

PRIVACY PRESERVING MEDIA SHARING WITH SCALABLE ACCESS CONTROL AND SECURE DEDUPLICATION IN MOBILE CLOUD COMPUTING

¹CHILUVERI MANOJ KUMAR, ²MURALI PONAGANTI

¹MCA Student, ²Associate Professor

DEPARTMENT OF MCA
SREE CHAITANYA COLLEGE OF ENGINEERING, KARIMNAGAR

ABSTRACT

Benefiting from cloud computing and mobile devices, a huge number of media contents such as videos are shared in mobile networks. Although scalable video coding can be utilized to provide flexible adaptation, the cloud poses a serious threat to media privacy. In this paper, we propose a privacy-preserving multi-dimensional media sharing scheme named SMACD in mobile cloud computing. Firstly, each media layer is encrypted with an access policy based on attribute-based encryption, which guarantees media confidentiality as well as fine-grained access control. Then we present a multi-level access policy construction with secret sharing scheme. It ensures that the mobile consumers who obtain a media layer at a higher access level must satisfy the access trees of its child layers at the lower access level, which is compatible with the characteristics of multi-dimensional media and also reduces the complexity of access policies. Moreover, we introduce decentralized key servers to achieve both intra-server and inter-server deduplication by associating different access policies into the same encrypted media. Finally, we conduct experimental evaluation on mobile device and cloud platform with real-world datasets. The results indicate that SMACD protects media privacy against cloud media center and unauthorized parties, while incurring less computational and storage cost.

I. INTRODUCTION

WITH the quick development of mobile computing technique and the prevalence of interpersonal sociality, mobile network has rapidly become popular in people's daily life for facilitating communications and building relationship with others [1], [2]. By using mobile devices, people can receive information from their service providers at any time or place, and also share their own data interactively to all related and connected users. Actually, along with the increasing population of mobile services and cloud computing [3], people are more likely to distribute and view media data (e.g. videos) rather than text data with the media center, such as YouTube and Netflix. Moreover, the cloud services such as Google Cloud and Microsoft Azure make it easy to use high-definition video services on most popular mobile devices. For example, with Google Cloud, the open platform Vimeo is able to provide high-definition videos hosting and sharing services, in which media creators can upload their videos, and also restrict access to specific people [4].

Although the media services allow media distributors to configure their privacy settings so that they are able to grant the media to be accessed by selected friends or subscribers, the media distributor may not trust the media center, especially the cloud media center [5]. In particular, once the media content is posted to cloud media center, the media distributor's direct control over the media content would be

deprived [6], [7]. The media content on cloud media center may be leaked to unauthorized media consumers, which will seriously threaten the media privacy, even the privacy of media distributor [8]. These privacy matters have raised wide concerns in existing media services, and require cryptographic algorithms to protect media confidentiality and guarantee authorized access when sharing the media content in mobile cloud computing [9], [10].

Currently, identity-based encryption (IBE) [11] and broadcast encryption [12] have been utilized to protect the media privacy. However, the traditional identity-based access control mechanism may not be appropriate for large scale media sharing due to the widespread dissemination of media content. The fact is that media distributors usually define the access privileges with the social or subscription relationships [13]. A promising cryptographic primitive known as attribute-based encryption (ABE) [14], [15] is a candidate to solve this challenge, since it can protect media privacy and realize fine-grained and one-to-many access control. Specially, cipher text-policy ABE (CP-ABE), enables the media distributor to enforce an access policy such as "Member" AND "Student" over the attribute universe on the media content such that a media consumer can access it only by possessing enough attributes. In this case, the media distributor can enforce expressive access privileges towards the media content.

On the other hand, media dissemination among heterogeneous networks and devices usually needs to store multiple versions of media content, which will incur a lot of storage overhead. The scalable structure of media content is applied to adjust the conditions of heterogeneous network environment [16], which encodes a single media content into a base layer with the lowest quality, and multiple enhancement layers providing high-definition

qualities by exploiting scalable video coding (SVC) technique [17]. The SVC provides a flexible decoding mechanism to deal with different mobile devices and networks. Hence, a media distributor can share a multi-dimensional media content which has diverse quality in terms of resolution, frame rate, and signal-noise-ratio (SNR), with different media consumers, and only some of them could view the content with higher quality. However, it introduces new challenges to the privacy-preserving media sharing.

Our Motivations

Considering the privacy and access control of multidimensional media, the media distributor may define individual access privilege for each media layer, which means multiple access policies should be enforced on the layers of a media content. The direct approach to settle the above challenging task is that media distributor encrypts each layer of media content with a complete individual access policy based on CP-ABE [18], and assigns the decryption key to corresponding media consumers on the basis of their access privileges. However, this approach causes lots of repeated operations since the access policy of a higher access-level layer contains the attributes in the access policies of its child layers in the lower access level. Considering this characteristic of multi-dimensional media, optimized access structure construction [19] was proposed to improve the system efficiency by reducing the number of non-leaf nodes in the access tree. However, there are still duplicate attributes in the access policies of multiple layers, which will incur relatively high computational and storage overhead. Another solution is to decrease the key recovery cost on the mobile consumer side with key graph [20], in which a hash chain is generated for all the access keys of access policies in the encryption phase, and a mobile consumer can derive all the authorized access keys with the access key of highest privilege

level granted to her/him. However, this solution cannot be directly applied to multi-dimensional scalable media stream since a certain layer might be extended simultaneously from multiple dimensions such as resolution and frame rate. Hence, it is essential to develop efficient mechanisms to protect the privacy of shared multi-dimensional media in mobile cloud computing.

Our Contributions

In this paper, we propose SMACD, a privacy-preserving media sharing scheme in mobile cloud computing for multidimensional media by providing scalable access control and secure de duplication. In our scheme, the media is first encoded into multiple layers with the SVC standard, and each layer is then encrypted with an owner-enforced access policy based on CP-ABE. The mobile consumer in our scheme can decrypt the encrypted media layers by satisfying their access policies and decode them into media content with various qualities. The main contributions of our scheme can be summarized as follows. _

We propose a scalable access control mechanism for multi-dimensional media sharing with an efficient multi-level access policy construction based on access tree and secret sharing. It integrates multiple access policies in a top-down manner and ensures that consumers who view the media layer at a higher access level must satisfy the access trees of its child layers at the lower level, which is compatible with the characteristics of multi-dimensional media, and reduces the complexity of access policies.

We achieve attribute-based secure de duplication by using decentralized key servers to support both intra-server and inter-server de duplication, in which the same encrypted scalable media content could be associated with different multi level access policies on the basis of the designed storage structure.

We conduct experimental evaluation on mobile device and cloud platform with real-world datasets. The results indicate that our scheme protects media privacy against the cloud media center, key servers and unauthorized consumers with fine-grained access control and incurs less computational and storage cost compared to existing schemes

Application Scenarios

We first take Vimeo which hosts high definition videos with Google Cloud as an example to explain the application of SMACD [4]. A media creator Carol can choose a private puzzle video and encode it to different qualities (e.g., 1080p,720p, and more). Then this end user can utilize our scheme to customize an access tree $T1 = ("Member" \text{ AND } "Student")$ to let as many young members as possible view the media content, while the followers satisfying the access tree $T2 = (T1 \text{ AND } Carol.Follower)$ can view higher quality content, and only the followers who have been following Carol for more than a week can view highest quality content by satisfying the access tree $T3 = (T2 \text{ AND } (Follow.Date < Oct. 1, 2019))$. Finally, this media creator can upload the encrypted video to the cloud-assisted media center equipped with secure deduplication mechanism. Hence, this video can be shared with different recipients in different qualities, while protecting the video privacy against the cloud media center and also unauthorized recipients including the Vimeo service provider.

In addition, SMACD can also be applied in privacy preserving media distribution scenario. Take Netflix which is powered with Amazon Web Services for an example [21], the professional media provider can encrypt the created video with multiple layers using our scheme, and distribute the encrypted video to Netflix consumers. Therefore, a basic member can view the media stream in standard

definition, while its ultra high definition is only available to the members with premium plan. Meanwhile, the secure de duplication design allows the media provider to later distribute the high definition version with the new mobile only monthly plan to Asian members in a storage-efficient way. In this distribution scenario, the Amazon Cloud will not reveal the media privacy.

II. SYSTEM ANALYSIS

EXISTING SYSTEM

Considering this data structure of media content, Zhu et al. [26] proposed a key generation scheme for MPEG-4, in which multiple layers of each video are encrypted by several relational keys. The keys in lower level can be generated from that in higher level based on a oneway hash chain, but it is vulnerable to collusion attack. Wu et al. [27] presented an encryption scheme for JPEG 2000 image code-streams in which the encrypted image can be decrypted in many ways, which is compatible with the characteristics of JPEG 2000 image code-streams. However, these two schemes need online key distribution and cannot support fine-grained authorization for each layer access. Selective encryption is also exploited to prevent unauthorized access to high-quality multimedia stream, by it only encrypts the base layer [28]. Since the unencrypted layers may leak private information, it is insufficient to protect the media stream confidentiality.

Yang et al. [30] proposed a time-domain access control scheme for secure video content sharing in cloud media center with CPABE, which encrypts the video content with an access policy and embeds the time into the ciphertext. Then the users can decrypt the video content by satisfying the access policy in a specific time period. Wu et al. [20] proposed the first scalable access control mechanism for SVC media content, which

employs a multi-message CP-ABE to encrypt the media layers and constructs a key graph that allows authorized users to derive all the layer keys with the key of highest access level. However, this scheme only considers onedimensional scalability. Deng et al. [31] proposed a layered access control for two-dimensional media streams which utilizes CP-ABE to enforce access control by disseminating the symmetric keys of the media layers to authorized users. This approach allows users of higher privilege to efficiently derive encryption keys for the lower privileges with the key allocation mechanism for access graph. However the access policy of each layer is individual, which causes heavy computational and communication cost as CP-ABE [18].

Ma et al. [32] proposed a scalable access control scheme for media sharing in cloud computing by distributing the access keys in a scalable way on the basis of CP-ABE. This scheme can protect the structure of two dimensional media content and reduce the key management cost by eliminating the same attributes of multiple access policies. In the extended version of [19], Ma et al. [33] then proposed an improved scalable media access control mechanism SCPABE for arbitrary dimensional scalable media streams. This scheme designed a single access tree structured by multiple access policies, hence multiple levels of access privileges can be enforced by decrypting different secrets from the tree. Compared to the traditional access tree in CP-ABE [18], this design decreases the number of non-leaf nodes, and eventually reduces the decryption cost.

Disadvantages

- 1) The system less effective since it is not implemented Multi-level access policy.

2) The system doesn't implement privacy-preserving multi-dimensional media sharing scheme named.

➤ The system is more effective due to presence of Multi-level access policy.

PROPOSED SYSTEM

We propose a scalable access control mechanism for multi-dimensional media sharing with an efficient multi-level access policy construction based on access tree and secret sharing. It integrates multiple access policies in a top-down manner and ensures that consumers who view the media layer at a higher access level must satisfy the access trees of its child layers at the lower level, which is compatible with

the characteristics of multi-dimensional media, and reduces the complexity of access policies.

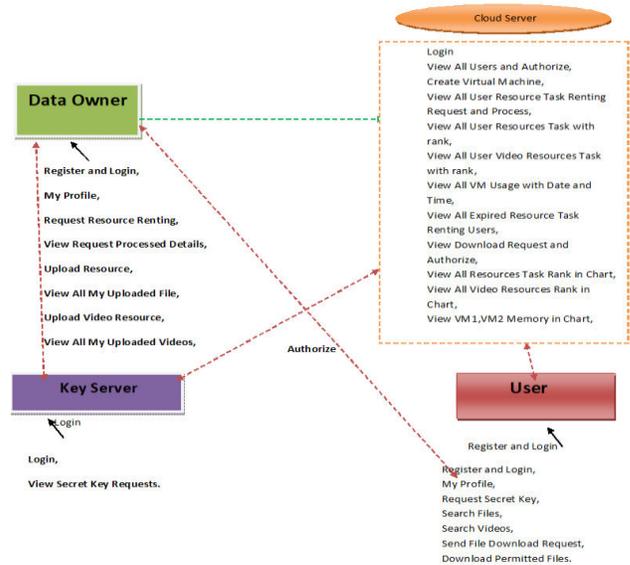
We achieve attribute-based secure deduplication by using decentralized key servers to support both intra-server and inter-server deduplication, in which the same encrypted scalable media content could be associated with different multi-level access policies on the basis of the designed storage structure.

We conduct experimental evaluation on mobile device and cloud platform with real-world datasets. The results indicate that our scheme protects media privacy against the cloud media center, key servers and unauthorized consumers with fine-grained access control and incurs less computational and storage cost compared to existing schemes.

Advantages

➤ The scalable media format encodes a media stream into a base layer which provides basic quality, and a number of enhancement layers which enhance the quality from multiple dimensions such as resolution, frame rate, and SNR.

Architecture Diagram



III. IMPLEMENTATION

• **Data owner**

In this module, the data owner should register by providing user name, password, email and group, after registering owner has to Login by using valid user name and password. The Data owner browses and uploads their data to the cloud server. For the security purpose the data provider encrypts the data file and then stores in the cloud server and manipulating the following operations such as My Profile, Request Resource Renting, View Request Processed Details, Upload Resource, View All My Uploaded File, Upload Video Resource, View All My Uploaded Videos, View All My Remaining Memory.

• **Key Server**

The Key server is responsible for generating the keys for different users and can View Secret Key Requests.

• **Cloud Server**

The cloud server is responsible for data storage and file authorization for an end user. The data file will be stored in cloud server with their tags such as View All Users and Authorize, Create Virtual Machine, View All User Resource Task Renting Request and Process, View All User Resources Task with rank, View All User Video Resources Task with rank, View All VM Usage with Date and Time, View All Expired Resource Task Renting Users, View Download Request and Authorize, View All Resources Task Rank in Chart, View All Video Resources Rank in Chart, View VM1, VM2 Memory in Chart, View Users Memory Usage in Chart, View Users No. Of Task in Chart.

- **Data Consumer(End User)**

The data consumer is nothing but the end user who will request and gets file contents response from the corresponding cloud servers and performs the following operations such as My Profile, Request Secret Key, Search Files, Search Videos, Send File Download Request, Download Permitted Files.

IV. CONCLUSION

The shared media content in mobile environment is usually encoded into several layers with the diverse quality after multi-dimensional extension. This brings greater challenges to data confidentiality and owner-enforced access control. In this paper, we propose a privacy-preserving media sharing scheme named SMACD in mobile cloud computing by utilizing CP-ABE technique. The media contributor firstly encodes the media with SVC standard and enforces access policies to each media layer. Then we provide a multi-level access policy construction with secret sharing scheme, in which each media layer is assigned a random secret that is shared by the access tree in this layer, and also the lower media layers. It

ensures that the users who view the higher media layer must satisfy the access sub-trees at a lower access level. Moreover, we achieve attribute-based intraserver and inter-server ciphertext deduplication, in which the same encrypted media layer could be associated with different access policies. The experimental evaluation shows that our scheme has less computational and communication cost, as well as storage overhead than relative schemes, which is practical for private media sharing in mobile cloud computing.

REFERENCES

- [1] Y. Meng, C. Jiang, T. Q. S. Quek, Z. Han, and Y. Ren, "Social Learning Based Inference for Crowdsensing in Mobile Social Networks," *IEEE Transactions on Mobile Computing*, vol. 17, no. 8, pp. 1966–1979, Aug. 2018.
- [2] T. Taleb, A. Ksentini, M. Chen, and R. Jantti, "Coping With Emerging Mobile Social Media Applications Through Dynamic Service Function Chaining," *IEEE Transactions on Wireless Communications*, vol. 15, no. 4, pp. 2859–2871, Apr. 2016.
- [3] M. Ambrosin, C. Busold, M. Conti, A.-R. Sadeghi, and M. Schunter, "Updicator: Updating Billions of Devices by an Efficient, Scalable and Secure Software Update Distribution over Untrusted Cache-enabled Networks," in *Computer Security – ESORICS 2014*, 2014, pp. 76–93.
- [4] "Vimeo Case Study," <https://cloud.google.com/customers/vimeo>.
- [5] J. K. Liu, M. H. Au, W. Susilo, K. Liang, R. Lu, and B. Srinivasan, "Secure sharing and searching for real-time video data in mobile cloud," *IEEE Network*, vol. 29, no. 2, pp. 46–50, Mar. 2015.
- [6] Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare Social

Networks in Cloud Computing,” IEEE Access, vol. 6, pp. 36 584–36 594, 2018.

[7] L. Y. Zhang, Y. Zheng, J. Weng, C. Wang, Z. Shan, and K. Ren, “You Can Access But You Cannot Leak: Defending against Illegal Content Redistribution in Encrypted Cloud Media Center,” IEEE Transactions on Dependable and Secure Computing, pp. 1–1, 2018.

[8] D. Lu, J. Sang, Z. Chen, M. Xu, and T. Mei, “Who Are Your Real Friends: Analyzing and Distinguishing Between Offline and Online Friendships From Social Multimedia Data,” IEEE Transactions on Multimedia, vol. 19, no. 6, pp. 1299–1313, Jun. 2017.

[9] T. Stutz and A. Uhl, “A Survey of H.264 AVC/SVC Encryption,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 22, no. 3, pp. 325–339, Mar. 2012.

[10] K. Zhang, X. Liang, X. Shen, and R. Lu, “Exploiting multimedia services in mobile social networks from security and privacy perspectives,” IEEE Communications Magazine, vol. 52, no. 3, pp. 58–65, Mar. 2014.

[11] S. Zhao, A. Aggarwal, R. Frost, and X. Bai, “A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks,” IEEE Communications Surveys Tutorials, vol. 14, no. 2, pp. 380–400, 2012.

[12] F. Beato, S. Meul, and B. Preneel, “Practical identity-based private sharing for online social networks,” Computer Communications, vol. 73, pp. 243–250, Jan. 2016.

[13] E. Luo, Q. Liu, and G. Wang, “Hierarchical Multi-Authority and Attribute-Based Encryption Friend Discovery Scheme in Mobile Social Networks,” IEEE Communications Letters, vol. 20, no. 9, pp. 1772–1775, Sep. 2016.

[14] A. Sahai and B. Waters, “Fuzzy Identity-Based Encryption,” in Advances in Cryptology EUROCRYPT 2005, 2005, pp. 457–473.

[15] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based Encryption for Fine-grained Access Control of Encrypted Data,” in

Proceedings of the 13th ACM Conference on Computer and Communications Security, 2006, pp. 89–98.