A Survey on Digital Rights Management (DRM) in Cloud Networking

Ms.Swapna D.Lokhande
ABHA Gaikwad Patil
College of Engineering

Mr.Girish Agrawal
ABHA Gaikwad Patil
College of Engineering

Ms.Parul Bhanarkar
ABHA Gaikwad Patil
College of Engineering

Abstract

Digital Rights Management (DRM) is mostly known as set of procedures , skills and trappings that is premeditated to securely manage, protect and give right to access the digital content to the authorized user. DRM is the "digital organization of rights" and not the "organization of digital rights". DRM manages all rights, not only the rights applicable to permissions over digital content but also on its security and privacy. Till now this concept is not used for cloud network where security is critical issue. In this proposed system an RSS (Rich Site Summary) is been created and used as information content. Then this digital content is been dropped in cloud network. Security of this content is been done by using DRM techniques. The main objective of this paper is to manage its rights over the cloud or server and preserve its privacy using double encryption technique.

Keywords: DRM, Privacy, multiple keys, encryption, RSS, security.

1. Introduction

The Digital Rights Management has to face one of the greatest challenges for digital content distribution and its security in this digital age. Digital rights management (DRM) is a class of access control technologies that are used by Hardware Company, publishers, copyright owner and users with the intent to limit the use of digital content and devices after sale. DRM is any technology that restrains uses of digital content that are not required or proposed by the content provider. DRM also take in specific instances of digital mechanism or procedure. Digital rights management (DRM) is about controlling the practice of digital content, supporting license sculpt that allow content providers the indict of content usage. The proposed system come up with a privacy-preserving DRM scheme for any computing network eg: cloud. In this proposed system.

- The first step is to create an RSS feed, which will be the collection on any information or digital data into one form.
- This feed is then published in the cloud as this system is not used in cloud. Which will help other distributor's to trade their digital data in cloud network with privacy and security.
- To keep the data secure and from the unauthorized user and to maintain its privacy of the content owner DRM techniques will be used.
-A furtive partaking scheme based on homomorphic encryption and further combines it with a double encryption scheme to accomplish privacy protection.

This development is different from usual computing where providers typically provide software and its implementation which does not satisfy the needs of users asking for an implementation of software not provided by the providers.The separation between the provision of software and its implementation make possible the market access of software providers and computing centres as they can focus on their core industry .In the future cloud computing, will make the demand of dedicated parties, they are known as service providers who act as representative for the users who make possible the use of cloud computing. Those service providers handle the users' payments for software bought from software providers and software carried out at computing centres. Moreover, the service providers handle the storage of the user's software within the cloud. They are also responsible for checking the licenses before allowing the software implementation. Cloud Computing are the tools that uses the web and central remote servers to maintain data and applications. Cloud computing allows patrons and companies to access application without installation and use their personal files at any computer with web. This technology allows for much more resourceful computing by centralizing data storage, processing and bandwidth. A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc.

2. Introduction to DRM

Digital Rights Management (DRM) is crucial issue to fight with copyright infringement online and that it can help the copyright owner maintain artistic control or ensure continued revenue streams.

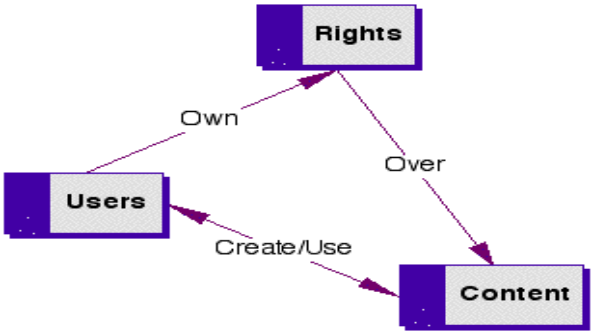
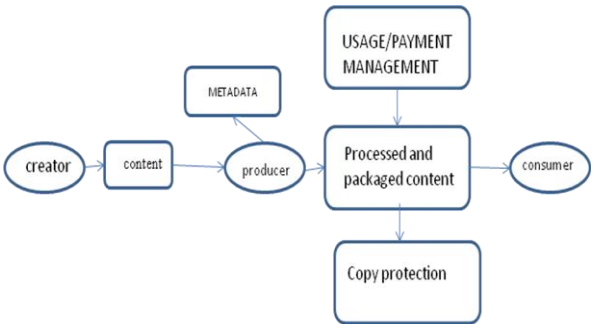


Fig - DRM Information Architecture - Core Entities Model

In this technique the user who buys the digital content owns the rights over the implementation of content when the service provider is satisfied with the user's identity and full payment is done for the content. The privacy and security is the job of DRM over the web. The overall DRM scaffold favourable for the making the digital rights facilitate systems which is modelled in following areas:

- How to manage the creation of content so it can be easily traded.
- How to manage and enable the trade of content.
- How to manage the usage of content once it has been traded. This includes supporting constraints over traded content in specific desktop systems/software.

The basic architecture for DRM is as follows:



3. Introduction to RSS.

RSS (Rich Site Summary) is a format for delivering regularly changing web content. Many news-related sites, weblogs and other online publishers syndicate their content as an RSS Feed to whoever wants it. Benefits and Reasons for using RSS solve a problem for people who regularly use the in internet. It allows you to easily stay informed by retrieving the latest content from the sites you are interested in. You save time by not needing to visit each site individually. You ensure your privacy, by not needing to join each site's email newsletter. The number of sites offering RSS feeds is growing rapidly and includes big names like News. Feed Reader or News Aggregator software allows you to grab the RSS feeds from various sites and display them for you to read and use. A variety of RSS Readers are available for different platforms. Some popular feed readers include Amphetadesk (Windows, Linux, Mac), Feed Reader (Windows), and NewsGator (Windows - integrates with Outlook). There are also a number of web-based feed readers available. My Yahoo, Bloglines, and Google Reader are popular web-based feed readers. Once you have your Feed Reader, it is a matter of finding sites that syndicate content and adding their RSS feed to the list of feeds your Feed Reader checks. Many sites display a small icon with the acronyms RSS, XML, or RDF to let you know a feed is available.

Companies are looking into ways to sell their content (eg: music /software/application etc) over the internet which are purchase and accessed by user without the buyer being able to further distribute the work. [1] Digital Rights Management (DRM) system major objective is to enable authorized user to access a version of digital content on the terms for which they are authorized whilst preventing all other access to digital content.DRM system aim to achieve a security goal. It consists of the rendering devices that communicate with the content server and license server via a network .The network can be LAN, MAN, internet or cloud computing or a mobile/wireless network .[2] The content server contains the packaged content or media of appropriate formats that can be played back on suitable content rendering devices. The licenses server generates and manages licenses that contain which tells what rights are given to which user .To protect the content from outside the system the content is stored inside a secure container. To access the container a valid license is needed .Licenses are expressed in Rights expression language. The license contains the rights object which contents the terms and conditions related to usage of the content. This requires encryption and decryption form using public and private key. In IEEE paper [3] DRM process is done between user, service provider and software provider which uses there public key and private key to give rights to access the software when the payment is done. This process includes following steps:

- Public key infrastructure (PKI) which issues certificates to the involved parties.
- Software any application buying.

- Software and retrieval which includes software encryption, secret sharing and software license and its retrieval.
- To secure its privacy re-encryption is done so that the data in secured.

There are various techniques used to secure the data such as ID techniques, terracing techniques, digital object identification, trusted computing base (TCB), evaluation techniques and security. [4] In some scenario privacy is of greater concern to the user then the payment required. In this the two basic concepts first of chaums's anonymous cash [5] and second on blind decryption [6] are used. A broad outline of a DRM system operation is presented [7] overview of the major operations in a typical DRM system. Some of the information in the content metadata, which are required for license generation, is sent from the content server to the license server. The devices (users) make a request to the content server for the desired content. If the content is packaged with the license, which is possible in case the device/user characteristics, requirements, credentials, and payment information are known beforehand, then it could be used by the devices immediately. Otherwise, a license needs to be generated after getting the required information from the user/device and before the content can be used. The content has a header that typically could consist of the license acquisition URL (the URL of the Web page of the license provider); the content ID, which uniquely identifies the content; content metadata such as author, title, descriptions, types of license; some user defined attributes; DRM version information; and the key ID. These are used by the devices and applications for appropriate rendering of content. The license can be obtained explicitly, when the device makes a license request, or implicitly, when the device attempts use the content. The device sends information about its characteristics (such as resolution and read/write capabilities), credentials (device serial number, IP address, if any), intended usage (number of times to play, to make a backup copy), and payment information. The license server uses the above information received from the device together with relevant information from content metadata to generate the rights object for the particular combination of content and intended usage. It then packages the rights object and the key (required to recover the content in case it is protected), produces the license, and sends it to the device. The device will now be able to consume the content based on the rules specified in the license .The major issues that need to be addressed include the interoperability of content format, secure delivery of content, the privacy of consumers, unmistakable specification of the rights objects.[2]The software or application execution contains following steps:

- Secret Combination in which the user and the service provider send their share values towards the computing centre to reconstruct the decryption key.
- To secure data and its privacy re-encryption scheme is used.

4. Proposed Work

- DRM in used in networking like LAN,MAN, internet, mobile or wireless but not implemented on cloud computing therefore privacy preserving and securing the data in cloud networking by using DRM techniques.
- In the proposed system we are creating an RSS is used as news feed.
- It is the application which can be purchased by other websites or application to appear on their pages but in this we are creating the application
- It can be used as Iframe on web/application pages.
- But direct use of this Iframe cannot be permitted without licensed
- It is protecting this with DRM and securing it over the network.
- The main objective of the project is to manage the rights over the cloud or server and not the design and working of an application.
- The important step is to keep the application on the cloud networking.
- As the clouding is not affordable for such a small application and it cost much, it can implemented by convert the home machine as cloud networking.

5. Common DRM techniques.

1) Digital Rights Management Techniques include:
Restrictive Licensing Agreements: The access to digital materials, copyright and public domain is controlled. Some restrictive licenses are imposed on consumers as a condition of entering a website or when downloading software.
2) Encryption, Scrambling of expressive material, and embedding of a tag. This technology is designed to control access and reproduction of online information. This includes backup copies for personal use.

6. Conclusion

In the proposed system it is pointed out that a DRM system is crucial for software providers therefore implementing in cloud computing. One major design goal of our concept is the protection of users' privacy.

The homomorphic encryption-based secret sharing scheme, combined with the software re-encryption scheme makes sure that users stay anonymous towards software providers and computing centres and profile building is not possible—not even under pseudonym—for any party. In this an application is purchased or installed in the server and its privacy is maintained using DRM in cloud server or network. In this home machine can be used as cloud, as cloud network installation or purchasing is very costly. DRM technologies may represent the future of information access. In the era of DRM, law and technology together must share responsibility for protecting intellectual privacy. Evaluating the security of DRM systems is a complex task. The issue is not solvable, i.e. there is not one denote technical solution that satisfies all security needs - amongst other reasons, the contexts in which DRM systems operate varies too greatly.

-

7. References.

[1] Eindhoven University of Technology, Department of Mathematics and Computer Science E-mail: h.l.jonker@stud.tue.nl, s.mauw@tue.nl

[2]DRM_Basics_01649008 MARCH/APRIL 2006 027- 6648©2006 IEEE.

[3] "Privacy-Preserving DRM for Cloud Computing" Ronald Petrlic Department of Computer Science University of Paderborn 33098 Paderborn, Germany ronald.petrlic@upb.de

[4] Perlman, C. Kaufman, and R. Perlner, "Privacy-Preserving DRM," in Proceedings of the 9th Symposium on Identity and Trust on the Internetser. IDTRUST'10. New York, NY, USA: ACM, 2010, pp. 69–83.[Online]. Available: http://doi.acm.org/10.1145/1750389.1750399

[5] J. E. Cohen, "DRM AND PRIVACY," Berkeley Technology Law Journal, vol. 18, pp.575–617, 2003, Georgetown Public Law Research Paper No.372741.

[6]C.Conrado, M. Petkovic, and W. Jonker, "Privacy-preserving digital rights management," in Secure Data Management, ser. Lecture Notes in Computer Science, vol. 3178. Springer, 2004, pp. 83–99.R.

[7] Iannella (2001, June). "Digital rights management Architectures" D-Lib R. L. Rivest, A. Shamir, and L. Adleman.

[8] "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, pp. 120–126, Feb. 1978. [Online]. Available: http://doi.acm.org/10.1145/359340.359342.