International Journal of Scientific Research in Engineering and Management (IJSREM)

Volume: 05 Issue: 04 | April - 2021 ISSN: 2582-3930

Defending against Illegal Content Redistribution in Encrypted Cloud Media Center

KIRUTHIGA P

Asso.Prof. Mr. J. JAYAPANDIAN

Krishnasamy College of Engineering and Technology,

Cuddalore.

ABSTRACT:

The wide adoption of cloud greatly facilitates the sharing of explosively generated media content today, yet deprives content providers' direct control over the outsourced media content. Thus, it is pivotal to build an encrypted cloud media center where only authorized access is allowed. Enforcing access control alone, however, cannot fully protect content providers' interests, as authorized users may later become traitors that illegally redistribute media content to the public. Such realistic threat should have been seriously treated yet is largely overlooked in the literature. In this paper, we initiate the first study on secure media sharing with fair traitor tracing in the encrypted cloud media center, through a new marriage of proxy re-encryption (for secure media sharing) and fair watermarking (for fair traitor tracing). Our key insight is to fully leverage the homomorphic properties residing in proxy re-encryption to embrace operations in fair watermarking. Two protocols are proposed for different application scenarios. We also provide complexity analysis for performance, showing that our work can also be treated as secure outsourcing of fair watermarking, and thus kills two birds with one stone. We thoroughly analyze the security strengths and conduct extensive experiments to validate the effectiveness of our design.

Keyterms:Big Data, proxy re-encryption, watermarking.

I. Introduction:

In today's big data era, consuming multimedia is increasingly becoming an essential part of the daily life for end users to access different systems, services, and applications. As more and more media content is being explosively generated, content providers now usually resort to cloud computing for media hosting and sharing, as it can provide economical and on-demand usage of abundant storage and computation resources. Despite the prominent benefits, deploying the cloud media center deprives content providers' direct control over the outsourced media content and raises security concerns. In fact, data disclosure frequently occurs in real-world cloud storage services. So, it is critically important to embed security in the cloud-based media sharing service design from the very beginning, enforcing access control so that only authorized access to the outsourced media content is allowed.

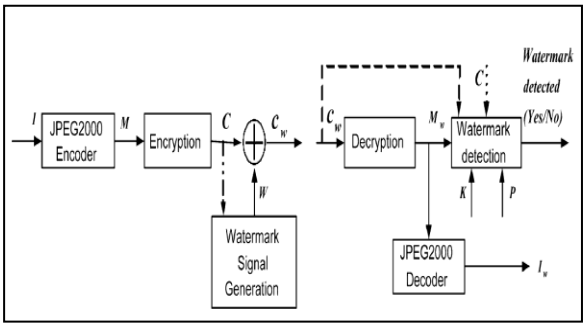

Figure 1: Proposed model for watermarkgeneration

II.Literature view:

1.Data-intensiveapplicationschallenges, techniques and technologieswritten by C. P. Chen and C.-Y. Zhang this paper is aimed to demonstrate a close-up view about big data including Big data applications

2.Towards end-to-end secure content storage and delivery with public cloud written by H. Xiong, X. Zhang, D. Yao, X. Wu, described as scheme for securely sharing and distributing content via the public cloud,It ensure the confidentiality of content in cloud environments with flexible access control policies

III.Proposed System:

To the best of our knowledge, our work is the first to support secure media sharing with fair traitor tracingin the encrypted cloud media center.Specifically, our work allows secure sharing of the outsourced media content to authorized users, while enabling tracing illegal content redistribution fairly.

We deliver two secure designs to accommodate two different application scenarios. The first design relies on an online trusted WCA for assistance, while the second one is WCA-free with a modest storage trade-off for the content provider.

2. We provide complexity analysis on performance to show that our work can also be treated as privacypreserving outsourcing of fair watermarking in cloud computing, and thus kills two birds with one stone.

3. We thoroughly analyze the security strengths and conduct extensive experiments to demonstrate the effectiveness and practicability of our design.

4.The access control has been developed as an inherent property in our protocol. Therefore, no additional special access control mechanism is needed, which reduces considerable cost for software/hardware development, integration, and maintenance.

5.The cloud cannot cheat a user by representing that an existing file does not exist, or a nonexistent file does exist.

6.Our theoretical analysis contributes to the foundation and understanding of the verifiable file search problem and the design of secure and efficient protocols.

7.Our experimental results validate the effectiveness and efficiency of the proposed protocols.

IV.Functions:

Data Owners:

The data owner outsources the data to an untrusted cloud. To prevent potential cheating of the cloud (either intentionally or unintentionally), the data owner embeds some secret information in the outsourced data to enable file search verifiability for data users. The data owner and data users possess some secret information to achieve verifiability; the secret information may be different in order to differentiate users with various security privileges.

Cloud Server:

We model the cloud as malicious, thus the cloud may fool the data user. Such an abnormal behavior may be caused by various factors such as the cloud being hacked, the cloud having software and hardware failures, employees of the cloud service providers intentionallyinterrupting

From the cloud's viewpoint, it is also rewarding to provide a verifiable search service. First, the search functionality over the outsourced data is highly expected by users. Meeting the requirements of users as best as possible can help the cloud service provider to gain more market share. Second, providing a verifiable file search service leads to the user having confidence that the cloud is indeed honest. This also helps the establishment of the cloud's reputation. Therefore, the cloud could attract more clients and further gain in market share. This also helps to eliminate various incentives for the cloud to cheat.

Data User:

When a data user wants a file that fits the user's privilege, the user sends the filename to the cloud. After receiving the searched filename, the cloud searches the outsourced data. Ifthe file exists, the cloud returns the corresponding file, along with

with a proof showing that the returned data is indeed valid. If the file does not exist, the cloud proves to the user that it has no such file. We argue that providing file search verifiability benefits both users and the cloud.

Verifiable File Search:

In this Module, we focus on designing a protocol to enable the verifiable file search over outsourced data with only one security level. Throughout this section, we do not differentiate the outsourced data and data users. We first propose a framework to formalize a verifiable file search protocol with a single security level, and define its security. Later, we propose a baseline protocol to solve verifiable file search using the concept of filename separation. The baseline protocol does not protect filename privacy. Finally, we propose a fully-fledged protocol for verifiable file search which possesses both search result verifiability and filename privacy protection.

V.Conclusion:

It have initiated the first endeavor toward secure media sharing with fair traitor tracing The work has newly and delicately bridged proxy re-encryption and fair watermarking, and delivered practically viable solutions to support secure sharing of outsourced media content to authorized users, while enabling fair tracing of illegal content redistribution.

VI.Future Scope:

In future this mechanism proxy reencryption and watermarking is used to avoid the explosion of personal data in the intenet

VII.References:

1.C. P. Chen and C.-Y. Zhang, "Data-intensiveapplications, challenges, techniques and technologies: A survey on big data," Information Sciences, vol. 275, pp. 314–347, 2014.

2. W. Zhu, C. Luo, J. Wang, and S. Li, "Multimedia cloud computing," IEEE Signal Processing Magazine, vol. 28, no. 3, pp. 59–69, 2011.

3.H. Xiong, X. Zhang, D. Yao, X. Wu, and Y. Wen, "Towards endto-end secure content storage

and delivery with public cloud," in Proc. of ACM CODASPY, 2012, pp. 257–266.

4. K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

5. Y. Zheng, H. Cui, C. Wang, and J. Zhou, "Privacy-preserving image denoising from external cloud databases," IEEE Transactions on Information Forensics and Security, vol. 12, no. 6, pp. 1285–1298, 2017.