International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

Secured Multimedia Content in Cloud

Yanamala Narendra & G.V.Manikanth
1PG Scholar, Dept of CSE, Prakasam Engineering College, kandukur,Prakasam(Dt), AP, India.
2Assistant Professor, Dept of CSE, Prakasam Engineering College,kandukur, Prakasam(Dt), AP, India.

ABSTRACT: *Cloud computing is getting more popular in the field of computer science because of its reliability instoring and assessing data remotely. Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services of the internet. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. It allows user to store large amount of data in cloud storage and use as and when required, from any part of the world, via any terminal equipment. Since cloud computing is rest on internet, security issues like privacy, data security, confidentiality, and authentication is encountered. we propose a new design for large-scale multimedia content protection systems. Our design leverages cloud infrastructures to provide cost efficiency, rapid deployment, scalability, and elasticity to accommodate varying workloads. The proposed system can be used to protect different multimedia content types, including 2-D videos, 3-D videos and images. The system can be deployed on private and/or public clouds. Our system has two novel components: (i) method to create signatures of videos and images, and (ii) distributed matching engine for multimedia objects. The signature method creates robust and representative signatures of videos and images that capture the depth signals in these videos and it is computationally efficient to compute and compare as well as it requires small storage. We implemented the proposed system and deployed it on two clouds: Amazon cloud and our private cloud.*

KEYWORDS: detection video; depth signatures; 3-D video; video fingerprinting; cloud applications.

I. INTRODUCTION

The cloud computing is internet based computer, shared software information and resources to world. We present a novel system for multimedia content protection on cloud infrastructures. 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 system can run on private clouds, public clouds, or any combination of public-private clouds. 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. The aim of this paper is on the other approach for protecting multimedia content, which content-based copy detection (CBCD). In this approach, signatures are extracted from original objects. Signatures are also created from query (suspected) objects downloaded from online sites. Then, the similarity is computed between original and suspected objects to find potential copies. The design also offers an auxiliary function for further processing of the neighbours. This two-level

design enables the proposed system to easily support different types of multimedia content. The system supports different types of multimedia content and can effectively utilize varying computing resources. Novel method for creating signatures for videos. This method creates signatures that capture the depth in stereo content without computing the depth signal itself, which is a computationally expensive process. This design provides the primitive function of finding -nearest neighbours for large-scale datasets. The focus of this paper is on the other approach for protecting multimedia content, which is content-based copy detection (CBCD). In this approach, signatures are extracted from original objects. Our results show that a matching index for video and images. . Digital signatures are used to detect unauthorized modifications to video and images. There are three algorithms that are suitable for digital signature generation used for copy detection process. The goal of the proposed system for multimedia content protection is to find illegally made copies of multimedia objects over the Internet. The system should have high accuracy in terms of finding all copies. *Computational Efficiency:* The system should efficient because system have short response time to report illegal copies of multimedia content, especially for timely multimedia ,system gives a matching index (%) for copied video and images. Digital signatures are generated by using the AES algorithm. Signature is based on the multimedia objects first 8 bit as well as last 8 bit or combination of both. 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 signature creation. The system also showed that it outperforms the closest system in the literature in terms of accuracy and computational efficiency.

II. OVERVIEW OF THE PROPOSED SYSTEM

The goal of the projected system for transmission content protection is to search out illicitly created copies of transmission objects over the web. In general, systems for transmission content protection square measure large-scale and sophisticated with multiple concerned parties. during this section, we tend to begin by distinctive the look goals for such systems and our approaches to attain them. Then, we tend to gift the high-level design and operation of our pro-posed system.

A. style Goals and Approaches

A content protection system has 3 main parties: (i) content owners(e.g.,Disney),
(ii)hosting sites (e.g., YouTube),and (iii) service suppliers (e.g., sounding Magic). the primary party is inquisitive about protective the copyright of a number of its transmission objects, by finding whether or not these objects or elements of them square measure denote on hosting sites (the second party). The third party is that the entity that gives the copy finding service to content house owners by checking hosting sites. In some cases the hosting sites supply the copy finding service to content house owners. associate degree example of this case is YouTube, that offers content protection services. And in different, less common, cases the content house owners develop and operate their own protection systems. we tend to outline and justify the subsequent four goals because the most significant ones in transmission content protection systems.Accuracy: The system ought to have high accuracy in terms of finding all copies

(high recall) whereas not news false copies (high precision). Achieving high accuracy is challenging, as a result of traced transmission objects usually undergo numerous modifications (or transformations). For ex-ample, traced videos may be subjected to cropping ,embed-ding in different videos, dynamic bit rates, scaling, blurring, and/or dynamic frame rates. Our approach to attain this goal is to extract signatures from transmission objects that square measure strong to as several transformations as attainable.

• Computational Efficiency: The system ought to have short latency to report copies, particularly for timely multimedia objects like sports videos. additionally, since several transmission objects square measure regularly other to on-line hosting sites, which require to be checked against reference objects, the content protection system ought to be able to method several objects over a brief amount of your time. Our approach to attain this goal is to create the signatures com-pact and quick to calculate and compare while not sacrificing their strength against transformations.

• Scalability and Reliability: The system ought to scale (up and down) to completely different variety of transmission objects. Scaling up suggests that adding a lot of objects thanks to monitoring a lot of on-line hosting sites, having a lot of content house owners victimization the system, and/or the prevalence of special events like sports tournaments and unleash of latest movies. Conversely, it's additionally attainable that the set of objects handled by the system shrinks, because, for instance, some content house owners might terminate their contracts for the protection service. Our approach to handle measurability is to style a distributed system that may utilize variable amounts of computing resources.

With large-scale distributed systems, failures oft times occur, that need the content protection system to be reliable in face of various failures. to deal with this reliability, we tend to style the core elements of our system on prime of the Map Reduce programming framework, that offers resiliency against differing kinds of failures.

• Cost Efficiency: The system ought to minimize the price of the required computing infrastructure. Our approach to attain this goal is to style our system to effectively utilize cloud computing infrastructures (public and/or private). Building on a cloud computing infrastructure additionally achieves the measurability objective mentioned higher than and reduces the direct value of the computing infrastructure.

B. Design and Operation

The projected cloud-based transmission content protection system is shown in Fig. 1. The system has multiple components; most of them square measure hosted on cloud infrastructures. The figure shows the final case wherever one or a lot of cloud suppliers may be utilized by the system. this is often as a result of some cloud suppliers square measure a lot of economical and/or offer a lot of value saving for various computing and communication tasks. for instance, a cloud supplier providing lower value for inward information measure and storage may be used for downloading and quickly storing videos from on-line sites (top cloud within the figure), whereas another cloud supplier (or non-public cloud) providing higher calculate nodes at lower prices may be accustomed maintain the distributed index and to perform the copy detection method (lower cloud within the figure). The projected system may be deployed and managed by any of the 3

parties mentioned within the previous section: content house owners ,hosting sites ,or service providers. The proposed system has the subsequent main elements, as shown in Fig. 1:

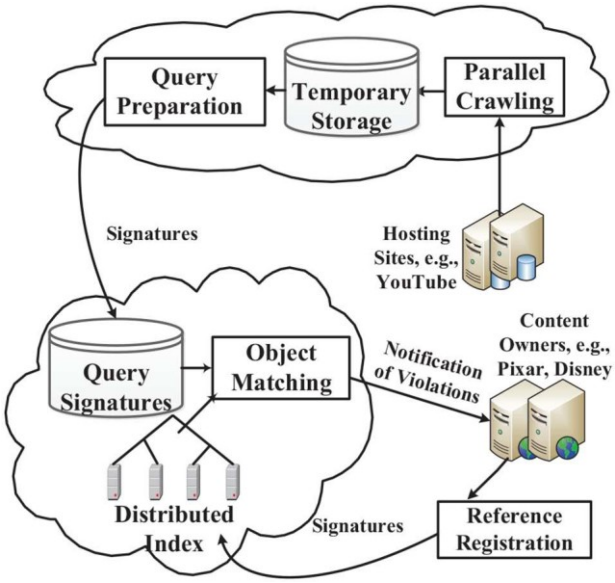

Fig. 1.Proposed cloud-based multimedia content protection system.

- Distributed Index: Maintains signatures of objects that need to be protected;
- Reference Registration: Creates signatures from objects that content owners are interested in protecting, and inserts them in the distributed index;
- Query Preparation: Creates signatures from objects down-loaded from online sites,which are called query signatures. It then uploads these signatures to a common storage;
- Object Matching: Compares query signatures versus reference signatures in the distributed index to find potential copies. It also sends notifications to content owners if copies are found;

- Parallel Crawling: Downloads multimedia objects from various online hosting sites.

The Distributed Index and Object Matching components form what we call the Matching Engine, which is described in Section V. The second and third components deal with signature creation, which is described in Section IV. For the Crawling component, we designed and implemented a parallel crawler and used it to download videos from YouTube. The details of the crawler are omitted due to space limitations. The proposed system functions as follows. Content owners specify multimedia objects that they are interested in protecting. Then, the system creates signatures of these multimedia objects (called reference objects) and inserts (registers) them in the distributed index. This can be one time process, or a continuous process where new objects are periodically added. The Crawl component periodically (e.g., once a day) downloads recent objects (called query objects) from online hosting sites. It can use some filtering (e.g., YouTube filtering) to reduce the number of downloaded objects. For example, for video objects, it can download videos that have a minimum number of views or be-long to specific genre (e.g., sports). The signatures for a query object are created once the Crawl component finishes down-loading that object and the object itself is removed. After the Crawl component downloads all objects and the signatures are created, the signatures are uploaded to the matching engine to perform the comparison. Compression of signatures can be performed before the upload to save bandwidth. Once all signatures are uploaded to the matching engine, a distributed operation is performed to compare all query signatures versus the reference signatures in the distributed index.

III. MATHEMATICAL MODEL

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

Let System is Z for describe Protection of Multimedia content with process illuminant estimation, The system have following elements in it. Let Z is the Whole System Consist of:

Z = { S; E; X; Y; F_{main}; DD; NDD; SW_r; HW_{rg} }

Where,

S= initial set such as Memory, Business Logics, Database.

E =the end of set where user can achieve result from hosting sites like YouTube.

X = {I1; I2}

Where, X= the set having two inputs I1 and I2,

I1 = used for uploading the video by Content owner ,

I2=Search Query

Y = {O1; O2}

Where Y is the set having two outputs O1 and O2

O1=search results

O2=Signature Violation Verification

F_{main}= Main Function

DD=Deterministic Data

NDD=Non Deterministic Data

1. Compute 8 bit for Left and Right visual parts of image:

For visual parts of image I is computed at a specific pixel in the image which has location of x_i, y_i .The result of this step is two sets of descriptors; one for left image and one for the right image.

$$D_i^L = (f_{i1}, f_{i1}, f_{i1}, f_{i1}, \dots\dots f_{iF}), i = 1,2, \dots, L_n$$
$$D_j^R = (f_{i1}, f_{i1}, f_{i1}, f_{i1}, \dots\dots f_{iF}), j = 1,2, \dots, R_n$$

2. Combine the left and right visual parts of images ($M_L : M_R$)

3. Matching visual parts of images:

4. Compute image disparity:

$$D_i^L - D_j^R = \sqrt{(f_{i1} - f_{j1})^2 + \dots + (f_{iF} - f_{jF})^2}$$

$$\sqrt{((x_i - x_j/W_b))^2 + ((y_i - y_j/H_b))^2}$$

IV. SYSTEM DESIGN AND DETAILS

3.1 Problem Definition

Protecting Various Multimedia Contents such as video and image by signature creation and Multimedia copy detection using matching index.

3.2 Proposed Architecture and work

By using composite signature creation method the accuracy and copy detection rate for image/video is improved Below figure 1 introduce the proposed architecture for overcome the limitations of previous methods. A content protection system has three main parties: (i) content owners (e.g., Disney), (ii) hosting sites (e.g., YouTube), and (iii) service providers (e.g., Audible Magic). The first party is interested in protecting the copyright of some of its multimedia objects, by finding whether these objects or parts of them are posted on hosting sites (the second party). The third party is the entity that offers the copy finding service to content owners by checking hosting sites. In some cases the hosting sites offer the copy finding service to content owners. An example of this case is YouTube, which offers content protection services. And in other, less common, cases the content owners develop and operate their own protection systems. The proposed system has the following main components, as shown in Fig. 1:

- **Content Owner:** View the video files and Images Uploading on online hosting sites such as YouTube.
- **Content Service Provider:** CSP Create Signature from object downloaded from online sites which are calledquery signatures then uploads this signature to a common storage.
- **Object Matching:** Compares query signature versus reference signatures which is previously created by serviceprovider also it sends notification to content owners if copies are found.

4. **User:** Downloads multimedia objects from various online hosting sites using the digital signature.

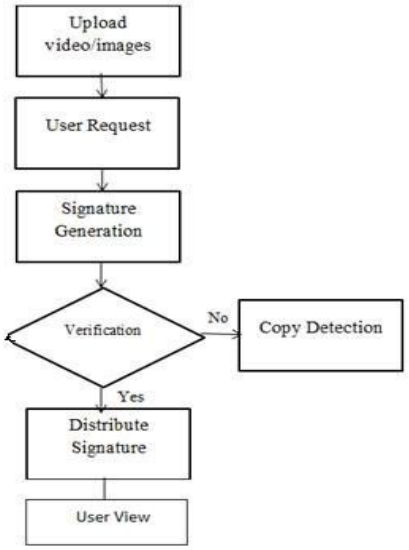

Fig. 1: System flow diagram

The Fig.1 shows data flow diagram of proposed system functions as: Content owners specify multimedia objects that they are interested in protecting. Then, the system creates signatures of these multimedia objects (called reference objects) and inserts (registers) them on online hosting sites such as YouTube. This can be one time process, or a continuous process where new objects are periodically added on hosting sites. The user (e.g., once a day) downloads recent objects (called query objects) from online hosting sites. It can modified downloaded video and again uploading same video on online hosting site then our system can compare reference signature and original signature for finding matching index to detect that copied video by using composite signature and achieve high accuracy in terms of detecting copied multimedia contents. Creation of composite signature for protecting Multimedia content i.e. videos and images. The signatures for a query object are created once the Crawl component finishes downloading that object and the object itself is removed.

Following four goals as the most important ones in multimedia content protection systems.

A. Computational Efficiency: The system should have short response time to report copies, especially for timelymultimedia objects such as sports videos. In addition, since many multimedia objects are continually added to online hosting sites, which need to be checked against reference objects, the content protection system should be able to process many objects over a short period of time.

B. Scalability and Reliability: The system should scale (up and down) to different number of multimedia objects.Scaling up means adding more objects because of monitoring more online hosting sites, having more content owners using the system, and/or the occurrence of special events such as sports tournaments and release of new

movies. Conversely, it is also possible that the set of objects handled by the system shrinks, because, for example, some content owners may terminate their contracts for the protection

service. Our approach to handle scalability is to design a distributed system that can utilize varying amounts of computing resources. With large-scale distributed systems.

C. Cost Efficiency: The system should minimize the cost of the needed computing infrastructure. Our approach toachieve this goal is to design our system to effectively utilize cloud computing infrastructures (public and/or private).

D. Accuracy: The system should have high accuracy in terms of finding all copies (high recall) while not reportingfalse copies (high precision). Achieving high accuracy is challenging, because copied multimedia objects typically undergo various modifications (or transformations).

V. RESULT AND DISCUSSION

Results of Practical Work

Practical work done for this is as shown in given below.

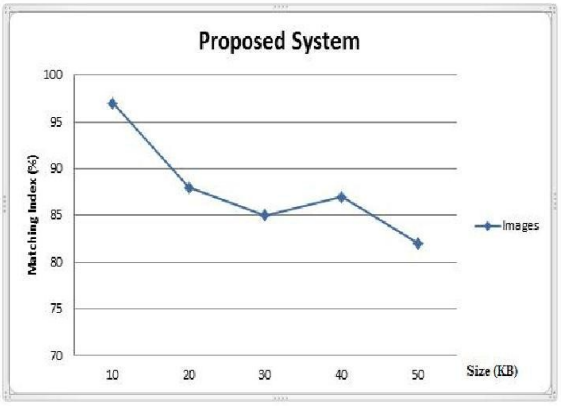

Fig.2: Graph 1(Images)

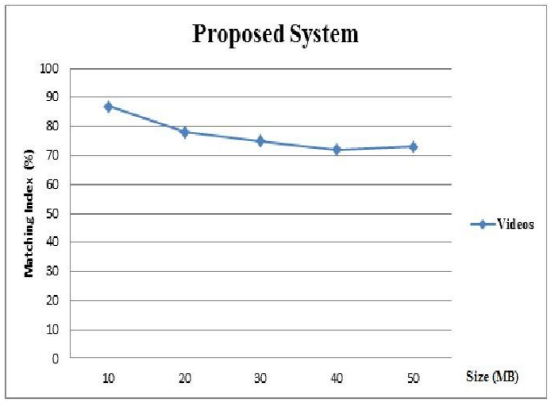

Fig.3: Graph 2(Videos)

Fig 2 and 3 shows graphical representation of copy detection detection for images as well as video & also shows that composite signature creation method work for both images and videos. Composite signature creation method is used for finding matching index for video and images uploaded on online hosting sites. Graph 1 repesents images (kb) which is uploaded on online hosting sites and our proposed system gives matching index (%) of uploaded image if matching index is 100% then it is automatically deleted because it is totally copied image. Graph 2 repesents videos (mb) which is uploaded on online hosting sites and our proposed system gives matching index (%) of uploaded video if matching index is 100% then it is automatically deleted because it is totally copied video.

VI. CONCLUSION AND FUTURE WORK

We have developed an efficient technique for protection multimedia content systems using multi-cloud infrastructures. Our experiments showed that the proposed signature produces high accuracy in terms of both recall and precision it is secure to different multimedia content. We take the help of DES algorithm for creating the signature. Our Proposed system showed results that: there

is necessary for designing secure signatures for 3-D videos since the current system used by the leading company in the industry fails to detect most modified copies, and our novel 3-D signature approach can cover this gap, because it is secure to different 2-D and 3-D video transformations.

In future we will provide protection of Multimedia content using Hadoop system. In addition, quickely identifying short video segments using composite signature schemes.

REFERENCES

[1] Rongxing et al, ―Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing‖, ASIACCS,,10, Beijing, China..

[2] R. La,,Quata Sumter, ―Cloud Computing: Security Risk Classification‖, ACMSE 2010, Oxford, USA

[3] 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 .

[4] Wenchaoet al, ―Towards a Data-centric View of Cloud Security‖, CloudDB 2010, Toronto, Canada

[5] SorenBleikertz et al, ―Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds‖, CCSW 2010, Chicago, USA.

[6] Flavio Lombardi& Roberto Di Pietro, ―Transparent Security for Cloud‖, SAC,,10 March 22-26, 2010, Sierre, Switzerland.

[7] Sara Qaisar**;** "Cloud Computing :Network/Security Threats and Counter Measures, *Interdisciplinary Journal of Contemporary Research InBusiness, Jan 2012,Vol 3, No 9*.

[8]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.

[9]Jiann-Liang Chen, Szu-Lin Wu, YanuariusTeofilusLarosa, 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.

[10] TamleekAli , Mohammad Nauman , Fazl-e-Hadi ,and Fahad bin Muhaya; "On Usage Control of Multimedia Content in and through Cloud Computing Paradigm".

[11] Zhang Mian, Zhang Nong; "The Study of Multimedia Data Model Technology Based on Cloud Computing"; 2010 2nd International Conference on Signal Processing Systems (ICSPS).

[12] 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.

[13] Neha Jain and GurpreetKaur; "Implementing DES Algorithm in Cloud for Data Security" *VSRD-IJCSIT, Vol. 2 (4), 2012,* 316-321.

[14] N. Saravanan, A. Mahendiran, N. VenkataSubramanian;An Implementation of RSA Algorithm in Google Cloud using Cloud SQL"*ResearchJournal of Applied Sciences, Engineering and Technology 4(19)*: 3574-3579, October 01, 2012.

[15] 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.

[16] PriyankaArora, Arun Singh; "Evaluation and Comparison of Security Issues on Cloud Computing Environment" *World of Computer Scienceand Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5,* 179-183, 2012.