ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Mobile Multi-source High Quality Multimedia Delivery Scheme

[1]Mr.V.Abishek, [2]Ms.N.Ramya, [3]Mr.C.Satheeshkumar, [4]Mr.V.Vijayragavan,
[5]Mr. S. Sivaprakash, [6]Mrs. M. Umamaheswari
Department of Computer Science and Engineering,
KSR College of Engineering, Tiruchengode, Tamilnadu, India
[1-4]UG Students, [5,6]Assistant Professor

Email id: [1]abishekvenkat22@gmail.com, [5]shivaiter@yahoo.co.in, [6]Umadeena@gmail.com

ABSTRACT

Increasing amount of multimedia content is being delivered over heterogeneous networks to diverse user types, holding various devices, many of them mobile. Mobile devices such as Smartphone's and tablets have already become both consumers and sources of multimedia content, but the delivery quality varies widely, especially due to their users' mobility. In order to support increasing the quality of the multimedia content delivered to a growing number of mobile users, this paper introduces a mobile multi-source high quality multimedia delivery scheme (M3QD). M3QD supports efficient high quality multimedia content delivery to mobile users from multiple sources.

Both simulations and prototyping-based perceptual tests show how increased user perceived video quality and improved mobility support is achieved when using M3QD in comparison with the case when a single source classic approach is employed. M3QD can be used in various scenarios involving multimedia content distribution between mobile users in leisure parks or around tourist attractions, content exchange between vehicles on urban roads and even information delivery in industrial applications, where content has to be shared between large number or diverse mobile users.

1. Introduction

The term “cloud computing” is a recent buzzword in the IT world. Behind this fancy poetic phrase there lies a true picture of the future of computing for both in technical perspective and social perspective. Though the term “Cloud Computing” is recent but the idea of centralizing computation and storage in distributed data centers maintained by third party companies is not new but it came in way back in 1990s along with distributed computing approaches like grid computing. Cloud computing is aimed at providing IT as a service to the cloud users on-demand basis with greater flexibility, availability, reliability and scalability with utility computing model.

The origin of cloud computing can be seen as an evolution of grid computing technologies. The term Cloud computing was given prominence first by Google's CEO Eric Schmidt in late 2006. So the birth of cloud computing is very recent phenomena although its root belongs to some old ideas with new business, technical and social perspectives. From the architectural point of view cloud is naturally build on an existing grid based architecture and uses the grid services and adds some technologies like virtualization and some business models. In brief cloud is essentially a bunch of commodity computers networked together in same or different geographical locations, operating together to serve a number of customers with different need and workload on demand basis with the help of virtualization.

Cloud Computing provides us a means by which we can access the applications as utilities, over the Internet. It allows us to create, configure, and customize applications online. The term Cloud refers to a Network or Internet. Cloud Computing refers to manipulating, configuring, and accessing the applications online. It offers online data storage, infrastructure and application. Cloud can provide services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN. Applications such as e-mail, web conferencing, customer relationship management (CRM), all run in cloud.

2. Related work

There are numerous works addressing searching for similar images, and most of them are based on the local invariant descriptors. Typically, high-dimensional descriptors are extracted from the interest regions of images to represent the visual characteristics. Different types of descriptors are proposed to achieve efficient and accurate image matching result, e.g. SIFT and SURF. The 128-dimension SIFT descriptor is most widely used for image search due to its distinctiveness and computational efficiency. Usually, content-based video search can be reduced to some sort of key frame search. For example, Video Google proposes an approach to search a user outlined object in videos using the pre-computed descriptor of the object. The search result is a ranked list of key frames. The most accurate approach to search similar images is to conduct the nearest neighbor search among image descriptors. But one high-resolution image is usually described by thousands of feature vectors and many image retrieval systems manage millions of images. Facing billions of high-dimensional vectors, the accurate nearest neighbor search is too expensive. Various feature vector indexing approaches are designed to boost up the search efficiency, e.g., cluster pruning and extended cluster pruning. Extended cluster pruning provides a promising way for efficient clusters construction and queries processing, which outperforms comparable solutions, like p-sphere tree and rank aggregation. FAST supports near-real-time semantic queries on cloud storage system via correlation-aware hashing and manageable flat-structured addressing. Recently, a lot of work speed up the search process based on visual words e.g., which somewhat decrease the search accuracy. As commercial data center get more and more popular, it is also possible to improve the large-scale image search using parallelize computing. There are some work using MapReduce accelerate the indexing and search process. However, few of image indexing and search systems consider privacy protection of the image owner and querier.

There are some applications protecting image privacy by simply encrypting the image or blacking out private content, e.g. human face. Removes facial characteristics from the video frame to protect the face privacy of individuals in video surveillance. P3 proposes a image into private part and public part. Both and P3 only support privacy protection in image storage, leaving the result image of limited use and no image search is supported for the private image. GigaSight proposes an Internet system for collection of crowd-sourced video from mobile devices, which blacks out sensitive information from video frames. For search purpose, each frame is analyzed by computer vision code to obtain tags as the index. Securing SIFT proposes to extract feature over massive encrypted image data. designs techniques to detect private images by learning privacy classifiers trained on a dataset of manually assessed Flickr photos. uses kNN to protect feature vectors and a standard stream cipher to protect image pixels. Those work offer techniques to protect image privacy, but cannot support image similarity based search and the indices also expose sensitive information. uses IES-CBIR to achieve encrypted storage and searching of images while preserving privacy. However, it cannot provide efficient search over large-scale image datasets.

The core of content-based image search is measuring the distance between vectors. There are many existing methods addressing privacy-preserving vector distance among parties using secure multi-party computation (SMC). There are some works providing privacy-preserving image matching using classic homomorphic encryption. Those methods provide privacy protection to the query image as well as the outcome of the matching algorithm, but the result is not secure against the service provider. They all require rounds of online interactions with users during the search and incur expensive computation cost, so none of them can be scaled to address large-scale image sets. Recently, Xiao et al. propose an efficient homomorphic encryption protocol for multi-user system. It is a non-circuit based symmetrickey homomorphic encryption scheme, whose security is equivalent to the large integer factorization problem. We employ this protocol to design our system.

To ensure the security, text documents are usually encrypted before uploading to cloud. Searchable symmetric encryption (SSE) is proposed to search over encrypted text documents or image through keywords/tags. Curtmola et.al. propose a thorough discussion on the framework of SSE. Cong et.al. extend the framework to ranked keyword search presents a keyword-based semantic search framework for encrypted cloud data by generating metadata for each file. and propose solutions for multi-keyword ranked search over encrypted data in cloud computing. Existing SSE approaches only support search encrypted keywords by accurately matching. They cannot measure distance of encrypted vectors, thus cannot support content-based image search.

3. Mobile Multi-Source High Quality Multimedia Delivery Scheme

Multimedia content exchanged by mobile devices is increasing dramatically in terms of both number of streams and their quality as the expectations of users also increase. Mobile devices including smartphones and tablets are overtaking classic devices such as desktops in terms of the amount of multimedia content they store, process and share. For instance, the mobile video traffic accounted for 55 percent of total mobile data traffic in 2015 and it is estimated that will reach 75 percent by 2020. At the same time, cloud computing is already supporting a wide range of flexible innovative applications and services, many multimedia-based. Lately mobile cloud is adding another dimension to cloud computing flexibility: user mobility. This encourages further development of existing services and proposal on new and potentially highly attractive applications for the increasing user base.

The highly popular social networking services for example are seeing an increased number of users sharing with peers multimedia content either originating from their mobile devices or previously received from media servers. Mobile users of such rich media communication-oriented applications possess increasingly sophisticated and capable portable devices, in terms of connectivity, processing and graphical display capabilities. Additionally, most mobile devices are already equipped with multiple wireless interfaces which allow them to connect simultaneously to multiple wireless networks using different wireless communication technologies, enabling them also to form ad-hoc networks. Although not yet available on the market, mobile devices equipped with multiple interfaces on the same technology are already discussed and designed both in the academia and industry, targeting an even better mobile inter-connectivity.

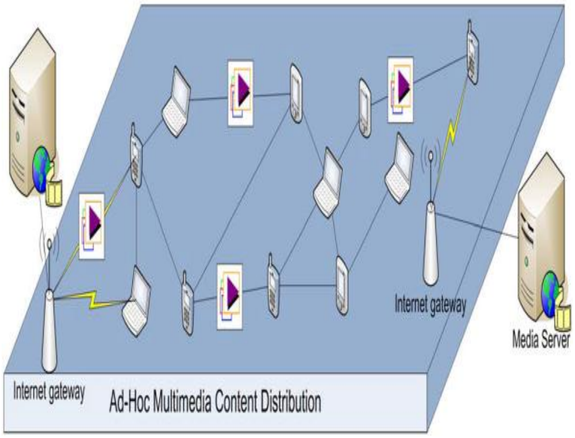

Fig. 1. Wireless Network Environment Supporting Mobile Multimedia Content Distribution

In these circumstances, as illustrated in Fig. 1, hybrid networks combining the benefits of both ad-hoc and infrastructure-based communications are an appealing option for enabling efficient multimedia content delivery between mobile devices. However, wireless communications in general, and mobile multi-hop content delivery in particular, are well known for their bandwidth and latency-related limitations. Consequently, in this context, the biggest challenge is to support high quality multimedia content delivery. This paper introduces a novel Mobile Multi-source High Quality Multimedia Delivery Scheme (M3QD) for high quality multimedia content distribution to mobile users over wireless networks. M3QD employs a multi-source multi-stream content delivery paradigm which stands at the basis of its flexibility, robustness and high quality of delivery. The proposed solution enables high quality multimedia content delivery, while also supporting user mobility.

The performance of M3QD is evaluated using both modeling and simulations, and perceptual-based real-life tests. M3QD is compared with a multimedia delivery approach where the content is transmitted from a single source. The comparative evaluation is made in terms of estimated user perceived video quality, assessed using both objective metrics and subjective methods.

4. Problem Statement

In Existing system Public Key Encryption (PKE), the privacy required by the patients could be ensured. Up to now, many cryptographic encryptions methods have been proposed to satisfy the requirements of privacy-preserving in big data storage. However, most encryption methods such as the public key encryption are not anonymous, i.e., if the adversaries obtain the ciphertexts, they can easily know the owner of the ciphertext as well as who will receive the ciphertext. The PKE cannot achieve the anonymity of the users send and receive the ciphertext, so personal information may be leaked. If an adversary is able to achieve the ciphertext, he can know whose key the ciphertext is encrypted under, thus knowing the owner of the ciphertext.

We propose a new notion called pre-authentication mechanism in the model of MH-IBCPRE. Different from the existing work, the proposed mechanism can verify users' attributes before data sharing, thus satisfying the actual needs of users. The data of users can be shared with users having appointed attributes, and others have no access to the data. Some existing work on multi sharing mechanism in big data. The comparison between our work and previous ones is shown afterwards.

- Encryption methods such as the public key encryption are not anonymous.
- The adversaries obtain the ciphertexts, they can easily know the owner of the ciphertext as well as who will receive the ciphertext.
- They may intend to share data only with receivers who have certain attributes. Data providers and receivers have to verify the authenticity of each other to make sure that data and the identity won't be leaked out.
- The attributes also need to be protected. proposed a verification mechanism to verify the authenticity of users' attributes.

5. ROI Based Content Aware Multimedia Sharing Scheme

The information of receivers will be exposed to the third party during the re-encryption process. Proposed a technique named File re encryption. By applying a semi-trusted File and re-encrypt the cipher text, data can be shared without exposing information to the third party. Furthermore proposed a technique called identity-based File re-encryption. They achieved control of access in storage in the network. The optimized towards encrypting a specific region in an File is proposed. The encryption of specific region(s) in an File is often of more practical relevance than encrypting the entire File, thus avoiding wastage of time and processing power. The algorithm proposed is ideal for encrypting Files with relatively small Region of Interest (ROI). It makes novel use of the XOR operation and the relative visual redundancy of the blue-plane components in a RGB color File. A pseudorandom number generator is used as a basic security feature. Furthermore, Cipher Block Chaining (CBC) is also suggested as an improvement to further enhance the security of the algorithm. The algorithm may be classified as lossy since some visual data is sacrificed in the decrypting process

This work proposes the notion of pre-authentication for the first time, i.e., only users with certain attributes that have already. The pre-authentication mechanism combines the advantages of File conditional re-encryption multi-sharing mechanism with the attribute-based authentication technique, thus achieving attributes authentication before re-encryption, and ensuring the security of the attributes and data. Moreover, this work finally proves that the system is secure and the proposed pre-authentication mechanism could significantly enhance the system security level.

First proposed the concept of the privacy of the keys is highly secure. The pre-authentication mechanism combines the advantages of File conditional re-encryption multi-sharing mechanism with the attribute-based authentication technique. Achieving attributes authentication before re-encryption, and ensuring the security of the attributes and data. Receivers who are qualified to know the data can use their keys to decrypt the ciphertext, but others cannot, so data providers' privacy can be protected. To perfect the existing PRE system considered the scenario that data providers may want the data to be conditionally shared. That means receivers just obtain a part of the data instead of the whole. Such an assumption is more close to the reality.

In this section, we present our whole system, including system set up, key generation, encryption, re-encryption, pre authentication and decryption. First, the parameters are set up and the secret keys are generated. The data is encrypted into cipher text. Then the generation of the re-encryption keys is carried on. After that, the attributes of the data receivers are verified, and only receivers with specific attributes have access to the re-encryption keys and re-encrypt the cipher texts. Finally, the decryption of the re-encrypted cipher texts is given.

5.1. ROI Based Privacy-Preserving File Sharing

In this module PKE cannot achieve the anonymity of the users send and receive the ciphertext, so personal information may be leaked. If an adversary is able to achieve the ciphertext, he can know whose key the ciphertext is encrypted under, thus knowing the owner of the ciphertext. To overcome this point, some anonymous encryption mechanisms have been proposed, e.g., anonymous mechanism. They achieve anonymity by removing the linkage between the data and the identity. Identities are splitted into two randomized complementary components and hide the identities of the receivers behind some randomization.

5.2. PRE-Authentication

This module is may intend to share data only with receivers who have certain attributes. Data providers and receivers have to verify the authenticity of each other to make sure that data and the identity won't be leaked out. The attributes also need to be protected. proposed a verification mechanism to verify the authenticity of users' attributes. By applying this technique, we propose a mechanism called pre-authentication approach to File re-encryption. In our scheme, data providers can verify the authenticity of receivers. Once receivers' attributes do not meet the conditions, provider will not communicate with him any more and he cannot obtain the data as well.

5.3. File Re-Encryption

This module is help to applying a semi-trusted File and re-encrypts the cipher text, data can be shared without exposing information to the third party. Furthermore, Green et al. proposed a technique called identity-based File re-encryption. They achieved control of access in storage in the network. Encryption techniques should be developed to meet requirements of the cloud users. Presented a File re-encryption technique called advanced multi hop- identity based conditional File re-encryption (Region of Interest) to realize receiver update and conditional share in big data storage.

5.4. ROI Key Generation

This module is entrusting the decrypt-encrypt-transmit task to a trusted third party is a good solution. But the information of receivers will be exposed to the third party during the re-encryption process. Proposed a technique named File encryption using Region of Interest. By applying a semi-trusted File and re-encrypt the cipher text, data can be shared without exposing information to the third party. Furthermore proposed a technique called identity-based File re-encryption. But the information of receivers will be exposed to the third party during the re-encryption process. proposed a technique named File encryption.

By applying a semi-trusted File and re-encrypt the ciphertext, data can be shared without exposing information to the third party. Furthermore proposed a technique called identity-based File re-encryption. They achieved control of access in storage in the network.

6. Performance Analysis

Comparing results when data are on disk versus in cache shows that disk throughput bounds ROI's performance when accessing all blocks. With the exception of the first blocks of a file, I/O and the challenge computation occur in parallel. Thus, ROIgenerates proofs faster than the disk can deliver data: 1.0 second versus 1.8 seconds for a 64 MB file.

Because I/O bounds performance, no protocol can outperform ROIby more than the startup costs. While faster, multiple-disk storage may remove the I/O bound today. Over time increases in processor speeds will exceed those of disk bandwidth and the I/O bound will hold. Sampling breaks the linear scaling relationship between time to generate a proof of data possession and the size of the file.

At 99% confidence, ROIcan build a proof of possession for any file, up to 64 MB in size in about 0.4 seconds. Disk I/O incurs about 0.04 seconds of additional runtime for larger file sizes over the in-memory results. Sampling performance characterizes the benefits of ROI. Probabilistic guarantees make it practical to use public-key cryptography constructs to verify possession of very large data sets. Table 1 and 2 shows the preprocessing accuracy and overall accuracy of the proposed and existing system.

Algorithm	Time in ms	File size in kb
Existing	4.5	2.5
Proposed	4.0	2.5

Table: 2 Overall Accuracy and Data Integrity Comparison between E-IBE with Proposed ROI

Comparing results when data are on disk versus in cache shows that disk throughput bounds ROI's performance when accessing all blocks. With the exception of the first blocks of a file, I/O and the challenge computation occur in parallel. Thus, ROI generates proofs faster than the disk can deliver data: 1.0 second versus 1.8 seconds for a 64 MB file.

Because I/O bounds performance, no protocol can outperform ROI by more than the startup costs. While faster, multiple-disk storage may remove the I/O bound today. Over time increases in processor speeds will exceed those of disk bandwidth and the I/O bound will hold. Sampling breaks the linear scaling relationship between time to generate a proof of data possession and the size of the file.

At 99% confidence, ROIcan build a proof of possession for any file, up to 64 MB in size in about 0.4 seconds. Disk I/O incurs about 0.04 seconds of additional runtime for larger file sizes over the in-memory results. Sampling performance characterizes the benefits of ROI. Probabilistic guarantees make it practical to use public-key cryptography constructs to verify possession of very large data sets. Table 1 and 2 shows the preprocessing accuracy and overall accuracy of the proposed and existing system.

Algorithm	Time in ms	File size in kb
Existing (E-IBE)	4.5	2.5
Proposed(ROI)	4.0	2.5

Table: 1 Preprocessing accuracy comparison between existing and proposed work

Algorithm	Over all Accuracy in percentage	Data integrity per block(for 100 percentage)
Existing (E-IBE)	78	93
Proposed(ROI)	83	98

Table: 2 Overall Accuracy and Data integrity comparison between E-IBE with Proposed ROI

7. Conclusion

In order to detect errors in big data sets from sensor net-work systems, a novel approach is developed with cloud computing. Firstly error classification for big data sets is presented. Secondly, the correlation between sensor net-work systems and the scale-free complex networks are introduced. According to each error type and the features from scale-free networks, we have proposed a time-efficient strategy for detecting and locating errors in big data sets on cloud. With the experiment results from our cloud computing environment U-Cloud, it is demonstrated that

1) the proposed scale-free error detecting approach can significantly reduce the time for fast error detection in numeric big data sets,

2) the proposed approach achieves similar error selection ratio to non-scale-free error detection approaches. In future, in accordance with error detection for big data sets from sensor network systems on cloud, the issues such as error correction, big data cleaning and recovery will be further explored.

REFERENCES

1) K. Collins, G.-M. Muntean, and S. Mangold, “Evaluation of dual transceiver approaches for scalable WLAN communications: Exploring the wireless capacity in entertainment parks,” in Proc. IEEE 35th Conf. Local Comput. Netw. (LCN), Denver, CO, USA, Oct. 2010, pp. 208–211.
2) Y. Cao, C. Xu, J. Guan, and H. Zhang, “QoS-driven SCTP-based multimedia delivery over heterogeneous wireless networks,” Sci. China Inf. Sci., vol. 57, no. 10, pp. 1–10, Oct. 2014.
3) J. Huang, C. Xu, Q. Duan, Y. Ma, and G.-M. Muntean, “Novel end-toend quality of service provisioning algorithms for multimedia services in virtualization-based future Internet,” IEEE Trans. Broadcast., vol. 58, no. 4, pp. 569–579, Dec. 2012.
4) T. Nuriel and D. Malah, “Region-of-interest based adaptation of video to mobile devices,” in Proc. 4th Int. Symp. Commun. Control Signal Process. (ISCCSP), Limassol, Cyprus, 2010, pp. 1–6.
5) O. Abboud, T. Zinner, K. Pussep, and R. Steinmetz, “On the impact of quality adaptation in SVC-based P2P video-on-demand systems,” in Proc. ACM Multimedia Syst. Conf., San Jose, CA, USA, Feb. 2011, pp. 223–232.
6) A.-N. Moldovan and C. H. Muntean, “Subjective assessment of bitdetect—A mechanism for energy-aware adaptive multimedia,” IEEE Trans. Broadcast., vol. 58, no. 3, pp. 480–492, Sep. 2012.
7) R. Trestian, O. Ormond, and G.-M. Muntean, “Enhanced power-friendly access network selection strategy for multimedia delivery over heterogeneous wireless networks,” IEEE Trans. Broadcast., vol. 60, no. 1, pp. 85–101, Mar. 2014.
8) R. Trestian, O. Ormond, and G.-M. Muntean, “Energy–quality–cost tradeoff in a multimedia-based heterogeneous wireless network environment,” IEEE Trans. Broadcast., vol. 59, no. 2, pp. 340–357, Jun. 2013.
9) A. Khan, L. Sun, E. Jammeh, and E. Ifeachor, “Quality of experiencedriven adaptation scheme for video applications over wireless networks,” IET Commun., vol. 4, no. 11, pp. 1337–1347, Jul. 2010.
10) O. Oyman and S. Singh, “Quality of experience for HTTP adaptive streaming services,” IEEE Commun. Mag., vol. 50, no. 4, pp. 20–27, Apr. 2012.
11) M. Seufert et al., “A survey on quality of experience of HTTP adaptive streaming,” IEEE Commun. Surveys Tuts., vol. 17, no. 1, pp. 469–492, 1st Quart., 2015.