A Secure System for Multimedia Content Protection on Cloud

Chaya M[1], Dr. K Thippeswamy[2]

[1]Department of Computer Science and Engineering,
Mysuru, Karnataka, India

[2]Department of Computer Science and Engineering,
Mysuru, Karnataka, India

Abstract

Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. Security and data protection are integral for cloud success. However, cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. Cloud Computing leverages many technologies it also inherits their security issues. Cloud may include any type of data like audio, video, images, data, text. The integration of these types is commonly known as multimedia. A system is presented for the protection of these multimedia contents on cloud infrastructure. The system can be used to protect various multimedia contents, including regular 2D videos, 3D videos, audios clips, images, animated graphics and music clips. The system can run on public clouds, public clouds, or any combination of public-private clouds. The system relates to the detection of the duplicated content using cloud system and method for the detection of duplication of content, copyright material in an online environment.

Keywords: *Cloud computing, Security, Multimedia, Signature creation, Distributed matching.*

1. Introduction

The importance of Cloud Computing is increasing and it is receiving a growing attention in the scientific and industrial communities. Cloud Computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud Computing appears as a computational paradigm as well as distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet. The cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing. Cloud Computing combines a numeral computing concepts and technologies such as Service Oriented Architecture (SOA), Web 2.0, virtualization and other technologies with trust on the Internet, providing common business applications online through web browsers to satisfy the computing needs of users, while their software and data are stored on the servers.

Although there are many benefits to adopting Cloud Computing, there are also some significant barriers to adoption. One of the most significant barriers to adoption is safety, followed by issues regarding fulfillment, solitude and legal matters. As Cloud Computing represents a relatively new computing model, there is a great deal of uncertainty about how protection at all levels (e.g., network, host, application, and data levels) can be achieved and how applications security is moved to Cloud Computing. Encryption procedure has been used for long time to secure sensitive data. Sending or storing encrypted data in the cloud will ensure that data is secure. However, it is true to assume that the encryption algorithms are strong. There are some well-known encryption schemes such as AES (Advanced Encryption Standard). Also, SSL technology can be used to protect data while it is in transit. Moreover, describes that encryption can be used to stop side channel attacks on cloud storage de-duplication, but it may lead to offline dictionary attacks reveling personal keys.

Multimedia is the field concerned with the computer-controlled integration of text, graphics, moving images, animation, audio, and any other media where every type of information can be represented, transmitted, stored and processed digitally. 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 2-D videos, 3-D videos, images, songs, audio clips, and music clips. 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. The proposed system is fairly complex with multiple components, including: (i) crawler to download huge number of multimedia items from online sites, (ii) signature method for every object and (iii) distributed matching engine to store signatures of original objects and match them against query objects. Many previous works proposed diverse methods for creating and matching signatures. These methods can be classified into four categories: spatial, temporal, color, and transform-domain. Spatial signatures are the most widely used. However, their weakness is the lack of resilience against large geometric transformations. Temporal and color signatures are less robust and can be used to enhance spatial signatures. This deployment model was used to show the flexibility of the system, which enables it to efficiently utilize varying computing resources

2. Related work

Here are some of the papers those are related to this project and that has been surveyed. Among them the below are some of the papers described.

Sonal Guleria et al. [1] presents a reference ontology framework for access control in cloud to facilitate the design of security system and to reduce the complexity of system design and implementation. To design an encryption algorithm based on combination on RSA and DES to have better security than RSA or DES alone to encrypt the data files before storing data on cloud. The combination of RSA and DES of secret Key encryption and homomorphism technologies are the secret sauce. To encrypt large messages a hybrid approach is used in which the messages are actually encrypted using symmetric schemes. Ujwala Pawar et al. [5] describe an approach to prevent the privacy of the data watermark technique is used which is one of the key aspects for the privacy of the data. In this watermarking technique, a digital signal or some message will be added both at the server and client sides as to protect the original content from the intruders. Mandeep Singh Sandhu, et al. [2] describe about distributed framework architecture in which the given data will be distributed into different cloud platforms in order to make it secure. To prevent unauthorized source to access data SMTP mailing services are used and also both MD5 and DES algorithms are used to save the original data. V. Ramachandra, et al. [9] describes mainly about SIFT method. A scale invariant feature descriptor (SIFT) computes SIFT points in each view and uses these points to verify the matches. A SIFT based fingerprinting mechanism can be used to identify the attacks. Mani Malekesmaeili et al[8] proposes an approach for generating representative images which carries both temporal as well as spatial information and these images are denoted as TIRIs(Temporally Informative Representative Images) and also applies simple image hashing technique on TIRIs of a video database. Priyanka Gupta et al.[3] describes the combinations of different algorithms are used. This uses roll based access control with the advanced encryption algorithm i.e, a combination of RSA algorithm and two fish , and also signature verification to enhance security when storing text, image ,audio ,video files onto cloud server. Youjin Song et al[6]. describes a BMIS model is used. Business Model for Information Security (BMIS) is a widely recognized and available model published by ISACA (Information Systems Audit and Control Association). The initial BMIS model is an interactive and dynamic model, which can act on both internal and external sides. Based on the cloud leveraged BMIS model, then considerate the new feature required in multimedia streaming service, remodel and adjust this model to the cloud streaming area. R.Amirtharathna et al[7] proposes techniques to avoid the duplication of the contents, these techniques involves the audio fingerprinting along with the K-medoids algorithm. By using these techniques the process of redistribution of audio contents are completely avoided. From the study of the related work it is clear that there are few techniques to protect the content in Cloud environment. By analysing these related work, we can identify the gaps that need to be addressed in order to achieve more protection to the content. Unlike previous works, the contribution of this paper is to design a large-scale system to find copies that can be used for different types of multimedia content and can leverage multi-cloud infrastructures to minimize the cost, expedite deployment, and dynamically scale up and down.

3. Proposed System

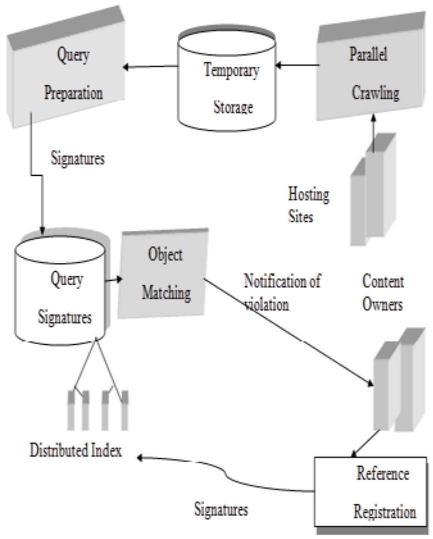

Fig. 1 Architecture of multimedia content protection system

The system provides a method for detecting copies of online multimedia content over distributed systems, the method comprising the steps of identifying multimedia content to be used as the basis for copy detection, calculating the resources required to extract features from the multimedia content, obtaining and deploying the required resources, extracting features from the multimedia content to form signature data, the signature data relating to the extracted features, inputting the signature data into a distributed index, identifying online content to be processed for copy exposure, calculating the supplementary resources required to extort features from the online content to be processed, obtaining and deploying the vital advance resources, extracting features from the online content to form online content data signatures, comparing the signature data with the online content data signatures, and determining whether the online content is a copy of the multimedia content. Preferably, the distributed system uses a cloud infrastructure. Conveniently, the step of extracting features from the multimedia content is undertaken on a system in the control of the multimedia content owner. The present system too provides a system for detecting copies of online multimedia content over distributed systems, the system including an item or items of multimedia content to be used as the root for copy detection, a processor to evaluate the resources required to extract features from the or each item of multimedia content, a resource, which when deployed, provides a platform on which to extract signature data from the multimedia content, a distributed index in which to store the signature data, online content to be processed for copy detection, a further resource, which when deployed, provides a platform on which to extract online content data signatures from the online content, and a data comparator, to compare the signature data and the online content data signatures, wherein the multimedia content is processed to extract signature data, the signature data is stored in the distributed index, and the data comparator receives signature data from the distributed index and compares it against the online content data signatures, to detect online copies of the multimedia content. Preferably, the resource is a cloud infrastructure. Generally, in the case of content protection systems, there may be three main parties involved, which may include content, hosting sites, and providers of a content protection service. In an effort to the unauthorized copying and distribution of online content, the system may be deployed and managed by any of the three parties. Firstly, content owners may set up a protection system to shield their own content. Further, hosting sites may tender a protection service by checking their own repositories and reporting to content owners. Also, independent third-party companies may propose such protection as a service to content owners by periodically checking contents posted on online sites.

3.1 Signature creation

The proposed system is designed to handle different variety of multimedia objects. The system abstracts the details of diverse media objects into multi-dimensional signatures. The signature creation and comparison component is media specific, while further parts of the system do not depend on media type. The step of forming the signature data includes the formation of a composite signature comprised of a blend of at least two of: a visual signature, an audio signature, a depth signature and metadata.

- Visual signature: Created based on the visual parts in multimedia objects and how they change with time.
- Audio signature: Created based on the audio signals in multimedia objects.
- Depth signature: If multimedia objects are 3-D videos, signatures from their depth signals are created.

- Meta data: Created from information associated with multimedia objects such as their names, tags, descriptions, format types.

Another aspect of the current system is, it provides a scheme of creating a composite signature, the routine comprising the steps of calculating a visual signature, based on the visual parts in multimedia objects, calculating an audio signature, based on the audio signal in the multimedia objects, calculating a depth signature, determined based upon the depth of the multimedia object, collecting metadata, created from information associated with multimedia objects, and combining at least two of the visual signature, audio signature, depth signature, and metadata to form a composite signature. Yet another characteristic is providing a composite signature comprising a combination of at least two of: a visual signature, an audio signature, a depth signature, and metadata.

Once the signatures have been created, a combined signature may be created. This step may combine different signatures and may assign diverse weights to each of them. It may also examine metadata associated with the multimedia object and may extract important information that can be used in the copy detection process. This important information may embrace the format of object, type of content, the number of downloads of the object, the IP address of the uploader, and any other suitable information.

3.2 Distributed matching engine

The distributed matching engine achieves high scalability and it is designed to support different multimedia objects. We design a matching engine suitable for different types of multimedia objects that is scalable and elastic. Scalability is needed to handle large datasets with millions of multimedia objects. Elasticity is a desirable feature that allows our system to utilize varying amount of computing resources offered on cloud infrastructures. In general, multimedia objects are characterized by many features and each feature is of high dimensions. For example, an image can be characterized by 100–200 SIFT descriptors, and each has up to 128 dimensions, and a video object will have even more features extracted from its frames. In addition, different types of multimedia objects require different number of features as well as different processing operations in order to decide on object matching. For example, matching two video clips requires not only matching individual frames, but also the temporal sequence of these frames. This is unlike image matching. To address this generality, we design the matching engine as two stages. In the first stage, the engine provides an efficient, distributed, implementation for computing nearest neighbors for high-dimensional data. In the second stage, the engine provides a generic interface for post processing these neighbors based on the different needs of various media types and applications. For instance, for video copy protection, the individual frame matching is done in the first stage and the temporal aspects are considered in the second stage.

The signature created during the signature creation method will be stored in the repository. The distributed matching engine mainly stores the signature of the original objects. This is mainly used to match the signatures against query object. Suppose the signature created does not match with the query objects then the content will be considered as a duplicated content. Then the user cannot get or download the content.

4. Conclusion and future work

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding the vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits the security issues. Systems needed to find illegal copies of multimedia objects are quite 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 to multimedia content. The second key component in our system is the distributed index, which is used to matching multimedia objects

The future direction for the work in this paper is to design signatures for recent and complex formats of 3-D videos such as multiview in addition with depth. A multiview and depth video has multiple texture and depth components, which allow users to view a scene from diverse angles. Signatures for such videos would need to capture this complexity, while being efficient to compute, compare and store.

References

[1] Sonal Guleria and Dr. Sonia Vatta, To Enhance Multimedia Security in Cloud Computing Environment using Crossbreed Algorithm, IJAIEM, Volume 2, Issue 6, June 2013.

[2] Er. Mandeep Singh Sandhu and Er. Sunny Singla, An Approach to Enhanced Security of Multimedia Data Model Technology Based on Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 7, July 2013.

[3] Priyanka Gupta, Amandeep Kaur Brar, An Enhanced Security Technique for Storage of Multimedia Content over Cloud Server, International Journal of Engineering Research and Applications Vol. 3, Issue 4, Jul-Aug 2013.

[4] Vaishali Dewar, Priya Pise, A Mechanism for Copyrighted Video Copy Detection and Identification, International Journal of Science and Research (IJSR), 2013.

[5] Ujwala Pawar, Prof. Dhara T. Kurian, Security of Multimedia Data Transmission stored on Cloud – Watermark Technique, iPGCON-2015.

[6] Youjin Song, Yasheng Pang, An Approach of Risk Management for Multimedia Streaming Service in Cloud Computing, International Journal of Multimedia and Ubiquitous Engineering, Vol.9, No.4 , 2014.

[7] R.Amirtharathna, Prevention Mechanism for Redistribution of Audio Contents in Cloud, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 9, September 2015.

[8] Mani Malekesmaeili, Mehrdad Fatourechi, and Rabab K. Ward, Video Copy Detection Using Temporally Informative Representative Images, International Journal of Engineering Research and Applications 2014.

[9] V. Ramachandra, M. Zwicker, and T. Nguyen, 3D Video Finger-printing, in Proc. 3DTV Conf.: True Vis.—Capture, Transmiss. Display 3D Video (3DTV’08), Istanbul, Turkey, pp. 81–84,May 2008.

[10] Aleksandar Stupar, Sebastian Michel, Ralf Schenkel, RankReduce – Processing K-Nearest Neighbor Querieson Top of MapReduce, LSDS-IR’10.