RESEARCH ARTICLE OPEN ACCESS

Privacy Preserving Media Sharing with Scalable Access Control and Secure Deduplication in Mobile Cloud Computing

Mrs J Sarada MCA,M.Tech,M.Phil,(Ph.D) [1], T.Gurupavan [2]

[1] Associate Professor, Department of Computer Application

[2] Student, Department of Computer Application

[1], [2] Chadalawada Ramanamma Engineering College (Autonomous)

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 project, 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 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, introduce decentralized key servers to achieve both intra-server and inter-server deduplication by associating different access policies into the same encrypted media. Finally, 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.

Keywords: - Benefiting from cloud computing and mobile devices, a huge number of media contents such as videos are shared in mobile networks

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 withdifferent 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.

II. LITERATURE SURVEY

Social Learning Based Inference for Crowdsensing in Mobile Social Networks

Mobile communication technology provides more service paradigms to social networks, allowing the development of mobile social networks (MSNs). An important scenario of MSNs is crowdsensing, which takes advantage of simple sensing and computation abilities on the portable devices of ordinary people, and fuses the sensing results to accomplish large-scale tasks. In crowdsensing, the integration of individual sensing data from users is of great significance, yet highly depends on the goal of tasks. In this paper, we propose a high-level distributed cooperative environmental state inference scheme based on non-Bayesian social learning, which can be applied to various crowdsensing tasks, e.g., traffic monitoring, air quality monitoring, and weather forecasting. In the proposed scheme, users exchange information with their neighbors and cooperatively infer the hidden state, which is the goal of the crowdsensing task but cannot be measured directly.

Coping With Emerging Mobile Social Media Applications Through Dynamic Service Function Chaining

User generated content (UGC)-based applications are gaining lots of popularity among the community of mobile internet users. They are populating video platforms and are shared through different online social services, giving rise to the so-called mobile social media applications. These applications are characterized by communication sessions that frequently and dynamically update content, shared with a potential number of mobile users, sharing the same location or being dispersed over a wide geographical area. Since most of UGC content of mobile social media applications are exchanged through mobile devices, it is expected that along with online social applications, these content will cause severe congestion to mobile networks, impacting both their core and radio access networks.

III. EXISTINGSYSTEM

Considering this data structure of media content, Zhu et al. [21] 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.

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.

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

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,SearchFiles,SearchVideos,Send File Download Request,Download Permitted Files.

V. RESULTS

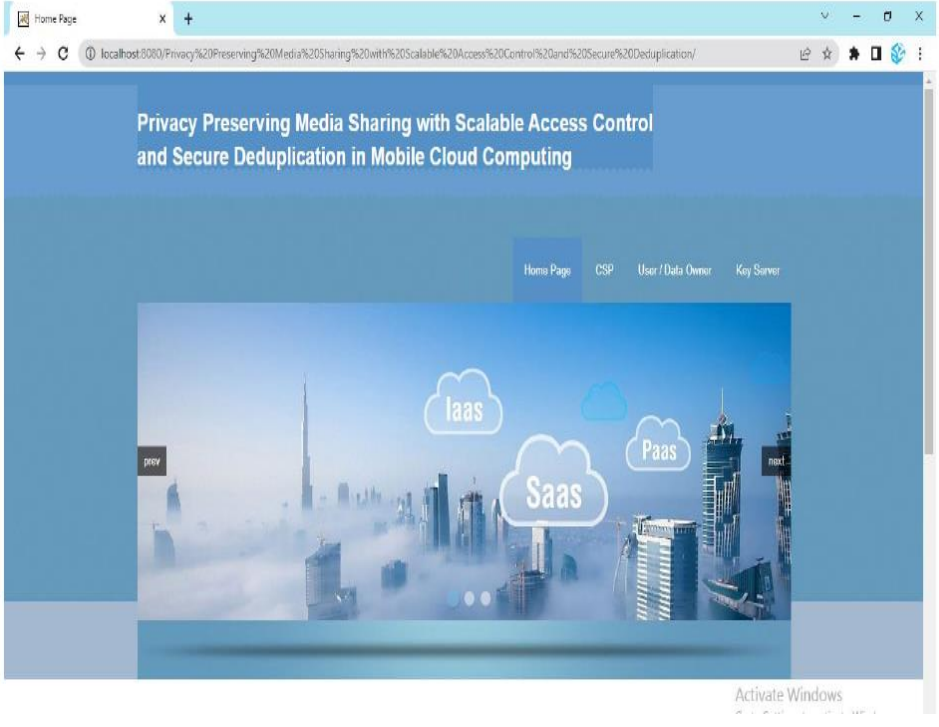

Fig1: Home Page

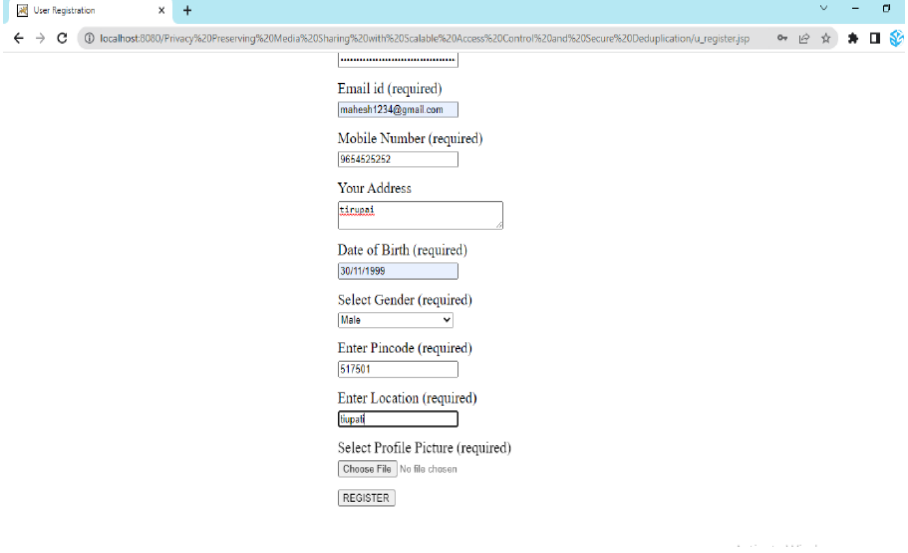

Fig2: Registration Page

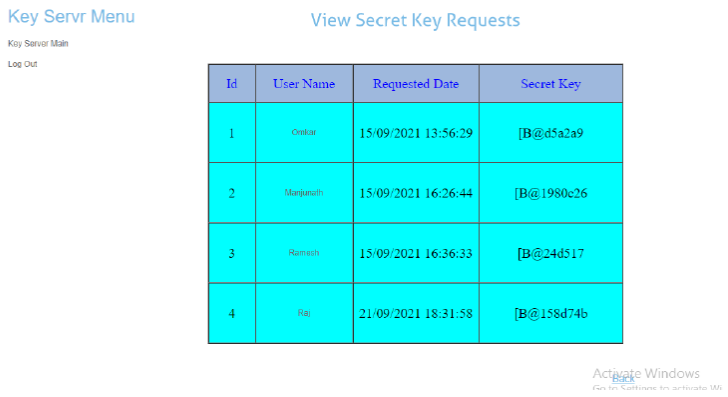

Fig3: Secret Key Request Page

Fig 4: Download Response

VI. 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 ciphertextdeduplication, 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 LearningBased 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, "CopingWith EmergingMobile Social Media Applications Through Dynamic ServiceFunction 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, andM. Schunter, "Updaticator: Updating Billions of Devices by anEfficient, Scalable and Secure Software Update Distribution overUntrusted Cache-enabled Networks," in Computer Security – ESORICS2014, 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 mobilecloud," IEEE Network, vol. 29, no. 2, pp. 46–50, Mar. 2015.
[6] Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure Identity-BasedData Sharing and Profile Matching for Mobile Healthcare SocialNetworks 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 IllegalContent Redistribution in Encrypted Cloud Media Center," IEEETransactions on Dependable and Secure Computing, pp. 1–1, 2018.
[8] D. Lu, J. Sang, Z. Chen, M. Xu, and T. Mei, "Who Are Your RealFriends: Analyzing and Distinguishing Between Offline and OnlineFriendships From Social Multimedia Data," IEEE Transactionson 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 multimediaservices in mobile social networks from security and privacyerspectives," 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 Applicationsof 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 privatesharing for online social networks," Computer Communications,vol. 73, pp. 243–250, Jan. 2016.
[13] E. Luo, Q. Liu, and G. Wang, "Hierarchical Multi-Authority andAttribute-Based Encryption Friend Discovery Scheme in MobileSocial Networks," IEEE Communications Letters, vol. 20, no. 9, pp.1772–1775, Sep. 2016.
[14] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," inAdvances in Cryptology EUROCRYPT 2005, 2005, pp. 457–473.
[15] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-basedEncryption for Fine-grained Access Control of Encrypted Data,"in Proceedings of the 13th ACM Conference on Computer and CommunicationsSecurity, 2006, pp. 89–98.
[16] B. Ciubotaru, C. H. Muntean, and G. Muntean, "Mobile Multi-Source High Quality Multimedia Delivery Scheme," IEEE Transactionson Broadcasting, vol. 63, no. 2, pp. 391–403, Jun. 2017.
[17] C. Hsu and M. Hefeeda, "Flexible Broadcasting of Scalable VideoStreams to Heterogeneous Mobile Devices," IEEE Transactions onMobile Computing, vol. 10, no. 3, pp. 406–418, Mar. 2011.
[18] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-PolicyAttribute-Based Encryption," in 2007 IEEE Symposium on Securityand Privacy (SP '07), 2007, pp. 321–334.
[19] C. Ma, Z. Yan, and C. W. Chen, "Attribute-based multi-dimensionscalable access control for social media sharing," in 2016 IEEEInternational Conference on Multimedia and Expo (ICME), 2016, pp.1–6.
[20] Y. Wu, Z. Wei, and R. H. Deng, "Attribute-Based Access to ScalableMedia in Cloud-Assisted Content Sharing Networks," IEEETransactions on Multimedia, vol. 15, no. 4, pp. 778–788, Jun. 2013.
[21] "Netflix on AWS," https://aws.amazon.com/solutions/case-studies/netflix.
[22] R. LI, C. Shen, H. He, X. Gu, Z. Xu, and C. Xu, "A LightweightSecure Data Sharing Scheme for Mobile Cloud Computing," IEEETransactions on Cloud Computing, vol. 6, no. 2, pp. 344–357, Apr.2018.
[23] K. Liu, M. Li, and X. Li, "Hiding Media Data via Shaders: EnablingPrivate Sharing in the Clouds," in 2015 IEEE 8th InternationalConference on Cloud Computing, 2015, pp. 122–129.
[24] J. M. Boyce, Y. Ye, J. Chen, and A. K. Ramasubramonian,"Overview of SHVC: Scalable Extensions of the High EfficiencyVideo Coding

Standard," IEEE Transactions on Circuits and Systemsfor Video Technology, vol. 26, no. 1, pp. 20–34, Jan. 2016.
[25] Z. Su, Q. Xu, F. Hou, Q. Yang, and Q. Qi, "Edge Caching for LayeredVideo Contents in Mobile Social Networks," IEEE Transactionson Multimedia, vol. 19, no. 10, pp. 2210–2221, Oct. 2017.