ISSN 2395-1621

# Multimedia Content Protection System for Cloud Based Multimedia

[#1]Priyanka V. Padwal, [#2]Prof. Sable N.P.

[1]padwalpriya1430@gmail.com
[2]nileshraje143@gmail.com

[#12]Department of Computer Engineering, Imperial College of Engineering & Research, Wagholi, Pune, India

**ABSTRACT**

**Cloud computing provides an emerging paradigm where computing resources make available as service of the Internet. This paradigm provides facility to Customer to Consumer and businesses without installation of this application and provides access to personal files at any computer with internet access. Internet multimedia computing provides technology to generate, process, search, and edit media contents, such as images, video, audio, graphics, and so on. Multimedia cloud computing has the potential for tremendous benefits, but wide scale adoption has number of difficulties/problems like *service and Multimedia,* QoS heterogeneity, heterogeneity, Device heterogeneity , Network heterogeneity Security, Power Consumption that must be met. But data security and access control is the main challenge when users outsource sensitive but when user try's to share data on cloud servers which is out of scope of trusted domain, data security and access control become main challenge. To keep data secure against untrusted servers, different approaches have been proposed in the literature. This paper explores a new method signature verification to enhance security when storing text, image, audio, video files onto cloud server. The proposed system provides facility to secure different multimedia information like, Images, 2-D videos, 3-D videos, audio clips, songs, and music clips. The proposed system can be publicly and privately make available on clouds. This system has two novel components: (i) Novel approach to generate signatures of 3-D videos, and (ii) For multimedia objects provides distributed matching engine. The signature method creates robust and representative signatures of 3-D videos that capture the strong signals in these videos and it is computationally powerful to compute and compare as well as it requires small storage. The distributed matching engine gain high scalability and it provide support for different multimedia object.**

**Keywords -** copy detection video,depth signatures, 3-D video, video fingerprinting, cloud applications

ARTICLE INFO

**Article History**

Received :24th December 2015

Received in revised form :

25th December 2015

Accepted : 26th December , 2015

**Published online :**

**28th December 2015**

## I. INTRODUCTION

Advances in processing and recording equipment of multimedia content as well as the availability of free online hosting sites have made it relatively easy to duplicate copyrighted materials such as videos, images, and music clips. Result is significantly loss of revenue when illegally redistributing content multimedia over the Internet can result in significant loss of revenues for content creators. Finding illegally-made copies over the Internet is a complex and computationally expensive operation, because of the sheer volume of the available multimedia content over the Internet and the complexity of comparing content to identify copies. We present an innovative system for protection of cloud based multimedia. The system can be used to protect various multimedia content types, including regular 2D videos, new 3D videos, images, audio clips, songs, and music clips. The novel system can run on public clouds, private clouds, or combination of private- public or public-private clouds. Our system gain fast deploying the protection of system content because it is related to cloud infrastructures that can quickly provide computing

hardware and software resources. On demand it uses the computing resources for thus our design is cost effective. System support to protecting various amount of multimedia content because our system can be scaled up and down. The novel system is quite complicated with different components, like: (i) Crawler to download thousands of multimedia objects from online hosting sites, (ii) Signature approach to generate ideal fingerprints from multimedia objects, and (iii) distributed matching engine to store signatures of original objects and match them against query objects. We are going to put forth new method in case of $2^{nd}$ as well as $3^{rd}$ element, and we also apply commercial tools for the crawler. We have evolved a fully running system of all elements and examined it with more than 11,000 3D videos and 1 million images. We deployed parts of the system on the Amazon cloud with varying number of machines (from 8 to 128), and the other parts of the system were deployed on our private cloud. This deployment model was used to show the flexibility of our system, which enables it to efficiently utilize varying computing resources and minimize the cost, since cloud providers offer different pricing models for computing and network resources. Through extensive experiments with real deployment, we show the high accuracy (in terms of precision and recall) as well as the scalability and elasticity of the proposed system. The contributions of this paper are as follows: • Complete multi-cloud system for multimedia content protection. The system supports different types of multimedia content and can effectively utilize varying computing resources.• Novel method for creating signatures for 3D videos. This method creates signatures that capture the depth in stereo content without computing the depth signal itself, which is a computationally expensive process. New design for a distributed matching engine for high-dimensional multimedia objects. This design provides the primitive function of finding K-nearest neighbours for large-scale datasets. The design also offers an auxiliary function for further processing of the K neighbours. This two-level design enables the proposed system to easily support different types of multimedia content. For example, in finding video copies, the temporal aspects need to be considered in addition to matching individual frames. This is unlike finding image copies. Our design of the matching engine employs the Map Reduce programming model. Rigorous evaluation study using real implementation to assess the performance of the proposed system and compare it against the closest works in academia and industry. Specifically, we evaluate the entire end-to-end system with 11,000 3D videos downloaded from YouTube. Our results show that a high precision, close to 100%, with a recall of more than 80% can be achieved even if the videos are subjected to various transformations such as blurring, cropping, and text insertion. In addition, we compare our system versus the Content ID system used by YouTube to protect videos. Our results show that although the Content ID system provides robust detection of 2D video copies, it fails to detect copies of 3Dvideos when videos are subjected to even simple transformations such as re-encoding and resolution change. Our system, on the other hand, can detect almost all copies of 3D videos even if they are subjected to complex transformations such as synthesizing new virtual views and converting videos to anaglyph and 2D-plus-depth formats.

## II. EXISTING SYSTEM

- The problem of protecting various types of multimedia content has attracted significant attention from academia and industry. One approach to this problem is using watermarking, in which some distinctive information is embedded in the content itself and a method is used to search for this information in order to verify the authenticity of the content.

- Many previous works proposed different methods for creating and matching signatures. These methods can be classified into four categories: spatial, temporal, color, and transform-domain. Spatial signatures (particularly the block-based) are the most widely used.

- Youtube Content ID, Vobile VDNA, and MarkMonitor are some of the industrial examples which use fingerprinting for media protection, while methods such as can be referred to as the academic state-of-the-art.

## III. DRAWBACKS OF EXISTING SYSTEM

- Watermarking approach may not be suitable for already-released content without watermarks in them. Watermarking may not be effective for the rapidly increasing online videos, especially those uploaded to sites such as YouTube and played back by any video player.
- Spatial signatures weakness is the lack of resilience against large geometric transformations. Temporal and color signatures are less robust and can be used to enhance spatial signatures. Transform-domain signatures are computationally intensive and not widely used in practice.

## IV. LITERATURE SURVEY

Number of studies showing 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] in this paper gave a new security and provenance proposal for data forensics and post examination in cloud computing. According to them their proposed system can provide the privacy and security on secret documents/files that are piled up in the cloud. It also provides secure authentication mechanism to control unauthorized user access, and provides track mechanism to resolves disputes of data. Their proposed secure provenance scheme is working on the bilinear pairing method . La,,Quata Sumter et al. [3] says: The rise in the scope of ―cloud computing has brought fear about the Internet Security and the threat of security in cloud computing is continuously increasing .To assure users that there information is secure, safe not accessible to unauthorized people, they have proposed the design of

a system that will capture the movement and processing of the information kept on the cloud. Wenchao et al. [5] in this paper have explored the security properties of secure data sharing among the applications hosted on clouds. They have proposed a new security platform for cloud computing, which is named as Declarative Secure Distributed Systems (DS2). Soren et al [6] in this paper have mentioned that benefits of clouds are shadowed with the security, safety and privacy .In this paper an approach has been presented for analysing security at client side and server side. Amazon„s Elastic Compute Cloud (EC2) has been chosen for this assessment. They have implemented the security analysis 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 targeted increasingly day by day. In this paper integrity protection problem in the clouds, sketches a novel Architecture and Transparent Cloud Protection System (TCPS) for improved security of cloud services has been discussed. Wenwu Zhu et.al [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] proposed a framework for the use of cloud computing for secure dissemination of protected multimedia content as well as documents and rich media. They have leveraged the UCON model for enforcing fine-grained continuous usage control constraints on objects residing in the cloud. Chun-Ting Huang [13] conduct a 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 integrity, data confidentiality, access control, and data manipulation in the encrypted domain. Neha Jain [14] presented a data security system in cloud computing using DES algorithm. N. Saravanan et.al [15] presented a data security system in cloud computing using RSA algorithm. They have implemented RSA algorithm in Google App engine using cloud SQL.

## V. PROPOSED SYSTEM

- We developed new system for multimedia content protection on cloud framework. This novel system can be used to protect different multimedia content types.
- In our novel system we evolved fully multi-cloud system for multimedia content protection. The proposed system supports various types of multimedia content and can actively occupy varying computing resources.
- New approach can be used generating signatures for videos. This novel approach generates signatures that occupy the depth in stereo content without computing the depth signal itself, which is a computationally expensive process.
- The novel design for capture high-dimensional multimedia objects for distributed matching engine. This design provides the primitive function of finding -nearest neighbours for large-scale datasets.
- The design also offers an auxiliary function for further processing of the neighbours. This two-stage design used in novel system to easily support various types of multimedia content.
- The focus of this paper is on the other approach for protecting multimedia content, which is content-based copy detection (CBCD). In this proposed system from original objects, signatures are extracted. Signatures are also generated from query and objects downloaded from web. Then, the complimentary is measure between original and suspected objects to find potential copies.

**SYSTEM ARCHITECTURE**

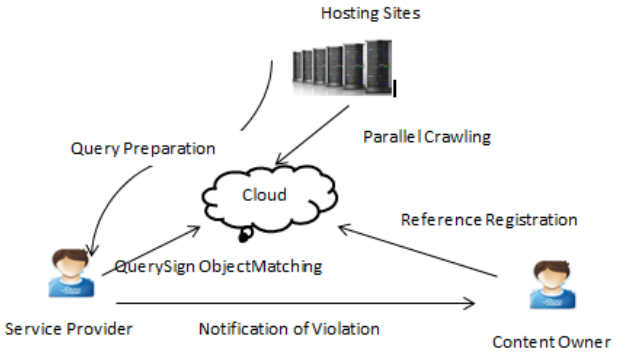


Fig 1. System Architecture

**ADVANTAGES OF PROPOSED SYSTEM**

- Accuracy.
- Computational Efficiency.
- Scalability and Reliability.
- Cost Efficiency.
- The system can run on private clouds, public clouds, or any combination of public-private clouds.
- Our design achieves rapid deployment of content protection systems, because it is based on cloud infrastructures that can quickly provide computing hardware and software resources.
- The design is cost effective because it uses the computing resources on demand.
- The design can be scaled up and down to support varying amounts of multimedia content being protected.

## VI. CONCLUSION

Distributing copyrighted multimedia objects by uploading them to online hosting sites such as YouTube can result in significant loss of revenues for content creators. Systems needed to find illegal copies of multimedia objects are complex and large scale. In this paper, we presented a new design for multimedia content protection systems using multi-cloud infrastructures.

The proposed system supports different multimedia content types and it can be deployed on private and/or public clouds. Two key components of the proposed system are presented. The first one is a new method for creating signatures of 3-D videos. Our method constructs coarse-grained disparity maps using stereo correspondence for a sparse set of points in the image. Thus, it captures the depth signal of the 3-D video, without explicitly computing the exact depth map, which is computationally expensive. Our experiments showed that the proposed 3-D signature produces high accuracy in terms of both precision and recall and it is robust to many video transformations including new ones that are specific to 3-D videos such as synthesizing new views. The second key component in our system is the distributed index, which is used to match multimedia objects characterized by high dimensions. The distributed index is implemented using the MapReduce framework and our experiments showed that it can elastically utilize varying amount of computing resources and it produces high accuracy. The experiments also showed that it outperforms the closest system in the literature in terms of accuracy and computational efficiency. In addition, we evaluated the whole content protection system with more than 11,000 3-D videos and the results showed the scalability and accuracy of the proposed system. Finally, we compared our system against the Content ID system used by YouTube. Our results showed that: (i) there is a need for designing robust signatures for 3-D videos since the current system used by the leading company in the industry fails to detect most modified 3-D copies, and (ii) our proposed 3-D signature method can fill this gap, because it is robust to many 2-D and 3-D video transformations. The work in this paper can be extended in multiple directions. For example, our current system is optimized for batch processing. Thus, it may not be suitable for online detection of illegally distributed multimedia streams of live events such as soccer games. In live events, only small segments of the video are available and immediate detection of copyright infringement is crucial to minimize financial losses. To support online detection, the matching engine of our system needs to be implemented using a distributed programming framework that supports online processing, such as Spark. In addition, composite signature schemes that combine multiple modalities may be needed to quickly identify short video segments. Furthermore, the crawler component needs to be customized to find online sites that offer pirated video streams and obtain segments of these streams for checking against reference streams, for which the signatures would also need to be generated online. Another future direction for the work in this paper is to design signatures for recent and complex formats of 3-D videos such as multiview plus depth. A multiview plus depth video has multiple texture and depth components, which allow users to view a scene from different angles. Signatures for such videos would need to capture this complexity, while being efficient to compute, compare, and store.

## 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.