International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

Review of Multimedia Content Protection Scheme in Cloud Based System

Sushil Khune[1], S. P. Gawate[2]

[1]PG Scholar, Department of Computer Science and Engineering, G. H. Raisoni College of Engineering, Nagpur, India

[2]Assistant Professor, Department of Computer Science and Engineering, G. H. Raisoni College of Engineering, Nagpur, India

Abstract: ***Cloud computing provides different computing services delivered to user over the internet. In the presence of consuming amount of multimedia content in the cloud, the requirement for computerized systems to protect owners against unauthorized use of their content. The secure processing of personal data in cloud represents a huge challenge. There are so many of system accessible that gives simple approach to altering, distributing or, then again transferring multimedia content which might prompts security issue. This paper discusses about the different challenges and techniques used for multimedia content protection for cloud platform.***

Keywords: Cloud, Multimedia, Security, Video Fingerprinting, Copy Detection.

1. Introduction

The National Institute of Standard and Technology (NIST) gives a definition for Cloud computing "It 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" [1]. 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. The cloud computing model enables to access the information and computer resources from anywhere that a network connection is available. Therefore, data transmission and storage can fall under many regional regulations involving the security and availability of personal information.

Cloud computing provides three main service models [2]:

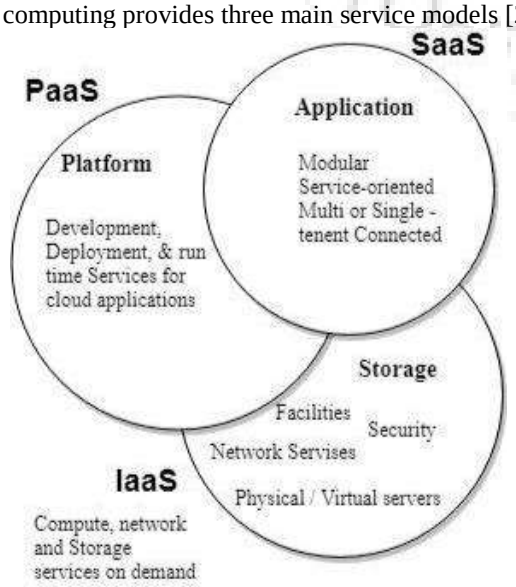

Figure 1: Service Models of Cloud Computing

a) Infrastructure as a Service (IaaS)
It provides storage, networks, and other fundamental computing resources where the client is able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure, but customer has control over operating systems, storage, and deployed applications.

b) Platform as a Service (PaaS)
It provides the capability to create and deploy applications onto the cloud infrastructure created by using programming languages, libraries, services, and tools supported by the provider. The client does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but client is responsible for installing and managing the application that it is deploying.

c) Software as a Service (SaaS)
It provides the capability to the customer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from different customer devices through web browser or program interface. Everything starting from the application to the infrastructure is the vendor's responsibility.

Cloud computing gives the following essential characteristics [3]:

On-demand self-service: A client can supply computer resources as needed automatically without requiring human interaction with each service provider.

Broad network access: Resources in cloud are available over the network and accessed through standard mechanisms that promote platform independent access to clients of all types.

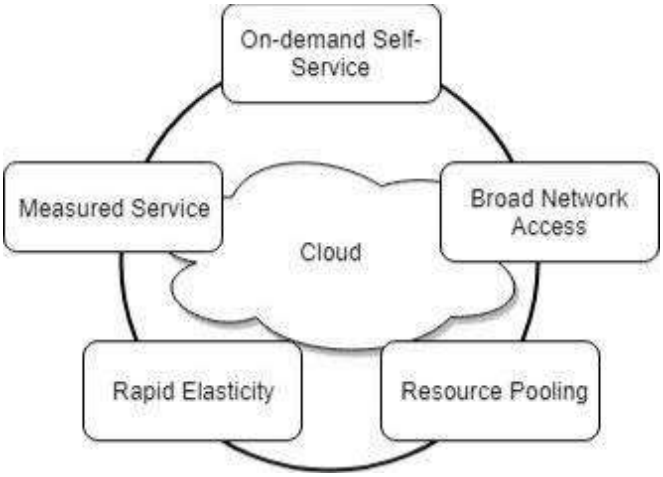

Figure 2: Characteristics of Cloud Computing

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Rapid elasticity: System can add resources by scaling up systems and can be elastically provisioned. Scaling can be automatic or manual.

Measured service: Cloud computing resources usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Nowadays information has a great role in our human society. Today, we can transmit information digitally over great distance in short time. This helps in connecting different societies, countries and cultures. Developments in digital technology help us to overcome many barriers in society but they also pose severe threats related to information. Various equipment of multimedia contents or availability of various free hosting sites makes easy to duplicate copyrighted materials such as- videos, images, music etc. Copying and illegally redistributing multimedia content over the Internet can bring about huge loss of incomes for content creators [16].

So, identification of duplicate copies of multimedia content has a broad variety of potential applications, forexample- copyright control, business insight, and so on., therefore it has attracted most lot of research work over most recent decade. The job of multimedia content protection system is to decide whether a given object (query) has its copy in a set of testing objects. Analyzing and comparing the elements between the querying and testing multimedia content are the standard strategies to cover this assignment.

This review paper gives information about service models and characteristics of cloud computing, Section 2 summarizes different analysis of different techniques used for multimedia content protection for cloud platform, Section 3 gives different challenges for data protection in cloud and we conclude the paper in section 4.

2. Related Work

Y. Chen, Wenbo He, Y Hua, W Wang [4] suggested a method for protection of data called CompoundEyes. It is formed by using an abstraction layer model. In this model, frames are tested at the Frame layer, in which features are obtained and characterized at the Feature layer. Then the patterns of NDVs rest in the Knowledge layer by using characterized features, which come out in the Decision layer and are utilized for predictions of duplicated videos.

Watermarking Technique [5] is used to scan the information which is already embedded in the content itself to check the legitimacy of the content. This method needs to put watermarks before publishing of the multimedia objects as well as framework to find objects and check the presence of correct watermarks in them. Therefore this method may not be suitable for already-released content without watermarks in them.

In this work first CNN features [6] are extracted from the densely sampled video frames and then afterward encode them into a fixed length vector by means of the sparse coding (SC) technique.

T. Yang, S. Jia [8] suggested an algorithm of reducing dimension and produce video fingerprint to find internet video copy. In this method video is composed into a fixed value by pre-treatment, to utilize hypergraph model video to divide video into various groups, and to optimize dimension reduction to low dimensional space and makes video fingerprint for securing content.

In [7] a scheme that supports CBIR over the encrypted images without publishing the sensitive information to the cloud server. The feature vectors are extracted to interpret the respective images. The pre-filter tables are designed with the locality-sensitive hashing. Then by using the secure k-nearest neighbour (kNN) the feature vectors are secured.

M. Diephuis [9] proposed an architecture in which contents are identified in images based on DCT (Discrete Cosine Transform). Adopted method protects the piracy in copy detection. The designed architecture replace the computational burden on the server where the encrypted data is searched. DCT coefficients for low frequency sign components of an image are taken for the generation of dual set of keys. These keys are used to encrypt the original image and hash value is calculated for content identification.

RankReduce system [10], which performs a distributed LSH (Locality Sensitive Hashing) index on a computing cluster using MapReduce. RankReduce allows to maintain multiple hash tables over a distributed cluster, which requires storing multiple replicas of the datasets in hash tables.

S. Lee and C. Yoo [11], provided a technique depends on centroid of gradient orientations for video fingerprinting which is pairwisely autonomous and furthermore robust against regular video processing steps including o frame rate change, loosy compression, resizing, global change in

brightness, colour, gamma,and so on. A threshold is utilized to choose matching of fingerprint is theoretically decide by displaying the fingerprint as a stationary ergodic process.

S. Lee, C. Yoo and Ton Kalkar [12], provided a technique for robust video fingerprinting which depends on binary fingerprint got by using the Symmetric Pairwise Boosting (SPB) algorithm. The SPB algorithm, utilizes suitable filters and quantizers from a class of candidate filters and quantizers such that perceptually comparative and unique sets of video clips are effectively classified as matching and non-matching sets, respectively.

In [13] gives the classification of different methods of creating and matching signatures i.e. spatial, temporal, color and transform-domain. Spatial signatures (in particular block-based) are most widely used and are susceptible to geometric transformations, for example, rotation cropping and scaling that changes the aspect ratios. Temporal and color signatures are less powerful and can be used to enhance spatial signatures. Transform-domain signatures are computationally intensive and not widely used in practice.

In [14], the local features are clustered into visual words and the image is represented with a BoW model. Then inverted file is adopted to index images for fast retrieval.

Jiang and Wang [15] sample frames at fixed time interval and extract CNN based features for each sampled frame. CNN features was implemented by two ways in his work i.e. Standard CNN which uses Caffe toolkit with AlexNet and Siamese Convolutional Neural Network (SCNN) which extracts local image patch features using a supervised CNN structure.

3. Different Challenges for Data Protection in Cloud

Identifying illegal copies over the cloud is very complex and it has different challenges for protecting multimedia content as follows [3] [18] [19]:

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.

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.

Data Loss Prevention (DLP): DLP 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.

Monitoring: Security monitoring techniques using intrusion detection, network flow analysis tools, and host-based 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.

4. Conclusion

Cloud computing have different attractive benefits for businesses and end users. Protecting the multimedia content is a challenging task. In this paper we have presented literature review of different methods for protecting multimedia contents and different challenges for data protection on cloud infrastructure. The various problem for protecting the various multimedia contents on cloud environment has been identified.

References

[1] www.nist.gov, “The NIST definition of Cloud Computing”. [Online].Available: https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published.
[2] Rahul Neware and Amreen Khan, “Cloud Computing Digital Forensic Challenges” *Second IEEE International conference on Electronics, Communication and Aerospace Technology* (ICECA 2018) IEEE.
[3] Barrie Sosinsky, “Defining Cloud Computing” in Cloud Computing Bible, Indianapolis, Indiana: Wiley Publishing, Inc. 2011
[4] “Challenges for Data Protection in Cloud”. [Online].Available: http://searchsecurity.techtarget.com/magazin eContent/Challenges-with-data-protection-in-the-cloud
[5] Neware, R,(n.d.) Recent Threats to Cloud Computing data and its Prevention Measures. International Journal of Engineering Sciences and Research Technology, 6(11), 234-238.
[6] Yixin Chen, Wenbo He, Yu Hua, Wen Wang “CompoundEyes: Near-duplicate Detection in Large Scale Online Video Systems in the Cloud”: *IEEE International Conference on Computer Communications*, 2016.
[7] K.N. Sowmya and H.R. Chennamma, “Video Authentication Using Watermark and Digital Signature-A Study”: *International Conference on Computational Intelligence and Informatics*, 2017 Springer.
[8] Ling Wang, Yu Bao, Haojie Li, Xin Fan and Zhongxuan Luo, “Compact CNN Based Video Representation for Efficient Video Copy Detection”:

International Conference on multimedia modeling, 2017 Springer.

[9] Zhihua Xia, Neal N. Xiong, A. V. Vasilakos, Xingming Sun, "EPCBIR: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing": *Published in Elsevier Journal of Information Sciences*, 2016.

[10] Tingting Yang ,Shuwen Jia, "Fingerprint Creation Algorithm based-on Dimensionality reduction": *IEEE International Conference on Computational Intelligence Theory, Systems and Applications*, 2015.*10th International Workshop on Content – Based Multimedia Indexing (CBMI) IEEE*, 2012.

[11] A. Stupar, S. Michel and R. Schenkel, "Rankreduce-Processing k-nearest neighbor queries on top of mapreduce" 8th Workshop on Large-Scale Distributed Systems for Information Retrieval (LSDS-IR'10), Geneva, Switerzerland, July 2010.

[12] Sunil Lee and Chang D. Yoo, "Robust videofingerprinting for content-based video identification", *IEEE transactions on Circuits and Systems for video technology, vol. 18 no. 7*, July 200

[13] S. Lee, C. Yoo and Ton Kalkar, "Robust Video Fingerprint Based on Symmetric Pairwise Boosting", *IEEE transactions on Circuits and Systems for video technology, vol. 19 no.9*, September 2009.

[14] Jian Lu, "Video fingerprinting for copy identification: from research to industry applications", *Procedings of SPIE- Media Forensics and Security XI, vol. 7254*, January 2009.

[15] M. Douze, H. Jegou and C. Schmid, "An Image Based Approach to Video Copy Detection with Spatio-Temporal Post-Filtering", *IEEE Transaction on Multimedia, Vol. 10, No.4*, June 2010.

[16] Y. Jiang and J. Wang "A Partial Copy Detection In Videos : A Benchmark And Evaluation Of Popular Methods", *IEEE Transaction on Big Data*, 2016.

[17] Rahul Neware, "Internal Intrusion Detection for Data Theft and Data Modification using Data Mining", International Journal of Science and Research (IJSR), https://www.ijsr.net/archive/ v6i8/v6i8.php, Volume 6 Issue 8, August 2017, 2176-2178, #ijsrnet.

[18] Rahul Neware. "Computer Forensics for Private Web Browsing of UC Browser." IOSR Journal of Computer Engineering (IOSR-JCE), vol. 19, no. 4, 2017, pp. 56-60.

[19] Rahul Neware, Nishi Walde. Survey on Security issues of Fog Computing. International Journal of Innovative Research in Computer and Communication Engineering. Vol. 5, Issue 10, October 2017, 15731-15736. DOI: 10.15680/IJIRCCE.2017. 0510009.

Author Profile

Sushil Khune received the B. E. degree Information Technology from Manoharbhai Patel Institute of Engineering and Technology, Gondia (Maharashtra), India in 2015. He now pursuing M. Tech. from G. H. Raisoni College of Engineering, Nagpur (Maharashtra), India.