPEG4 [18] stream may have two types of quality scalabilities—either PSNR or bit rate scalability. Zhu et al. [19] 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. H.264/SVC [20] is an efficient video codec standard which specifies temporal, quality and spatial scalabilities. Selective encryption (e.g.,[21], [22], [23], [24]) encrypts portions of the bit-stream such as sign of motion vector so as to protect theSVC bit-stream in a fast and flexible way. However, selective encryption is usually insecure. By exploiting the tree-structures of H.264 SVC bitstreams, schemes in[25], [26] produce secure scalable bitstreams with relatively high overhead.

All the above media structure based access control schemes exploit the format of media data to generate protected objects so that users with the necessary keys can decrypt the corresponding ciphertext. These schemes are limited to efficient key generations and normally assume the existence of an online key distribution center; and they don’t deal with access policies, e.g., how to assign user attributes to access privileges

III. PRELIMINARIES

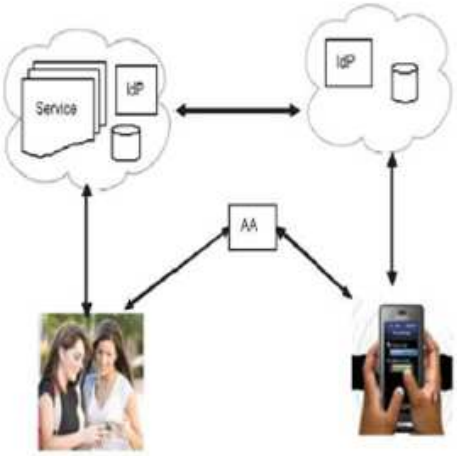
To make the paper self-contained, this section introduces the basic concepts of oneway hash function, bilinear map, access tree, and CP-ABE [3]. For simplicity, we assume that

A. System Architecture

With reference to Fig. 2, a media sharing application in cloud environment is composed of the following parties: backend servers, foreground servers, AA, and data consumers

(or users). Backend server is part of the infrastructure of the cloud computing platform. According to the National Institute of Standards and Technology (NIST) [5], cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider's interaction. Cloud computing platforms are assumed to have abundant storage capacity and computation power. Hence, from the viewpoints of network service providers, cloud computing significantly decreases the traffic and storage requirements incurred by their applications.

Foreground server provides the services which are always online. A server is often operated by a cloud service provider (CSP), but sometimes, a user is able to run his/her own services on the cloud platform too. The foreground services may include web service, database service, media maker service, media de-coding service, identity management service, etc.



Attribute Authority (AA), a trusted third party [6], sets up the system parameters of attribute-based encryption system (such as system-wide public key and master key), verifies every user's attributes (e.g., group membership, role, security clearance or authorization information) and issues personal secret key corresponding to the set of attributes of the user. In practice, there could be multiple AAs in a system. For example, a university or corporate may run an AA, and a user may act as an AA for his/her extended family members. To keep the presentation simple, we assume a single AA in the rest of the paper. User may be a data owner, or a data consumer, or both. A data owner produces (protected or unprotected) media content (text, voice, video, etc.), and uploads the media content to cloud servers. To enforce access control to his data, the data owner assigns assigns access privileges to data consumers whom the data owner may or may not know.

A data consumer downloads media con-tent of her interest from cloud servers, and obtains the content based on her attributes and the access policy of the data owner. To this end, the data consumer must obtain from AA a personal secret key bound to her set of attributes. In this data owner-consumer model, the backend servers pro-vide the fundamental platform for storage, networking, etc; the foreground servers provide the interface for media generation, transmission, and computational assistance to users; while AA issues personal secret keys so that access

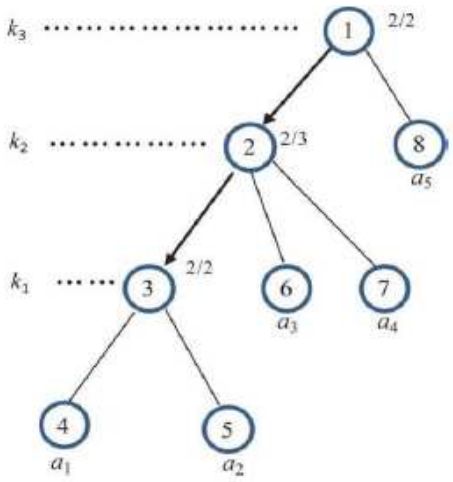
control can be en-forced flexibly based on user attributes and media scalability.

B. Data Structure of Media

In media sharing applications, files of almost all formats could be exchanged. Particularly, for some media file formats such as text, PDF, Microsoft word, JPEG2000, H.26x, SVC files, and presentations, their content can be segmented into logical units. Each unit itself is meaningful, and more units provide more information. Thus, different sets of units can be viewed by different groups of consumers. We refer to such media content as scalablemedia content. For example, assuming that an SVC video file includes one base layer and two enhancement layers, we may assign three access privileges to users. If the unit for base layer is assigned to a consumer, she obtains a video experience of basic quality, but if the base layer and the two enhancement layers are available, the video shown to her will be of full fidelity. Fig. 3 illustrates a mapping between access privileges and media units, where a consumer with privilege is allowed to access media units . To simplify the description and without loss of generality, we will assume the linear mapping given in Fig. 3 in the following.

IV. ACCESS CONTROL ON SCALABLE MEDIA

Components in an attribute -based access control scheme includes subjects each specified by a set of attributes, objects and access policies. For example, a user's age, reputation, role are the subject attributes, while SVC stream files or presentation files are objects. An access policy defines the minimal attribute set which a subject should have in order to access the object. Therefore, the challenge in attribute- based access control is how to provide flexible and finegrained access control at low cost.



Access tree for the example, where the arrows in the tree "trunk" indicate dependence of unit keys.

A. One-Way Hash Function

A hash function takes a variable-length input string and converts it into a fixed-length output string, called a hash value. A one-way hash function, denoted as , works in one direction only: it is easy to compute a hash value from a pre-image ; however, given an image , it is hard to find a pre-image such that . There are many one-way hash functions, such as SHA-1 [4].

B. Bilinear Map

Let and be two multiplicative cyclic groups of prime order , and is a generator of . A bilinear map has the following properties:. In this example, there are four attributes, and the Boolean function representation of the access policy is . If an user has attribute , is assigned to be TRUE. • Bilinearity: for all and ZZ , we have • Non-degeneracy: where both the group operation in and the bilinear map are efficiently computable. The input group in a bilinear map is usually a point group over an elliptic (or hyperelliptic) curve.

C. Access Tree

In any access control scheme, there is an access policy which defines the access conditions under which a subject can access an object. An access tree is a graph representation of the access policy. Such a tree includes non leaf nodes and leaf nodes. Each leaf node is associated with a user attribute (e.g., age, gender, profession), while each non-leaf node has child nodes which may be leaf nodes, other non-leaf nodes or both. The root, a special non-leaf node, has no parent node. Without loss of generality, we tag the nodes in an access tree as follows. The root node is tagged with 1, and all the other nodes are tagged with sequentially. For simplicity, this paper refers a node using either or interchangeably unless otherwise stated. Each non-leaf node is associated with a Boolean function derived from the access policy1. With reference to Fig. 1, the Boolean function of non-leaf node is represented with , which means that has child nodes, and its Boolean value is evaluated to be TRUE if it has at least child nodeswhose Boolean functions are evaluated to be TRUE.For instance, the Boolean function for node is 2/3, or equivalently , and it's TRUE if and .

Note that we use to denote a Boolean variable which takes value TRUE if the attribute . We say that the set of attributes of a user satisfies the access tree if =TRUE, which is iteratively defined as follows. For any leaf node which is associated with an attribute , its Boolean value is TRUE. For any non-leaf node, its Boolean value is the value of its Boolean function. If and only if the root node's Boolean value is TRUE, then =TRUE. For example, given an attribute universe , let the access policy be " if AND Any two out of three in set are included in set , the access is granted ", access tree in Fig. 1 is the graph representation of the access policy. Table I lists some results on with respect to various user attributes .

TABLE I
EVALUATION OF THE ACCESS TREE IN FIG. 1.

	$\mathcal{A}$	Node N_2	Node N_1 (T($\mathcal{A}$))	Access
1	a_1, a_2, a_3	TRUE	FALSE	No
2	a_3, a_4	FALSE	FALSE	No
3	a_1, a_2, a_4	TRUE	TRUE	Yes
4	a_2, a_3, a_4	TRUE	TRUE	Yes
5	a_1, a_3, a_4	TRUE	TRUE	Yes
6	a_1, a_2, a_3, a_4	TRUE	TRUE	Yes

V. EXPERIMENTS

A. Configuration

We set up a private cloud with three computers supporting BIOS virtualization technology so as to simulate a group of computers. We also set up a console with Ubuntu Desktop 11.04 and use OpenStackFlat Network mode to configure the computer network. In the experiments, a virtual PC (over a Dell Precision 390 with Intel Core2Duo@2.4GHz) is used as a cloud server for assisting decryption operations for mobile devices, and a smart phone SAMSUNG (s5830@800MHz) is used as the platform for a data consumer. Besides, a desktop PC is used as AA for generating keys, and pack media data for a data owner. To implement the access control scheme, we adopted the bi-linear map software pbc2[29] which uses a

160-bit elliptic curve group based on the super singular curve over a 512-bit finite field. In addition, the hash function SHA-1 is used to generate the key chain.

VI. 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.

VII. 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 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 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.

VIII. CONCLUSIONS AND FUTURE WORK

In order to share media content in a controllable manner, a suitable access control mechanism should be deployed. CPABE based access control allows a data owner to enforce access control based on attributes of data consumers without explicitly naming the specific data consumers. However, CP-ABE supports only one privilege level and hence is not suitable for access control to scalable media. In this paper we extended CP-ABE to a novel MCP-ABE and proposed a scheme to support multi-privilege access control to scalable media. As cloud computing is increasingly being adopted and mobile devices are becoming pervasive, the present access control scheme allows a mobile user to offload computational intensive MCP - ABE operations to cloud servers while without compromising user's security. The experimental results indicated that the proposed access control scheme is efficient for securely and flexibly managing media content in large, loosely-coupled, distributed systems. With the assistance of the cloud server, the decryption opera-tion is accelerated significantly at the consumer side. However,the decryption may be still slow for low-end devices because a modular exponentiation operation is required. Thus, one future work is how to speed-up the decryption operation at low-end devices.

REFERENCES

[1] E. Messmer, "Are security issues delayingadoption of cloud computing?," NetworkWorld, Apr. 2009 [Online]. Available:http://www.networkworld.com/news/2009/042709-burning-secu-rity-cloud-computing.html

[2] E. Messmer, "Security of virtualization, cloud computing divides IT and security pros," Networkworld.com, Feb. 2010 [Online]. Available: http://www.networkworld.com/news/2010/022 210-virtual-ization-cloud-security-debate.html

[3] . Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. SecurityPrivacy, 2007, pp. 321–334.

[4] National Inst. Standards and Technol., SecureHash Standard (SHS), FIPS Publication 180- 1, 1995.

[5] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145, 2011.

[6] M. D. Soete, "Attribute certificate," in Encyclopedia of Cryptography and Security, H. C. A. Van Tilborg and S. Jajodia, Eds., 2nd ed. Berlin, Germany: Springer, 2011, p. 51.

Ms. NUNNA SARASWATHI, pursuing her M.Tech degree in Computer science & Engineering from Chalapathi Institute of Technology, A.R.Nagar,Mothadaka,Guntur dist.

S. Santhi Priya has been graduated with B.Tech in 2002 from Nagarjuna University, and post graduated in Software engineering from JNTU Hyderabad, India. She has around 12 years of teaching experience.. She is currently working with Chalapathi Institute of Technology,Motadaka Andhra Pradesh, India.