Cloud based multimedia content protection system

S. Lokesh
Associate Professor, Dept.of CSE
National Institute of Engineering, Mysuru

DeepashreeHiremath.V,PriyankaFernandis,Shwetha.B,Vidyashree.N
Computer Science and Engineering,
National Institute of Engineering, Mysuru

ABSTRACT

It is necessary to protect the content as multimedia content is increasing exponentially. For large scale multimedia content protection a new design was proposed. To provide cost efficiency, rapid deployment, scalability, and elasticity to adjust varying workloads our design leverages cloud infrastructures. The proposed system can be used to protect different multimedia content types, including 2-D videos, 3-D videos, images, audio clips, songs, and music clips. On private and/or public clouds the system can be deployed. Our system has two novel components: (i) method to create signatures of 3-D videos, and (ii) distributed matching engine for multimedia objects. In this method signatures are extracted or created from original multimedia objects and through online sites . Signatures are also created from query (suspected) objects downloaded from online sites. As this design is based on cloud infrastructures it achieves rapid deployment on content protection system. Our experiments with more than 11,000 3-D 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 3-D videos, while our system detects more than 98% of them. Our analysis shows that the system is more efficient both cost and storage wise.

Index Terms*- 3-DVideo, Cloud Applications, Depth Signatures, Video Copy Detection, Video Fingerprinting.*

1. .INTRODUCTION

The technological progress as multimedia technology has become much easier to store large amount of data. Illegally redistributing multimedia content over the Internet can result in significant loss of revenues for content owner. This leads to the duplication of content owner's data. Duplication of copy righted material has become complex over the internet and also loss of data. The multimedia content protection system is used to protect various multimedia content types, such as 2-Dvideos, 3-D videos, images, audio clips, songs. The system can be deployed on both private cloud or public cloud or hybrid cloud. Our design is cost effective because it uses the computing resources on demand. The proposed system is complex with multimedia components including:

(i) Method to create signature of 3-D videos.
(ii) Distributed matching engine to store signatures of objects and match them against query objects.
(ii) Crawler to download thousands of multimedia objects from online hosting sites.

In this method signatures are extracted from original multimedia objects. Signatures are also created from query objects downloaded from online sites. Since cloud providers offer different pricing models for computing and network resources, 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. We show the high accuracy 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. Different types of file content the system can support and can effectively use varying computing resources.
- It is simple and effective method for generating signature for any multimedia or large text files.
- New design for a distributed matching engine for high-dimensional multimedia objects.

2. EXISTING AND PROPOSED SYSTEM

2.1 EXISTING SYSTEM

The problem of securing the multimedia content has given much importance from industry and academia. One solution to this issue is using watermarking, in which some individual information is computed in the content itself and in addition there is also a method which is used to search the information in order to verify the authenticity from the content. In watermarking technique, it needs to insert the watermarks within multimedia objects just before releasing them and also to find objects and validate the existence of correct watermarks in them. Thus, this solution may not be appropriate for pre-released content without watermarks in them. The watermarking technique is more acceptable or suitable for controlled environments (I.e., multimedia content on DVDs, custom players and special sites). Rapid increase online videos, especially uploaded to sites such as YouTube and played back by any video player are not much effective in this approach.

2.1.1 SECURITY AND PRIVACY CHALLENGES

It's impossible to develop a single data-protection solution for the cloud because the term means too many different things. Any progress must first occur in a particular domain accordingly, our work focuses on an important class of widely used applications that includes e-mail, personal financial management, social net-works, and business tools such as word processors and spreadsheets. The following criteria define this class of applications:

- Provide services to a large number of distinct end users, as opposed to bulk data processing or workflow management for a single entity.
- Use a data model consisting mostly of sharable units, where all data objects have access control lists (ACLs) with one or more users.
- Developers could run the applications on a separate computing platform that encompasses the physical infrastructure, job scheduling, user authentication, and the base software environment, rather than implementing the platform themselves.
- Overly rigid security is as detrimental to cloud service value as inadequate security. A primary challenge in Designing a platform-layer solution useful to many applications is ensuring that it enables rapid development and maintenance. To ensure a practical solution, we considered the following goals relating to data protection as well as ease of development and maintenance.
- Integrity: The user's stored data won't be corrupted.
- Privacy: Private data won't be leaked to any unauthorized entity.
- Access Transparency: Logs will clearly indicate who or what accessed any data.
- Ease of Verification: Users will be able to easily verify what platform or application code is running, as well as whether the cloud has strictly enforced their data's privacy policies.
- Rich Computation: The platform will allow efficient, rich computations on sensitive user data.
- Development and Maintenance Support: Because they face a long list of challenges—bugs to find and fix, frequent software upgrades, continuous usage pattern changes, and user demand for high performance— developers will receive both development and maintenance support.

2.1.2 DATA PROTECTION AS A SERVICE

Currently, users must rely primarily on legal agreements and implied economic and reputational harm as a proxy for application trustworthiness. As an alternative, a cloud platform could help achieve a robust technical solution by making it easy for developers to write maintain-able applications that protect user data in the cloud, thereby providing the same economies of scale for security and privacy as for computation and storage and enabling independent verification both of the platform's operation and the runtime state of applications on it, so users can gain confidence that their data is being handled properly.

2.2 PROPOSED SYSTEM

The goal of the proposed system for multimedia content protection is to find illegally made copies of multimedia objects over the Internet. We present complete multi-cloud system for multimedia content protection. The proposed system uses spatial signature techniques and distributed matching engine for high-dimensional multimedia objects. The proposed system has multiple components,where as most of components are hosted on cloud infrastructures. The system use one or more cloud provider. These is because only few cloud providers are high efficient and provide more cost saving for different communication tasks and computing. For example if a cloud provider offers low cost for inbound bandwidth and storage. This storage can be used for downloading and temporarily storing videos, from online sites while other cloud provider provides at low cost for better computing nodes which can be used to perform the copy detection process, and maintain distributed index.

The proposed system uses spatial signature techniques. There are two main components, the cloud server and the clients. The client users are given provision to store their files in the cloud. But how safe will their data or copy write contents be from any third party ? Chances are that the files can be viewed and copied. To prevent this copying and duplication of data we have come up with a simple content protection method that can assure the user that no matter who views the file, they will not be able to replicate the data in the system. Example. You tube videos can be seen by everyone but our system will not allow any two users to have the same videos. The credit always goes to the owners and not anyone else. The working of the system is simple and can be explained as follows: The client users upload and save their files in the server, during this process the unique which is placed in the server. When another user also uploads signatures of that file is generated and stored in another file any file signatures are generated for his file too and before it is placed in the server , the signatures are compared with the signature files that are already placed in the server to know the potential copied file. If the signature is not matching with any file then the file is said to be unique and its signature copy is placed in the server. If suppose the signature matches to any one file already in the server then the level or percentage of copy is determined.

Design Goals and Approaches

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.

We define and justify the following four goals as the most important ones in multimedia content protection systems.

- Accuracy: The system should have high accuracy in terms of finding all copies (high recall) while not reporting false copies (high precision). Achieving high accuracy is challenging, because copied multimedia objects typically undergo various modifications (or transformations). For example, copied videos can be subjected to cropping, embedding in other videos, changing bit rates, scaling, blurring, and/or changing frame rates. Our approach to achieve this goal is to extract signatures from multimedia objects that are robust to as many transformations as possible.
- Computational Efficiency: The system should have short response time to report copies, especially for timely multimedia 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. Our approach to achieve this goal is to make the signatures compact and fast to compute and compare without sacrificing their robustness against transformations.
- 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 tournament 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, failures frequently occur, which require the content protection system to be reliable in face of different failures. To address this reliability, we design the core parts of our system on top of the MapReduce programming framework, which offers resiliency against different types of failures.
- Cost Efficiency: The system should minimize the cost of the needed computing infrastructure. Our approach to achieve this goal is to design our system to effectively utilize cloud computing infrastructures (public and/or private). Building on a cloud computing infrastructure also achieves the scalability objective discussed above and reduces the upfront cost of the computing infrastructure.
- 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.

3. SYSTEM ARCHITECTURE

The proposed cloud-based multimedia content protection system . The system hasmultiple components; most of them are hosted on cloud infrastructures. The figure shows the where one or more cloud providers can be used by the system. This is because some cloud providers are more efficient and/or provide more cost saving for different computing and communication tasks. Cloud computing resources are distributed over the network which resolves the issue of massive computations being limited to one site. Cloud Computing is an Internet-based model that provide an on-demand access to the network that consists

of shared computing resources , with minimal management effort. For example, a cloud provider offering lower cost for inbound bandwidth and storage can be used for downloading and temporarily storing videos from online sites , while another cloud provider offering better compute nodes at lower costs can be used to maintain the distributed index and to perform the copy detection process.

The proposed system can be deployed and managed by any of the three parties mentioned in the previous section: content owners, hosting sites, or service providers. The proposed system has the following main components, as shown in Figure 1:
• Distributed Index: Protecting the signature of the object
• Reference Registration: It protects the signature of the object created by the content owner and inserts into the distributed index.
• Query Preparation: It Creates signatures from objects downloaded from online sites, then uploads these signatures to a common storage.
• Object Matching: It checks the signature from query signature and reference signature in the distributed index to find possible copies and also sends notification to content owners if copies are found.
• Parallel Crawling: Downloads multimedia objects from various online hosting sites.

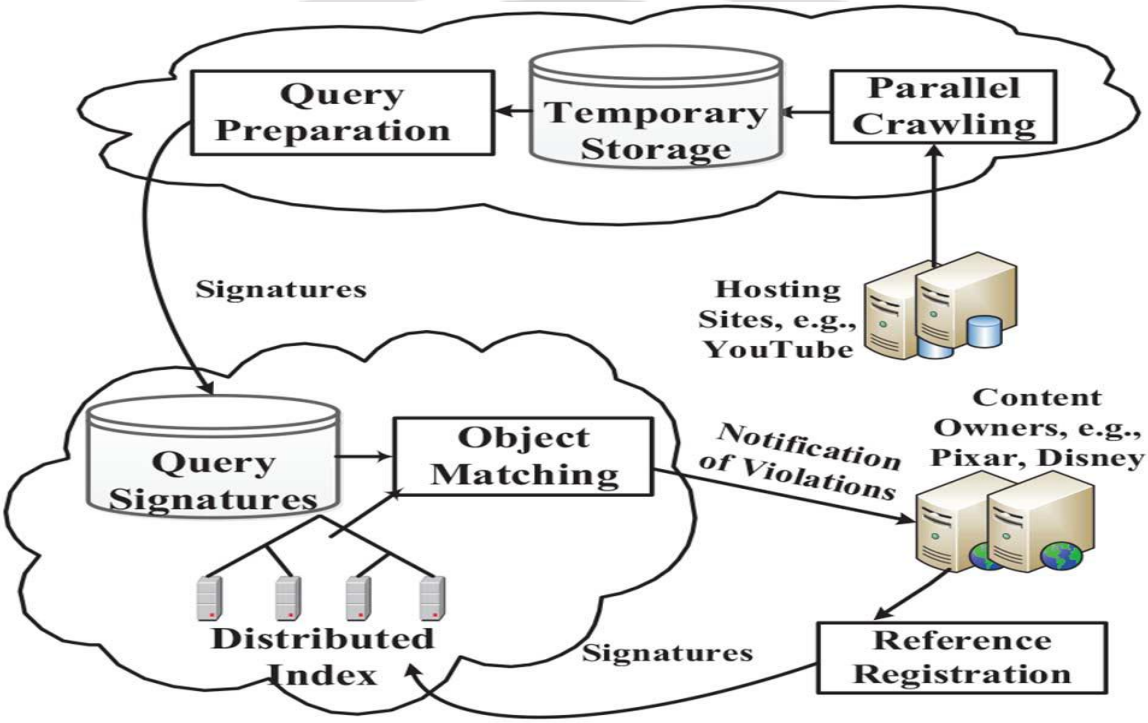

Fig-1 Proposed multimedia content protection system

The Distributed Index and Object Matching components form the Matching Engine. The Reference Registration and Query Preparation components deal with signature creation. 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 excluded due to space limitations.

The proposed system functions as follows:
Content owners protecting the multimedia objects. Then, the system creates signatures of these multimedia objects is called reference objects and inserts 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 downloads recent objects that is query objects from online hosting sites. It can use some 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 belong to specific category.If signature is created for query then crawl component download that object and 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. Compressionof signatures can be performed before the upload to save bandwidth. Once all signatures are uploadedto the matching engine, a distributed operation is performed to compare all query signatures versus thereference signatures in the distributed index.

4. CONCLUSION

In this paper, we presented a new design using multi-cloud infrastructures for multimedia content protection systems. The proposed system can be deployed on private and/or public clouds and it also supports different multimedia content types. Two key components of the proposed system are presented. The first method is for creating signatures of 3D 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 3D video, without explicitly computing the exact depth map, which is computationally expensive. Our experiments showed that the proposed 3D 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 3D 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 experiments also showed that it outperforms the closest system in the literature in terms of accuracy and computational efficiency.

5.REFERENCES

[1] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data wit Efficient User Revocation in the Cloud," Proc. IEEE INFOCOM, pp. 2904-2912, 2013.
[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. aharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.
[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07), pp. 598-610, 2007.
[4] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'08), pp. 90-107, 2008.
[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th ACM/IEEE Int'l Workshop Quality of Service (IWQoS'09), pp. 1-9, 2009.