International Journal of Recent Trends in Engineering & Research
ISSN(ONLINE) : 2455-1457
IMPACT FACTOR : 3.344

A SURVEY ON MULTIMEDIA CONTENT PROTECTION ON CLOUD

Chaya M[1], K. Thippeswamy[2]
[1,2]Department of Computer Science and Engineering, VTU PG Centre, Mysuru,

Abstract - Security and data protection are integral for cloud success. Security concerns are increasingly important in the online world. It is widely accepted that cloud computing has the potential to be privacy disabling. The decision for choosing cloud is not just because of its security aspect it is also because of its agility, cost and time to market. The secure processing of personal data in cloud represents a huge challenge. Security is also one of the major factor to accomplish high performance on Cloud. For the protection purpose, a system for multimedia content protection on cloud infrastructure is presented. The system can be used to protect various multimedia contents, including regular 2D videos, new 3D videos, animated graphics, images, audios clips, songs, and music clips. With the advances in digital information, the latest buzzword is multimedia. Multimedia is the integration of data, text, image, audio, or video in a single application. The system can run on private clouds, public clouds, or any combination of public-private clouds. The system is scalable and cost effective. This system relates to the detection of duplicated content using cloud systems, and more particularly to a system and method for the detection of duplicated, copyright material in an online environment.

Keywords — cloud, multimedia, security, depth signatures, signature Creation.

I. INTRODUCTION

Cloud computing is a model for enabling 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 provides an emerging paradigm where computing resources make available as service of the Internet. This paradigm provides facility to Customer to Consumer and businesses without installation of this application and provides access to personal files at any computer with internet access. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. This also provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Upon these benefits, there are privacy and security concerns too. For the past few years, cloud-based storage has oscillated somewhere between a replacement strategy for existing back-up storage solutions (i.e. tape) and a typically inexpensive but complex real-time storage solution for online web properties and enterprises. Data transmission and storage can fall under many regional regulations involving the security and availability of personal information.

Multimedia can be defined as multi and media, where multi means many, much or multiple and medium means an intervening substance through some data is transmitted or carried on. Media has two broad classes: (a) Static, time-independent discrete media (b) Dynamic, time-dependent continuous media. The static class mainly includes text, images, graphics and is independent of time component. The dynamic class mainly includes sound, video and is dependent on the time component. Multimedia is typically used to mean the combination of different content forms such as

text, audio, images, animation, video and interactive content. Multimedia contrasts with media that use only rudimentary computer displays such as text-only or traditional forms of printed or hand-produced material. Multimedia can be broadly divided into linear and non linear categories. There are number of fields where multimedia could be used like business, education, entertainment and fine arts, home shopping, industry, medicine, journalism, engineering, virtual reality, digital video editing and production systems. Multimedia system provides some benefits like increasing the understanding in cases, controlling flow of the case, simplifying complex issues, Instant access and control over the law and facts of the case, saves the time.

Advances in processing and recording equipment of multimedia contents as well as the availability of free online hosting sites have made it relatively easy to illegally duplicate copyrighted materials such as videos, songs, images, and music clips. Copyright is the legal protection of all forms creative expression on any form of media. Copying and illegally redistributing multimedia contents over the Internet can result in significant loss of revenues for content creators. The content owners could be YouTube, Google etc. To the general public, intellectual property, in the form of computer software and digitized entertainment, is a highly tempting target for reproduction and distribution. But intellectual property is protected under copyright law in cyberspace as well as the real world, and one should need to be aware of the limits of your fair use. Illegal duplication, file sharing or use of any type of intellectual property constitutes copyright infringement and could be subject to university disciplinary action and civil and criminal penalties, including fines. Finding illegally-made copies over the Internet is a complex and computationally expensive operation, on account of the huge numbers of available multimedia content items across the Internet and the complexity involved in comparing content items to identify copies. According to Ohio State's document on Virtual Legality, "copyright law generally gives authors, artists, composers, and other such creators the exclusive right to copy, distribute, modify, and display their works or they can authorize other people to do so. Moreover, creators' works are protected by copyright law from the very moment that they are created ".

II. RELATED WORK

A substantial amount of research has been devoted to the problem of protecting the multimedia content in cloud. In this section, the most relevant approaches are described, their limitations and gaps are also discussed. 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] This paper 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] In this paper, 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]. In this paper, 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]This paper 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.

III. SIGNIFICANCE OF PROTECTING MULTIMEDIA CONTENT ON CLOUD

Cloud computing is one of the most important current trends in the field of information and communications technology, and ICT management. Hardware and software are no longer procured and operated by users themselves but obtained as services. Cloud service providers enable users to access and use the necessary resources via the internet.Cloud computing services are used both by consumers as well as by organisations and companies Offers in cloud computing comprise, among other things, the provision of calculating and storage capacity; the provision and operation of development environments and of operating- and database-management systems; of web hosting; of web mail services; and of a growing number of different types of application software; for word processing and other office applications; customer relationship management; supply chain management; or for the storage and management of photos or personal health-related data (electronic health records).Well-known examples of cloud computing services are Amazon Simple Storage Services, Amazon Web Services, Google App Engine, Microsoft Azure Services Platform or Salesforce.com. Other examples of cloud computing include peer-to-peer networks based on BitTorrent or Skype. Numerous internet service providers also use cloud computing as a basis for search engines, blogs and social networks, among others.

IV. CHALLENGES WITH DATA PROTECTION IN CLOUD

Within virtualized environments, numerous virtual machines are housed on a single physical system, a condition known as multi-tenancy. The hypervisor software is responsible for maintaining segmentation and isolation between virtual machines. This can be augmented with open source or commercial virtual network and virtual security appliances or add-ons. However, there are still challenges to traditional security best practices that stem from multi-tenancy, such as separation of duties and system segregation.

(a) Policy – Different virtual systems and data sets may have widely differing classifications and sensitivity levels. To ensure the proper security policy is applied to sensitive data, systems, and applications that store or process this data are often kept physically separate from others.
(b) Encryption – Encryption can be challenging to implement internally due to key management and maintenance, performance issues, and access controls. Extending internal encryption platforms and capabilities into the cloud can seem daunting at best.
(c) DLP – Data loss prevention is another common data protection technology that may require adaptation for virtualized and cloud environments. Data loss prevention (DLP) requires a number of distinct technologies and processes to be effective. First, sensitive data needs to be fingerprinted so DLP monitoring tools can recognize the data based on string matching, file types and other attributes. Second, a centralized policy creation and implementation

infrastructure needs to be in place to push policy to DLP monitoring tools, and these monitoring tools need to be in place to inspect traffic on network segments and critical host systems alike. Finally, quarantine and response measures should be implemented to take a variety of actions when a potential policy violation is detected.

(d) Monitoring – Security monitoring techniques using intrusion detection, network flow analysis tools, and hostbased agents are common in internal data centers. However, ensuring systems are properly monitored in the cloud is a different story. In many cases, cloud providers may not allow or support advanced monitoring technologies or processes, although some may offer this as a service.

V. PROPOSED METHODOLOGY

Multimedia typically refers to the combination of audio, video, images. To protect these multimedia contents from being pirated here is a new design for large-scale multimedia content protection systems. This design leverages cloud infrastructure to improve cost efficiency, scalability and elasticity. The proposed system can protect 2D videos, 3D videos, images, audio clips. The system comprising the steps (a) method to create the signature (b) distributed matching engine for multimedia objects.

Extracting features from the multimedia content to form signature data. The signature data comprising a combination of at least two of a visual signature, an audio signature, a depth signature, or metadata, also identifies online content to be processed for copy detection and finally comparing the signature data against the online content data signatures, and determining whether this online content is a copy of the multimedia content.

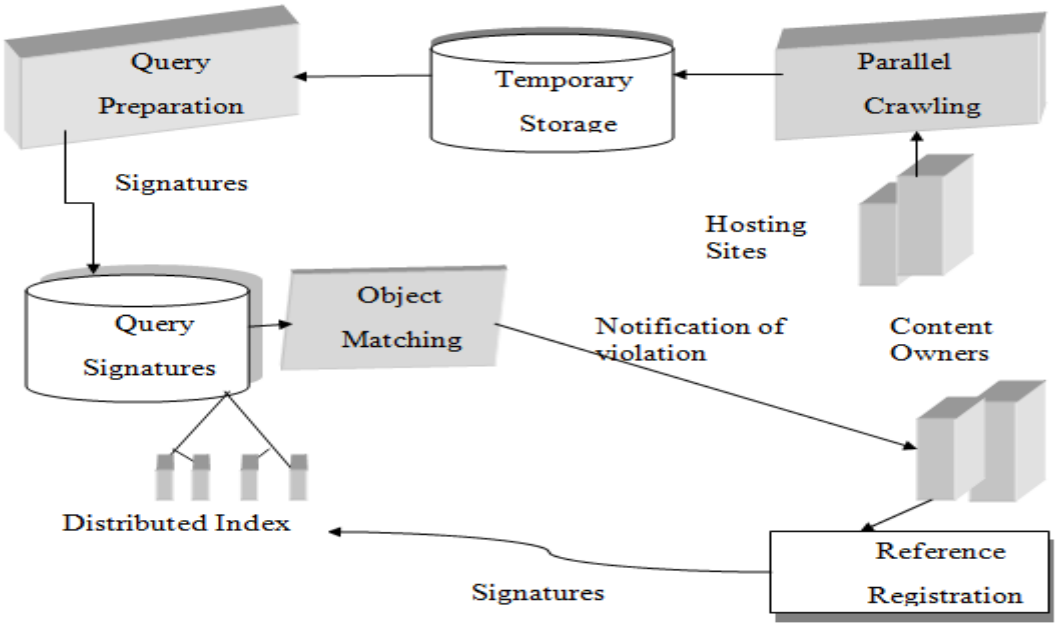

Figure 1. Architecture of proposed system

The proposed system has multiple components as shown in figure 1. The cloud providers are more efficient and/or provide more cost saving for different computing and communication tasks. 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 (or private cloud) 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.

• Distributed Index: Maintains signatures of objects that need to be protected;
• Reference Registration: Creates signatures from objects that content owners are interested in protecting, and inserts them in the distributed index;
• Query Preparation: Creates signatures from objects downloaded from online sites, which are called query signatures. It then uploads these signatures to a common storage;
• Object Matching: Compares query signatures versus reference signatures in the distributed index to find potential copies. It also sends notifications to content owners if copies are found;
• Parallel Crawling: Downloads multimedia objects from various online hosting sites. The Distributed Index and Object Matching components form what we call the Matching Engine. The second and third 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 omitted due to space limitations.
The proposed system mainly uses Signature Creation which is designed to handle different types of multimedia objects. The system abstracts the details of different media objects into multi-dimensional signatures. The signature creation and comparison component is media specific, while other parts of the system do not depend on the media type. Our proposed design supports creating composite signatures that consist of one or more of the following elements:
• 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, and IP addresses of their uploaders or downloader's.

VI. CONCLUSION

Cloud computing promises several attractive benefits for businesses and end users. Protecting the multimedia content is a challenging task. In this paper the survey has been done for protecting these multimedia contents on cloud infrastructure. The various problem for protecting the various contents on cloud environment has been identified. After studying the concepts from several papers a method is also proposed to protect the multimedia content on cloud infrastructures.

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.

