Providing Security to Mobile Video Streaming and Video Sharing in the Cloud

Dattatray Reddy
Department of Computer Engineering
Dr. D. Y. Patil SOET, Lohegaon,
Savitribai Phule Pune University
Pune, Maharashtra, India

Madhuri Patil
Assistant Professor Department of Computer Engineering
Dr. D. Y. Patil SOET, Lohegaon,
Savitribai Phule Pune University
Pune, Maharashtra, India

ABSTRACT

Demand on video traffic over mobile network is increasing in year on year basis, wireless link capacity cannot satisfying the traffic requirement. The difference in the traffic demand and the link capacity with varying link conditions results in poor quality of videos such as intermittent disruptions and long buffering time over mobile networks. Due to such environments, we propose a new mobile video streaming and sharing system, which efficiently stores videos on the cloud (VC) and construct agent (subVC) for each mobile user at client side to offer “non-terminating” video streaming. And also proposed system will monitor the social network communication among mobile users and their private agent prefetch videos in advance according to social activities. The security of videos and private data of user is provided by using AES algorithm and secure key exchange by using Diffie Hellman Key Exchange algorithm.

General Terms

Cloud Computing Security

Keywords

Social activities, Prefetching, Video streaming, Encryption, Decryption, cloud Computing.

1. INTRODUCTION

Over the last decade video traffic has increased on the internet. There are number of different factors that lead to increase in video traffic over internet. Such as different formats of video data like MPEG, AVI, 3GPP, FLV etc. These different formats differ in Video size and quality of videos. The video quality demand leads to increase in size of videos in bulks. Such a bulk data leads to interruption and long buffering time. Generally, it will badly affect in mobile users that has signal strength problem. For such users, there is need of faster and interrupt less access of videos.

Cloud computing can solve this problem, cloud computing is leading and latest technology which is increasing in use in the market, which provides number of services to users on demand. These are software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS) with greater scalability and availability. Infrastructure as a service provides storage space for data on the cloud. Data storage on the cloud has number of benefits like faster data store and access anywhere in the world on demand. By using this principal, we are going to store videos on the cloud so that can be accessed faster.

Cloud computing can also be used for video sharing purpose. Currently, everyone is on the social media sites and wants to share the video in community, in friends, in public and in subscribed users. The videos that has stored on the cloud are easy to share and can be accessible anywhere in the world. Sharing on the cloud is as simple as linking the video to other user.

2. RELATED WORK

Cloud services are provided by number of different venders and these venders are not trust worthy. Cloud computing services are given irrespective of geo-location. On cloud environment location transparency is maintained from cloud users and Sometimes there is risk of stealing data on cloud by hackers and there is also possibility that cloud service provider may not be cloud operator, but provides a value added services on top of another cloud providers service.

To maintain data privacy user data is stored in encrypted form, So that the malicious user or the intruders cannot access data. There are different types of cryptographic technique like Symmetric and Asymmetric keying. These types are made based on sharing of encryption key for decryption at the recipient. Symmetric key cryptographic type uses single key for both encryption and decryption. But, Asymmetric key cryptographic type uses different keys for encryption and decryption purposes.

3. LITERATURE REVIEW

Nowadays Mobile phones becomes essential part of every person and that is most likely to be with all. Also mobile phones has becomes more sophisticated device with number of functionalities like camera, multimedia player, video shooting and GPRS, Wi-Fi, 3G like network support etc., due to such a functionalities users are using mobile phones as high end device. With the invent of such a technologies, users also need more sophisticated, faster and stream less access and sharing of videos over internet. But videos are bulk in size and different in formats. Such formats produce challenge [1] in searching and faster download of videos [2]. Formats differ in quality of data, because it’s a current need of mobile users in which they want quality of video [3]. Mobile phones always get affect by low signal strength of network. It leads to use of encoding technique and compression technique [4], [5]. Signal strength and wireless nature will leads to noisy communication and causes unreliable transmission problem, solved by using session in [6] and by using light weight verification algorithm [7]. These challenges influence towards use of cloud computing as a solution to above problem [8].

Cloud computing is growing technology in IT sector and provide number of services to user. It provides services on demand [9] and with great comfort [10]. Infrastructure as a service (IaaS) of cloud services can be used for storing videos on the cloud [8], [11] so that it can be accessed faster and easily. Cloud computing has number of benefits [12] for users like on demand service, pay per use, scalability and availability services. Cloud services are on demand that is resources are allocated [13] according to users requirement and are available all the time. But, there are number of challenges in adaption of cloud services which is discussed in [20] such as security [21].Videos that has stored on the cloud can be shared in group [22], in friends or in public [16]. Sharing of videos can be done by using profile matching [27], [29], by using social relationship [32] etc. Videos have to be shared streamlessly and without buffering [16]. Video streaming has to be done on prediction basis by using social activities such as sharing in friends, in subscribers, in group or in public is explained in [16]. As discussed videos are in different format [1], such videos have to be viewed or searched and download effortlessly [30]. But there is security threat in adoption of cloud services, because cloud venders are not trusty.

Mainly security threat for data stored [21] on the cloud that can be hacked, steeled etc. Even though cloud providers are not trusted, how to identify is explained in [18]. There has also provided multicloud architecture [31] for security improvement by using security at multiple clouds simultaneously. Security, while travel of data in transmission line can be solved by using cloud based center for security check, explained in [14], [19].

There are number of solutions provided for storing data on the cloud so that data stored is secure [23], [24]. In those solutions, main solution is to store the videos after encryption [22] by using cryptographic technique. The data that has stored after encryption will only decrypt by users or intruders who has decryption key. The privacy of user data is one of the biggest challenges which has solved in [17], [22], [23], [24], [25], [28]. The data that has stored after encryption and shared by authorized users can create multiple copies of data in [16], is solved in [26] which has given revocation list for secure sharing purpose.

4. PROPOSED SYSTEM

We propose a new video streaming and video sharing system on the cloud which is shown in Figure 1, the entire video storing and sharing system on the cloud called Video Cloud (VC). The video cloud contains video base (VB) which stores videos that are fetched from video service providers (VSPs) and that are stored by users. The temporary video base (tempVB) is used to fetch new popular videos from VSPs. tempVB notes the access count of each video and fetch according to popularity. The video cloud continuously keeps running a collector to fetch videos from VSPs and user and then forwards video to encoder to encode the collected videos from collector into SVC format and then store into tempVB latter into VB. By using this 2-tier storage, the proposed system keeps serving most of popular videos. The whole management work is handled by the controller in the VC called VC controller.

For each mobile user a new private agent gets created at client side which is called as sub-video cloud (subVC). The subVC has a subVB called sub video base which stores the recently fetched video segments according to social activities. If there is any video shared or recommended then streaming and prefetching gets stated in background and the pre-fetched video gets stored into subVC then into subVB. If user wants to watch new video then he has to give request for video and decryption key then only actual streaming gets started. This whole system at client side gets controlled by app controller.

The security of user's private data and videos on the cloud is given by using encryption technique which stores videos and private data after encryption. And the video is decrypted at client side. The exchange of decryption key depends on the users activities like if video is shared then decryption key send along with video and if user request for new video from the VB then he must have to request for decryption key also.

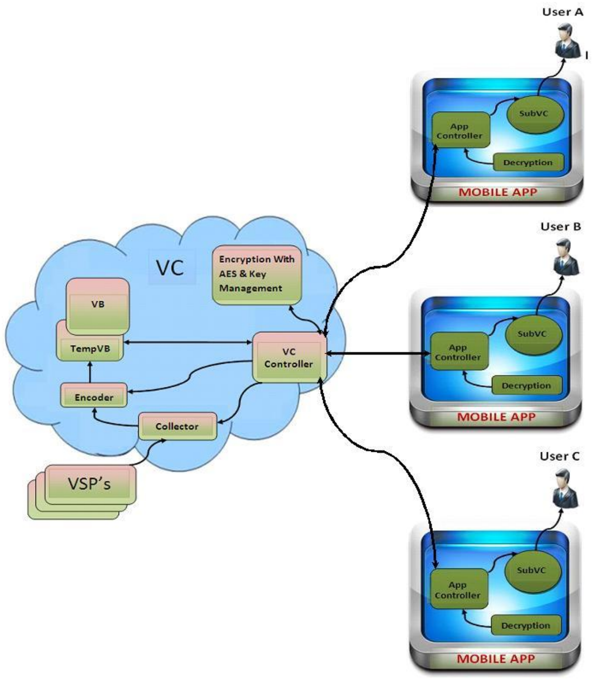

Figure 1: Architecture Diagram

5. SOLVING APPROACH

The proposed system is depending on techniques like Upload video, sharing video, video streaming and providing security by encryption and decryption technique.

5.1 Video Upload

In this phase, user will upload his private video or upload video from VSP into the VC. In this paper, we consider mobile network for content uploading on the cloud. We know that mobile phones are equipped with multiple wireless network support like 3G, Wi-Fi and Bluetooth. The mobile device can communicate with cloud via multiple routing paths and upload user videos on the cloud. So our file upload model consists of three parts that are source, destination and set of paths in network. On the source side, content of file with k packets are transferred into p disjoint paths through the network. The path i have assumed to carry Ki packets. On the network side path i can be model as an independent FIFO queue. We can denote delay model by using the delay of packet j along the routing path i can be denoted as V. In addition, we assumed that delays occurred by different packets on the same path is independently distributed and delays occurred by different packets on different paths in the network are independent. Therefore the delay of transferring Ki packets can be denoted as Ti and can be expressed as,

$$Ti = \sum_{j=1}^{Ki} V_j^i$$

On the destination side, file is reconstructed upon receiving k packets and the end-to-end file delay T is defined as the max of the entire path delays that can be denoted as,

$$T = \max \{ Ti, i = 1, 2, \ldots, p \}$$

5.2 Video Sharing

In this phase, user will share the data that is loaded on the cloud called video cloud (VC).

5.3 Video Streaming

In this phase, system will stream the video according to social activities. According to that prefetching in system takes place. Prefetching levels divided in three types called parts, all and little.

5.4 Encryption and Decryption of Data

In this phase, we are going to encrypt the data by using AES algorithm and secure key exchange by using Diffie Hellman Key Exchange algorithm. The encrypted data will get decrypt by only those users who has decryption key and has access to data.

6. AES AND KEY EXCHANGE USING DIFFIE HELLMAN

We are using Advanced Encryption Standard cryptographic algorithm for Encryption and Decryption of the video by using an input of 128 bits size of data and key all time. The key gets exchanged in the users by using the Diffie-Hellman key exchange Algorithm. The process that involves in this system starts by inputting video file by the user as an input file for encryption and store on the cloud called video cloud (VC).

6.1 AES Algorithm

AES is a Symmetric block cipher that means it use the same key for both encryption of data and decryption of data. In an AES algorithm same size of both the key and the data block used. The length of the key used defines the number of AES parameters. As we are using a Key of length 128 bits, we can use 10 rounds in our algorithm. It can be 12 rounds for 192 bits key size and 14 rounds for 256bits Key sizes. Currently, 128 bit key size used mostly. AES algorithm used to protect against all known attacks.

The Input of 128 bits block and the 128 bits of key. The block data pass into a State array which will alter every stage of the algorithm. 128 bits State array and key can be depicted into a matrixof4x4 sizes, so total of 16 Bytes. The all operations and steps involved in AES algorithm has shown in the Figure 2.

AES Algorithm starts with an Add Round Key operation which will be followed by nine rounds of four operations that are,

i. Substitute Bytes.

ii. Shift Rows.

iii. Mix Columns.

iv. Add Round Key.

The round number 10 just leaves the Mix Columns step. Similarly in the decryption process in AES the first nine rounds four basic operations are performed.

i. Inverse Shift rows.

ii. Inverse Substitute bytes.

iii. Inverse Add Round Key.

iv. Inverse Mix Columns.

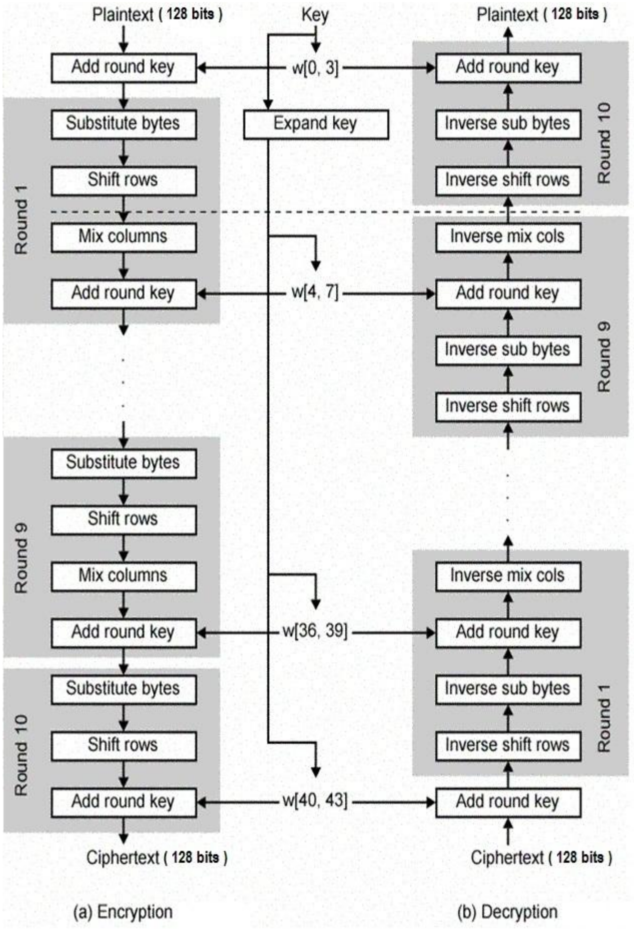

Figure 2: Rounds in AES

6.2 Distribution of Key using Diffie-Hellman

Diffie-Hellman is a key distribution algorithm that shares secret key between users. A review of the algorithm has given below.

- To share secret key the two devices D1 and D2agrees on numeric constants q and r. Here q is any random prime number and r is the generator.
- Suppose A and B be the private key of the devices D1 and D2 respectively, the selected A and B by D1 and D2can be any random prime number and also it must be less than q.
- Let s1=rA mod q and s2=rB mod q were computed by devices D1 and D2 respectively.
- The computed s1 and s2 were exchanged between D1 and D2.

- The end D1 computes (s2)A mod q.
- The end D2 computes (s1)B mod q.

Since K=rBA mod Q=rAB mod q, shared secret key=K.

7. IMPLEMENTATION

Our proposed system based on client server architecture. On the client side we have implemented android mobile application with android version 4.0 and on the server side deployed java application. It consists of main program handling all task of video cloud (VC) and also system will automatically initiates and terminates the instances. We have tested our system using Wi-Fi.

We have tested how long one user has to wait from the moment that he clicks the video to the moment video streaming segment arrives, which is called as "click-to-play" delay. We have shown the chart in Figure 3, it shows how long system will take the moment user clicks and video segment arrives according to video that is located in VB or in subVC or in VSP.

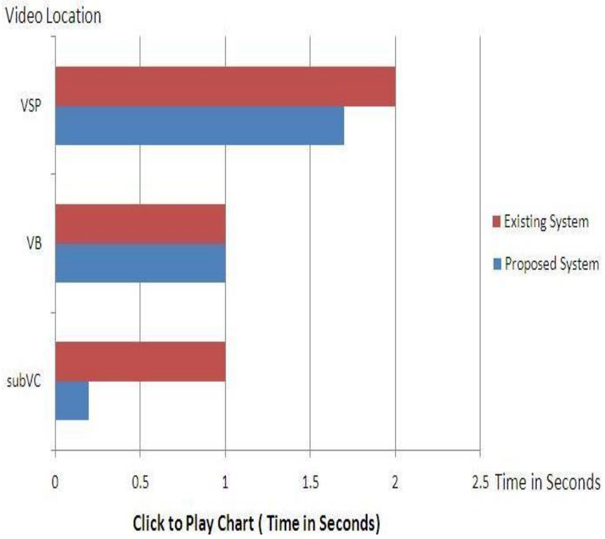

Figure 3: Click-to-play delay

8. CONCLUSION

Cloud We discussed our proposed system called Secure Mobile video streaming and Effective video sharing in the cloud, which efficiently stores videos on the cloud (VC) and construct agent (subVC) for each mobile user at client side to offer "non-terminating" video streaming and further willing to provide "non-buffering" experience of video streaming by background prefetching among the VB, tempVB and subVC of mobile user. And also Proposed System is going to provide security of user's private data and videos by using AES algorithm and secure key exchange by using Diffie Hellman Key Exchange algorithm.

The focus of this system is to see how cloud computing can improve streaming and sharing of videos for mobile users. We can develop the same system for different mobile operating systems as a future work and also we have not considered the security of data while user is storing data in the cloud called video cloud(VC), it has kept for future work.

9. ACKNOWLEDGMENTS

The authors would like to thank Chairman of D. Y. Patil Knowledge City and Management and the Principal Dr. Uttam Kalwane, Colleagues of the Department of Computer Engineering and Colleagues of the varies Department at the D. Y. Patil School of Engineering and Technology, Charoli, Pune. Dist. Pune Maharashtra, India, for their support, suggestions and encouragement.

10. REFERENCES

[1] Rong Yan Facebook, Benoit Huet EURECOM, Rahul Sukthankar Intel Labs and Carnegie Mellon University, "Large-Scale Multimedia Retrieval and Mining", Published by the IEEE Computer Society in 1070-986X/11/$26.00 _c 2011 IEEE.

[2] Yanhua Yu, Meina Song, Yu Fu, and Junde Song, "Traffic Prediction in 3G Mobile Networks Based on Multi-fractal Exploration", TSINGHUA SCIENCE AND TECHNOLOGY ISSN 1007-0214 08/10 pp398-405 Volume 18, Number 4, August 2013.

[3] A. Nafaa, T. Taleb, and L. Murphy, "Forward Error Correction Adaptation Strategies for Media Streaming over Wireless Networks", in IEEE Communications Magazine, vol. 46, no. 1, pp. 72–79, 2008.

[4] Andreas Panayides, Zinonas C. Antoniou, Yiannos Mylonas, Marios S. Pattichis, Andreas Pitsillides, and Constantinos S. Pattichis, "High-Resolution, Low-Delay, and Error-Resilient Medical Ultrasound Video Communication Using H.264/AVC Over Mobile WiMAX Networks", IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, VOL. 17, NO. 3, MAY 2013**.**

[5] Dong Zhang, Bin Li, Houqiang Li, "Intermedia-Based Video Adaptation System: Design and Implementation", TSINGHUA SCIENCE AND TECHNOLOGY ISSN 1007-0214 01/12 pp113-127 Volume 17, Number 2, April 2012.

[6] Suárez, E. Macías y F. J. Espino, "Automatic Resumption of RTSP Sessions in Mobile Phones using JADE-LEAP", IEEE TRANSACTIONS, VOL. 7, NO. 3, JULY 2009.

[7] S.M.Nandhagopal, S.N.Sivanandam, "Data Delivery in Mobile Adhoc Networks Using Light Weight Verification Algorithm with High Node Mobility", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-305, Volume-2, Issue-5, April 2013.

[8] S.P.Warhekar, Prof. V.T.Gaikwad, Prof. H.N.Datir, "Development and Evaluation Mobile Multimedia Cloud Application", IJCSMC, Vol. 3, Issue. 4, April 2014.

[9] Sheng Di, Member, IEEE, and Cho-Li Wang, Member, IEEE, "Error-Tolerant Resource Allocation and Payment Minimization for Cloud System", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL:24 NO:6 YEAR 2013.

[10] Amir Vahid Dastjerdi and Rajkumar Buyya, Fellow, IEEE, "Compatibility-aware Cloud Service Composition Under Fuzzy Preferences of Users", IEEE TRANSACTIONS ON CLOUD COMPUTING, 2168-7161 (c) 2013.

[11] Yu Wu, Zhizhong Zhang, Chuan Wu, Zongpeng Li, and Francis C. M. Lau, "CloudMoV: Cloud-Based Mobile Social TV", IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 15, NO. 4, JUNE 2013.

[12] Liang Zhou, "CloudFTP: A Case Study of Migrating Traditional Applications to the Cloud", School of Software, Shanghai Jiao Tong University, Shanghai, 200240, China, 2013.

[13] Simon Caton, Christian Haas, Kyle Chard, Kris Bubendorfer, and Omer Rana, "A Social Compute Cloud: Allocating and Sharing Infrastructure Resources via Social Networks", IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. ?, NO. ?, MONTH 2014.

[14] Zhen Chen, Fuye Han, Junwei Cao, Xin Jiang, and Shuo Chen, "Cloud Computing-Based Forensic Analysis for Collaborative Network Security Management System", TSINGHUA SCIENCE AND TECHNOLOGY ISSN 1007-0214 05/12 pp40-50 Volume 18, Number 1, February 2013.

[15] Giani Carla Ito, Mauricio G. Ferreira, Nilson Sant'Anna, "A Strategy of Development for Web Interfaces in Mobile Devices", IEEE TRANSACTIONS, VOL. 6, NO. 5, SEPTEMBER 2008.

[16] Xiaofei Wang, Min Chen, Ted "Taekyoung" Kwon, Laurence T. Yang, Victor C.M. Leung, "AMES-Cloud: A Framework of Adaptive Mobile Video Streaming and Efficient Social Video Sharing in the Clouds", IEEE TRANSACTIONS ON MULTIMEDIA VOL:15 NO:4 YEAR 2013.

[17] A. Dunning, and Ray Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 2, FEBRUARY 2013.

[18] Nuttapong Pumvarapruek and Twittie Senivongse, "Classifying Cloud Provider Security Conformance to Cloud Controls Matrix", Department of Computer Engineering, Faculty of Engineering Chulalongkorn University Bangkok, Thailand, 978-1-4799-5822-1/14/$31.00 @2014.

[19] Ting Sang, "A Log-based Approach to Make Digital Forensics Easier on Cloud Computing", THIRD INTERNATIONAL CONFERENCE ON INTELLIGENT SYSTEM DESIGN AND ENGINEERING APPLICATIONS YEAR 2013, Shanghai Jiao Tong University, Shanghai, 200240, China.

[20] William C. Chu, Tunghai University, Taiwan, William R. Claycomb, Carnegie Mellon University, USA, George O. Strawn, National Coordination Office, OSTP, USA, Stephen S. Yau, Arizona State University, USA, "Challenges towards the Global Adoption of Cloud Computing".

[21] Mukesh Singhal and Santosh Chandrasekhar, University of California, Merced Tingjian Ge, University of Massachusetts Lowell Ravi Sandhu and Ram Krishnan, University of Texas at San Antonio Gail-Joon Ahn, Arizona State University Elisa Bertino, Purdue University, "Collaboration in Multicloud Computing Environments: Framework and Security Issues", 0018-9162/13/$31.00 © 2013 IEEE.

[22] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013.

[23] Lukas Malina and Jan Hajny, "Efficient Security Solution for Privacy-Preserving Cloud Services", 6TH INTERNATIONAL CONFERENCE ON TELECOMMUNICATIONS SIGNAL PROCESSING YEAR 2013, 978-1-4799-0404-4/13/$31.00 ©2013 IEEE.

[24] Ayad F. Barsoum and M. Anwar Hasan Department of Electrical and Computer Engineering, University of Waterloo, Ontario, Canada, "Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing Storage Systems", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSYEMS VOL:PP NO:99 YEAR 2013.

[25] Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING VOL.9 NO.4 YEAR 2012.

[26] Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud", IEEE TRANSACTIONS 1939-1374 (c) 2013 IEEE.

[27] Ming Li, Member, IEEE, Shucheng Yu, Member, IEEE, Ning Cao, Student Member, IEEE, and Wenjing Lou, Senior Member, IEEE, "Privacy-Preserving Distributed Profile Matching in Proximity-based Mobile Social Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS VOL:12 NO:5 YEAR 2013.

[28] Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE TRANSACTIONS ON COMPUTERS VOL:62 NO:2 YEAR 2013.

[29] Lexing Xie, Apostol Natsev, Xuming He, John R. Kender, Matthew Hill and John R. Smith, "Tracking Large-Scale Video Remix in Real-World Events", IEEE TRANSACTIONS ON MULTIMEDIA, VOL.15, NO.6, OCTOBER 2013.

[30] Yonggang Wen, Xiaoqing Zhu, Joel J. P. C. Rodrigues, and Chang Wen Chen, "Cloud Mobile Media: Reflections and Outlook", IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 16, NO. 4, JUNE 2014.

[31] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Member, IEEE, Luigi Lo Iacono, and Ninja Marnau, "Security and Privacy-Enhancing Multicloud Architectures", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 4, JULY/AUGUST 2013.

[32] Haiying Shen, Senior Member, IEEE, Ze Li, Student Member, IEEE, Yuhua Lin and Jin Li, Fellow, IEEE, "SocialTube: P2P-assisted Video Sharing in Online Social Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL:PP NO:99 YEAR 2013.