



# Survey: Multimedia Copyright Protection on Cloud

Nivedita S. Konde<sup>1</sup>, Prof. Shital P. Kakade<sup>2</sup>

Student, Department of Information Technology, DACOE, Karad, India<sup>1</sup>

Professor, Computer Science & Engg, DACOE, Karad, India<sup>2</sup>

**Abstract:** The Internet regarded as an amorphous omnipresent space for processing and storage is called as Cloud computing. In other words Cloud Computing is defined as operations which are based on internet. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. A legal way of protecting user's data which means that data the user has created and uploaded cannot be published by anyone except the user without his permission is Multimedia copyright protection on cloud. The development of Internet has led the multimedia computing to emerge as a technology for generating, editing, processing and searching contents of media like image, audio, video, graphics and such others. Multimedia cloud computing has much challenges like Network heterogeneity, Device heterogeneity, Multimedia and service heterogeneity, Security, Power Consumption, QoS heterogeneity which has to be met. Besides this there is a big challenge for data security and access control when the user uploads any data in the form of multimedia content for sharing on cloud. In this paper we can see detection of copyright violation of multimedia content like images and videos. This paper proposed a new method of creating and comparing signatures of data on cloud. This paper travel through a method for enhancing security for copyright protection of multimedia content like images and videos.

**Keywords:** Cloud, Multimedia, DES, Security, Copy Detection.

## I. INTRODUCTION

Due to the availability of free online hosting sites that has led to very easy way of duplicating the copyrighted multimedia data such as images and videos, development is needed for storing, recording and processing data of multimedia content. Such illegal change or reposition of multimedia content on the cloud can led to the loss of revenues for the actual owner of data. Since there is much more amount of multimedia content occupying over the internet and finding illegal copies over the internet is very complex task. Also comparing of unauthorized or illegal copies with authorized copies is very complex and it will be very costly which is not affordable. We design a novel system for multimedia copyright protection on cloud infrastructure. The system can be used to provide the protection to the copyright of multimedia content like images and videos. The private or public cloud or even in any combination of public and private clouds the system can run. There is guarantee of fast deployment of multimedia copyright protection due to novel system is based on infrastructure of cloud which provides fast access to computing software and hardware resources.

As in case of computing resources, resources are used on demand basis in cloud, hence the system is cost effective. By scaling up and down for supporting large volumes of multimedia content to be copyright protected i.e. the system can provide scalability. The proposed system includes two components which include: (i) a method to create signature of multimedia content like images and videos at the time of uploading the content on any online

hosting site on cloud and (ii) distributed matching engine which stores signatures of authorized uploaded multimedia content and will match them against unauthorized or illegal multimedia content. Through performing experiments on multimedia content like images and videos, we show the more accuracy and scalability and even elasticity of the proposed system. We performed experiment of copyright protection by uploading images and videos on DriveHQ Cloud File Server and achieved success in it. Firstly we choose image file as animal called koala after that we choose Flicker as a hosting site and start uploading that image on DriveHQ Cloud File Server which is Cloud File Server. For the uploaded image the signature was created with the help of signature creation method which was saved in the database.

Then we tried to upload the same image of koala with the same hosting site as well we tried with different hosting site, then the signature was created and we received one message that this image already exists, and image failed to upload hence we achieved copyright protection. Again we tried to upload the same image which is saved with different name and tried with different hosting sites, then again we received the message that this image already exists, and image failed to upload hence we achieved copyright protection. Then for the further testing we tried to upload the same image with editing also we converted into different format and saved it with different name and tried with different hosting sites, then the signature was created and image was uploaded. Here the concept of



distributed matching engine come into existence where it creates the percentage of matching of images and if the percentage exceeds threshold value then image will not be uploaded but if it didn't exceed threshold value then image will be uploaded and the matching percentage notification will be send to data owner and service provider and they will have the right to discard the image if they found any copyright violation. Here the signature plays very important role since distributed matching engine creates percentage of matching by comparing image's signatures. The same theory we tried for videos and got success in performing copyright protection. We found accurate result even if the videos were subjected to various transformations such as cropping, or blurring.

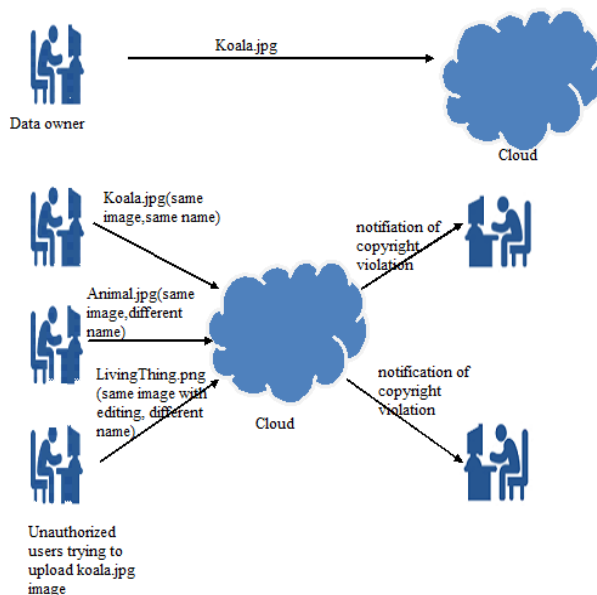


Fig. 1 Example of copyright protection of image

#### The contribution of this paper is as follows:

- For multimedia copyright protection the fully cloud based system is used.
- The system supports many multimedia contents like images and videos etc.
- Cloud computing resources utilizes by the system efficiently.
- The system uses a method to create signature of images by taking input as codec of images which is uploaded and applies Data Encryption Algorithm (DES). DES algorithm is used to produce a sixteen bit digital signature which randomly takes first and last eight bits of codec. Copyright violation takes place and notification will go to service provider as well to data owner whenever the signature matches with any of the uploaded images. Even when its matching percentage will exceed threshold value it sends notification.
- By taking input as frames per rate of videos the system uses a method to create signature of videos and applies Data Encryption Algorithm (DES) which captures the depth of signature in stereo content. If the signature of

uploaded video will match with any of the previously uploaded videos then copyright violation takes place and notification will go to service provider and as well to data owner if its matching percentage will exceed threshold value.

Our design also provides primitive function for finding the K-nearest neighbours of large scale datasets. Also, for processing of K-nearest neighbours our system helps. This two-level design helps the proposed system to support easily for multimedia content like videos where in addition to matching the frames individually, the temporal aspect of videos also has to be considered. This is not with the case of images. The distributed matching engine of our design introduces the MapReduce programming model for faster processing or accessing of data.

## II. EXISTING SYSTEM

- One of the approaches is present for the protection of various types of multimedia contents i.e. watermarking. In this approach some distinctive information is embedded in content. Main purpose of this method is used to search for information order for verifying authenticity of the content.
- There are many methods are used for creating and matching signatures. Four categories are introduced by these methods: 1) Spatial, 2) Transform-domain, 3) Temporal, 4) Color. The block based i.e. spatial signatures are widely used.
- Some of the industrial examples such as YouTube, Content Id which uses Fingerprint method for protecting media.

## III. DRAWBACKS OF EXISTING SYSTEM

- For online videos which are rapidly increasing watermarking approach may not be effective, especially uploaded to the YouTube and many more hosting sites. For the already released content without watermark this method is not suitable.
- In case of large geometric transformation spatial signatures having lack of resilience. Transform domain signatures are intensive in nature. To enhance spatial signatures temporal and color are used.

## IV. LITERATURE SURVEY

Number of studies introduced the need of security in cloud computing especially for the multimedia content storage and the various proposed techniques to enhance security. Rongxing et al [2] a new security and forensics and post examination in cloud computing introduced in this paper. Also introduces provenance proposal for data. According to them their proposed system can provide the privacy and security on secret documents/files that are piled up in the cloud. To control unauthorized user access, they provides secure authentication mechanism and provides track mechanism to resolves disputes of data.



Their proposed scheme is working on the bilinear pairing method. La.,Quata Sumter et al. [3] says: The rise in the scope of — the threat of security in cloud computing is continuously increasing. They have proposed the system that will capture the recording and processing of the information kept on the cloud for assuring users that there information is secure, and not accessible to unauthorized people. Wenchao et al. [5] in this paper have explored the security properties of secure data sharing the applications which hosted on clouds. They have proposed a Declarative Secure Distributed Systems (DS2) which is a new security platform for cloud computing. Soren et al [6] Says: benefits of clouds are shadowed with the security, safety and privacy. For analysing security at client side and server side an approach has been presented in this paper. Amazon's Elastic Compute Cloud (EC2) has been chosen for this assessment. They have introduced the security analysis model. And also introduces weigh up it for realistic environments. In Python, security assessment has been implemented and weigh up was calculated on Amazon EC2. [9] Presented the fundamental concept and a framework of multimedia cloud computing. They addressed multimedia cloud computing from multimedia-aware cloud and cloud-aware multimedia perspectives. Tamleek Ali [11] for secure dissemination of protected multimedia content proposed a framework for the use of cloud computing. They have leveraged the UCON model. Chun-Ting Huang [13] this paper conduct a depth survey on recent multimedia storage security research activities in association with cloud computing. They focus on four hot research topics. Data integrity, data confidentiality, access control, and data manipulation in the encrypted domain.

## V. PROPOSED SYSTEM

- The system supports multimedia content types like images and videos etc. The system we present is a novel system used for multimedia copyright protection on cloud infrastructure.
- The proposed system is completely based on cloud system for multimedia copyright protection. The system efficiently utilizes varying computing resources.
- Novel method which is used creating signatures for images creates signature that takes input as image which will be uploaded. After that method applies Data Encryption Algorithm (DES) and creates unique signature.
- Novel method for matching signatures for creating percentage of matching signatures. It takes the signature from the database stored by the distributed matching engine and uses it to compare it with illegal distribution of multimedia content copies.
- The proposed system also offers a primitive function for finding the K-nearest neighbors and also processing of K-nearest neighbors. This two-level design helps the proposed system to support easily for multimedia content especially videos where the temporal aspect of videos also has to be considered, in addition to matching the frames individually.

- The focus of this paper is on approach for copyright protection for multimedia content on cloud. In this approach, the signature is created for the uploaded images and videos at the time of uploading and then that signature is used to compare with illegal copies by extracting their signatures. Then the signatures are compared to find the matching percentage of copyright violated images or videos.

## VI. SYSTEM ARCHITECTURE

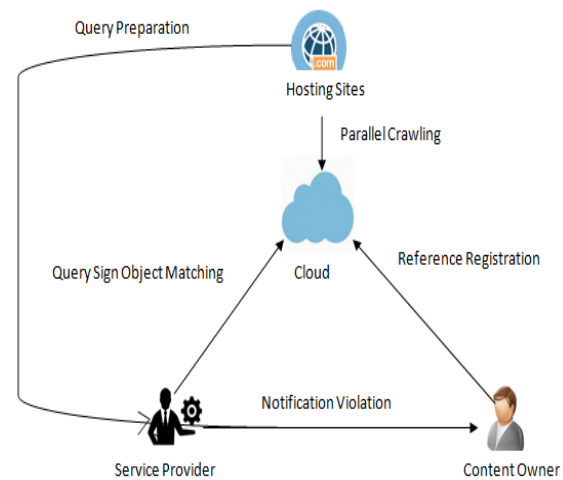


Fig. 2 System Architecture

The figure shows the general case where one or more cloud providers can be used by the system. The proposed system can be managed by any of the three parties mentioned in this section: content owners, hosting sites, or service providers.

- **Distributed Index:** Maintains signatures of protected objects.
- **Reference Registration:** Creates signatures from objects that content owner want to protect, and inserts them in the distributed index.
- **Query Preparation:** Creates signatures from objects downloaded from online sites, which are called query signatures and uploads these signatures to a common storage;
- **Object Matching:** Compares query signatures and reference signatures in the distributed index to find potential copies. It also sends notifications to content owners once copies are found;
- **Parallel Crawling:** Downloads multimedia objects from various online hosting sites. For the Crawling component, we designed and implemented a parallel crawler and used it to download videos from YouTube and many other websites. The details of the crawler are omitted due to space limitations.

## VII. ADVANTAGES OF PROPOSED SYSTEM

- The system shows accurate results i.e. system provides high accuracy.



- It maintains scalability.
- It provides reliability.
- Computing resources used by the system efficiently i.e. it is fully cloud-based system on demand basis.
- It uses the computing resources on demand that's why the system is cost effective.
- The system can be present on public and/or private clouds.

The key is in encrypted form before saving into database that's why if any unauthorized user will try to get the key of the multimedia content, then he will not be able to misuse the content of data owner. Again DES is performed, hence double encryption is provided. No need of decryption of signature of the copyrighted data.

### VIII. CONCLUSION

The unauthorized multimedia content redistribution on any hosting sites on cloud can led to the significant loss of revenues of the data owner. It can be very complex to build a system that will detect the illegal copies of multimedia content. It has to detect all the multimedia content which is large in number. In this we introduced a novel system for multimedia copyright protection system using cloud-based infrastructure. The proposed system supports multimedia content like images and videos etc. And this system can be deployed on private and/or public clouds. Our system contains two key components: - i) a method of creating signature of multimedia content like images and videos.

Our system uses data encryption algorithm and uses input as video which will be uploaded. At the time of creation of signature of video uses frames per rate of ii) the distributed matching engine, which is used for matching the percentage of matching signatures. The MapReduce framework used by the distributed matching engine for fast processing of operations.

The system efficiently utilizes varying amounts of We performed experiments on cloud and our result showed that: (i) it creates unique signature of multimedia content, and (ii) distributed matching engine matches the signature of multimedia content with illegal copies to find the percentage of matching multimedia contents such as images or videos. The system can be further extended in various directions.

For example, this system can be extended to audio copyright protection. for any social sites the system can be useful.. Due to the notion of freedom of information and the ease of copying of original data and posting has led to copyright violation. This system is a new approach to provide copyright protection for data owner's multimedia content like images and videos. If any hosting site provides access for our system to be implemented for their site, then it will be great advantage for the data owner to

be relaxed for the security of their content since there copyrighted content will not be violated.

### REFERENCES

- [1] Mohamed Hefeeda , Senior Member, IEEE, Tarek ElGamal , Kiana Calagari, and Ahmed Abdelsadek , "Cloud-Based Multimedia Content Protection System", IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 17, NO. 3, MARCH 2015
- [2] Rongxing et al, "Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing", ASIACCS,,10, Beijing, China.
- [3] R. La.,Quata Sumter, "Cloud Computing: Security Risk Classification", ACMSE 2010, Oxford, USA
- [4] Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia (2009, Feb. 10); "Above the clouds: A Berkeley view of cloud computing" EECS Dept., Univ. California, Berkeley, No. UCB/EECS-2009-28 .
- [5] Wenchaot et al, "Towards a Data-centric View of Cloud Security", CloudDB 2010, Toronto, Canada
- [6] Soren Bleikertz et al, "Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds", CCSW 2010, Chicago, USA.
- [7] Flavio Lombardi& Roberto Di Pietro, "Transparent Security for Cloud", SAC,,10 March 22-26, 2010, Sierre, Switzerland.
- [8] Sara Qaisar; "Cloud Computing, Network/Security Threats and Counter Measures", Interdisciplinary Journal of Contemporary Research In Business, Jan 2012, Vol 3, No 9.
- [9] Wenwu Zhu, Chong Luo , Jianfeng Wang, and Shipeng Li, "Multimedia Cloud Computing", Digital Object Identifier 10.1109/MSP.2011.940269 Date of publication: 19 April 2011.
- [10] Jiann-Liang Chen, Szu-Lin Wu, Yanuaris Teofilus Larosa, Pei-Jia Yang, and Yang-Fang Li, "IMS Cloud Computing Architecture for High-Quality Multimedia Applications", 978-1-4577-9538-2/11/\$26.00 ©2011 IEEE.
- [11] Tamleek Ali, Mohammad Neumann, Faze-e-Hadi ,and Fahd bin Muhaya; "On Usage Control of Multimedia Content in and through Cloud Computing Paradigm".
- [12] Zhang Mian, Zhang Nong, "The Study of Multimedia Data Model Technology Based on Cloud Computing", 2010 2nd International Conference on Signal Processing Systems (ICSPS).
- [13] Chun-Ting Huang, Zhongyuan Qin, C.-C. Jay Kuo, "Multimedia Storage Security in Cloud Computing: An Overview", 978-1-4577-1434-4/11/\$26.00©2011IEEE.
- [14] Neha Jain and Gurpreet Kaur, "Implementing DES Algorithm in Cloud for Data Security", VSRD-IJCSIT, Vol. 2 (4), 2012, 316-321.
- [15] N. Saravanan, A. Mahendiran , N. Venkata Subramanian, "An Implementation of RSA Algorithm in Google Cloud using Cloud SQL", Research Journal of Applied Sciences, Engineering and Technology 4(19): 3574-3579, October 01, 2012.
- [16] M. Sudha, Dr.Bandaru Rama Krishna Rao, "A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment", International Journal of Computer Applications (0975 – 8887) Volume 12– No.8, December 2012.
- [17] Priyanka Arora, Arun Singh, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and Information Technology Journal (WCSTIT) ISSN: 2221-0741 Vol. 2, No. 5, 179-183, 2012.

### BIOGRAPHIES



**Nivedita Kaonde** is pursuing B. E. in Information Technology from AGTI's Dr. Daulatrao Aher College Of Engineering, Karad, India. My area of Interest is Cloud Computing.





**Shital P. Kakade** received Diploma in Electrical Engineering from Government Polytechnic Karad, Maharashtra in 2003. B. E. degree from Annasaheb Dange College of Engg . Ashta (Sangli) Maharashtra in Information Technology in 2007, the M. Tech degree from Bharati

Vidyapeeth College of Engg. Pune, Maharashtra in 2014. From August 2007 to June 2008 she worked as an Assistant Professor in Department of Information Technology of Rajendra Mane College of Engg. And Technology Devrukh Dist. Ratnagiri, Maharashtra. Since July 2008 she is working as an Assistant Professor in Information Technology Department of Dr. Daulatrao Aher College of Engineering, Karad, District Satara, Maharashtra. Her area of interest includes Database, Security.