

MULTIMEDIA DATA SECURITY SCHEME IN THE CLOUD

GUIDE : RAJALAKSHMI M.E,PH.D

STUDENT NAME : JAGADEESWARI (38110165)

ABSTRACT:

A novel design for large-scale multimedia content protection systems is proposed. Our architecture makes use of cloud infrastructures to enable cost effectiveness, fast deployment, scalability, and elasticity to suit varied workloads. The suggested system can secure many forms of multimedia material, such as movies, photos, audio clips, songs, and music clips. The system may be installed in either private or public clouds. Our system includes two innovative components: A method for creating video signatures and a distributed matching engine for multimedia items. The signature approach generates robust and representative signatures of films that capture the depth signals in these videos, and it is computationally efficient to calculate and compare, as well as requiring little storage. The distributed matching engine is intended to accommodate various multimedia items and has a high scalability.

Keywords: *Cloud Infrastructures, Internet, Index Multimedia, Internet of things.*

1. INTRODUCTION

Illegally transferring visual and auditory content via the Internet can result in significant economic losses for content creators. Finding illegally created copies on the Internet is a complicated and computationally expensive task due to the huge number of available mixed media information on the Internet and the multifarious character of contrasting substance with recognising duplicates [1]. We present a unique framework for sight and sound material security on cloud bases. The framework may be used to

protect many media material types, including standard 2-D recordings, novel 3-D recordings, images, sound clasps, tunes, and music cuts. The framework can continue to run on private mists, open mists, or any combination of the two. Because it is based on cloud bases that can quickly provide processing equipment and programming assets, our configuration achieves quick creation of substance security frameworks. Because it makes use of registering assets on interest, the plan is financially wise. The setup can be scaled here and there to support altering

measurements of sight and sound material being guaranteed. Complete multi-cloud solution for multimedia content protection. The system supports several forms of multimedia material and can efficiently use a variety of computing resources. A novel way for making video signatures. This approach generates signatures that capture the depth in stereo material without having to compute the depth signal itself, which is a computationally intensive procedure. A new design for a distributed matching engine for high-dimensional multimedia artifacts. For large-scale datasets, this approach provides the fundamental function of locating K-nearest neighbours. The design additionally includes an auxiliary function for further processing of the K neighbours. Because of its two-tiered design, the suggested system may readily accommodate various forms of multimedia material. In order to discover video duplicates, for example, the temporal characteristics must be addressed in addition to matching individual frames. This is not the same as detecting image copies [2]. The Map Reduce programming approach is used in our matching engine design. In addition, we compare our solution to YouTube's Content ID scheme for video protection. Our findings reveal that, while the Content ID system detects video copies reliably, it fails to detect

duplicates when videos are subjected to relatively minor changes such as re-encoding and resolution adjustment. Our method, on the other hand, can detect practically all copies of videos, even if they have undergone extensive alterations such as the creation of new virtual perspectives and the conversion of videos to anaglyph and plus-depth formats.

2. RELATED STUDY

The issue of securing various forms of multimedia material has gotten a lot of attention from academics and business. Watermarking is one approach to this challenge, in which some distinguishing information is encoded in the material itself and a mechanism is used to search for this information in order to authenticate the validity of the content. Watermarking necessitates the incorporation of watermarks into multimedia objects prior to their release, as well as mechanisms/systems for locating objects and verifying the presence of correct watermarks within them. As a result, this method may not be appropriate for previously released content that lacks watermarks [3]. The watermarking approach is better suited for somewhat controlled environments, such as the distribution of multimedia content on DVDs or the use of special sites and custom players. Watermarking may not be

effective for the constantly growing number of internet videos, particularly those posted to sites like YouTube and played back by any video player. This paper is not about watermarking. The focus of this study is on the other method for securing multimedia material, which is content-based copy detection (CBCD). Signatures (or fingerprints) are retrieved from original items in this method. Signatures are also generated from query (suspected) items retrieved from web sources. The similarity between the original and suspected items is then calculated to identify probable duplicates. Many prior studies provided various ways for producing and matching signatures. These approaches are divided into four categories: spatial, temporal, colour, and transform-domain. The most common are spatial signatures (especially block-based signatures). Their shortcoming is a lack of resistance to significant geometric alterations. Temporal and colour signatures are less robust and can be used to supplement spatial signatures. Transform-domain signatures are computationally demanding and are not extensively employed in practise. For further information, check the surveys for audio fingerprinting and 2D video fingerprinting [4]. YouTube Content ID, Vobile VDNA, and Mark Monitor are some industry examples that employ

fingerprinting for media protection, whereas approaches like ours are considered academic state-of-the-art.

3. AN OVERVIEW OF EXISTING SYSTEM AND DISADVANTAGES

The issue of securing various forms of multimedia material has piqued the interest of academics and industry. Watermarking is one approach to this challenge, in which some distinguishing information is placed in the material itself and a mechanism is used to search for this information in order to validate the content's validity. Watermarking necessitates the incorporation of watermarks into multimedia items prior to their release, as well as mechanisms/systems for locating objects and confirming the presence of proper watermarks inside them. As a result, this strategy may not be appropriate for previously published content that lacks watermarks. Watermarking is better suited to relatively regulated circumstances, such as the dissemination of multimedia content on DVDs or the use of particular sites and bespoke players [5]. The purpose of this work is not to discuss watermarking. That is, we construct our system in such a way that earlier content-based copy detection approaches for producing and matching signatures may be used inside it. We offer

a novel approach for 3D video fingerprinting, as well as a new architecture for the distributed matching engine, in addition to our cloud-based system.

4. AN OVERVIEW OF PROPOSED SYSTEM AND ADVANTAGES

The focus of this study is on the other method for securing multimedia material, which is content-based copy detection (CBCD). Signatures (or fingerprints) are retrieved from original items in this method. Signatures are also generated from query (suspected) items retrieved from web sources. The similarity between the original and suspected items is then calculated to identify probable duplicates. The most common are spatial signatures (especially block-based signatures). Temporal and colour signatures are less robust and can be used to supplement spatial signatures [6]. Transform-domain signatures are computationally demanding and are not extensively employed in practise. That is, we construct our system in such a way that prior content-based duplicate detection approaches for producing and matching signatures may be applied within it. In addition to our cloud-based approach, we offer a novel method for 3D video fingerprinting and a new architecture for the distributed matching engine.

5. SYSTEM IMPLEMENTATION:

Every user must authenticate in the form of a login, and to do so, they must first register. Once a person has registered their information, they must wait for clearance from the administrator. The administrator is checking the information and approving their request to login to the system. The file is uploaded together with the key. The user-supplied key is used to encrypt the uploaded file using Advanced Encryption Standard. The keys were also used to decrypt, therefore maintaining confidentiality is critical. The encryption and decryption are carried out with the authentication of both users by a trusted authority. The user must request the file, and the key will be provided by the administrator using encrypted communications such as an SSL account. The letter is only sent to the registered email address. Then they may decrypt using the desired key. The file can then be shared with the specified user. The suggested system is analysed using several graphs. Graphs have been plotted to confirm the system's quality. A range of charts, such as a pie chart, a bar chart, and a spline chart, will provide you with concise and straightforward comparisons of details.

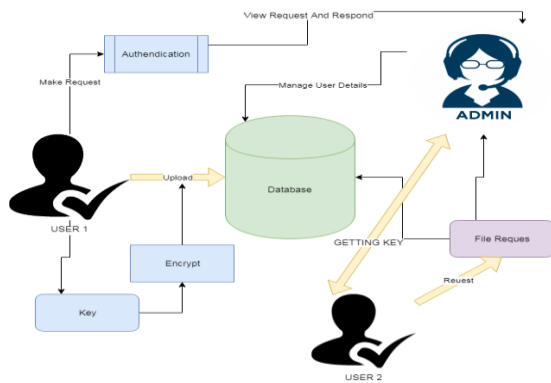
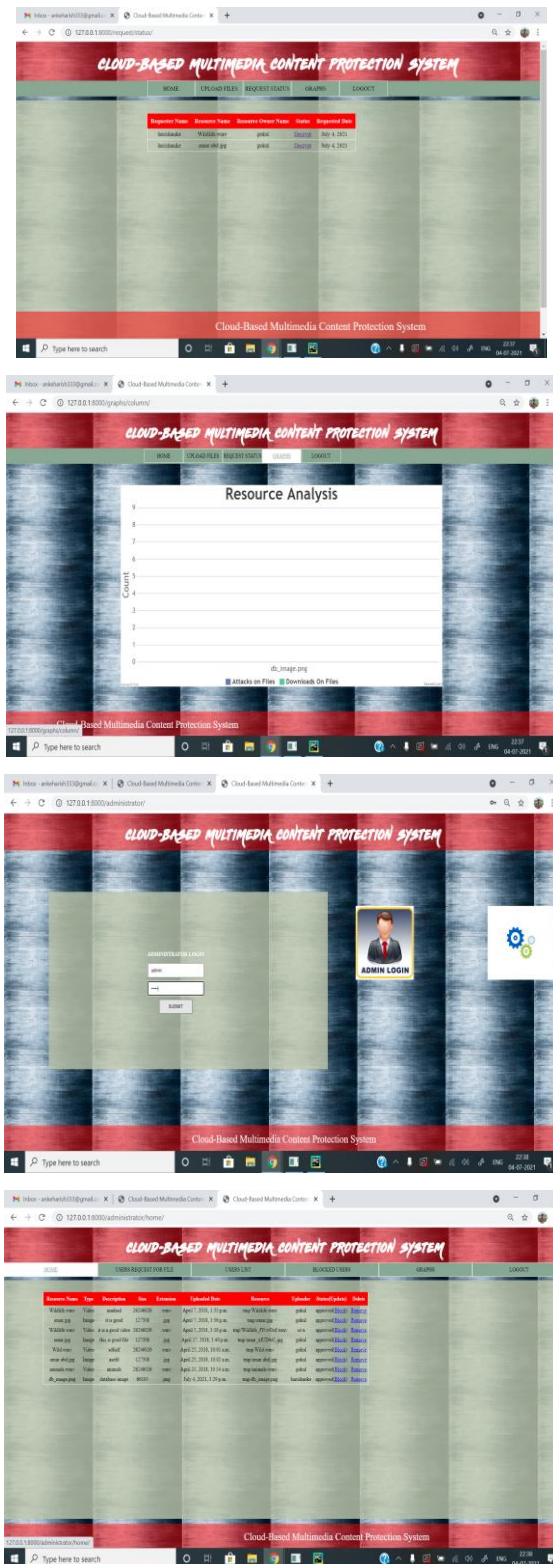
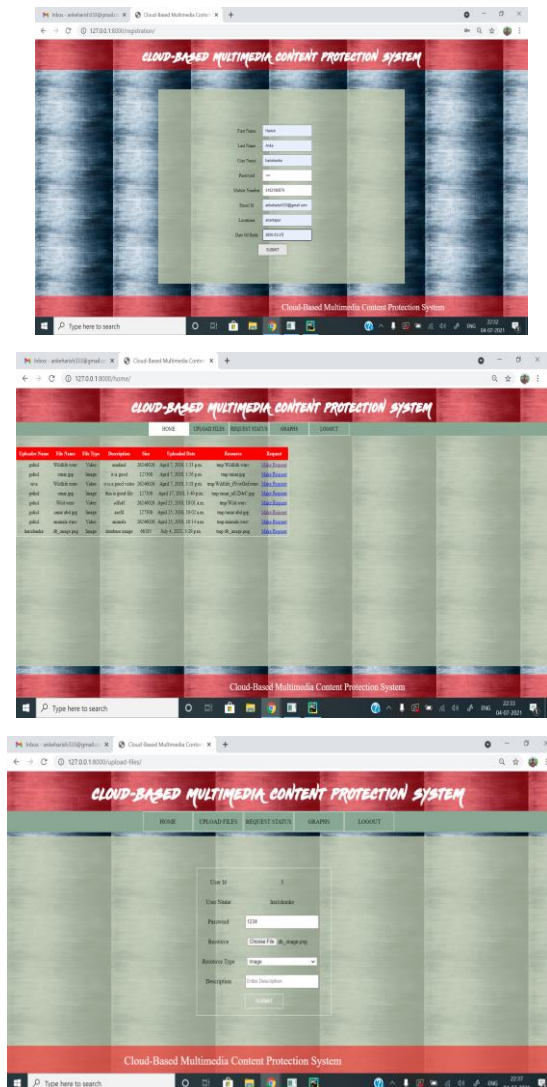
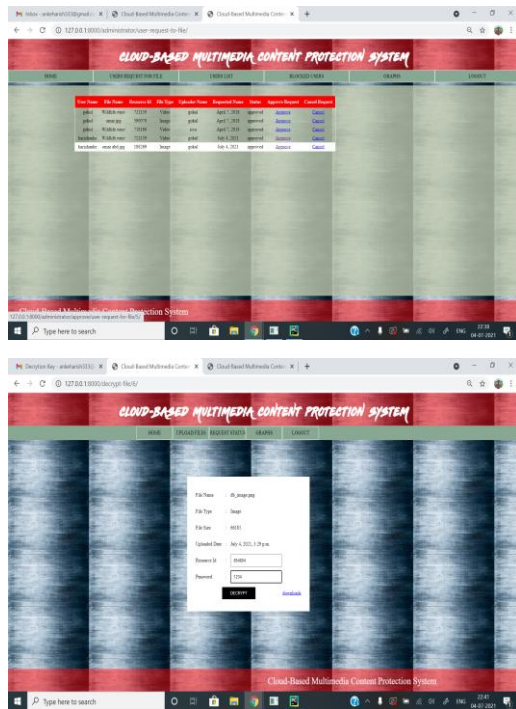


Fig.5.1. Application Work Flow.

RESULT SCREENS:





4. CONCLUSION & FUTURE WORK

Distributing copyrighted audiovisual assets by uploading them to internet hosting platforms such as YouTube can result in considerable financial loss for content providers. The systems required to detect unlawful copies of multimedia artifacts are complicated and huge in size. In this study, we introduced a new architecture for multimedia content protection systems based on multi-cloud infrastructures. The suggested system may be installed on private and/or public clouds and supports various forms of multimedia content. The suggested system's two major components are outlined. As a result, it may not be ideal for detecting illegally disseminated multimedia broadcasts of live events such

as soccer games online. Only limited portions of the video are available during live events, therefore detecting copyright infringement quickly is critical to minimizing financial losses. To allow online detection, our system's matching engine must be built with a distributed programming framework that supports online processing, such as Spark. To swiftly identify brief video clips, composite signature systems that incorporate various modalities may be required.

REFERENCES

- [1] A. Abdelsadek and M. Hefeeda. Dimo: Distributed index for matching multimedia objects using mapreduce. In Proc. of ACM Multimedia Systems Conference (MMSys'14), pages 115–125, Singapore, March 2014.
- [2] M. Aly, M. Munich, and P. Perona. Distributed Kd-Trees for Retrieval from Very Large Image Collections. In Proc. of British Machine Vision Conference (BMVC), Dundee, UK, August 2011.
- [3] J. Dean and S. Ghemawat. Mapreduce: simplified data processing on large clusters. In Proc. of Symposium on Operating Systems Design and

Implementation (OSDI'04), pages 137–150, San Francisco, CA, December 2004.

[4] J. Deng, W. Dong, R. Socher, L. Li, K. Li, and L. Fei-Fei. Imagenet: A large-scale hierarchical image database. In Proc. of IEEE Conference on Computer Vision and Pattern Recognition (CVPR'09), pages 248–255, Miami, FL, June 2009.

[5] H. Liao, J. Han, and J. Fang. Multi-dimensional index on hadoop distributed file system. In Proc. of IEEE Conference on Networking, Architecture and Storage (NAS'10), pages 240–249, Macau, China, July 2010.

[6] Z. Liu, T. Liu, D. Gibbon, and B. Shahraray. Effective and scalable video copy detection. In Proc. of ACM Conference on Multimedia Information Retrieval (MIR'10), pages 119–128, Philadelphia, PA, March 2010.