International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 08, August-2015

DRM Mechanism without Third Party using System Verification Technique

Sheryl D'mello
Department of Computer Engineering
St. Francis Institute of Technology
Mumbai,India

Bidisha Roy
Department of Computer Engineering
St. Francis Institute of Technology
Mumbai, India

Pradnya Rane
Department of Computer Engineering
St. Francis Institute of Technology
Mumbai, India

***Abstract*—The advance in computing and easy availability of technology has led to an increase in the consumption of digital content. It has also led to illegal replication and distribution of digital contents. This poses to huge threat to organizations dealing with highly confidential digital contents and could drastically affect its financial standing. Digital Rights Management (DRM) technologies aim to provide protection and secure distribution of the digital contents. The proposed DRM mechanism focusses on protecting and securing the distribution of digital content in a small organization. It aims to benefit the small organizations by providing security, privacy, accountability as well revocation of malicious users. It eliminates the need for third party by using the system details to provide controlled access and prevent illegal redistribution of the digital content. Various security layers have been proposed at each level that enhance the security of digital content and simultaneously achieve privacy, accountability and revocation of a malicious user without the use of third party.**

Keywords — ***Digital Rights Management (DRM), system details, revocation, accountability***

I. INTRODUCTION

The proliferation of affordable computing devices and broadband Internet access have led to increasing demand for multimedia digital content which include news, movies and music [1]. The digital methods of communication and marketing are faster, more versatile, practical and streamlined. The use of digital content in our day to day life through mobile phones, laptops, desktop computers at work, and more has drastically increased with the widespread use of Internet. Digital content mainly refers to information that can be downloaded or distributed on electronic media. The term "content" broadly refers to any processed and packaged digital information, such as digital text, audio, video, graphics, animation, images or any combinations of these types [2].With the availability of different types of digital contents, the rising question isn't what kind of content to create, but how securely can it be delivered. The rapidly growing Internet has made it easier for the replication and distribution of digital contents without leading to any particular damage to the quality of the digital contents. This has mainly led to the illegal copyright violation of the digital contents. Thus to succeed in today's digital content realm, content creators need to identify an appropriate way to present their digital content to consumers. The choice of a particular business or organization to deliver its digital content could drastically affect its financial standing. Thus Digital Rights Management (DRM) technologies were developed to provide persistent rights management for digital contents. Digital Rights Management aims towards prevention of unauthorized redistribution of digital content and restriction in the different ways in which a digital content can be copied.

.With the advent of personal computers it has become easy to copy digital content unlimited number of times and also maintain the quality level in each copy. This is likely to encourage problems such as copyrights violation and unauthorized use. Copyright is mainly the legal authority or ownership rights related to the usage or distribution of the digital content granted to the any author for his original work [3]. Violation of the ownership rights of an author or owner of digital content is called copyright violation. This can be perceived as a massive threat to organisations dealing with confidential digital content as well as in the music and movie industries. It deprives the digital content owners from receiving payment and the content consumers from obtaining the benefits of the digital content. For eg. A company paying an hefty amount to purchase a highly confidential digital content to create a new application. An employee leaving the organisation could easily leak the confidential digital content thus causing massive losses to the organisation. The DRM systems must set certain goals and aim to achieve them so as to provide a trusted platform to the users of the system. The basic goals of the DRM must be to provide protection and secure distribution of the digital content of the digital content and ensure the authenticity of the content. The use of DRM [4] can:

- Limit the devices on which the media can be consumed.
- Limit the number of times the media can be downloaded.
- Limit the number of devices onto which the media can be loaded.
- Limit the use as long as the user maintains an internet connection
- Limit the time period to use the digital content.

II. RELATED WORK

Several DRM techniques have been proposed to satisfy many of the desirable properties of DRM. Digital rights management systems are required to provide security and accountability without violating the privacy of the involved entities. It has been very difficult to achieve privacy and accountability in the same framework as they are contradictory attributes. Many DRM schemes need the user to trust a third party to provide accountability and privacy within the same framework. Moreover the use of third party is undesirable in DRM as privacy of the users cannot be assured [5] A Privacy preserving DRM scheme using trusted third party proposed in [6] uses content classification and superdistribution to balance the DRM and user privacy. Content classification means division of the digital products into groups based on rules such as content, quality and popularity. Superdistribution of digital products is done in such a way that the products are completely free of copy protection and made publicly available and distributed in encrypted form instead of being sold in retail outlets or online shops. The authors have proposed a complete framework of content classification and superdistribution, a key management scheme to protect the users' privacy. The authors have used the RSA-based key management system and traitor tracing algorithm to identify the person leaking the secret. The license management scheme with anonymous trust named LMSAT proposed in [7] provides with a powerful license acquisition and usage tracking scheme. It facilitates the user to access the contents anonymously anytime, anywhere, and on any compliant devices. LMSAT uses the Elliptic Curve Diffie-Hellman key agreement scheme to establish a secure communication channel. LMSAT can defense against a malicious attacker and protect user's privacy. Traditional super distribution schemes fail to address the consumer privacy issues and prevention of the malicious users from copying and redistributing the decryption keys or the decrypted content. The layered nature of digital contents can also be exploited to provide the consumer with choices over content quality and permit him to pay less that the quality of content used. The authors in [1] have proposed a system that superdistributes encrypted layered content and

(1) Enables the consumer to select a quality level at which the content can be decrypted and consumed.

(2) Prevents the merchant from knowing the exact content package consumed by the consumer thus improving consumer privacy

(3) Prevents the consumer from copying and redistributing the decryption keys or the decrypted content thus achieving a type of digital rights management.

The Multiparty Multilevel architecture proposed [8] focuses mainly on the scalability of the business. Multiparty refers to the involvement of many parties such as the owner, distributors, sub-distributors and consumers and the term 'multilevel' refers to multiple levels of distributors/sub-distributors. It provides log files based violation detection to support accountability. The authors have proposed a content encryption scheme based on two content encryption keys global encryption key (GEK) to prevent unauthorized use of contents and local encryption key (LEK) to prevent overloading of content servers of the owner and distributors by consumers of other distributors. The proposed mechanism uses the TTP called certification authority to issue the digital certificates. In the DRM system in [9] the license server generates the content decryption key for a user to play an encrypted content object without gaining any information to link to the specific content encrypted by the content encryption key. It is achieved by applying a (partially) blind signature primitive in the license acquisition protocol and by adopting a specific key scheme. The DRM system uses symmetric encryption is used to encrypt a content object during content packaging thus the encryption and decryption keys are the same. A key ID is used instead of a content ID since it enables a content to be packaged into different content objects by encrypting it with different encryption keys. The privacy preserving content distribution mechanism in [5] uses of the concept of tokens to secure the content and revoke the malicious users. The Owner generates anonymous tokens and is responsible for the registration of legitimate users and the revocation of malicious users. Each token consists of a expiry time and each time the token expires the Owner needs to generate new sets of Anonymous Token Set with the new expiry time and delete the expired tokens. To purchase the content the user registers himself with the owner and obtains the anonymous token set. The content usage of a User is tracked by the Content Provider using the token purchased by the user. However it increases the overhead as the owner constantly needs to generate a new set of tokens each time the token expires. The Owner and the Content Provider need to store the encrypted token Ids in the Anonymous Token Set for each unexpired and revoked token.

III. PROPOSED WORK

The proposed DRM mechanism aims to benefit the owner or admin as well as the authorized users of an organization by providing a security to their digital content using encryption and hashing algorithms, controlling access to the digital content, tracking the illegal attempts and restricting the malicious users using different security mechanism. It consists of two modules: the user and the admin/owner. In the proposed DRM mechanism the user is the consumer of the digital content. The admin can be the owner of the digital content or authorized person with proper rights to provide access to the digital content. The user module of the DRM mechanism consists of various sub modules that provides the user with a number of facilities to gain a secure access to the digital contents. The detailed working of every submodule of User DRM module depicted in Figure 3.1 is given below

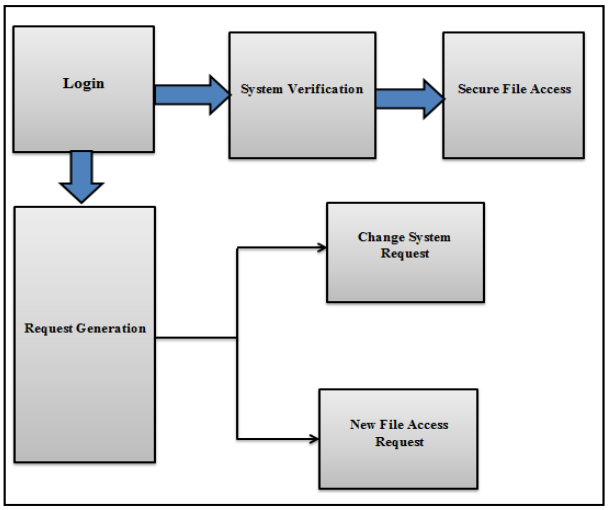

Figure 3.1 Working of User DRM

1. User DRM Module

The User DRM module of the proposed DRM mechanism facilitates the user to gain a secure access to the digital content and also maintain their security of the digital content. It uses various security measures at each step to make the DRM mechanism more robust and secure.

1) Login Module

The Login module of the DRM mechanism employs security measures to authenticate the users and prevent unauthorized access to the digital contents. The One Time Password (OTP) scheme[10] is used to generate the activation code that activates the user account after the registration process. The use of OTP makes it difficult for the attacker to impersonate the user thus limiting the damage caused. Incase if the user fails to remember the password, the user can avail the benefit of forgot password and according gain access to the system.

2) System Verification Module

The System Verification module is the second most important module of the User DRM. During the registration process, the user's system details (Hard Disk Serial Number and MAC Address) are captured and a hash value is created using the one way hash SHA-512 (Secure Hash Algorithm) [24] The computed hash value will be used to authenticate the user each time the user perform login. Thus along with the usual login ID and password an additional security mechanism is implemented to authenticate the user. This mechanism eliminates the need for any third party to authenticate the user and also allows to maintain the security of digital contents.

3) Secure File Access Module

The Secure File access module employs various security measures to provide a secure access to the digital content and also to revoke the malicious users. The OTP mechanism is used to access to the digital contents. The OTP is sent on the registered user's email ID. The RSA cryptosystem in [32] is used for the encryption and decryption of digital contents.

4) Request Generation Module

The request generation module enables the authorized users to request the owner or admin for access to new files or access from another system. It employs a proper procedure to request the admin for resolving the above issues. Request to the admin can be of the following type:

Change System Request: The Change System Request employs the OTP mechanism to generate the Change System Authentication Key. The Change System Authentication key is used to request the user to provide the facility to access the documents from any other system.

New File Access Request: The user is provided with a list of files uploaded by the admin .A facility for the user to request the admin for the desired digital content is provided. The admin can take the final decision regarding the provision of digital contents to the user's request.

2. Admin DRM module

The admin DRM module of the proposed mechanism is constructed to provide the user's with access to the digital content in a secured and controlled manner. The admin DRM focusses on the achieving accountability as well as revocation of malicious users. It employs various security mechanisms to assure the security of digital content and privacy of user's confidential details.

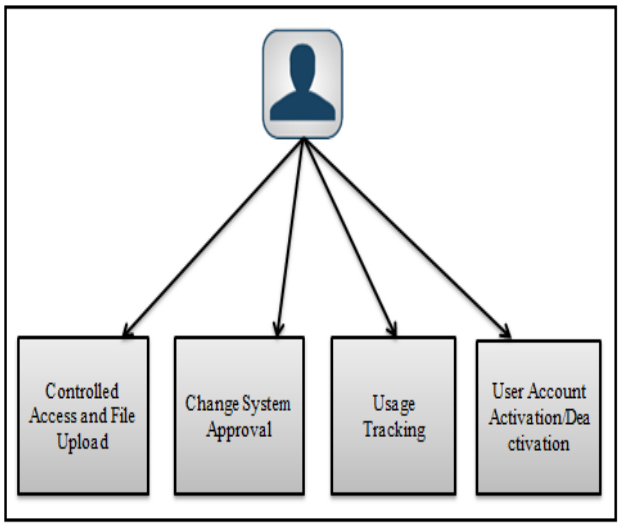

Figure 3.2 Working of Admin DRM

1) Controlled Access and File Upload Module

This module facilitates the admin to encrypt and upload the files based on the user request to access the digital content. The files are encrypted using the RSA encryption technique. The encrypted files are decrypted by the user using the RSA decryption technique. The various applications of RSA include industry, Internet, banking, online shopping, cell phones, smart cards, secure information transfers [11].

2) Change System Approval Module

The Change System Request of the User DRM module facilitates the user to request the owner to change the system using OTP mechanism. The Change System Approval module

uses the SHA-512 and Base64 Encoding Technique. The user's new system details (Hard Disk Serial number and MAC Address) are captured and a hash value is computed using the SHA-512andSalt. SHA-512.The salt value and password are encrypted with Base64 encoding technique and stored in the database.

3) Usage Tracking Module

The usage tracking module of the proposed DRM mechanism provides the facility to identify the attempts made by a malicious user to illegally use the digital content. The beauty of the mechanism is that it provides accountability without degrading the privacy of the user. The malicious user attempts to illegally access the digital content are identified by the Admin and access of the user can be completely blocked. The usage tracking module of the proposed mechanism uses Message Digest5 (MD5) algorithm as in [12] to compute a hash value of the authorized user keys and the malicious attempts are made clearly visible to provide accountability. This prevents the admin from obtaining a pattern of the keys entered by the authorized user to access the digital content and also allows the admin to know the malicious keys entered by any user.

4) User Account Activation/Deactivation

The revocation module provides with revocation of malicious users. Using the accountability feature a record of malicious attempts is obtained. The malicious attempts can be prevented by restricting the access of the malicious user to the digital contents. This module enables to prevent malicious user from causing any damage to the security of digital contents.

IV. RESULTS

To implement the proposed DRM mechanism a system to access digital contents was developed for a small organization that offered security of the digital contents, privacy of the user's details, accountability as well as revocation of malicious users. The proposed system is implemented using XAMPP server, phpMyAdmin and MySql. The graphical user interface of the User Panel is as depicted in Figure 4.1

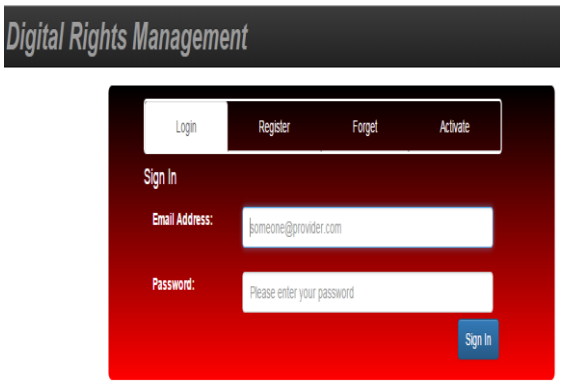

Figure 4.1 GUI User Login

The user needs to enter the activation code to activate his account. Once the user activates his account, the user home page will be shown as in Figure 4.2

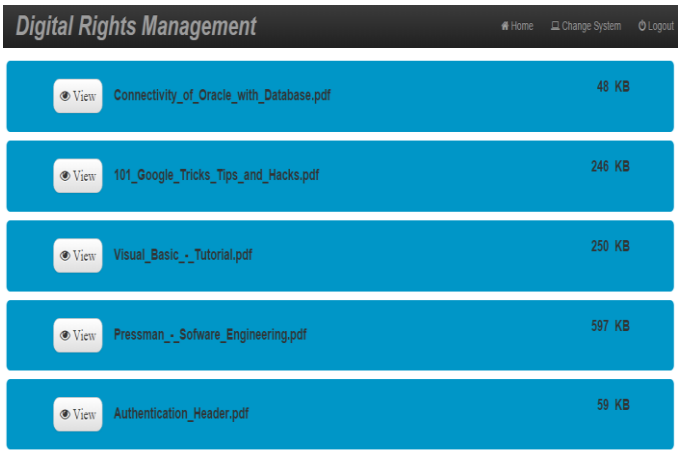

Figure 4.2 User Home Page

The admin provides access rights to the digital contents from the access file page of admin panel as shown in Figure 4.3

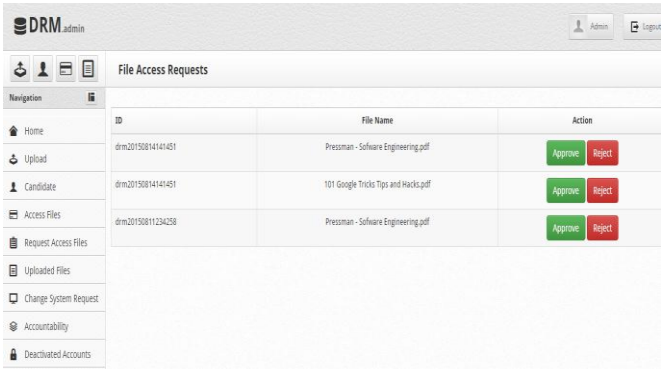

Figure 4.3 File Access Requests

V. PERFORMANCE ANALYSIS

The performance analysis of the system is done based on the key features of the proposed mechanism. The key features of the proposed mechanism are listed in the Table 5.1 given below:

Table 5.1 Key features of proposed DRM Mechanism

System Key Features	Uses	Technique Used
Activation of User Account	Verification of User's registration details	One Time Password (OTP)
Hashing of System details	Securing the user's system details	SHA-512 + Salt
System Verification Process	Control access to digital content	SHA-512 + Salt + Base64
Change System Request Process	Facility to request admin to change system	One Time Password (OTP)
User's content access Key	To prevent user from knowing the actual key	One Time Password (OTP)
Encryption and Decryption	Secure encryption and decryption of digital contents	RSA cryptosystem
Accountability	To hide authorized user's access key and display wrong keys	MD5
Revocation	To prevent attempts to access the digital content	One Time Password (OTP

The system verification process includes verification of login ID and password, capturing and computing hash of system details and comparing with the hash value stored in the database. The system verification process provides controlled access to the digital content. Thus the system verification time recorded for different users accessing the digital content using the proposed DRM mechanism is given below in Table 5.2

Table 5.2 System Verification Time (in seconds) for different Users

Number of System Users	Time required to verify the system (seconds)
User 1	0.35
User 2	0.46
User 3	0.50
User 4	0.48
User 5	0.49

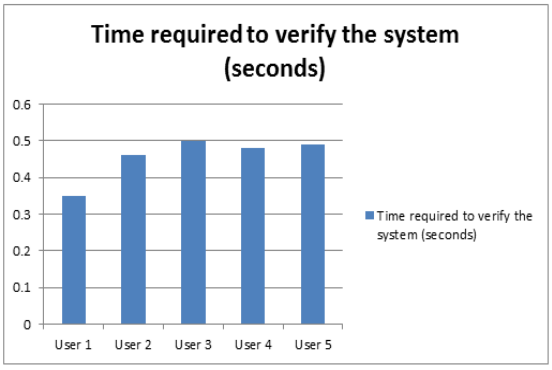

Figure 5.1 Time required to verify the system

VI. CONCLUSION

The rising popularity and widespread use of Internet has resulted in increase in the amounts of digital content being generated, stored, distributed, and consumed. The growing Internet has made it easier for the replication and distribution of digital contents without causing damage to the quality of the digital contents. Taking into consideration (account) the impacts of misuse of digital content, this research work is aimed to develop a DRM mechanism that provides with enhanced security of digital contents. The proposed mechanism provides accountability to detect any attempts to misuse the digital content. Such attempts can be detected and further prevented using the revocation feature of the DRM mechanism. The revocation feature of the DRM mechanism can prevent the malicious users from making any further malicious attempts to illegally consume the digital content. The mechanism provides with privacy of users confidential details. The beauty of the proposed system is, it provides security accountability and privacy of the users confidential details without the use of any third party. The mechanism uses the user's system itself to authenticate the user as well as to provide the security of the digital contents thus eliminating the need for third party. The proposed DRM mechanism not only minimizes illegal consumption but also eliminates the problem of illegal redistribution of malicious contents. It has the potential to detect and further prevent the malicious attempts to access and redistribute the digital content. If used effectively, it can be helpful in enhancing the security and reducing the misuse of digital contents.

REFERENCES

[1] D. J .T Chong and R.H. Deng, "Privacy Enhanced Superdistribution of Layered Content with Trusted Access Control," Copyright 2006 ACM

[2] S.R.Subramanya and K.YI.Byung ,"Digital Rights Management ", March/Arpil 2006 .

[3] Copyright [Online]. Available: http://searchsecurity.techtarget.com/definition/ copyright

[4] DRM [ONLINE]. Available: http://www.cnet.com/news/do-we-really-need-drm/.

[5] L. Win, T. Thomas, and S. Emmanuel, Member, IEEE " Privacy Enabled Digital Rights Management Without Trusted Third Party Assumption " IEEE Trans. Multimedia, VOL. 14, NO. 3, JUNE 2012

[6] J. Yao, S. Lee, and S. Nam, "Privacy Preserving DRM Solution With Content Classification and Superdistribution," *in Proc. CCNC, Las Vegas, NV,* 2009,pp.1–5

[7] J. Zhang, B. Li, L. Zhao, and S. Yang, "License management scheme with anonymous trust for digital rights management," in Proc. ICME , 2005, pp. 257–260

[8] A. Sachan , S. Emmanuel, A. Das and M. Kankanhalli, "Privacy Preserving Multiparty Multilevel DRM Architecture," National University of Singapore, Nanyang Technological University, Singapore

[9] M. Feng and B. Zhu, "A DRM system protecting consumer privacy," in Proc. CCNC, Las Vegas, NV, 2008, pp. 1075–1079. K.G.Paterson and D.Stebila, "One-time-password-authenticated key exchange," *Information Security Group Information Security Institute September 4, 2009*

[11] B. Kaliski ,"The Mathematics of the RSA Public-Key Cryptosystem," RSA Laboratories

[12] R. Rivest, "MD5," Attributed to [Wikipedia] April 1992