International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 7, July - 2014

Digital Rights Management Mechanism without Third Party

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

Asst.Prof. Bidisha Roy
St. Francis Institute of Technology
Mumbai, India

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

***Abstract*— Security of the digital content and accountability without violating the privacy of the entities are the major requirements of the Digital Rights Management Mechanisms today. It is difficult to achieve accountability and privacy within the same framework as they are mutually contradictory attributes. Trusted third parties are used by current digital rights management mechanism to provide privacy to the involved entities. Trusted third party can become malicious and break the privacy of the entities. Therefore a new content distribution mechanism for digital rights management which does not rely on the third party is proposed in this paper. The proposed mechanism supports both accountability and privacy. It makes use of the entities system details to authenticate themselves to each other. It also provides a privacy preserving revocation of malicious user. The proposed mechanism is well suited for organizations in which the security of the digital content is of utmost importance.**

Keywords*— Digital Rights Management (DRM), privacy, accountability , blind decryption, hash chain*

I. INTRODUCTION

The use of digital content has increased greatly in our day to day life due to its high quality and efficiency in storage and distribution. Digital content comes in many forms like text audio ,video ,graphics images and pdf documents. Digital content can be referred to as information available for download or distribution on electronic media like ebooks or iTunes song [1] .The availability of computing devices at a affordable rate and broadband internet access has increased the demand for multimedia digital content which includes news , movies and music[2]The growth of internet has made it easy for replication and distribution of the digital contents. This has resulted in illegal copyright violation of digital contents. Copyright is the ownership rights of an intellectual property prescribed by a national or international law. Copyright is provided automatically to the author of any original work covered by the law as soon as the work is created. The author does not have to formally register the work, although registration makes the copyright more visible [3].

Digital Rights Management is a technology that provides that provides management of rights for digital contents. For example, the Apple iTunes Music Store uses a DRM system to limit the numbers of computers that songs can be played on. Every downloaded audio file from the iTunes music store contains the information about the owner of the file and how many times the file has been transferred. The protected files will not play on computers that have not been authorized to play the music [6].Digital Rights management systems kept evolving over years due to the increase in copyright violation of the digital contents. The different generations of the digital rights management systems intended to control different malicious practices related to the use of the digital content. The aim of the first generation DRM software was to control copying while the second generation intended to control viewing, copying, printing and the altering of works or devices. The advanced DRM systems succeeded in controlling the copyright violation of digital contents. This has resulted in the violation of the privacy of the entities involved. The DRM systems must provide accountability in which the distributer or user must be accountable for the misuse of the contents or licenses purchased by them. Accountability will make sure that the users or distributers be careful and knowledgeable in using the content as even slight negligence can cause them to be legally responsible. Accountability and privacy need to be achieved together within the same framework .This was achieved with the help of a trusted third party (TTP).However a trusted third party can also become malicious and break the privacy of the involved entities. Thus both these attributes need to be achieved without the use of a third party.

In this paper we propose a digital rights management mechanism without third party. The proposed mechanism is constructed with the help of blind decryption and hash chain. The proposed mechanism makes use of the system details of both the parties to authenticate themselves thus avoiding the use of a third party. This mechanism will also provide anonymity of the users system details even after the user has been blocked for its misbehavior. The mechanism can be used for organizations trying to maintain the security of the high budget digital documents.

II. RELATED WORK

Different privacy preserving mechanism for digital rights management have been proposed in [2][5]. Simultaneous consideration of accountability and privacy has not been

addressed well yet. Achieving privacy and accountability in the same framework is difficult as they are mutually contradictory attributes[11]. Schemes that address accountability and privacy need the user to trust a third part. The use of trusted third party is undesirable as the users of the system can never be assured of their privacy

In [2] the authors have proposed a DRM system in which the license server generated the content decryption key for the user to play the encrypted content object without any information to link to the specific content object encrypted by content encryption key. It was constructed by applying a (partially) blind signature primitive in the license acquisition protocol and using a key scheme in which the content encryption key depends on the information retrieved from the content object and a secret only known to the license server. It enabled the license server to generate and deliver decryption keys to the users without any knowledge of the corresponding key IDs or the contents played by the user. The decryption key in the license is encrypted by the public key bound to the user's device so that only the desired device can play the protected content. In [4], the authors have proposed the system and corresponding protocols for privacy enhanced super distribution with trusted access control. It allows the consumer to select a quality level at which to decrypt and consume the content and prevents the merchant from knowing which exact content package is consumed by the consumer. It focuses on enhancing the consumer privacy. It also prevents the consumer from copying and redistributing the decryption keys or the decrypted contents. In [9], the authors have proposed powerful and flexible license acquisition and usage tracking scheme named LMSAT (License Management Scheme with Anonymous Trust) to allow the user access the contents anytime, anywhere, and on any compliant devices in a anonymous manner. It makes use of the Elliptic Curve Diffie Hellman key agreement scheme that establishes a secure communication channel. LMSAT can defend against a malicious attacker and protect the user's privacy. The authors in [15] have constructed a dynamic k-TAA (k-times anonymous authentication) scheme in which the authentication protocol only requires constant time and space complexities at the cost of O (k)-sized public key. The anonymous authentication systems such as *k*-TAA systems are suitable cryptographic primitives for secure applications with privacy concern like e-voting.

The system proposed in [16] makes use of anonymous token sets to provide privacy and accountability without third party within the same framework. The owner provides the user with the anonymous token set which consist of *l* anonymous tokens which the user uses for content purchase. The tokens are also used to identify the malicious user and to provide a privacy preserving revocation of malicious user. The proposed scheme provided access control without degrading the users privacy. It satisfies the conflicting requirements of accountability and privacy in digital content distribution.

III. PROPOSED WORK

The proposed digital rights management mechanism provides accountability and privacy without the use of third party. The proposed mechanism makes use of the system details (Hard disk serial number and MAC address) of both the parties to authenticate themselves. It makes use of simple cryptographic primitives like blind decryption and one way hash chain. The proposed mechanism is constructed using RSA cryptosystem. The proposed mechanism provides privacy preserving revocation of malicious users. The security of the users system details is maintained inspite of being blocked for its misbehavior.

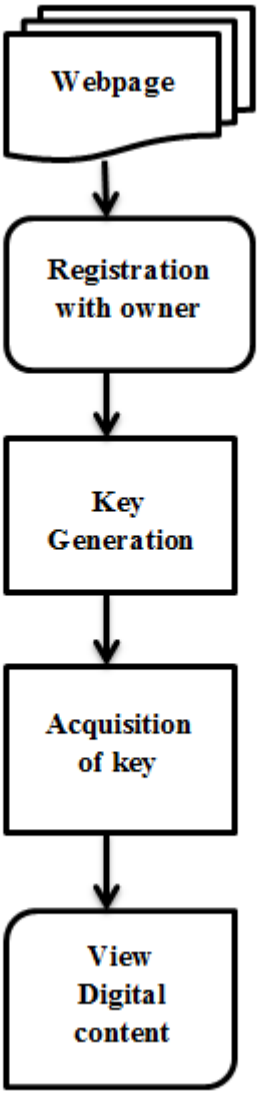

Figure 3.1.Proposed Mechanism

The implementation of the proposed system contains the following core modules:

Registration with the Owner: Inorder to purchase the digital content the user needs to be registered with the owner.The steps to register with the owner are as follows :

- The user selects the desired digital content from the list of the digital content displayed on the website.
- Once the digital content is selected the user needs to fill the registration form providing appropriate details.

- After filling the registration form ,once the use makesthe payment the users system details (Hard disk number and Mac address) are acquired.
- The acquired Hard disk and Mac address details are encrypted and stored in the database.

Key Generation : The acquired system details (Hard disk serial number and Mac address) are used to generate the key.

- The Hard disk serial number and the Mac address obtained during registration are combined and a hash value of the combination is used to generate the key .

k=H (Hard disk serial number + Mac address)

- The generated hash value of the above combination is sent to the user on the email ID mentioned by him.
- Each time the user views the digital document with the help of new hash value generated from the above combination.
- The use of hashing improves the security of the digital content by preventing hacking of the key.
- SHA-1 hash algorithm is used for the performing the hash operation.

Acquisition of key :

Once the user is registerd with owner and makes the payment for the digital content , the user requests for the key using the blind decryption mechanism [4]. The major advantages of using the blind decryption mechanism are :

- Using the blind decryption mechanism the owner is not aware of the users sensitive system details as the users acquired details are encrypted and stored in the database.
- The user too is unaware of the actual key value as each time a hash value is sent to the user on the email id registered with the owner to view the digital content.
- Thus using the blind decryption mechanism the owner will have any access to the user's sensitive system details and the user will not have any knowledge of the actual key value.
- The digital rights management mechanism thus provides security of the digital content and privacy of the users sensitive details.

Privacy preserving revocation of malicious users : In context to the application in which the proposed digital rights management mechanism will be used,a malicious user is the user entering the wrong key numer of times greater than the threshold value.

- The user's account details (user name,user type) will be sent to the admin and the users system details will be sent in encrypted form.
- The user will be notified via mail about his misbehaviour on the email ID registered with the owner.
- If the misbehaviour still persists the user's account will be blocked from further use.
- The malicious user is blocked from further use while the privacy of the system details is still preserved.
- The proposed DRM mechanism maintains the privacy of the malicious users system details and blocks the malicious user thus provides accountability for the purchased digital contents.

The proposed mechanism was implemeted in Java with eclipse-jee- kepler-SR1-win32 using MySql database and Apache Tomcat-7.0.34 preconfigured.

IV. RESULTS

The proposed digital rights manangement mechanism was applied for a website selling high budget digital contents . The user needs to log into the system to purchase if the documents. Incase the user is not registered, the user needs to perform the registration process

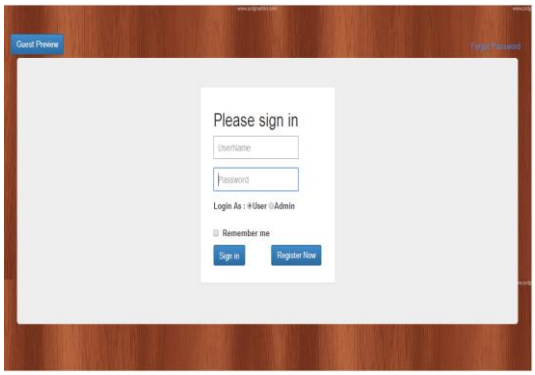

Figure 4.1.Website of digital contents

The register now tab directs the user to the registration form where the user fills the required details.

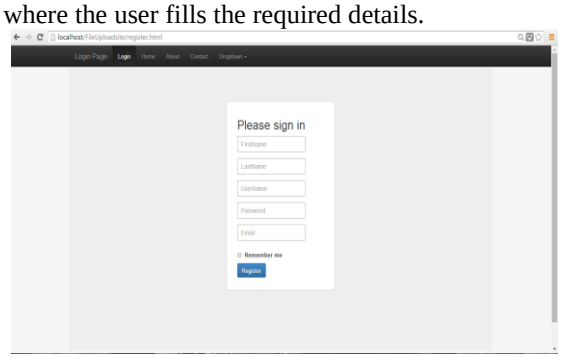

Figure 4.2.Registration Process

Once the user makes the payment and registers with the owner the user can log into system with the registered username and password.
The digital content (pdf document) uploaded from the admin is shown below

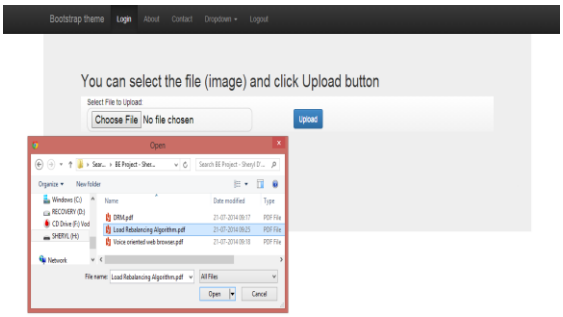

Figure 4.3.Upload Process

The uploaded digital contents can be viewed from the users account as shown below

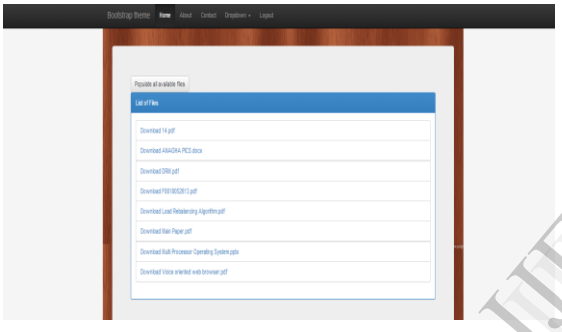

Figure 4.4.User view of digital contents

The details of the uploaded digital contents are displayed in the following manner

```
Tomcat v7.0 Server at localhost [Apache Tomcat] C:\Program Files (x86)\Java\jre7\bin\javaw.exe (21-Jul-2014 8:36:20 pm)
FieldName=fileName
FileName=Load Rebalancing Algorithm.pdf
ContentType=application/pdf
Size in bytes=234863
Absolute Path at server=C:\tempFile\tmpfiles\Load Rebalancing Algorithm.pdf
FieldName=fileName
FileName=Voice oriented web browser.pdf
ContentType=application/pdf
Size in bytes=366099
```

Figure 4.5.Information of uploaded contents

The user selects the desired digital content and the key is sent to the user on the email id given by him during registration process.

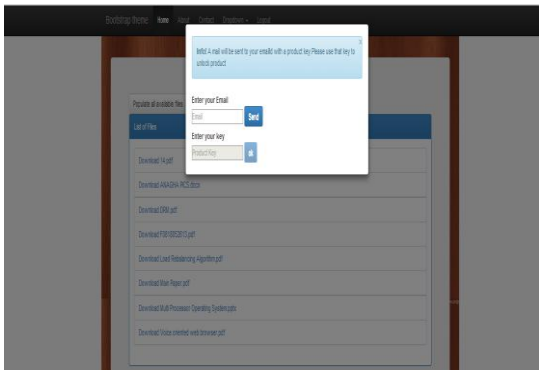

Figure 4.6. Procedure to receive key on email ID

The key generated is generated with hard disk and mac address of the users's system. The generated key is too large as it makes use of RSA cryptosystem.

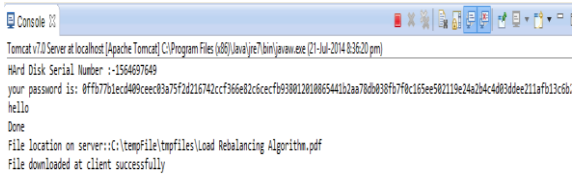

Figure 4.7. View of the generated Key

Once the key is enterd correctly the digital content can be viewed by the users.

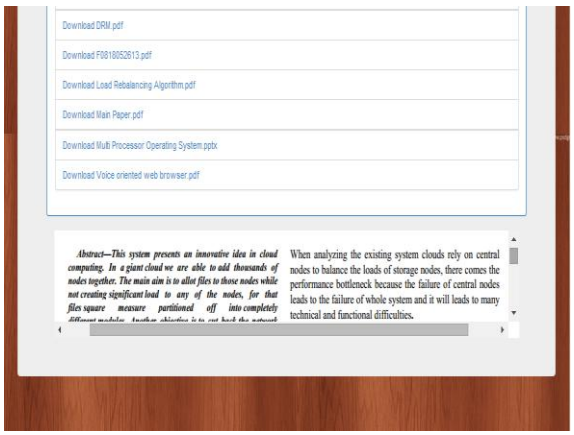

Figure 4.8.Viewing the digital content

The proposed mechanism use SHA-1 hash algorithm to enhance the security of the system. Since the mechanism makes use of the user's system details to enhance the security of the digital content and to provide accountability,the user system details must securely stored in the database.The user system details acquired during registration are encrypted and securely stored in the data.

SystemInfo
HFmi3Ige79wqYKBRjOTvKiaJKQ0axYZR49+/HJMvZK4=
HFmi3Ige79wqYKBRjOTvKiaJKQ0axYZR49+/HJMvZK4=
HFmi3Ige79wqYKBRjOTvKiaJKQ0axYZR49+/HJMvZK4=
CEdf+Hz3iqoFkVPEHMXocA==
HFmi3Ige79wqYKBRjOTvKiaJKQ0axYZR49+/HJMvZK4=
HFmi3Ige79wqYKBRjOTvKiaJKQ0axYZR49+/HJMvZK4=
CEdf+Hz3iqoFkVPEHMXocA==
HFmi3Ige79wqYKBRjOTvKiaJKQ0axYZR49+/HJMvZK4=
CEdf+Hz3iqoFkVPEHMXocA==
CEdf+Hz3iqoFkVPEHMXocA==
HFmi3Ige79wqYKBRjOTvKiaJKQ0axYZR49+/HJMvZK4=
CEdf+Hz3iqoFkVPEHMXocA==
CEdf+Hz3iqoFkVPEHMXocA==

Figure 4.9.Encrypted user's system details in database

The features supported by our proposed digital rights management mechanism are shown below

Features	Proposed Mechanism
Non Anonymous User Authentication	Y
Content Accountability	Y
No Reliance on TTP	Y
Prevent Hacking of Key	Y
Privacy of User's system details	Y
Revocation of malicious User	Y
High security of Digital Content	Y

V. CONCLUSION

The proposed digital rights management mechanism aims to focus on the high security of the digital content and privacy of the user's sytem details.The key generated using the user's system details (hard disk serial number and mac addres)s is to enhance the secuirty of the digital content and to prevent the piracy of the secure digital content.The proposed mechanism can be applied to organisations that pay heavily for purchasing digital documents for their projects.The employees of the organisation can never circulate the digital content or use it for personal benefits.The proposed mechanism provides accountabilty along with security of the digital content.The proposed mechanism also provides the revocation of malicious user but the system details of the malious user are not disclosed

REFERENCE

[1] R.Perlman Intel ,C. Kaufman Microsoft, R. Perlner NIST " Privacy-Preserving DRM" *IDtrust '10, April 13-15, 2010, Gaithersburg, MD.* Copyright © 2010 ACM ISBN 978-1-60558-895-7/10/04…

[2] M. Feng and B. Zhu, "A DRM system protecting consumer privacy," in *Proc. CCNC*, Las Vegas, NV, 2008, pp. 1075–1079.

[3] http://searchsecurity.techtarget.com/definition/copyright, Copyright, September 2013

[4] K. Sakurai and Y. Yamane, "Blind decoding, blind undeniable signatures, and their applications to privacy protection," in *Proc. 1st Int. Workshop Inf. Hiding*, May/Jun. 1996, pp. 257–264

[5] L. Wenjing and R. Kui, "Security, privacy, and accountability in wireless access networks," *IEEE Wireless Commun.*, vol. 16, no. 4, pp. 80–87, 2009.

[6] 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

[7] 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. S

[8] 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.

[9] S.Nair, Bogdan C. Popescu, C. Gamage, B. Crispo, A. Tanenbaum "Enabling DRM-preserving Digital Content Redistribution**"** Dept. of Computer Science

[10] http://www.techterms.com/definition/drm ,DRM September 2013W.

[11] http://www.cs.columbia.edu/~evs/intro/Oracle.html September 2013 Eric Siegel, "The Oracle Problem" [online]

[12] Hyun, Kim, S. Hun, Jin,The Dept. of Information Security, University of Science and Technology, Daejeon, Korea " Accountable Privacy Based on Publicly Verifiable Secret Sharing" *ISBN* 978-89-5519-146-2 Feb. 7-10, 2010 ICACT 2010;

[13] http://www.econtentmag.com/Articles/Resources/Defining-EContent/What-is-Digital -Content-79501.html Digital Content September 2013 .

[14] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol.24,no.11, pp. 770–772, 1981.

[15] M.H.Au, W.Susilo and Y.Mu," Constant-sizek-TAA,"*LNCS*,vol.4116,pp.11-125,2006