Secured and Memory Concerned Data Handling Management in Cloud Environment: A Survey

[1] D. Pradeepa ,
[1]Research Scholar,
PG & Research Department of Computer Science,
Government Arts College, Coimbatore India.

[2] Dr. P. Sumathi
[2]Assistant Professor,
PG & Research Department of Computer Science,
Government Arts College, Coimbatore India.

Abstract :- **The explosive growth of multimedia contents, especially videos, is pushing forward the paradigm of cloud-based media hosting today. The wide attacking surface of the public cloud and the growing security awareness from the society are both calling for data encryption before outsourcing to cloud. Data de-duplication has been widely used in backups to save storage space and network bandwidth. Under the circumstance of encrypted videos, how to still preserve all the service benefits of cloud media centre remains to be fully explored. Videos may have to be encrypted before outsourcing for privacy concerns. For practical purposes, the cloud media centre should also provide the adaptively disseminate videos to heterogeneous networks and different devices to ensure the quality of service. This paper discusses various ideas related to security and video de-duplication when user stores data in the cloud.**

Keywords: ***De-duplication, Security, Memory Management, cloud Storage***

1. INTRODUCTION

De-duplication strategies can be considered according to the basic data units they handle. One strategy is file-level de-duplication which eliminates redundant files [4]. The other is block-level de-duplication, in which files are segmented into blocks and duplicate blocks are eliminated. De-duplication strategies can also be categorized according to the host where de-duplication happens. In server-side de-duplication, all files are uploaded to the storage server, which then deletes the duplicates. Clients are unaware of de-duplication. This strategy saves storage but not bandwidth. In client-side de-duplication, a client uploading a file first checks the existence of this file on the server (by sending a hash of the file). Duplicates are not uploaded. This strategy saves both storage and bandwidth, but allows a client to learn if a file already exists on the server. With the explosive growth of multimedia technology and mobile devices with high-definition cameras, multimedia contents, especially videos, have already dominated the network traffic and demanded a great amount of hardware storage.

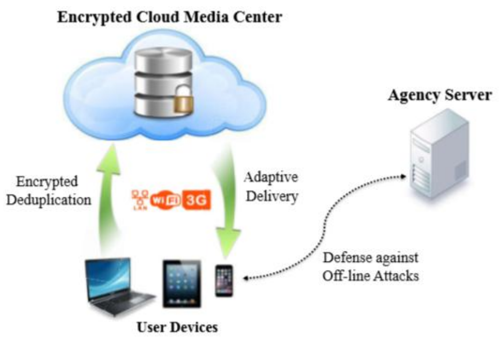
To handle such a rapidly growing trend, many existing and emerging applications based on videos are deployed at public clouds for its well-known advantages, e.g., availability, scalability, and economy [11]. However, the user privacy could be violated if content-sensitive videos are not protected properly in such an outsourcing environment [15]. In fact, current cloud-based data hosting services are shown to be vulnerable to security breaches. Data disclosure occurs frequently in recent years. Therefore, addressing the privacy concerns becomes significant for building a cloud media centre. A credible approach is to require each user to encrypt the videos using their secret key before sending them to public clouds. As long as the user's secret key is protected, video confidentiality can be guaranteed. But this approach prevents the cloud media centre from supporting de-duplication, a crucial function that can greatly save the network bandwidth and eliminate the storage redundancy in cloud services [1]. Identical videos encrypted by different user's secret keys would lead to different cipher texts, making de-duplication infeasible.

2. SYSTEM ARCHITECTURE

The cloud storage system involves three entities [2][14] the cloud media centre, the user, and the agency, as illustrated in FIG 1. Their roles are described below:

1. The cloud media centre (abbr. cloud) provides a video hosting platform, which stores users' encrypted videos and adaptively distributes them to cater for heterogeneous user devices and network bandwidth. It enforces secure client-side de- duplication, i.e., duplicate check is performed before users upload videos.
2. The user outsources their encrypted videos to the cloud, and possibly deletes the original ones at local. Later, the user may access their own videos.
3. The agency, hosted by a third party (e.g., a video service provider), facilitates our system to safeguard the confidentiality of user videos against off-line brute force attacks. It assists users and cloud to perform the duplicate check in a controllable fashion, and enables users to perform the encryption that supports de-duplication.

Fig: 1 System Architecture



3. RELATED WORK

Many systems have been established to provide secure storage but traditional encryption techniques are not suitable for de-duplication purposes. Li et al. proposes convergent key management in secure de-duplication [4] offline brute-force dictionary attacks can be easily caused because of the determination of CE keys. Moreover, current de-duplication schemes [4] [5] de-duplicate the encrypted data, which increases the computational overhead. but it suffers from well-known weaknesses which do not ensure protection of predictable files against dictionary attacks [4], [7]. In order to overcome this issue, Wen Bing Chuan et al. [10] have proposed to add a secret value S to the encryption key. De-duplication will thus be applied only to the files of those users that share the secret. The new definition of the encryption key is K = H(S|M) where | denotes an operation between S and M. However, this solution overcomes the weaknesses of convergent encryption at the cost of dramatically limiting.

Li et al. [1] present a key management scheme based on secret sharing to protect the convergent keys in secure de-duplication. The scheme constructs and distributes secret shares of keys across multiple independent servers.

Another work proposed by Puzio et al. [9] employ a server to perform additional encryption over the convergent-encrypted data collected from all users. Without knowing the server's secret key, cloud cannot launch off-line brute-force attacks over predictable files. However, their design is only suited for server-side de-duplication and the server has to suffer from heavy communication overhead.

Yixin Chen et al. [13] Proposed and developed an efficient NDVD cloud system, called Compound Eyes, by using a new detection paradigm. Instead of designing a sophisticated video representation, the focus has been shifted to the design of a well-organized system. Rather than feature design, they introduced improvements in accuracy through classifiers. Through use of reduced dimensionality and parallelism, and reduced the duration required for precise duplicate detection. But there is a limitation of shared memory parallel computing architectures.

Liu et al. [6] proposed a scheme capable of defending offline brute-force attacks without introducing additional independent server. However, their scheme requires a number of online users to actively assist the cloud to perform duplicate check and help transfer encryption keys. Despite useful in defending off-line brute-force attacks, all these work do not consider any bounded data leakage setting, in which the data encryption key might be leaked.

Xu et al. [8] proposed a secure source-based de-duplication scheme that is resilient to bounded data leakage. However, the scheme does not offer the defence against offline brute-force attacks over predictable data.

Xue Yang, et al.[12] investigate a three-tier cross-domain architecture, and propose an efficient and privacy-preserving big data deduplication in cloud storage (hereafter referred to as EPCDD). EPCDD achieves both privacy-preserving and data availability, and resists brute-force attacks.

Zheng Yan et al.[16] proposed a practical scheme to manage the encrypted big data in cloud with de-duplication based on ownership challenge and proxy re-encryption and evaluate its performance based on extensive analysis and computer simulations

Fatema Rashid [3] proposed a secure video de-duplication scheme through video compression in cloud storage environments. Its design consists of embedding a partial convergent encryption along with a unique signature generation scheme into a H.264 video compression scheme

4. ANALYSIS OF EXISTING SYSTEM

From the above discussion we can find drawbacks in existing systems such as Hash function and symmetric encryptions are not highly secured, consume more time for key generation, and it face different attacks on data storage and cost effective. The file- level and block- level de-duplication leads to the huge storage cost, as users must be billed for storing the large number of keys in the cloud. In our study we also found the layer level de-duplication is used for Scalable Video Coding (SVC) techniques. This existing work requires comparing both base layers and enhancement layers for de-duplication which requires more computation overhead. Storing and retrieving the video files in the cloud storage would leads to more memory storage. Security of the video files is complex to ensure in case of available more number of videos

These problems need to be focused in the proposed research method for the better performance and improvement.

5. CONCLUSION

In this paper we have presented a review on secure de-duplication techniques. From the study of existing system we conclude that which requires comparing both base layer and enhancement layer for de-duplication which requires more computational overheads. Security of the video files is complex to ensure in case of available more number of videos.

These problems needs to be focused in the proposed research method for the better performance improvement by Indexing table would be constructed for all videos before uploading it into the server, After index construction, videos would be compressed to reduce its size, thus the cloud storage can be optimized, finally retrieval accuracy and memory optimization is carried out by storing video index files in the agency server in the encrypted format.

These research implementations contribute towards the secured de-duplication process which attempts result with the secured and memory concerned video sharing in the real world environment.

REFERENCES

[1] Atul Adya, William J Bolosky, Miguel Castro, Gerald Cermak, Ronnie Chaiken, John R Douceur, Jon Howell, Jacob R Lorch, Marvin Theimer, and Roger P Wattenhofer. "Farsite: Federated, available, and reliable storage for an incompletely trusted environment" ACM SIGOPS Operating Systems Review, 36(SI):1–14, 2002.

[2] E. Manogar , S. Abirami "A study on data de-duplication techniques for optimized storage" 2014 Sixth International Conference on Advanced Computing (ICoAC), 31 August 2015, DOI: 10.1109/ICoAC.2014.7229702, Print ISSN: 2377-6927

[3] Fatema Rashid, Ali Miri, Isaac Woungang "A Secure Video Deduplication Scheme in Cloud Storage Environments using H.264 Compression" 2015 IEEE First International Conference on Big Data Computing Service and Applications (BigDataService), IEEE

Xplore: 13 August 2015, DOI: 10.1109/BigDataService.2015.15, ISBN: 978-1-4799-8128-1

[4] J. Li, X. Chen, M. Li, J. Li, P. P. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," IEEE transactions on parallel and distributed systems, vol. 25, no. 6, pp. 1615–1625, 2014, DOI: 10.1109/TPDS.2013.284, PRINT ISSN: 1045-9219

[5] J. Li, C. Qin, P. P. Lee, and J. Li, "Rekeying for encrypted deduplication storage," in Dependable Systems and Networks (DSN), 2016 46th Annual IEEE/IFIP International Conference on. IEEE, 2016, pp. 618–629, DOI: 10.1109/DSN.2016.62, Electronic ISSN: 2158-3927

[6] J. Liu, N. Asokan, and B. Pinkas, "Secure de-duplication of encrypted data without additional independent servers," in Proc. of ACM CCS, 2015.

[7] John R Douceur, Atul Adya, William J Bolosky, P Simon, and Marvin Theimer. Reclaiming space from duplicate files in a serverless distributed file system. In Distributed Computing Systems, 2002. Proceedings. 22nd International Conference on, pages 617–624. IEEE, 2002. DOI: 10.1109/ICDCS.2002.1022312, Print ISSN: 1063-6927

[8] J. Xu, E. Chang, and J. Zhou, "Weak leakage-resilient client-side de-duplication of encrypted data in cloud storage," in Proc. of ACM AISACCS, 2013.

[9] P. Puzio, R. Molva, M. ¨Onen, and S. Loureiro. Cloudedup: secure de-duplication with encrypted data for cloud storage. In Proc. of IEEE CloudCom, 2013. DOI: 10.1109/CloudCom.2013.54, INSPEC Accession Number: 14146200.

[10] Wen Bing Chuan, Shu Qin Ren, Sye Loong Keoh "Flexible Yet Secure De-duplication Service for Enterprise Data on Cloud Storage" 2015 International Conference on Cloud Computing Research and Innovation, IEEE, DOI: 10.1109/ICCCRI.2015.11, Electronic ISBN: 978-1-5090-0144-6

[11] W. Zhu, C. Luo, J. Wang, and S. Li. Multimedia cloud computing. IEEE Signal Processing Magazine, page 28(issue 3):59–69, 2011, DOI: 10.1109/MSP.2011.940269, ISSN: 1053-5888.

[12] Xue Yang, Rongxing Lu, Senior Member, IEEE, Kim Kwang Raymond Choo, Senior Member, IEEE, Fan Yin, and Xiaohu Tang, Member, IEEE"Achieving Efficient and Privacy-Preserving Cross-Domain Big Data Deduplication in Cloud", IEEE Transactions on Big Data, 29 June 2017 , Volume: PP, Issue: 99 , ISSN: 2332-7790, DOI: 10.1109/TBDATA.2017.2721444,

[13] Y. H. W. W. Yixin Chen, Wenbo He, "Compoundeyes: Near-duplicate detection in large scale online video systems in the cloud," in Proc. of IEEE INFOCOM, April 2016, DOI: 10.1109/INFOCOM.2016.7524429, INSPEC Accession Number: 16192254

[14] Y. Wu, Z. Wei, and R. H. Deng. Attribute-based access to scalable media in cloud-assisted content sharing networks. IEEE Trans. on Multimedia, page 15(issue 4):778–788, 2013, DOI: 10.1109/TMM.2013.2238910, INSPEC Accession Number: 13499786

[15] Y. Zheng, X. Yuan, X. Wang, J. Jiang, C. Wang, and X. Gui, "Enabling encrypted cloud media center with secure de-duplication," in Proc. of ACM ASIACCS, 2015.

[16] Zheng Yan, Senior Member, IEEE, Wenxiu Ding, Xixun Yu, Haiqi Zhu, and Robert H. Deng, Fellow, IEEE "Deduplication on Encrypted Big Data in Cloud", IEEE TRANSACTIONS ON BIG DATA, VOL. 2, NO. 2, June 1 2016, ISSN: 2332-7790, DOI: 10.1109/TBDATA.2016.2587659