ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

National Conference on Innovative Applications and Research in Computer Science and Engineering (NCIARCSE-2017)

AGTI's Dr. Daulatrao Aher College Engineering, Vidyanagar Extension, Karad

Vol. 4, Special Issue 4, January 2017

Copyright Protection for Multimedia Content on Cloud

Miss. Dikshita R. Shetty[1], Prof. Shital P. Kakade[2]

Student, Department of Information Technology, AGTI's DACOE, Karad, India[1]

Assistant Professor, Computer Science and Eng, AGTI's DACOE, Karad, India[2]

Abstract: Cloud computing is the Internet regarded as a shapeless omnipresent space for processing and storage. Cloud computing can be defined with having two word which includes "cloud" means internet and "computing" means operations. In short, Cloud Computing can be defined as an internet based operations. Multimedia copyright protection on cloud is a legal way of protecting user's data which means that whatever data the user has created and uploaded cannot be used or published by anyone else without the consent of the user. 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. This system explores detection of copyright violation of multimedia content like images and videos and will create a method to deny access for uploading such copyright violated images and videos. To keep uploaded data to be copyright protected and deny uploading of copyright violated data by other user's, various methods have been proposed in this literature.

Keywords: cloud, multimedia, DES, security, copyright.

I. INTRODUCTION

There has been tremendous benefits for multimedia cloud computing and has much challenges like Network heterogeneity, Device heterogeneity , Multimedia and service heterogeneity, Security, Power Consumption, QoS heterogeneity which has to be met. But besides this there is also a big challenge for data security and access control when users upload their data which can be in the form of multimedia content for sharing on cloud. This system travels through a new method of creating and comparing signatures of data on cloud for enhancing security for copyright protection of multimedia content like images and videos. This system can be deployed on private and/or public clouds. The system has two new components: (i) method of creating signatures of multimedia content (ii) distributed matching engine to match the signatures. The signature method will create a strong and unique signature while uploading multimedia content like image and video and this method will be used for computation and comparing. The distributed matching engine obtains high scalability. Development in storing and processing data of multimedia content and due to the availableness of free online hosting sites has led to easeful of duplicating the copyrighted multimedia data such as images and videos.

Such unauthorized redistribution of multimedia content on the cloud can led to eloquent loss of revenues for the owner of data. Since there is large amount of multimedia content residing over the internet and finding unauthorized copies over the internet is very complex task and comparing of unauthorized copies with authorized copies is very complex and will be very costly which is not affordable. We design a system for multimedia copyright protection on cloud infrastructure. The system can be used to protect the copyright of multimedia content like images and videos. The system can run on private or public cloud or even in any combination of public and private clouds. Since our system is based on infrastructure of cloud which provides fast access to computing software and hardware resources hence there is assurance of fast deployment of multimedia copyright protection. As in cloud, computing resources are used on demand basis, our system is cost effective. The system can provide scalability by scaling up and down for supporting large volumes of multimedia content to be copyright protected. The proposed system is somewhat complex since it includes two components which include: (i) a method to create signature of multimedia content like images and videos while uploading the content on any online hosting site on cloud and (ii) distributed matching engine will store signatures of authorized uploaded multimedia content and will match them against unauthorized 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 animal called koala and choose Flicker as a hosting site and uploaded that image on DriveHQ Cloud File Server.

Then one signature was created for the uploaded image 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

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
National Conference on Innovative Applications and Research in Computer Science and Engineering (NCIARCSE-2017)
AGTI's Dr. Daulatrao Aher College Engineering, Vidyanagar Extension, Karad
Vol. 4, Special Issue 4, January 2017

achieved copyright protection. Then we tried to upload the same image and saved it with different name and tried with different hosting sites, then the signature was created and again we received the message that this image already exists, and image failed to upload hence we achieved copyright protection. Then 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 we tried for videos and got success in performing copyright protection. We found accuracy even if the videos were subjected to various transformations such as cropping, blurring or even text insertion.

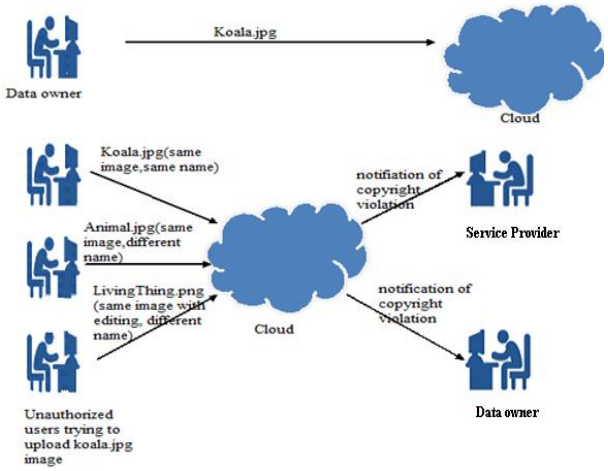

Fig. 1 Example of copyright protection of image

The contribution of this paper is as follows:

- The system is fully cloud based system used for multimedia copyright protection
- The system supports multimedia content like images and videos
- The system efficiently utilizes varying cloud computing resources
- 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) to produce a sixteen bit digital signature which randomly takes first and last eight bits of codec. If the signature matches with any of the uploaded images 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.
- The system uses a method to create signature of videos by taking input as frames per rate of videos and applies Data Encryption Algorithm (DES) which captures the depth of signature in stereo content. If the signature of uploaded frames per rate of videos will match with any of the 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 helps for providing primitive function for finding the K-nearest neighbours of large scale datasets. Also, our system helps for processing of K-nearest neighbours. 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 employs the MapReduce programming model for faster processing of data.

II. EXISTING SYSTEM

- The need to protect all the multimedia content has increased especially from industry and academia. The existing approach uses watermarking approach in which discrete information of multimedia content is embedded in the content itself and this method is also used to search this information in order to justify the authenticity of the multimedia content.

Advantages of watermarking:

- Watermarking is a method uniquely identifies the author of copyrighted content.
- Watermarking method can be implemented of personal computer.
- Watermarking method uses technique of embedding of distinctive information in content with a ease.
- There are different methods for creating and matching signatures proposed previously. These methods are classified into four groups: spatial, color, temporal and transform domain. The spatial signature is a block-based method is the most widely used.
- Some industries use fingerprinting for multimedia content protection, for example in Youtube, Vobile VDNA, and Content ID.

III. DRAWBACKS OF EXISTING SYSTEM

- Watermarking approach may be unsuitable for the multimedia content which is already released without watermarks in them.
- Watermarking approach doesn't protect image copying but we can track down and detect ownership of copyrighted images.
- Watermarking approach vanishes if someone manipulates the image.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
National Conference on Innovative Applications and Research in Computer Science and Engineering (NCIARCSE-2017)
AGTI's Dr. Daulatrao Aher College Engineering, Vidyanagar Extension, Karad
Vol. 4, Special Issue 4, January 2017

- Compression of images and resizing of images from one file type to another may decline the watermark and it becomes difficult to read.
- Watermarking approach may not be capable for the rapidly growing online videos those are uploaded to online hosting sites like YouTube and played back by any media player.

Spatial signatures impairment is the lack of resilience against large geometric transformations. Color and Temporal are not much robust and these methods can be used to enhance spatial signatures. Transform-domain signatures are not mostly used in practice since they are computationally intensive.

IV. LITERATURE SURVEY

In cloud computing, there is need for security for multimedia content storage and various techniques to enhance security. Ronxing et al[2] In this paper, there is a new security and provenance proposal for data forensic and post examination in cloud computing. According to them their proposed system can provide the privacy and security on secret files that are piled up on the cloud. It also provides security on authentication mechanism to detect an unauthorized user access, and provides trace mechanism to resolves problem of conflict of data. They proposed secure derivation scheme which is working on the bilinear Pairing method. La, Quatta sumter et al [3] This paper shows the increase in the scope of cloud computing has brought fear about security on the internet and continuously increasing threat of security on cloud computing. To assure users that their information is secure, safe not accessible to unauthorized people, they have proposed architecture of system that will capture the activities and processing of the information kept on the cloud. Wenchao et al [5] In this paper, they have explored security properties of secure sharing of data among the applications hosted on the clouds. They have proposed new security platform for cloud computing, which named as Declarative Secure Distributed Systems (DS2). Soren et al [6] In this paper, they included benefits of clouds are shadowed with security, safety and privacy. In this paper an approach has been presented to analyze security at client as well as server side. Amazons Elastic Compute Cloud (EC2) has been chosen for this assessment; they have implemented security model weigh up it for realistic environments. Security assessment has been implemented in python and weigh up was calculated on Amazon EC2.

Flavi and Roberto [7] stated that clouds are being focused increasingly day by day. In this paper Integrity protection problem in the clouds, design a novel Architecture and transparent cloud protection system (TCPS) for improved security of cloud services has been discussed. Wenwu Zhu et al [9] this paper presented the fundamental concept and framework of multimedia cloud computing. They addressed multimedia cloud computing from multimedia-aware cloud and cloud-aware multimedia perspectives. Tamleek Ali [11] proposed a framework for the use of cloud computing for secure dissemination of protected multimedia content as well as document and rich media. They have leveraged the UNCON model for enforcing fine-grained continues usage control constraint on object residing in the cloud. Chun Ting Haung [13] conduct depth survey on recent multimedia storage security research activities in association with cloud computing. After an overview of the cloud storage system and its security problem, they focus on four hot research topics. They are data confidentiality, data integrity, access control, and data manipulation in the encrypted format. Neha Jain [14] presented data security in cloud computing using DES algorithm. N Saravanan et al [15] presented security on data in cloud computing using RSA algorithm. They have implemented RSA algorithm in Google App engine using cloud SQL.

V. PROPOSED SYSTEM

- The system we present is a novel system used for multimedia copyright protection on cloud infrastructure. The system supports multimedia content types like images and videos.
- The proposed system is completely based on cloud system for multimedia copyright protection. The system efficiently utilizes varying computing resources.
- Novel method for creating signatures for images. This method creates signature that takes input as image which will be uploaded and apply Data Encryption Algorithm (DES) and creates unique signature.
- Novel method for matching signatures for creating percentage of matching signatures. The distributed matching engine stores the signature into the database 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 image 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

- **Data owner**: The user who creates the data and uploads the data on cloud on any online hosting sites.
- **Service provider**: The organization who provides the services for accessing and using the internet

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
National Conference on Innovative Applications and Research in Computer Science and Engineering (NCIARCSE-2017)
AGTI's Dr. Daulatrao Aher College Engineering, Vidyanagar Extension, Karad
Vol. 4, Special Issue 4, January 2017

- **Reference Registration**: When data owner uploads any content for copyright that content, then Reference Registration creates signature for it.

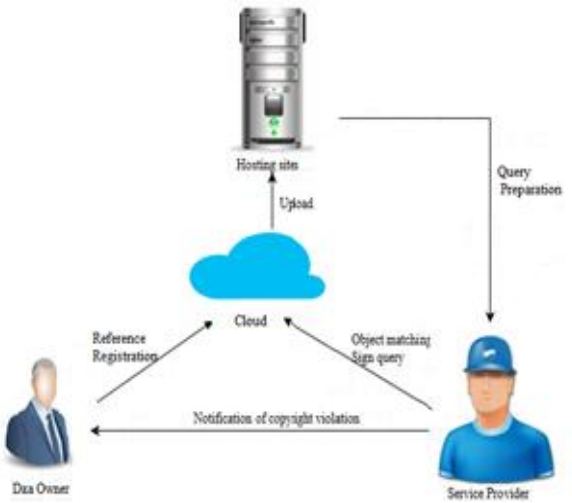

Fig. 1 System Architecture

- **Hosting sites**: It enables any website to be accessible through internet.
- **Query Preparation**: It creates signature from the contents which will be downloaded by any user from online hosting sites and that signature is termed as query signature.
- **Object Matching**: It compares query signatures versus reference signatures in the distributed index (stores signatures of copyrighted content) to find illegal copies. If any violation of copyrighted content will occur then Service provider sends notification to data owner.

VII. IMPLEMENTATION

The unauthorized multimedia content redistribution on any hosting sites on cloud can led to the significant loss of revenues of the data owner. If we try to build a system that will detect the illegal copies of multimedia content, then it can be very complex system since it has to detect all the multimedia content which is large in number. In this paper, we presented new design for multimedia copyright protection system using cloud-based infrastructure. The proposed system supports multimedia content like images and videos and this system can be deployed on public and/or private cloud. There are two key components which build our system. The first one is a method of creating signature of multimedia content like images and videos. Our system applies data encryption algorithm and uses input as an image which will be uploaded to create signature of images and uses frames per rate of videos to create signature of videos. In case of videos, the system captures the depth signal of videos. Our system provides accuracy in terms of both recall and precision and it is robust to any video transformations. The second component is the distributed matching engine, which matches the percentage of matching signatures. The distributed matching engine uses the Map Reduce framework for fast processing of operations since it efficiently utilize varying amount of computing resources and it provides high accuracy of the result.

The DES algorithm works as following:
STEP-1 First, pick the any file, image and/ or video and upload these at cloud computing work.
STEP-2 The DES uses the first eight bits and last bits of codec of image and frames per rate of video to create digital signature.
STEP-3 Image or video is shown at DriveHQ Cloud Computing.
STEP-4 If any user tries to upload image or video which exactly matches the signature of copyrighted content, then image will be discarded.
STEP-5 If any user tries to upload image or video by editing the copyrighted content, then the percentage of matching signature will be send as a notification to service provider and data owner who will have the rights to delete the data if they find it as copyright violated.

VIII. ADVANTAGES OF PROPOSED SYSTEM

- The system shows high accuracy.
- The system maintains scalability, it can scale up and down to support varying number of multimedia contents being copyright protected.
- The system provides reliability.
- The system uses computing resources efficiently, since it is fully cloud-based system it can quickly provide computing hardware and software resources on demand basis.
- The system is cost effective since it uses the computing resources on demand.
- The system can run on public and/or private clouds.
- If any unauthorized user will try to get the key of the multimedia content, then also he will not be able to misuse the content of data owner since the key is encrypted before saving into database and again DES is performed, hence double encryption is provided. No any need of decryption of signature of the copyrighted data.

IX. CONCLUSION

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 images or videos. The system can be further extended in various directions. For example, this system can be extended to audio copyright protection. In crime branch, the system can be used to find the biography of criminals by matching their images with the data stored on internet. The system can also be useful for any social sites where the user wants to apply copyright

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

National Conference on Innovative Applications and Research in Computer Science and Engineering (NCIARCSE-2017)

AGTI's Dr. Daulatrao Aher College Engineering, Vidyanagar Extension, Karad

Vol. 4, Special Issue 4, January 2017

protection for his content. Here the advantage is that copyright is automatically provided to the content of data owner as soon as he uploads his multimedia content like images or videos. The data owner does not have to formally register the multimedia content for copyright protection. The development of internet is now becoming a lair of copyright abuse. Due to the notion of freedom of information and the ease of copying of original data and posting has led to copyright violation. Our 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] Wenchaoet 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, Yanuarius 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 Nauman, Fazl-e-Hadi ,and Fahad 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 (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5, 179-183, 2012.

BIOGRAPHIES

Dikshita Shetty is percesuing B. E. from AGTI's DACOE, Karad, India. Her 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 DACOE, Karad, District Satara, Maharashtra. Her area of interest includes Database, Security.