Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 11, November 2017, pg.7 – 11

A Survey on Protection of Multimedia Content in Cloud Computing

Dr. K.Sai Manoj[1], Mrudula Kudaravalli[2], K Phani Srinivas[3]
CEO Amrita Sai Institute of Science and Technology, Paritala, AP, India
Assistant Professor, Amrita Sai Institute of Science and Technology, Paritala, AP, India
Head R&D, Amrita Sai Institute of Science and Technology, Paritala, AP, India
Email: amritasairesearchhead@gmail.com

Abstract:- In this Modern Online World Security Plays an Important role. Cloud Computing algorithms have Capability to Disable the Privacy. Multi-Media is the Clear Integration of data, text, image, audio, video in one application. In this Paper We Introduced Algorithm with Good Concept to Protect 2-D Videos, 3-D Videos, Audio and Image. This New type of Cloud Computing system detects Duplicate and Copy righted material in the Online.
Keywords:- Cloud, Multi-Media, 2-D Video, 3-D Video.

I. INTRODUCTION

Cloud computing is a Practical approach for Making 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 and also service provider interaction. Cloud computing provides a Computing 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. In this Cloud Services Large Pool of Systems Can be able to be connected. With the advance of Cloud Computing technology the cost of computation, application hosting, content storage and delivery is reduced significantly/ 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.

Cloud Providers offer services that can be grouped into three categories. 1. Software as a Service (SaaS): In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customer's side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is

offered by companies such as Google, Sales force, Microsoft, Zoho, etc. 2. Platform as a Service (Paas): Here, a layer of software, or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySql and PHP), restricted J2EE, Ruby etc. Google App Engine, Force.com, etc are some of the popular PaaS examples. 3. Infrastructure as a Service (Iaas): IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure. Some common examples are Amazon, GoGrid, Tera, etc.

Understanding Public and Private Clouds Enterprises can choose to deploy applications on Public, Private or Hybrid clouds. Cloud Integrators can play a vital part in determining the right cloud path for each organization. Public Cloud Public clouds are owned and operated by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual client an attractive low-cost, "Pay-as-you-go" model. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These are managed and supported by the cloud provider. One of the advantages of a Public cloud is that they may be larger than an enterprises cloud, thus providing the ability to scale seamlessly, on demand. Private Cloud Private Clouds are built exclusively for a single enterprise. They aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variations to a private cloud: - On-premise Private Cloud: On-premise private clouds, also known as internal clouds are hosted within one's own data center. This model provides a more standardized process and protection, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources. This is best suited for applications which require complete control and configurability of the infrastructure and security. - Externally hosted Private Cloud: This type of private cloud is hosted externally with a cloud provider, where the provider facilitates an exclusive cloud environment with full guarantee of privacy. This is best suited for enterprises that don't prefer a public cloud due to sharing of physical resources. Hybrid Cloud Hybrid Clouds combine both public and private cloud models. With a Hybrid Cloud, service providers can utilize third party Cloud Providers in a full or partial manner thus increasing the flexibility of computing. The Hybrid cloud environment is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.

Cloud Computing Benefits Enterprises would need to align their applications, so as to exploit the architecture models that Cloud Computing offers. Some of the typical benefits are listed below: 1. Reduced Cost There are a number of reasons to attribute Cloud technology with lower costs. The billing model is pay as per usage; the infrastructure is not purchased thus lowering maintenance. Initial expense and recurring expenses are much lower than traditional computing. 2. Increased Storage With the massive Infrastructure that is offered by Cloud providers today, storage & maintenance of large volumes of data is a reality. Sudden workload spikes are also managed effectively & efficiently, since the cloud can scale dynamically. 3. Flexibility This is an extremely important characteristic. With enterprises having to adapt, even more rapidly, to changing business conditions, speed to deliver is critical. Cloud computing stresses on getting applications to market very quickly, by using the most appropriate building blocks necessary for deployment.

Cloud Computing Challenges Despite its growing influence, concerns regarding cloud computing still remain. In our opinion, the benefits outweigh the drawbacks and the model is worth exploring. Some common challenges are: 1. Data Protection Data Security is a crucial element that warrants scrutiny. Enterprises are reluctant to buy an assurance of business data security from vendors. They fear losing data to competition and the data confidentiality of consumers. In many instances, the actual storage location is not disclosed, adding onto the security concerns of enterprises. In the existing models, firewalls across data centers (owned by enterprises) protect this sensitive information. In the cloud model, Service providers are responsible for maintaining data security and enterprises would have to rely on them. 2. Data Recovery and Availability All business applications have Service level agreements that are stringently followed. Operational teams play a key role in management of service level agreements and runtime governance of applications. In production environments, operational teams support appropriate clustering and Fail over Data Replication System monitoring (Transactions monitoring, logs monitoring and others) Maintenance (Runtime Governance) Disaster recovery Capacity and performance management If, any of the above mentioned services is under-served by a cloud provider, the damage & impact could be severe. 3. Management Capabilities Despite there being multiple cloud providers, the management of platform and infrastructure is still in its infancy. Features like „Auto-scaling for example, are a crucial requirement for many enterprises. There is huge potential to improve on the scalability and load balancing features provided today. 4. Regulatory and Compliance Restrictions In some of the European countries, Government regulations do not allow customer's personal information and other sensitive information to be physically located outside the state or country. In order to meet such requirements, cloud providers need to setup a data center or a storage site exclusively within the country to comply with regulations. Having such an infrastructure may not always be feasible and is a big challenge for cloud providers. With cloud computing, the action moves to the interface — that is, to the interface between service suppliers and multiple groups

of service consumers. Cloud services will demand expertise in distributed services, procurement, risk assessment and service negotiation — areas that many enterprises are only modestly equipped to handle.

II. Main Concept in this Research Paper

In this Research Paper We Analyzed the new type of approach for Protecting the Multi-Media Content in the Cloud.

EXISTING SYSTEM:

- The problem of protecting various types of multimedia content has attracted significant attention from academia and industry. One approach to this problem is using watermarking, in which some distinctive information is embedded in the content itself and a method is used to search for this information in order to verify the authenticity of the content.
- Many previous works proposed different methods for creating and matching signatures. These methods can be classified into four categories: spatial, temporal, color, and transform-domain. Spatial signatures (particularly the block-based) are the most widely used.
- Youtube Content ID, Vobile VDNA, and MarkMonitor are some of the industrial examples which use fingerprinting for media protection, while methods such as can be referred to as the academic state-of-the-art.

DISADVANTAGES OF EXISTING SYSTEM:

- Watermarking approach may not be suitable for already-released content without watermarks in them. Watermarking may not be effective for the rapidly increasing online videos, especially those uploaded to sites such as YouTube and played back by any video player.
- Spatial signatures 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. Transform-domain signatures are computationally intensive and not widely used in practice.

PROPOSED SYSTEM:

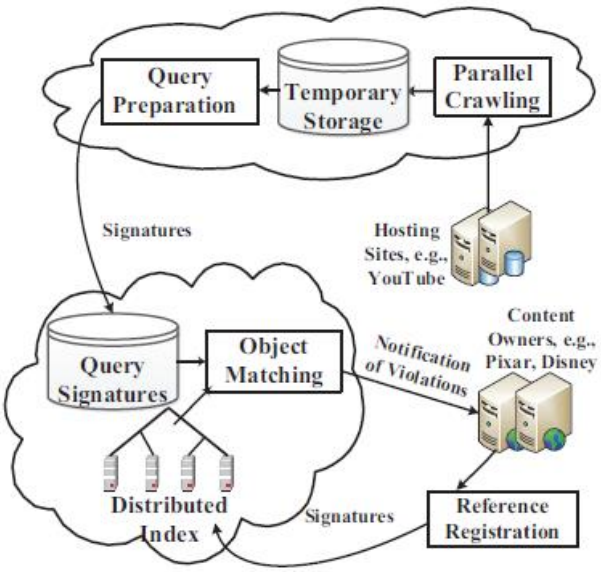
- We present a novel system for multimedia content protection on cloud infrastructures. The system can be used to protect various multimedia content types.
- In our proposed system we present complete multi-cloud system for multimedia content protection. The system supports different types of multimedia content and can effectively utilize varying computing resources.
- Novel method for creating signatures for videos. This method creates signatures that capture the depth in stereo content without computing the depth signal itself, which is a computationally expensive process.
- New design for a distributed matching engine for high-dimensional multimedia objects. This design provides the primitive function of finding -nearest neighbors for large-scale datasets.
- The design also offers an auxiliary function for further processing of the neighbors. This two-level design enables the proposed system to easily support different types of multimedia content.
- The focus of this paper is on the other approach for protecting multimedia content, which is content-based copy detection (CBCD). In this approach, signatures are extracted from original objects. Signatures are also created from query (suspected) objects downloaded from online sites. Then, the similarity is computed between original and suspected objects to find potential copies.

ADVANTAGES OF PROPOSED SYSTEM:

- Accuracy.
- Computational Efficiency.
- Scalability and Reliability.
- Cost Efficiency.
- 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.

III. Architecture of multimedia content Protection of the Proposed System

The original antenna is chosen to be a square in order to excite two modes with close resonant frequencies required for circular polarization. Asymmetry in the structure is introduced through edges, so that co-axial line feed point is along the diagonal of the patch. Both LHCP and RHCP can be obtained by shifting the feed point to accurate positions on the diagonal axis.



Fig

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.

The proposed system has multiple components as shown in figure. 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 multidimensional 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 up- loaders or downloader's.

Conclusion

In this paper a Clear survey has been done for protecting the multi-media contents on cloud infrastructure. The Different types of problems for protecting the various contents on cloud environment has been identified. After the Extensive Literature Survey the concepts from several papers a method is also proposed to protect the multimedia content on cloud infrastructures. We have been Implemented Perfect Architecture and Clear Method to Protect 2D Videos, 3D Videos, text, data and Audio Contents.

References:

1) K. Phani Srinivas "Clock Harmonization during Time - Variant Under water International Journal of Engineering Trends and Technology (IJETT). V4(4):1158-1163 Apr 2013. ISSN:2231-5381. www.ijettjournal.org. published by seventh sense research group.
2) Manas Pulipat, K. Phani Srinivas, "Comparison of Various Short Range Wireless Communication Technologies withNFC", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2 Issue April 2013.
3) J. F. Yang and Z. B. Chen, "Cloud Computing Research and Security Issues," 2010 IEEE International Conference on Computational Intelligence and Software Engineering (CiSE), Wuhan pp. 1-3, DOI= 10-12 Dec. 2010.
4) S. Zhang, S. F. Zhang, X. B. Chen, and X. Z. Huo, "Cloud Computing Research and Development Trend," In Proceedings of the 2010 Second International Conference on Future Networks (ICFN '10). IEEE Computer Society, Washington, DC, USA, pp. 93-97. DOI=10.1109/ICFN.2010. 58.
5) J. J. Peng, X. J. Zhang, Z. Lei, B. F. Zhang, W. Zhang, and Q. Li, "Comparison of Several Cloud Computing Platforms," 2009 Second International Symposium on Information Science and Engineering (ISISE '09). IEEE Computer Society, Washington, DC, USA, pp. 23-27, DOI=10.1109/ISISE.2009.94.
6) S. Zhang, S. F. Zhang, X. B. Chen, and X. Z. Huo, "The Comparison between Cloud Computing and Grid Computing," 2010 International Conference on Computer Application and System Modeling (ICCASM), pp. V11-72 - V11-75, DOI= 22-24 Oct. 2010.
7) M. M. Alabbadi, "Cloud Computing for Education and Learning: Education and Learning as a Service (ELaaS)," 2011 14th International Conference on Interactive Collaborative Learning (ICL), pp. 589 – 594, DOI=21-23 Sept. 2011.
8) P. Kalagiakos "Cloud Computing Learning," 2011 5th International Conference on Application of Information and Communication Technologies (AICT), Baku pp. 1 - 4, DOI=12-14 Oct. 2011.
9) P. Mell and T. Grance, "Draft nist working definition of cloud computing - vol. 21, Aug 2009, 2009.
10) "Sun Microsystems Unveils Open Cloud Platform," [Online]. Available: http://www.sun.com/aboutsun/pr/2009-03/sunflash.20090318.2.xml,2 009.
11) W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a Service Security: Challenges and Solutions," 2010 7th International Conference on Informatics and System, pp. 1-8, March 2010.

