Fuzzy Systems and Soft Computing
ISSN : 1819-4362

SECURE MEDIA SHARING IN MOBILE CLOUD COMPUTING: SCALABLE ACCESS CONTROL AND PRIVACY PRESERVATION

[#1]SOTKU ABHISHEK, [#2]ODELA JYOTHIKA,
[#3]CH. SAMPATH REDDY, *Associate Professor,*
Department of Computer Science and Engineering,
Sree Chaitanya Institute Of Technological Sciences, Karimnagar.

ABSTRACT: Mobile networks are full of media content, like videos, being shared. This is possible with cloud computing and mobile devices. It's possible that scalable video coding in the cloud will give you more freedom, but it also poses a big threat to media privacy. This article talks about SMACD, a way to share media in multiple dimensions while keeping your privacy safe in mobile cloud computing. An attribute-based encryption-based access policy is used to encrypt each layer of the system at the start to protect media privacy and fine-grained access control. Then you will show how a multi-level access policy's secret sharing scheme works. It makes access policies easier to enforce and supports multidimensional media properties by making mobile users who get a media layer at a higher level also meet the access trees of its child layers at a lower level. Decentralized key servers can also do deduplication within and between servers by setting up different access policies that are linked to the same encrypted media. Finally, real-world datasets should be used for experimental testing on a mobile device and a cloud platform. The results show that SMACD lowers the cost of computing and storage while protecting media from cloud media centers and other unauthorized parties.

Keywords: - Benefiting from cloud computing and mobile devices, a huge number of media contents such as videosareshared in mobilenetworks

1.INTRODUCTION

With the quick development of mobile computingtechniqueandtheprevalenceofinterpersonalsociality, A combination of people's natural inclination to connect with one another and the proliferation of powerful mobile computing capabilities has resulted in ubiquitous mobile networks serving as primary means of communication and relationship development. Whenever and wherever their service providers release new information, mobile device users will be the first to know. Connected users can also access and share their data. Media data, such as videos, is more likely to be shared and viewed on sites like YouTube and Netflix than text data, due to the abundance of cloud computing and mobile computing services. The majority of smartphones now have easier access to high-definition video services thanks to a variety of cloud services, including Microsoft Azure and Google Cloud Platform. Through the open-source platform Vimeo, Google Cloud hosts and transmits high-definition videos. Video creators can use Vimeo to publish their work and choose who can view it.The media distributor may still have doubts about the media center, even though it allows them to restrict access to their media to specific friends or subscribers (particularly with cloud media centers). To be more precise, the media distributor will lose all direct control over the media content once it is uploaded to the cloud media center. Unauthorized users may be able to access media content stored in cloud media centers. The confidentiality of media producers and distributors is greatly jeopardized by this. Cryptographic algorithms are necessary to safeguard media privacy and ensure that authorized individuals can access shared media content via mobile cloud computing, which is a major concern for current media services due to privacy concerns.

Currently, identity-based encryption (IBE) and broadcast encryption are employed to safeguard media privacy. Due to the ubiquitous nature of online media, traditional methods of access control based on user identities may fail in highly disseminated instances. In fact, media distribution platforms

frequently use subscriptions or social media to determine user access. To address this issue, attribute-based encryption (ABE) can be implemented to safeguard media privacy while also enabling granular and one-to-many access control. As a means of controlling access, media distributors can employ cipher text-policy ABE (CP-ABE). Using string combinations such as "Member" AND "Student," they can establish access rules that are applicable to all of the attributes. Only users who fulfill specific criteria will be able to access this content. Whether or not the media distributor chooses to restrict access to the material is contingent upon the user's freedom of expression.

The storage requirements for storing various versions of media content across various networks and devices are substantial. Multiple high-definition improvement layers and a low-quality base layer are created from a single media file using scalable video coding (SVC). The structure can then be used to change the conditions of a heterogeneous network environment. Managing various mobile networks and devices is made easier with the SVC's built-in flexible decoding mechanism. More specifically, only a subset of the population that purchases their media from a media distributor has access to high-definition, multi-dimensional media. Reasons for this include factors such as SNR, frame rate, and resolution. Still, this makes it more difficult to safeguard users' privacy while sharing media.

2.LITERATURESURVEY

SocialLearningBasedInferenceforCrowdsensinginMobileSocial Networks

3.EXISTINGSYSTEM

Zhu et al. developed a key generation scheme for MPEG-4 that encrypts each video layer using a combination of relational keys. This data structure for media content serves as its foundation. While it is possible to generate lower-level keys from higher-level ones using a one-way hash chain, this method is vulnerable to collusion attacks. Mobile social networks (MSNs) expanded due to new service paradigms made possible by mobile communication technology, according to Wu et al. Using the low-cost sensing and computing power of portable devices that the majority of people own, crowdsensing is an important use of MSNs that combines sensing results to finish large-scale tasks. The goal of the task determines how many users' sensing data points are combined in crowdsensing. This article presents the first discussion of a distributed cooperative environmental state inference scheme at a high level. Many crowdsensing domains, such as weather prediction, air quality management, and traffic finding, can benefit from this strategy, which is based on non-Bayesian concepts of social learning. Users would pool their data with neighboring nodes in an effort to deduce the hidden state—which cannot be directly measured—according to the proposed plan.

Coping With Emerging Mobile Social MediaApplications Through Dynamic Service FunctionChaining

Mobile internet users are flocking to user-generated content (UGC) applications in droves. A profusion of these apps can be found on various online social media sites because a large number of users utilize them on video platforms. These apps allow a large number of people to communicate and share media in real time, regardless of their physical location (which could be anywhere from a single room to an entire country). Users are putting a lot of pressure on mobile networks by posting user-generated content (UGC) on social media apps for mobile devices. Core and radio access networks are both encompassed in this.A code-stream encryption method for JPEG 2000 images that is compatible with all of their features and allows for multiple decryptions. However, due to the requirement for online key transmission, layer-by-layer authorization cannot be accomplished using these two schemes. With precision, As an additional use of encryption, encrypting just the base layer can prevent unauthorized access to high-quality multimedia streams. Security measures aren't robust enough to prevent personal information from leaking out through the media stream since the layers aren't encrypted.

4.PROPOSEDSYSTEM

We propose a method for controlling who can view what and when when sharing multidimensional media, based on access trees, and for sharing secrets. Setting up multi-level access policies is a breeze with this mechanism. While preserving the characteristics of multidimensional media, this approach streamlines access policies. It achieves this by integrating various top-down policies and directing the access trees of lower-level child layers to higher-level media layer viewers.

The use of decentralized key servers for attribute-based secure deduplication facilitates deduplication on-and-off-server. The storage configuration determines how many multi-level access policies can be associated with the same encrypted scalable media.

Our experiments make use of real-world datasets sourced from cloud platforms and mobile devices. According to the findings, our proposed solution safeguards media privacy in the cloud media center, from critical server compromise to unauthorized access. It improves the efficiency of both storage and computation. To achieve this, we also implemented granular access control.

Advantages

- The scalable media format specifies the division of a media stream into multiple enhancement layers. A number of quality metrics, including frame rate, resolution, and signal-to-noise ratio (SNR), are enhanced by these layers. Additionally, this layer has a foundational layer that supplies fundamental quality.
- The multi-level access policy improves the system's performance.

5.IMPLEMENTATION

Data owner

Data owners can't use this module unless they create an account with an email, password, and group. Once owners have finished registering, they are required to log in with their actual credentials. When information is saved to a cloud server, its owner can access it from any location with an internet connection. The data provider encrypts the file before storing it in the cloud. It allows users to see their profiles, rent resources, track the progress of their requests, upload resources, view all of their uploaded files and videos, and view their remaining memory.

Key Server

The Key server is responsible for both generating keys for various users and processing requests for secret keys.

Cloud Server

Data storage and user file access are the responsibilities of the cloud server. For instance, the cloud will store the data file along with its associated tags. The ability to see any user's permissions can be granted.Install a virtual computer system. View the Comprehensive Procedure for Granting Access to User Resources to Hiring Users.Take a look at each user's resources, like their video resources, to see where they stand. You can view the usage of each virtual machine broken down by time and date.Verify that all users have completed their resource tasks. Your responsibilities include monitoring and approving download requests.Take a look at the pie chart to discover the ranking of each resource task.View the top video sites on the web by checking out our list.Virtual Machine 1, Virtual Machine 2, and the users' memory consumption are displayed in the chart, along with the number of tasks assigned to each user.

Data Consumer(EndUser)

Download Files, SearchFiles, Request Secret Key, My Profile, Send File Download Request, and Download Permitted Files allow users to access and retrieve file contents from the appropriate cloud servers.

6.RESULTS

Fig1:HomePage

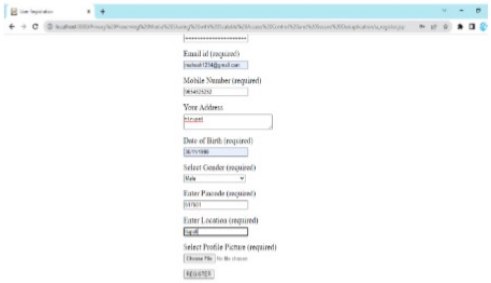

Fig2:RegistrationPage

Fig3:SecretKeyRequestPage

Fig4: DownloadResponse

7.CONCLUSION

It is customary to apply multiple layers of quality to media prior to transferring it to a mobile device. As a result, adhering to the proprietor's access regulations and safeguarding confidential information become more arduous. This paper will examine SMACD, a media-sharing solution for mobile cloud computing that protects privacy by utilizing the CP-ABE technique. Once the media provider has encrypted the content in accordance with SVC standards, access controls are implemented across the entire media. Following that, we will discuss a method for sharing secrets that enables the creation of policies with varying degrees of access. A random access tree secret is produced and subsequently distributed to the layers that lie beneath each media layer. Customers have nothing to worry about in this regard.

The access subtrees of the lower access level must be fulfilled by the media layer above in this case. A single encrypted media layer can be associated with multiple access policies, and attribute-based intra-server and inter-server ciphertext deduplication is also achieved. The outcomes indicate that our approach optimizes utilization of storage capacity, communication bandwidth, and processing capability in comparison to alternative methodologies. As a result, it is highly compatible with mobile cloud computing and private media sharing.

REFERENCES

1. Y. Meng, C. Jiang, T. Q. S. Quek, Z. Han, andY.Ren,"SocialLearningBasedInference forCrowdsensinginMobileSocialNetworks, "IEEETransactionsonMobileComputing,v ol.17,no.8,pp.1966–1979, Aug.2018.
2. T. Taleb, A. Ksentini, M. Chen, and R. Jantti,"CopingWithEmergingMobileSocial MediaApplicationsThroughDynamicServi ceFunctionChaining,"IEEETransactionson WirelessCommunications,vol. 15, no. 4, pp. 2859–2871, Apr.2016.
3. M.Ambrosin,C.Busold,M.Conti,A.-R.Sadeghi, andM. Schunter, "Updaticator: UpdatingBillionsofDevicesbyanEfficient,S

calableandSecure Software Update Distribution overUntrustedCache-enabled Networks," inComputer Security – ESORICS2014, 2014,pp. 76–93.
4. "VimeoCaseStudy,"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 forreal-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, "SecureIdentity-BasedData Sharing and Profile Matching forMobileHealthcareSocialNetworksinCloudComputing,"IEEEAccess,vol.6,pp.36584–36594, 2018.
7. L. Y. Zhang, Y. Zheng, J. Weng, C. Wang, Z.Shan, and K. Ren,"You Can Access But You CannotLeak:DefendingagainstIllegalContentRedistributioninEncryptedCloudMediaCenter,"IEEETransactionsonDependableandSecureComputing,pp. 1–1,2018.
8. D. Lu, J. Sang, Z. Chen, M. Xu, and T. Mei,"WhoAreYourRealFriends:AnalyzingandDistinguishing BetweenOfflineandOnlineFriendshipsFromSocialMultimediaData,"IEEE Transactionson Multimedia, vol. 19, no. 6, pp.1299–1313,Jun. 2017.
9. T.StutzandA.Uhl,"ASurveyofH.264AVC/SVCEncryption,"IEEETransactionsonCircuits and Systems for Video Technology,vol. 22,no.3, pp.325–339, Mar. 2012.
10. K.Zhang,X.Liang,X.Shen,andR.Lu,"Exploitingmultimediaservicesinmobilesocialnetworksfromsecurityandprivacyerspectives," IEEECommunicationsMagazine,vol.52,no. 3,pp.58–65,Mar. 2014.
11. S. Zhao, A. Aggarwal, R. Frost, and X. Bai, "ASurveyofApplicationsofIdentity-BasedCryptographyinMobileAd-HocNetworks,"IEEECommunications Surveys Tutorials, vol. 14, no. 2,pp.380–400,2012.
12. F. Beato, S. Meul, and B. Preneel, "Practicalidentity-basedprivatesharingforonlinesocialnetworks,"ComputerCommunications,vol.73,pp.243–250,Jan. 2016
13. E.Luo,Q.Liu,andG.Wang,"HierarchicalMulti-AuthorityandAttribute-BasedEncryptionFriendDiscoverySchemeinMobileSocialNetworks," IEEE Communications Letters, vol. 20,no.9, pp.1772–1775, Sep. 2016.
14. A. Sahai and B. Waters, "Fuzzy Identity-BasedEncryption,"inAdvancesinCryptologyEUROCRYPT2005, 2005,pp. 457–473.
15. V. Goyal, O. Pandey, A. Sahai, and B. Waters,"Attribute-basedEncryption for Fine-grained AccessControlofEncryptedData,"inProceedingsofthe13thACMConferenceonComputerandCommunicationsSecurity,2006, pp.89–98.