International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 11 (2014), pp. 1043-1050

http://www. irphouse.com

Self Annihilating Data Storage and Location Based non-terminating Video Streaming Services for Mobile Users in CLOUD Environment

Mohan Sadasivam[1], S.Gayathri[2]

[1]M.Tech Information and Communication Technology, [2]Assistant Professor
J.J College of Engineering and Technology - Trichy
Anna University – Chennai, INDIA
[1]mohansivam.network@gmail.com, [2]gayathrisivaa@yahoo.com,

Abstract

Cloud Computing has become a popular buzzword and it has been widely used to refer to different technologies, services, and concepts. With the use of cloud computing, here we are trying to give the location based efficient video information to the mobile users. Location Based Service(LBS) is an information service and has a number of uses in social networking today as an entertainment service, which is accessible with mobile devices through the mobile network and which uses information on the geographical position of the mobile device. While the demands of video streaming services over the mobile networks have been souring over these years, the wireless link capacity cannot practically keep up with the growing traffic load. In this project, we propose and discuss a Adaptive video streaming framework to improve the quality of video services in the location based manner. Through this system, video content can be segmented by an automatic shot/scene retrieval technology and stored in the database (DB). In the client side, two threads will be formed. One is for Video streaming and another one is for Location searching and updating. For the security purpose, we are using self destruction algorithm where the uploaded video is been destructed automatically after the user defined time. Thus the location based Video information can be streamed efficiently and securely by the mobile users.

Keywords— Cloud Computing, Video Streaming, Self Annihilation Data, Mobile Computing, SVC, Data Privacy, Location Based Service(LBS).

1. Introduction

Cloud computing, or the cloud, is a colloquial expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. Cloud computing is a term without a commonly accepted unequivocal scientific or technical definition. In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time.

While the demands of video streaming services over the mobile networks have been souring over these years, the wireless link capacity cannot practically keep up with the growing traffic load. The gap between the traffic demand and the link capacity, along with time-varying link conditions, results in poor service quality of video streaming services over the mobile networks, such as intermittent disruptions and long buffering delays. Leveraging the current cloud computing technology, we propose and discuss a framework to improve the quality of video services for mobile users, ie Segmented video streaming. Through this system, video content can be segmented by an automatic shot/scene retrieval technology and buffered independently.

Location-based services (LBS) are a general class of computer program-level services used to include specific controls for location and time data as control features in computer programs. As such LBS is an information service and has a number of uses in social networking today as an entertainment service, which is accessible with mobile devices through the mobile network and which uses information on the geographical position of the mobile device. This has become more and more important with the expansion of the smart phone and tablet markets as well.

2. Related Work

2.1. Adaptive Video Streaming

In the adaptive streaming, the video traffic rate is adjusted on the fly so that a user can experience the maximum possible video quality based on his or her link's time-varying bandwidth capacity [1]. There are mainly two types of adaptive streaming techniques, depending on whether the adaptivity is controlled by the client or the server. The Microsoft's Smooth Streaming [2] is a live adaptive streaming service which can switch among different bit rate segments encoded with configurable bitrates and video resolutions at servers, while clients dynamically request videos based on local monitoring of link quality. Adobe and Apple also developed client-side HTTP adaptive live streaming solutions operating in the similar manner. There are also some similar adaptive streaming services where servers control the adaptive transmission of video segments, for example, the Quality Adaptive Streaming. However, most of these solutions maintain multiple copies of the video content with different bit rates, which brings huge burden of storage on the server. Regarding rate adaptation controlling techniques, TCP-friendly rate control methods for streaming services over mobile networks are proposed [3], [4], where TCP throughput of a flow is predicted as a function of packet loss rate, round trip time, and packet size. Considering the estimated throughput, the bit rate of the streaming traffic can be

adjusted. A rate adaptation algorithm for conversational 3G video streaming is introduced by [5]. Then, a few cross-layer adaptation techniques are discussed [6], which can acquire more accurate information of link quality.
Recently the H.264 Scalable Video Coding (SVC) technique has gained a momentum [10]. An adaptive video streaming system based on studies the real-time SVC decoding and encoding at PC servers. The work in [11] proposes a quality-oriented scalable video delivery using SVC, but it is only tested in a simulated LTE Network.

2.2. Data Self-Destruction

The self-destructing data system in the Cloud environment should meet the following requirements: i) How to destruct all copies of the data simultaneously and make them unreadable in case the data is out of control? A local data destruction approach will not work in the Cloud storage because the number of backups or archives of the data that is stored in the Cloud is unknown, and some nodes preserving the backup data have been offline. The clear data should become permanently unreadable because of the loss of encryption key, even if an attacker can retroactively obtain a pristine copy of that data; ii) No explicit delete actions by the user, or any third-party storing that data; iii) No need to modify any of the stored or archived copies of that data; iv) No use of secure hardware but support to completely erase data in HDD and SSD, respectively.

Tang et al. [7] proposed FADE which is built upon standard cryptographic techniques and assuredly deletes files to make them unrecoverable to anyone upon revocations of file access policies. Wang et al. [8] utilized the public key based homomorphism authenticator with random mask technique to achieve a privacy-preserving public auditing system for Cloud data storage security and uses the technique of a bilinear aggregate signature to support handling of multiple auditing tasks. Perlman et al. [9] present three types of assured delete: expiration time known at file creation, on-demand deletion of individual files, and custom keys for classes of data. Vanish is a system for creating messages that automatically self-destruct after a period of time. It integrates crypto-graphic techniques with global-scale, P2P, distributed hash tables (DHTs): DHTs discard data older than a certain age. The key is permanently lost, and the encrypted data is permanently unreadable after data expiration. Vanish works by encrypting each message with a random key and storing shares of the key in a large, public DHT.

3. Design and Implementation

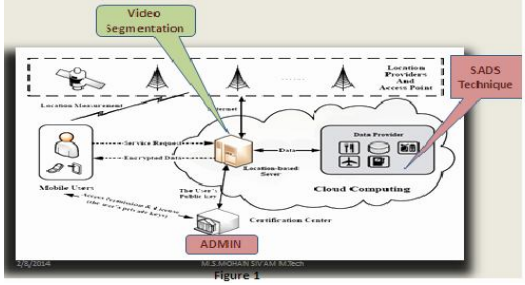


Figure 1

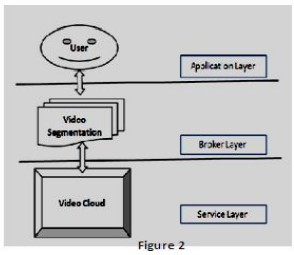


Figure 2

3.1 Enabling Location Based Service

Each location has several Cloud Units(CU) which acts as mobile support station to support services for mobile users in this location. Cloud units in every location are connected to Cloud Service Provider (CSP). For example, when a user arrives at a new city, he may want to know the typical or popular food or restaurant in this city. Then it is very hard for him to search. Each cloud stores restaurant related information like address, contact number, food style information etc. The cloud enabled mobile application is shown. **Role of LSP and User:** When a user enters into the coverage area of LSP, user needs to register with LSP to access the available services. LSP performs authentication by assigning user with unique ID i.e., Phone Number. User is able to access required service by providing unique ID.

3.2 Enabling LBS Using GPS

All cell phones constantly broadcast a radio signal, even when not on a call. The cell phone companies have been able to estimate the location of a cell phone for many years using triangulation information from the towers receiving the signal. However, the introduction of GPS technology into cell phones has meant that cell phone GPS tracking now makes this information a lot more accurate. With GPS technology now more commonplace in many new smartphones, this means that the location of anyone carrying a GPS enabled smartphone can be accurately tracked at any time.

Cell phone GPS tracking can therefore be a useful feature for business owners, parents, friends and co-workers looking to connect with one another. Since a cell phone already works like a two-way radio when communicating with cell towers, the GPS capability simply extends the radio signal reach to space satellites. A-GPS technology is the advanced technology which suited for mobile devices more accurately. A-GPS takes assistance from GPRS and at times, the service provider network information, to pin-point the current location accurately. Moreover the amount of CPU and programming required for a GPS phone is reduced by diverting most of the work to the assistance server instead. A typical A-GPS enabled Cell phone uses a GPRS or other such Internet based data connection to build a contact with the assistance server for A-GPS. This exercise usually is a bit slow if we are connecting with the server for the first time. As this technique does not take into account the cell phone service provider network completely, we only pay the GPRS usage charges and nothing else. The only down-side to this technology is that an A-GPS server cannot utilize any of the three standby satellites available for GPS connections.

3.3. Self Annihilating Data Storage System

An active storage object derives from a user object and has a time-to-live (*ttl*) value property. The *ttl* value is used to trigger the self-destruct operation. The *ttl* value of a user object is infinite so that a user object will not be deleted until a user deletes it manually. The *ttl* value of an active storage object is limited so an active object will be deleted when the value of the associated policy object is true. Interfaces extended by Active Storage Object class are used to manage *ttl* value. The create member function needs another argument for *ttl*. If the argument is 1, User *Object:: create* will

be called to create a user object, else, Active Storage *Object::create* will call User Object::create first and associate it with the self-destruct method object and a self-destruct policy object with the *ttl* value. The *getTTL* member function is based on the *read_attr* function and returns the ttl value of the active storage object. The *setTTL*, *addTime* and *decTime* member function is based on the *write_attr* function and can be used to modify the *ttl* value. To use the SADS system, user's applications should implement logic of data process and act as a client node. There are two different logics: uploading and downloading.

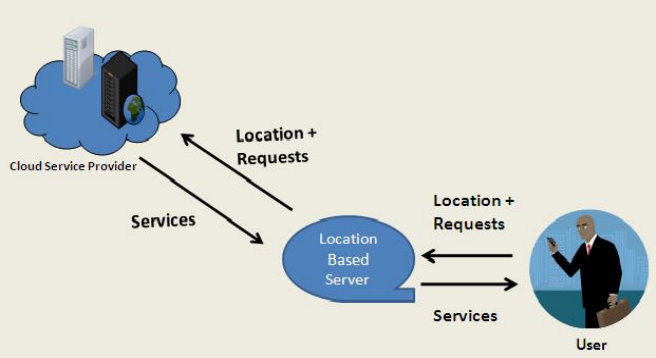
We are using two kinds of algorithm for done this project in secure way. First algorithm called Random Key generation, the main class for done this algorithm called Random class. This algorithm mainly used for generate the secret key for file uploading and downloading. Second algorithm is AES (Advanced Encryption Slandered), which is used for encrypt the file content. Our contributions are we focus on the related key distribution algorithm, Shamir's algorithm, which is used as the core algorithm to implement client (users) distributing keys in the object storage system. We use these methods to implement a safety destruct with equal divided key. Based on active storage framework, we use an object-based storage interface to store and manage the equally divided key. We are implementing a proof-of-concept SADS prototype. Through functionality and security properties evaluation of the SADS prototype, the results demonstrate that SADS is practical to use and meets all the privacy-preserving goals. The prototype system imposes reasonably low runtime overhead. SADS supports security erasing files and random encryption keys stored in a hard disk drive (HDD) or solid state drive (SSD), respectively.

3.4 Video Streaming

While streaming a video over the mobile, the video is being segmented by the broker layer. Video content can be segmented by an automatic shot/scene retrieval technology and stored. Service Layer will be in the cloud and the broker layer will be in between application layer and the service layer. As soon as the Video is been demanded, video is transferred into the broker layer(Figure 2) and the video is segmented as per the designed algorithm. Each segmented video clip is streamed separately, so that the buffering delay has been reduced.

4. Summary

In this paper, the data(Video) can be stored in the cloud by the Video Service Provider(VSP). That video will be getting deleted after the predefined time by the VSP. SAD architecture is used to do the self annihilation job. The video is being serviced in the location based manner. According to the location, related video is streamed. To avoid the buffering delay and to give non terminating video service, video is being segmented in the location based server. Thus the location based video streaming is established with the use of active storage system in the cloud.



5. Conclusion

Providing dynamic location-based service and increase the information retrieve accuracy especially in the limited mobile screen have become the important research areas in the development of location-based services. In this paper, we have proposed an Android based application to retrieve video information in mobile device accessing CSP based on the locations. While streaming the video the total video is segmented according to the bandwidth allocated and size of the video. So that the buffering delay can be reduced as the user moves one place to another. To give a service through the cloud computing technology, security is challenging one until now. To enable the secure service we proposed SADS system where the data is been deleted automatically from the cloud storage after the user specified time. Our plan to release the current SADS system will help to provide researchers with further valuable experience to inform future object-based storage system designs for Cloud services

References

[1] Y. Li, Y. Zhang, and R. Yuan, "Measurement and analysis of a large scale commercial mobile Internet TV system," in Proc. ACM Internet Meas. conf., 2011, pp. 209-224

[2] A. Zambelli, "IIS smooth streaming technical overview," Microsoft Corp., 2009.

[3] Y. Fu, R. Hu, G. Tian, and Z. Wang, "TCP-friendly rate control for streaming service over 3G network," in Proc. WiCOM, 2006, pp. 1-4.

[4] K. Tappayuthpijarn, G. Liebl, T. Stockhammer, and E. Steinbach, "Adaptive video streaming over a mobile network with TCP-friendly rate control," in Proc. IWCMC, 2009, pp. 1325-1329.

[5] V. Singh and I. D. D. Curcio, "Rate adaptation for conversational 3G video," in Proc. IEEE INFOCOM Workshop, 2009, pp. 205-211.

[6] S. Akhshabi, A. C. Begen, and C. Dovrolis, "An experimental evaluation of rate-adaptation algorithms in adaptive streaming over HTTP," in Proc. ACM MMSys, 2011, pp. 157-168.

[7] Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, "FADE: Secure overlay cloud storage with file assured deletion," in Proc Secure Comm, 2010.

[8] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for storage security in cloud computing," in Proc. IEEE IN-FOCOM, 2010.

[9] R. Perlman, "File system design with assured delete," in Proc. Third IEEE Int. Security Storage Workshop (SISW), 2005.

[10] H. Schwarz, D. Marpe, and T. Wiegand, "Overview of the scalable video coding extension of the H.264/AVC standard," IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 9, pp. 1103-1120, Sep. 2007.

[11] P. McDonagh, C. Vallati, A. Pande, and P. Mohapatra, "Quality-oriented scalable video delivery using H. 264 SVC on an LTE network," in Proc. WPMC, 2011.