International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET207448

Cloud-Based Multimedia Content Protection System

B. Aparna, S. Madhavi, G. Mounika, P. Avinash, S. Chakravarthi

Department of CSE, BITS Vizag, Visakhapatnam, Andhra Pradesh, India

Article Info
Volume 7 Issue 4
Page Number: 164-169
Publication Issue :
July-August-2020

Article History
Accepted : 20 July 2020
Published : 30 July 2020

ABSTRACT

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 videos, images, audio clips, songs, and music clips. 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 (ii) distributed matching engine for multimedia objects. The signature method creates robust and representative signatures of videos that capture the depth signals in these videos and it is computationally efficient to compute and compare as well as it requires small storage. The distributed matching engine achieves high scalability and it is designed to support different multimedia objects. We implemented the proposed system and deployed it on two clouds: Amazon cloud and our private cloud. Our experiments with more than 11,000 videos and 1 million images show the high accuracy and scalability of the proposed system. In addition, we compared our system to the protection system used by YouTube and our results show that the YouTube protection system fails to detect most copies of videos, while our system detects more than 98% of them.

Keywords : Multi-cloud,distributed matching engine, depth signatures,k-nearest, auxiliary function, steoricscopic cotent, robust signatures.

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. Illegallredistributing multimedia content 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 to identify copies.

Problem Definition: 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 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 neighbors for large-scale datasets. The design also offers an auxiliary function for further processing of the K neighbors. 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 MapReduce 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 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 video copies, it fails to detect copies of videos 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 videos even if they are subjected to complex transformations such as synthesizing new virtual views and converting videos to anaglyph and plus-depth formats.

Furthermore, we isolate and evaluate individual components of our system. The evaluation of the new signature method shows that it can achieve more than 95% precision and recall for stereoscopic content subjected to 15 different video transformations; several of them are specific to videos such a view synthesis. The evaluation of the distributed matching engine was done on the Amazon cloud with up to 128 machines. The engine was used to manage up to 160 million data points, each with 128 dimensions, extracted from over 1 million images. The results show that our design of the matching engine is elastic and scalable. They also show that our system outperforms the closest object matching system in the literature, called Rank Reduce, by a wide margin in accuracy and it is more efficient in terms of space and computation.

II. METHODS AND MATERIAL

2.1 Data owner

Ensure distinctive interactive media content writes, including pictures, sound clasps, tunes, and music cuts. Theframework can be sent to private as well as open mists. Our framework has two novel parts: (I) technique to make marks (ii) disseminated coordinating motor for interactive media objects. The marking technique makes hearty and delegate marks that catch the profundity motions in these recordings and it is computationally proficient to register and think about and in addition, it requires little stockpiling.

2.2 Data User

Coordinating motor accomplishes high versatility and it is intended to help distinctive sight and sound items. We actualized the proposed framework and conveyed it on two veils of mist: Amazon cloud and our private cloud. Our tests with more than 11,000 and 1 million pictures demonstrate the high precision and adaptability of the proposed framework. Also, we contrasted our framework with the security framework utilized by YouTube and our outcomes demonstrate that the YouTube assurance framework neglects to identify most duplicates, while our framework distinguishes over of them.

2.3 Encryption

Mixed media content assurance frameworks utilizing multi-cloud foundations. The proposed framework bolsters distinctive mixed media content composes and it can be conveyed on private or potentially open mists. Two key parts of the proposed framework are displayed. The first is another technique for making marks. Our technique builds coarse-grained divergence maps utilizing stereo correspondence for an inadequate arrangement of focuses in the picture.

2.4 Rank Search

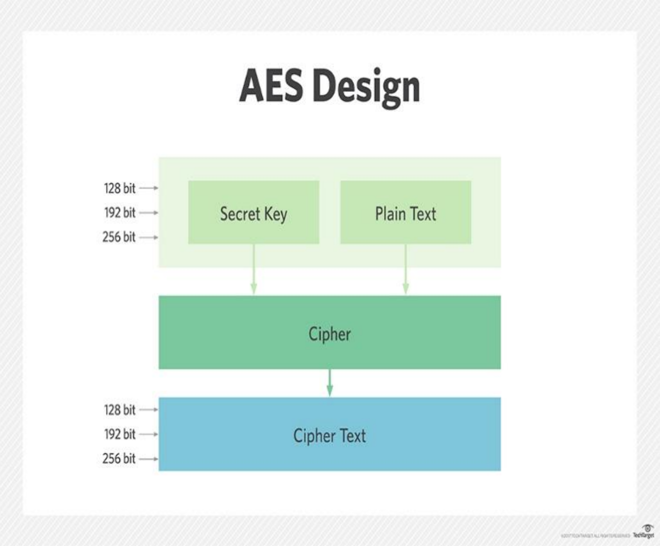
Rank needs to store the entire reference dataset different circumstances in hash tables; up to 32 times. Then again, our motor stores the reference dataset just once in containers. Capacity necessities for a dataset of size 32,000 focuses show that Rank needs up to 8 GB of capacity, while our motor needs up to 5 MB, which is in excess of 3 requests of extent less. These capacity necessities may render Rank not material for huge datasets with a huge number of focuses, while our motor can scale well the help huge datasets.

III. ADVANCED ENCRYPTION STANDARD ALGORITHM

AES comprises three block ciphers: AES- 128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. The Rijndael cipher was designed to accept additional block sizes and key lengths, but for AES, those functions were not adopted. Symmetric (also known as secret-key) ciphers use the same key for encrypting and decrypting, so the sender and the receiver must both know -- and use -- the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of cipher text.

The AES encryption algorithm defines a number of transformations that are to be performed on data stored in an array. The first step of the cipher is to put the data into an array; after which the cipher transformations are repeated over a number of encryption rounds. The number of rounds is determined by the key length, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

The first transformation in the AES encryption cipher is substitution of data using a substitution table; the second transformation shifts data rows, the third mixes columns. The last transformation is a simple exclusive or (XOR) operation performed on each column using a different part of the encryption key -- longer keys need more rounds to complet.



IV. OVERVIEW OF THE PROPOSED SYSTEM

We show a novel framework for media content insurance on cloud foundations. The framework can be utilized to ensure different media content writes. In our proposed framework we introduce finish multi-cloud framework for media content insurance. The framework bolsters distinctive kinds of media content and can viably use fluctuating processing assets.

A novel strategy for making marks for recordings. This strategy makes marks that catch the profundity in stereo substance without registering the profundity flag itself, which is a computationally costly process. olsters distinctive kinds of media content and can viably use fluctuating processing assets.

New plan for a dispersed coordinating motor for high-dimensional mixed-media objects. This outline gives the crude capacity of finding – closest neighbors for expansive scale datasets.

The plan additionally offers a helper work for additionally preparing of the neighbors. This two-level plan empowers the proposed framework to effortlessly bolster diverse kinds of interactive media content.

The focal point of this paper is on the other approach for securing mixed media content, which is content-based duplicate discovery (CBCD). In this approach, marks are removed from unique items. Marks are likewise made from inquiry (suspected) objects downloaded from online destinations. At that point, the comparability is figured amongst unique and suspected items to discover potential duplicates.

4.1 Advantages:

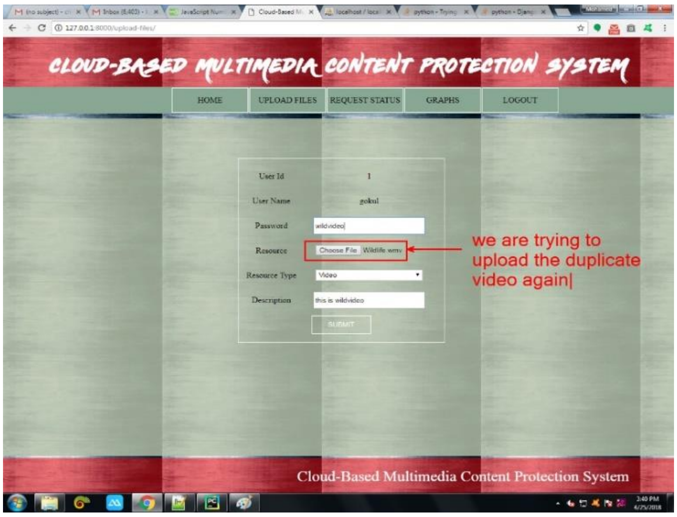
Accuracy.
Computational Efficiency.
Scalability and Reliability.
Cost Efficiency.

The framework can keep running on private mists, open mists, or any blend of open private mists.

Our plan accomplishes fast sending of substance security frameworks since it depends on cloud foundations that can rapidly give registering equipment and programming assets.

The outline is financially savvy since it utilizes the registering assets on request.

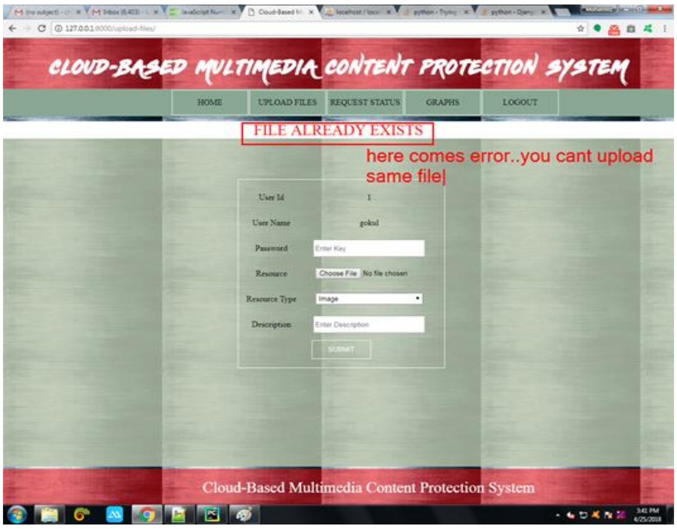
The outline can be scaled here and there to help to shift measures of mixed media content being secured.In the below picture we are trying to upload the duplicate picture and it fails and show us as you can't upload same file.Then we take a new file and upload it and it is said to be uploaded.


CLOUD-BASED MULTIMEDIA CONTENT PROTECTION SYSTEM
HOME
UPLOAD FILES
REQUEST STATUS
GRAPHS
LOGOUT
SUBMIT
Cloud-Based Multimedia Content Protection System

127.0.0.1:8000/upload-files/

User Id 1
User Name gokul
Password wildvideo
Resource Choose File Wildlife.wmv
Resource Type Video
Description this is wildvideo

we are trying to upload the duplicate video again

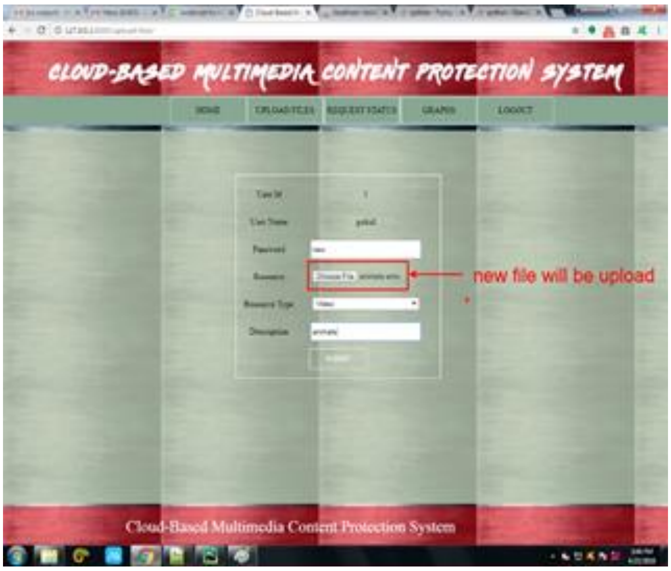

CLOUD-BASED MULTIMEDIA CONTENT PROTECTION SYSTEM
HOME
UPLOAD FILES
REQUEST STATUS
GRAPHS
LOGOUT
SUBMIT
Cloud-Based Multimedia Content Protection System

127.0.0.1:8000/upload-files/

FILE ALREADY EXISTS

here comes error..you cant upload same file

User Id 1
User Name gokul
Password Enter Key
Resource Choose File No file chosen
Resource Type Image
Description Enter Description


CLOUD-BASED MULTIMEDIA CONTENT PROTECTION SYSTEM
HOME
UPLOAD FILES
REQUEST STATUS
GRAPHS
LOGOUT
new file will be upload
Submit
Cloud-Based Multimedia Content Protection System

User Id 1

User Name [illegible]

Password [illegible]

Resource Choose File [illegible]

Resource Type Video

Description [illegible]

V. 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 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 video, without explicitly computing the exact depth map, which is computationally expensive. Our experiments showed that the proposed 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 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 Map Reduce 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 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 videos since the current system used by the leading company in the industry fails to detect most modified 3D copies, and (ii) our proposed signature method can fill this gap, because it is robust to many video transformations.

VI. REFERENCES

[1]. Mohamed Hefeeda, Tarek El Gamal, Kiana Calagari and Ahmed Abdelsadek,2015 IEEE," Cloud based Multimedia Content Protection System".

[2]. R. Amirtharathna1, Mrs. P. Vijayasarathy," Copy Detection of Multimedia Contents in Cloud",2016, International Journal of Engineering and Computer Science.

[3]. Vaishali Dewar, Priya Pise," A Mechanism for Copyrighted Video Copy Detection and Identification",2015, International Journal of Science and Research (IJSR).

[4]. A. Perumal Raja, B. Venkadesan," Efficient Framework for Video Copy Detection Using Segmentation and Graph-Based Video Sequence Matching",2014., IEEE Paper.

[5]. Pratheep Anantharatnasamy, Kaavya Sriskandaraja, Vahissan Nandakumar," Fusion of Colour, Shape and

[6]. Texture Features for content-based image retrival",2013, International Journal of Science and Research (IJSR).

[7]. M. Ramya, R. Kanthvel,” Efficient and Scalable Content- based Video Copy Detection System”,2012, International Journal of Computer Applications® (IJCA).

[8]. Vishwa Gupta, Parisa Darvish Zadeh Varcheie,2012,” Content-based video copy detection using nearest neighbor mapping.

Cite this article as :

B. Aparna, S. Madhavi, G. Mounika, P. Avinash, S. Chakravarthi, "Cloud-Based Multimedia Content Protection System", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 7 Issue 4, pp. 164-169, July-August 2020. Available at doi : https://doi.org/10.32628/IJSRSET207448
Journal URL : http://ijsrset.com/IJSRSET207448