Journal of Science and Technology
ISSN: 2456-5660 Volume 8, Issue 07 (July -2023)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2023.v8.i07.pp193- 197*

A Protection System For Securing Multimedia Content In The Cloud

Venkata Sivaram Kumpati[1] |Polu Sathish[2] |Dr.V.Bapuji[3]

[1]Department of MCA, Vaageswari College Of Engineering, Karimnagar
[2]Assistant Professor, Department of MCA, Vaageswari College Of Engineering, Karimnagar.
[3]Professor& HoD, Department of MCA, Vaageswari College Of Engineering, Karimnagar.

To Cite this Article
Venkata Sivaram Kumpati |Polu Sathish |Dr.V.Bapuji**, "A Protection System For Securing Multimedia Content In The Cloud "** *Journal of Science and Technology, Vol. 08, Issue 07,- July 2023, pp193-197*
Article Info
Received: 04-06-2023 Revised: 05-07-2023 Accepted: 15-07-2023 Published: 27-07-2023

ABSTRACT

Every day, a vast amount of multimedia content is generated and shared on the internet. Unfortunately, it has become all too easy to duplicate copyrighted materials. To address this issue, in this work to introduces an innovative system for safeguarding multimedia content on cloud infrastructures. When these duplicated multimedia materials are illicitly distributed online, Content creators suffer significant revenue losses. Detecting these unauthorized copies of multimedia content is a challenging task. This paper presents a pioneering system designed to protect various types of multimedia content, including 2-D/3-D videos, audios, images, and more. Built upon cloud infrastructure, this system offers rapid access to computing hardware and software resources. Its key components involve generating signatures for 3-D videos and utilizing a distributed index to match multimedia object.

KEYWORDS: *Multimedia, Cloud computing, Protection, Copyrighted ,images,videos,*

1. INTRODUCTION

The advancement of multimedia processing and recording equipment, combined with the proliferation of free online hosting platforms, has greatly facilitated the unauthorized replication of copyrighted materials such as videos, images, and music clips. This illicit distribution of content is a challenging and computationally intensive task, requiring complex comparisons to identify duplicates. To handle this issue, a comprehensive system has been developed to safeguard various type of multimedia content, including 2D and 3D videos, images, audio clips, songs.

The system is designed to operate seamlessly on private clouds, public clouds, or a combination of both. Leveraging cloud infrastructure enables rapid deployment of content protection system by providing instant access to necessary computing hardware and software resources. This design is

cost-effective as it optimizes resource usage based on demand and can easily scale to accommodate varying volumes multimedia content requiring protection.

The proposed system encompasses multiple components, including a crawler for downloading numerous multimedia object from online hosting platforms, a signature method for generating distinctive fingerprints from these objects, and a distributed matching engine for storing original object signatures and comparing them against query objects.

The system utilizes a combination of amazon cloud and private cloud deployments to showcase its flexibility. This approach optimises the utilization of computing resources and helps minimize costs. It is worth noting that the costs of different cloud services vary, but they all provide improved performance compared to other options. Through extensive experimentation, This have validated the system's high accuracy, scalability, and elasticity.

This paper provides valuable information. Firstly, it explores the topic of safeguarding multimedia content within a multi-cloud environment, emphasizing the utilization of multiple cloud platforms to enhance protection measures. Secondly, it highlights the versatility of protecting any type of multimedia content by dynamically
adjusting computing resources.This adaptive approach allows for efficient and
customized protection based on the specific requirement of the content. The paper presents a novel method for creating signatures specifically tailored to safeguard 3D videos, offering a robust mechanism to ensure the integrity and security of such content

2. RELATED WORK

In the field of multimedia object matching and retrieval, significant contributions have been made by several researches.

Ahmed Abdel sadek [1] has proposed a distributed system specifically designed for matching multimedia objects. This system efficiently stores and indexes large-scale high-dimensional datapoints to facilitate fast searching and matching. It is particularly useful for multimedia applications that require finding nearest neighbours in extensive datasets.

Ahmed Abdel sadek and M.Hafeeda[2] have introduced a novel method for partitioning, searching, and storing high-dimensional datasets on distributed infrastructures that support the Map Reduce programming model. The system utilizes SIFT features, each consisting of 128 dimensions. The experimental results demonstrate and impressive accuracy of 95% compared to the ground-truth nearest neighbour. Furthermore, the system exhibits scalability and elasticity, allowing it to effectively utilize varying amounts of computing resources.

Mohamed Aly [3] has presented a method for constructing image retrieval systems
capable of handling a vast number of images.

The approach involves dividing the KD-Tree into a "root sub tree" residing on a root machine and
multiple" leaf sub trees" distributed across leaf machines. The implementation offers two variations, independent KD-Tree and Distributes
KD-Tree, which parallelize KD-Tree using the MapReduce architecture. The Distributed KDA-Tree (DKDT) outperforms the independent KD-Tree (IKDT)with over 30% higher accuracy and 30 times greater throughput for100 million images. Additionally, DKDT can process a query image within a fraction of a second.

Jon L. Bentley [4] has introduced the multidimensional binary search trees an efficient data structure for storing and retrieving information through associative searches. This structure demonstrates remarkable efficiency in terms of storage requirements. A significant advantage is its ability to handle various types of queries with high efficiency. The author presents an algorithm capable of efficiently handling general intersection queries.

3.METHODOLOGY

The proposed system offers comprehensive protection for diverse multimedia content types. It introduces a fully integrated multi-cloud solution specifically designed for safeguarding multimedia content. This system is capable of effectively utilizing different computing resources and provides support for a wide range of multimedia content formats.

The utilization of video copy detection complements the use of water making in safeguarding multimedia content. While

Water making relies on the insertion of a distinct pattern into the video stream, video copy detection techniques rely on content-based copy detection. However, this paper proposes the introduction of two performances by comparing them to an existing method.

The objective of the proposed multimedia content protection system is to identify unauthorized copies of multimedia content protection are extensive and intricate, multiple parties. In this section, begin by outlining the design objectives for such systems and our strategies for accomplishing them. Subsequently, This paper provide an overview of the high-level architecture and functioning of our proposed system.

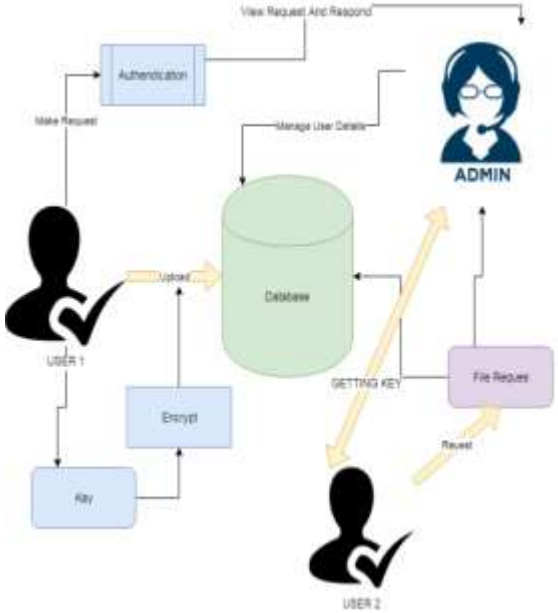

Figure 1. System Architecture of securing multimedia content in the cloud

The Cloud-Based Multimedia Content Protection system consists of the following modules

a) User Verification
b) File Encryption with Key
c) Resource Transmit
d) System Analysis

3.1.User Verification

To access the system, each user must authenticate themselves through a login process, which necessitates registration. Upon registering, users are required to provide their details and await approval from the administration. The administration carefully

verifies the provide information and grants permission for the user to login to the system.

3.2.File Encryption with Key

When a file is uploaded, it is accompanied by a user provided key. The uploaded file is then encrypted using the Advanced Encryption Standard(AES) and the user's specified key. It is of paramount important to preserve the secrecy of these keys, as they are utilized for both decryption and encryption purposes, the authentication of both users is required, which is carried through a trusted authority. This authentication process guarantees that the encryption and decryption operations are performed exclusively by the respective users, adding an additional layer of security.

3.3.Resource Transmit

In order to access a file, the user is required to submit a request, and subsequently, the administration will provide the key through secure communication channels, such as an SSL account. The key is exclusively sent to the user's registered email address, ensuring privacy and security. Using the received key, the user can decrypt the file and gain access to its contents. Once decrypt, the user has the ability to share the file specifically with the intended recipient who made the initial request.

3.4.System Analysis

The proposed system utilizes graphs to perform analysis, ensuring its quality. To enhance clarity and facilitate comparisons,
a diverse range of charts such as pie charts, bar charts and alpine charts have been plotted. These charts offer concise and comprehensible representation, enabling easy comparison of the details

4.PROPOSED SYSTEM

Your description outlines a novel framework for media content insurance on cloud foundations, introducing a complete multi-cloud framework for media content protection. This framework can ensure various types of media content and efficiently utilize various computing resources.

The key components of your proposed framework are as follows:

1. Novel strategy for creating marks for recordings: This strategy creates marks that capture the depth in stereo content without directly computing the depth signal itself, thus avoiding computationally expensive processes.

2. Distributed matching engine for high-dimensional multimedia objects: This design enables the efficient finding of nearest neighbors for large-scale datasets. It also provides a supporting function for further processing of the neighbors, allowing the system to easily support various types of multimedia content.

3. Content-based copy detection (CBCD): This approach focuses on securing multimedia content by extracting marks from original items and creating marks from query (suspected) objects downloaded from online sources. Similarity is then calculated between the original and suspected items to identify potential duplicates.

By combining these elements, your framework aims to provide robust media content insurance that can be effectively applied to different types of media content and leverage various computing resources available in a multi-cloud environment. The system's ability to efficiently find nearest neighbors for large datasets also makes it suitable for handling high-dimensional multimedia objects.

4.1 Advantages

1. Accuracy: The framework aims to accurately protect media content by using a novel strategy for creating marks and implementing a content-based copy detection approach. The accuracy of the system is crucial to ensure that legitimate media content is adequately protected, and potential duplicates are correctly identified.

2. Computational Efficiency: By leveraging cloud foundations and computing resources on-demand, the framework is designed to achieve fast deployment of content security systems. Cloud infrastructures can quickly provide the necessary hardware and software resources, leading to improved computational efficiency.

3. Scalability and Reliability: The framework is capable of being scaled up or down to accommodate varying amounts of multimedia content to be secured. This scalability ensures that the system can handle growing volumes of media content effectively. Additionally, the framework's reliance on cloud infrastructures contributes to its reliability, as cloud providers typically offer high uptime and redundancy.

4. Cost Efficiency: The design's cost-effectiveness stems from its utilization of computing resources on demand from cloud providers. Instead of maintaining and investing in dedicated hardware, the framework can dynamically allocate resources as needed, optimizing costs.

Regarding the provided picture, it seems to demonstrate the system's behavior in preventing the upload of duplicate images. When attempting to upload a duplicate image, the system correctly identifies it as a duplicate and prevents the upload. However, when a new file is selected for upload, the system allows it to be uploaded successfully.

Overall, the framework's focus on accuracy, computational efficiency, scalability, reliability, and cost-efficiency suggests a comprehensive approach to media content insurance on cloud foundations. The ability to operate on various types of clouds (private, public, or hybrid) further enhances its flexibility and applicability in different environments.

5.CONCLUSION

The act of uploading copyrighted multimedia objects to online hosting sites like YouTube and distributing them can have a considerable impact on content creators, leading to substantial revenue losses. In this paper, the outline of a fresh approach to designing multimedia content protection system by incorporating multi-cloud infrastructures. The proposed system is designed to accommodate diverse multimedia content types and offers the flexibility of deployment on private, public, or hybrid cloud environments. This paper introduces and elaborates on two key components of the system. Out approach utilizes stereo correspondence to construct coarse-grained disparity maps for a select set of points in the image. As a result, it effectively captures the depth signal of the video without the need for computationally expensive computations of the exact depth map. Based on our experiments, the proposed signature demonstrates high accuracy in terms of precision and recall. It exhibits robustness to various video transformation, including novel once that are specifically related to video content, such as synthesizing new views.
The results of study indicate two key findings:

a) There is a clear requirement for the development of robust signatures tailored to videos, as the existing system employed by the industry leader struggles to identify the majority of modified 3D copies, and

b) our proposed signature method exhibits the capability to address this gap by demonstrating robustness against a wide range of video transformations.

This paper lays the foundation for several potential extensions. For instance, while our current system is well optimized for batch processing, its effectiveness in detecting illegally distributed multimedia streams during live events, like soccer games, may be limited in an online setting. To address this, future research can focus on adapting the system to enable efficient and real-time detection in such dynamic scenarios.

6.REFERENCES

[1]A. Abdelsadek, “Distributed index for matching multimedia objects, “M.S. thesis, school of computer Science, Simon Fraser University, Burnaby, BC, Canada,2014.

[2] A.Abdelsadek and M. Hafeeda, “Dimo:Distributed index for matvhing multimedia objects using MapReduce,” in Proceeding of the ACM Multimedia System Conference(MMSys’14), Singapore, Mar.2014,pp.115—125.

[3] M. Aly M. Munich, and P. Perona, “Distributed KD-Trees for retrieval from very large image collection.”in Proceeding of the British Machine vision Conference (BMVC), Dundee, U.K, Aug.2011.

[4] J.Bentley, “Multidimensional binary search used for associative searching,” in communication of the ACM, vol. 18, no. 9, Sep. 1975, pp. 509-517

[5] Prasad, M., Naik, R., Bapuji, V.: Cloud Computing: Research Issues and Implications. International Journal of Cloud Computing and Services Science 2(2), 134–140 (2013)