Preserving Privacy and Illegal Content Distribution for Cloud Environment

[1] Manish H. Gourkhede, [2] Deepti P. Theng

[1]CSE Department, GHRCE
Nagpur Maharashtra India

[2]CSE Department, GHRCE
Nagpur, Maharashtra, India

Abstract - Cloud computing is an emerging technology where a huge amount of copyrighted data is stored from different vendors and organizations. The digital content can be easily copied and distributed over the internet; moreover the users who are involved in the content transaction need to authenticate themselves by login process to access the data. This login detail and usage patterns of user can be used to generate user's complete profile thus revealing the identity of the user. A trusted third party can be used for mutual trust but there is a possibility that the TTP being malicious. We are focusing on these problems and using an enhanced scheme enabled with Digital rights management to prevent illegal distribution of the content. The proposed scheme also preserves the privacy of the users without relying on any third party for mutual trust.

***Keywords* - Cloud computing, Privacy, Security, Digital rights management, Trusted Third Party.**

1. Introduction

With the increased use of the internet and invent of cloud computing technology which provides storage as a service for huge amount of data the usage of digital content in the world has increased tremendously. It is easy to copy, share and distribute this digital content via internet. To prevent this illegal distribution of copyrighted data the use of digital rights management has started but the use of digital rights management requires content provider to gather the information of the user who are using this technology either through a direct or an indirect way by license acquisition process or user authentication. The users who are involved in the content transaction require the privacy of their identity so that the content provider cannot infer their profiles and track the pattern of content they are using. Some mechanism preserving the privacy of the user has been proposed in [2], [7], [13], [15], [24] but this mechanism compromised with the accountability of content usage by the user. Some mechanisms rely on a trusted third party for accountability and privacy purpose whereas other mechanism based on complex cryptographic algorithms doesn't satisfy most of the required DRM properties; moreover user can't rely completely on any trusted third party as there is possibility that a TTP become malicious. Some trusted third party assumption based DRM scheme has been proposed in [4-5], [14-15], [18-20]. In [19] the researchers have proposed a mechanism based on anonymity ID for providing privacy in DRM but in this mechanism the user needs to trust an authentication server that can relate these all anonymity IDs to the user identities. Same problem has been mentioned in [8] and [20] by separating the responsibilities between certification authorities and content providers. However to block a user from future use the TTP requires to combine and relate the anonymity ID with the real identity of that user. In [25], "verifiable secret sharing," "zero knowledge proofs," and "time capsule" cryptographic primitives have been used to design a privacy preserving scheme for DRM.

However, this scheme requires trusting a user and two revocation authorities. Reliance on TTP assumption has been avoided in [2], [16-19], [21]. A prepayment anonymous scheme is used in [19] to get anonymous ID due to which the identity of user is not authenticated. [16] uses the concept of partial blind signature method for anonymous use of digital content this scheme does not support tracing and revocation of malicious users. The schemes mentioned in [18], [2] lacks accounting of contents sold..Scheme proposed in Tsang et al. [17] have provided a privacy preserving accountability mechanism for DRM using "zero-knowledge proofs." However, their mechanism requires many rounds of communications and assumes that a user has unlimited computational power. This paper is an extension to the paper mentioned in [1] where detailed literature survey and comparison with different schemes is presented. In this paper we are showing the experimental results of the proposed scheme for cloud environment

This paper is organized as follows: Proposed Scheme is discussed in section 2, Experimental results are carried out in section 3, and section 4, gives the conclusion.

2. Proposed Scheme

Our approach is based on the scheme mentioned in [3]. In literature survey [1] we have discussed various schemes and based on the comparison we have selected this privacy enhanced Scheme which overcomes the drawback of preserving privacy of user and preventing illegal distribution of copyrighted data for cloud environment.

In this scheme we have a data owner, a cloud service provider and an end user. The data owner is an entity who uploads its copyrighted content on the cloud. An end user is a person who wants to access the data stored in the cloud. Our system architecture of proposed scheme for cloud environment is given in Figure 1.

Step by step explanation is given below.

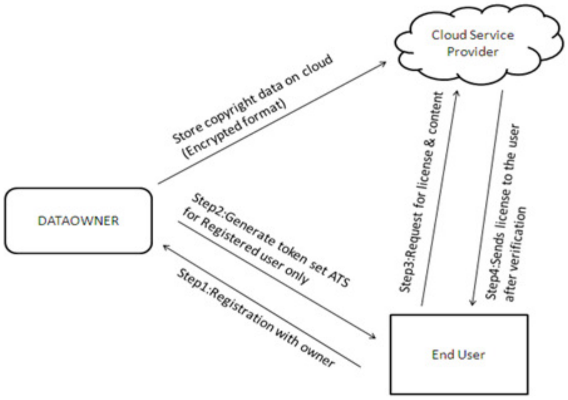

Cloud Service Provider
Store copyright data on cloud (Encrypted format)
DATAOWNER
Step2:Generate token set ATS for Registered user only
Step1:Registration with owner
Step3:Request for license & content
Step4:Sends license to the user after verification
End User

Fig.1 System Architecture

STEP I: The owner will upload its copyrighted content on the cloud

STEP II: The user who wants to access the Cloud content will register with data owner by making payment.

STEP III: The data owner will now generate Anonymous Token Set for the registered users only.

STEP IV: The end user now request for license to access the encrypted content.

STEP V: The DRM agent on the cloud will now send the License for accessing the content to the user only if the token presented by end user is found to be a valid token. Detailed explanation of our scheme is given below:

2.1 Token Generation:

The dataowner will generate a set of anonymous token sets:

$\{ATS_1, \ldots\ldots ATS_n\}$ only for the users who are registered with dataowner and have paid the required amount using one of the scheme mentioned in [22-23]. Each ATS consist of n number of tokens ATS= $\{T_1 \ldots \ldots T_n\}$. A user U_i will request for ATS_i to the dataowner and used each token in the set ATS_i for each transaction with Cloud service Provider (CSP).
Let $TID_{(i,j)}$ denotes the ID of the token $T_{(i,j)}$ and
$TID^{enc}_{(i,j)} = \varepsilon_{pub}(TID_{(i,j)}, K_{pb})$ denotes the encryption of $TID_{(i,j)}$ with the public key K_{pb} of the owner.
Let T_{exp} denotes the expiry time of all the tokens and
$TID^{sgn}_{(i,j)} = S_{ign}(TID^{enc}_{(i,j)} \parallel T_{exp}, K_{pr})$
Denotes the Digital signature of the concatenation of $TID^{enc}_{(i,j)}$ with T_{exp} using the private key K_{pr} of the Owner.
Now, each token $TID_{(i,j)}$ in the token set ATS_i is given by
$TID_{(i,j)} = \{TID^{enc}_{(i,j)}, TID^{sgn}_{(i,j)}, T_{exp}\}$.

2.2 Content and License Creation with Access Control

The dataowner defines the usage attribute Key KU_{att} for the usage of the content. The dataowner defines this attribute for each content separately. Only the user who has the required usage attribute key can access the content. The user gets the usage attribute key during the registration process from the dataowner on the basis of the given details by the user during registration.
For example, if the specified usage attribute for the usage of the content X are the user must be a citizen of USA, resident of New York, and age must be above 18 year then the attribute key for the usage of the content can be the three tuple,

$KU_{att} = \{KU_{USA}, KU_{NY}, KU_{over18}\}$
The data owner generates the Content Encryption Key (CEK) on the basis of the usage attribute key KU_{att} and content usage key KU_x. The content encryption key CEK is generated using a hash functions as follows:
$CEK_x = H(KU_{att} \parallel KU_x)$ Where H is a hash function. The dataowner encrypts the content X with the CEK_x. The

usage Key will be inserted into the usage license and the usage license $\mathrm{L_x}$ will be created as:
$\mathrm{L_A} = (\mathrm{UserID}, \mathrm{UsageRights}, \mathrm{ContentID_x}, \mathrm{KU_x})$

Where UserID is the token used in the transaction, usage rights are the rights predefined by the data owner, $\mathrm{ContentID_x}$ a unique ID of the content. Therefore, only eligible and authentic end-users can get the correct $\mathrm{CEK_x}$. The data owner stores the content package in the cloud which consists of two parts the content header and the encrypted content the content header part stores the necessary information about the content and the required attributes which are necessary for eligible end users. If a user qualifies for the attributes which are mentioned in the header part, the user can access and download the content package from the cloud.

2.3. Registration and Acquisition of Anonymous Token

Each user needs to be registered with the dataowner to obtain the anonymous token set package from the dataowner only if that particular user has made payment for service using anonymous payment scheme as mentioned in [22-23].

To use the Anonymous Token Set Package $\{K_i^{enc}, \mathrm{ATS}_i^{\mathrm{enc}}\}$ user needs the decryption of the key K_i, at a later point (the Owner will not know with which user he is interacting) of time requests the decryption of using the following blind decryption protocol [24].

1) User Chooses a random secret blinding factor r_i such that
$0 < r_i < \mathrm{n}$ user then computes $x_i = \ r_i^e \mathit{mod}\ n$ and sends
$K_i^{enc} x_i$ to the owner together with its PKI certificate, identity information and decryption request encrypted with owner’s public key.

2) Owner decrypts and verifies the PKI certificate and the identity information of U_i.

Owner then computes
$z_i = y_i^d \quad modn = K_i r_i \quad modn$ and sends z_i to $\mathrm{U_i}$. Owner saves the PKI certificate and the identity information of U_i in its database.

3) U_i computes $K_i = \left(\frac{z_i}{r_i}\right) mod\ n$ and obtains the decryption key $k_i = H(K_i)$.
After obtaining the decryption key k_i, U_i uses it to decrypt $\mathrm{ATS}_i^{\mathrm{enc}}$ to get the Anonymous token set ATS_i. U_i uses each token $\mathrm{TID}_{(i,j)}$ Є ATS_i for each transaction with the Content Provider. Content Provider only verifies the signature on the encrypted ID of the token $TID_{(i,j)}^{enc}$ Є $\mathrm{T}_{(i,j)}$ Thus the Content Provider will not get the real ID of the token $\mathrm{T}_{(i,j)}$.This is to avoid any misuse of the token ID by the Content Provider. Thus, U_i will not be required to decrypt $TID_{(i,j)}^{enc}$ the protocol for the decryption of K_i^{enc} is required to be performed by U_i only at the first contact of U_i to the system. The protocol is executed again only if the anonymous tokens of U_i are expired.

2.4 License Acquisition

In license acquisition phase the registered user will send one of the token in the $\mathrm{ATS_i}$ to get the license which is required to access and decrypt the encrypted content. While sending the request for the license of the content user will send one of his valid token for authentication, license request for content X let it be $\mathrm{L_x}$, and a secret key $\mathrm{K_x}$. This license request is encrypted with the Public Key of the content provider. Content provider decrypts this request and checks the time stamp of the token, whether it belongs to the revocation list. If everything is found correct then the content provider will send the License $\mathrm{L_x}$ to the user which contains usage key $\mathrm{K_{U_x}}$of the content x.
{ $\mathrm{K_{U_i}}$,$\mathrm{TID}_{(i,j)}$, License $\mathrm{L_x}$ request }

2.5 Privacy Preserving Revocation of User:

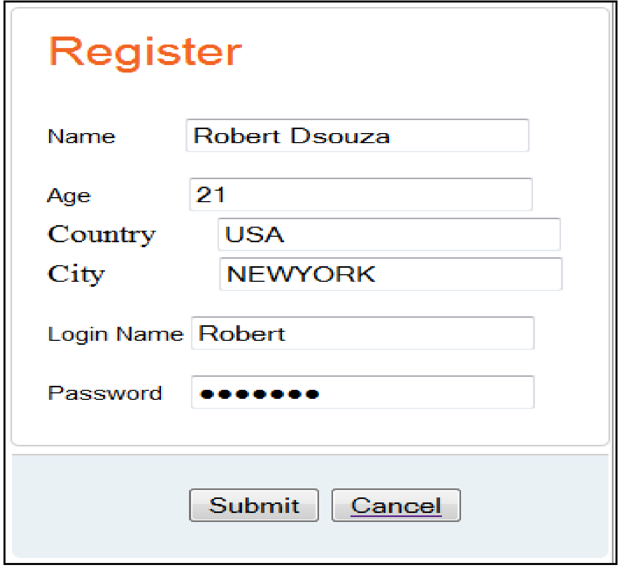
If a user violates the license by using the token in an illegal way then that user will get revoked by the data owner. Initially the revocation is performed by the CSP then the CSP sends the token to the data owner. The data owner will perform reverse hashing and generate all token in that ATS and Revoke it.

3. Experimental Results

The proposed scheme is implemented on php using the xammp 1.7.4 simulator which provide virtual environment for cloud; on a system having configuration 2.5 GHz Processor, 1 GB of RAM, Windows XP 2007 Operating system on Mozilla Firefox browser.

A step by step execution detail is given with each Snapshot

Snap1:



Register

Name: Robert Dsouza

Age: 21

Country: USA

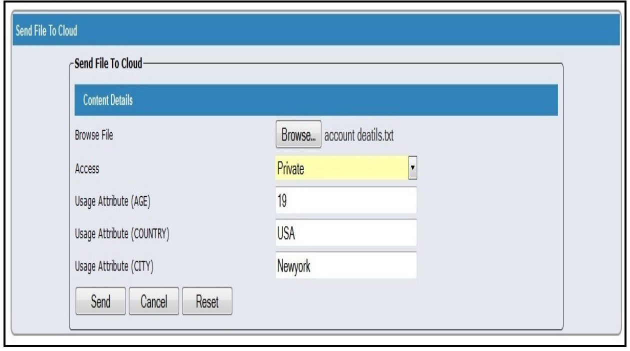
City: NEWYORK

Login Name: Robert

Password: ●●●●●●●

User register with dataowner with the required details.during this process the user get the required usage attribute key.

Snap2:



Send File To Cloud

Send File To Cloud

Content Details

Browse File: account deatils.txt

Access: Private

Usage Attribute (AGE): 19

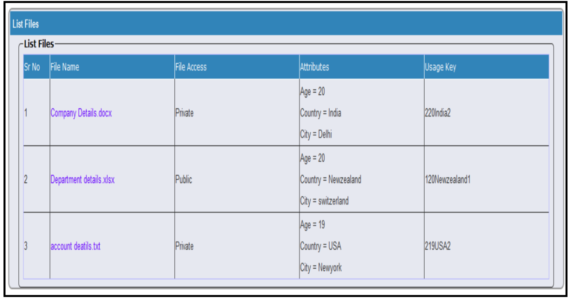
Usage Attribute (COUNTRY): USA

Usage Attribute (CITY): Newyork

First the dataowner will send the copyrighted file into the cloud. During this process the dataowner set the usage attribute for that particular content such as Age, Country, and City also dataowner set the type of access private or public. Public files are directly access by the users whereas private files require tokens generated by dataowner for registered user to access the private content.

This usage attributes and digital signature of token is checked at the time of license request to get the usage key for accessing the content. Thus the copyrighted content will be access by only legitimate users only who have the required attributes as mention in section 2.2

Snap3:



List Files

List Files

Sr No	File Name	File Access	Attributes	Usage Key

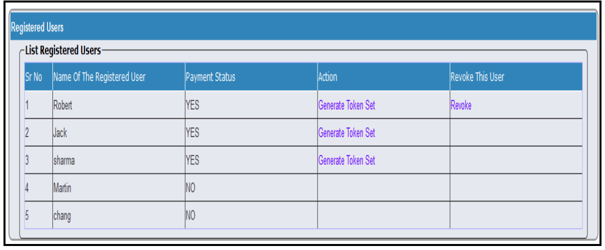
1	Company Details.docx	Private	Age = 20
			Country = India
			City = Delhi
				220India2

2	Department details.xlsx	Public	Age = 20
			Country = Newzealand
			City = switzerland
				120Newzealand1

3	account deatils.txt	Private	Age = 19
			Country = USA
			City = Newyork
				219USA2

This snap shows some files and their attributes which are defined by data owner

Snap 4:



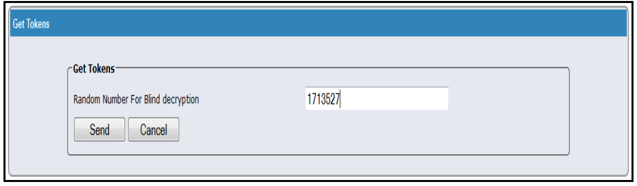
Registered Users

List Registered Users

Sr No	Name Of The Registered User	Payment Status	Action	Revoke This User
1	Robert	YES	Generate Token Set	Revoke
2	Jack	YES	Generate Token Set	
3	sharma	YES	Generate Token Set	
4	Martin	NO		
5	chang	NO		

The registered user needs to pay for the service using one of the schemes as mentioned in [22-23] after payment is done by user the data owner will generate the set of tokens for the registered user.

Snap 5:



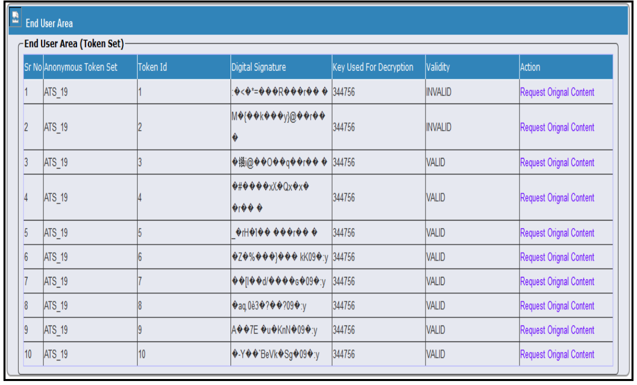
Get Tokens

Get Tokens

Random Number For Blind decryption: 1713527

When user request to get token at that time blind decryption is performed [24] for blind decryption user sends a secret value to get the token decryption key to decrypt the ATS and to get the list of tokens.

Snap 6:



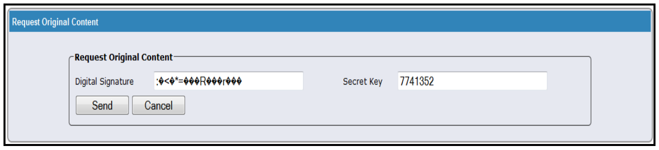
End User Area

End User Area (Token Set)

Sr No	Anonymous Token Set	Token Id	Digital Signature	Key Used For Decryption	Validity	Action
1	ATS_19	1	:�<�*=���R���r�� �	344756	INVALID	Request Orignal Content
2	ATS_19	2	M�{��k���y}@��r�� �	344756	INVALID	Request Orignal Content
3	ATS_19	3	�鑶i@��O��q��r�� �	344756	VALID	Request Orignal Content
4	ATS_19	4	�#����xX�Qx�x� �r�� �	344756	VALID	Request Orignal Content
5	ATS_19	5	_�rH�1�� ���r�� �	344756	VALID	Request Orignal Content
6	ATS_19	6	�Z�%���}��� kK09�:y	344756	VALID	Request Orignal Content
7	ATS_19	7	��[l��d/����ɞ�09�:y	344756	VALID	Request Orignal Content
8	ATS_19	8	�aq,0ė3�?��?09�:y	344756	VALID	Request Orignal Content
9	ATS_19	9	A��7E �u�KnN�09�:y	344756	VALID	Request Orignal Content
10	ATS_19	10	�-Y��`BeVk�Sg�09�:y	344756	VALID	Request Orignal Content

This snap shows the list of token after blind decryption is performed

Snap 7:



Request Original Content

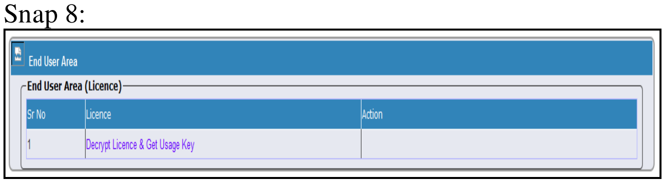
Request Original Content

Digital Signature: :�<�*=���R���r���

Secret Key: 7741352

User sends one of his token (digital signature) to request the license from the CSP

Snap 8:



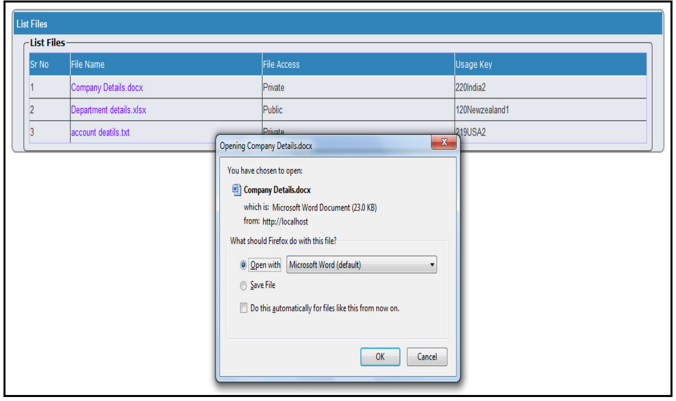
End User Area

End User Area (Licence)

Sr No	Licence	Action
1	Decrypt Licence & Get Usage Key	

User after getting the license, performing decryption to get the usage key to access the content

Snap 9:



List Files

List Files

Sr No	File Name	File Access	Usage Key
1	Company Details.docx	Private	220India2
2	Department details.xlsx	Public	120Newzealand1
3	account deatils.txt	Private	219USA2

Opening Company Details.docx

You have chosen to open:

Company Details.docx

which is: Microsoft Word Document (23.0 KB)

from: http://localhost

What should Firefox do with this file?

● Open with: Microsoft Word (default)

○ Save File

□ Do this automatically for files like this from now on.

User finally getting the content after decrypting the content using the usage key in license.

3.1 Performance Analysis:

TABLE-I: EXECUTION TIME (IN MILLISECONDS) FOR TOKEN GENERATION AND BLINDING:

Operations	Entity	Input data	Process	Key Size (bit)	Execution Time (ms)	
Token Generation	Owner	Token ID(50 bytes)	SHA-1 Hashing (160 bits)			
		10 Token IDs (200 bytes)	RSA Encryption of 10 Token ID	Key Size	e=65537	e=3
				1024	195	142
				2048	210	157
				4096	213	161
				8192	223	187
		Encrypted ID and Timestamps (440 bytes)	RSA Signature Generation	1024	242	172
				2048	245	198
		10 Tokens	3DES Encryption of 10Tokens	192	192	
			AES Encryption of 10 Tokens	256	73.5	
Blinding	User	Random Integer r (32 bytes)	RSA Encryption of Blinding factor	2048	21~32	18~25
		X and Encrypted K	Blinding Encrypted Key	2048	21	19

TABLE-II: EXECUTION TIME (IN MILLISECONDS) FOR LICENSE ACQUISITION PROCESS:

Process	Entity	Input data	Process	Key Size (bit)	Execution Time (ms)
License Acquisition	Content provider	License Response License Size< 1 KB	3 DES Encryption	192	132
			AES Encryption of 10Tokens	256	64.3
	user	License Request	RSA encryption	2048	172.12

The token $\mathbf{TID}_{(i,j)}$ is obtained as an output of the SHA-1 hash algorithm. The output of hash function is then encrypted using RSA algorithm with modulus n to obtain $\mathbf{TID}^{enc}_{(i,j)}$, The computed time for RSA encryption of 10 token IDs having different modulus n of sizes 1024, 2048, 4096 and 8129 bits are calculated. Then we generated signature of the token ID and time stamp using RSA Signature algorithm. Finally at the end the anonymous token set of 10 tokens is encrypted using both 3DES and AES block ciphers The computed results are shown in Table-I The time taken for blinding operation at user side is also tested. The major computations involved at the user side and the CSP side in the license acquisition process is one public-key encryption and then one symmetric key encryption.

We computed the time taken for symmetric encryption of a license of maximum size 1 KB using both 3DES and.AES block ciphers. The results of license acquisition process are given in Table II.

4. Conclusions

After implementation of proposed scheme for cloud computing environment we analyze that it overcome both the problems of illegal distribution of copyrighted digital content as well as preserves the Privacy of the user who is involved in content transaction by using only simple cryptographic algorithms and without relying on any third party for mutual trust and authentication. Analysing the execution time shows that proposed scheme is efficient. Comparative analysis with different schemes shows that proposed scheme overcome the drawback of other schemes and hence more suitable for upcoming cloud based systems.

References

[1] Manish H. Gourkhede, Deepti P. Theng, “Analysing Security and Privacy Management For Cloud Computing Environment”, Communication Systems and Network Technologies, 2014 Fourth International Conference on, pp. 677, 680, 7- 9 April 2014.

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

[3] Lei Lei Win, Tony Thomas, and Sabu Emmanuel, “Privacy Enabled Digital Rights Management without Trusted Third Party Assumption”, IEEE Transaction on Multimedia. 2012.

[4] Petrlic, R., "Privacy-Preserving Digital Rights Management in a Trusted Cloud Environment," Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on , June 2012.

[5] Ronald Petrlic; Christoph Sorge, Privacy-Preserving DRM for Cloud Computing, 26th International Conference on Advanced Information Networking and Applications Workshops, 2012

[6] Theng, D.; Hande, K.N., "VM Management for Cross-Cloud Computing Environment," Communication Systems and Network Technologies (CSNT), 2012 International Conference on , vol., no., pp.731,735, 11-13 May 2012

[7] Khaled M. Khan and QutaibahMalluhi,”Establishing Trust In Cloud Computing”,IEEE Computer Society, September/October 2010

[8] L. L.Win, T. Thomas, and S. Emmanuel, “A privacy preserving content distribution mechanism without trusted third parties,” in Proc. IEEE Int. Conf. Multimedia, Barcelona, Spain, 2011,

[9] Qian Wang; Cong Wang; KuiRen; Wenjing Lou; Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," Parallel and Distributed Systems, IEEE Transactions, May 2011.

[10] Chih-Ta Yen; Hrong-TwuLiaw; Nai-Wei Lo; Ting-Chun Liu; Stu, J., "Transparent Digital Rights Management System with Superdistribution," Broadband, Wireless Computing, Communication and Applications (BWCCA), 2010 International Conference on, Nov. 2010

[11] A. O. Durahim and E. Savas, “A-MAKE: An efficient, anonymous and accountable authentication framework for WMNs,” in Proc. ICIMP, 2010

[12] E. McCallister, T. Grance, and K. Scarfone, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),” National Institute of Standards and Technology (NIST), Special Publication 800-122, Apr. 2010.

[13] Beum-Su Park,shirlyl Lee,Hoon-Jae Lee, On A Digital-Right-Management System using One-Time-Password,2010

[14] R. Perlman, C. Kaufman, and R. Perlner, “Privacy-preserving DRM,” in Proceedings of the 9th Symposium on Identity and Trust on the Internet,ser. IDTRUST ACM, 2010.

[15] T. Thomas, S. Emmanuel, A. V. Subramanyam, and M. Kankanhalli, “Joint watermarking scheme for multitiparty multilevel DRM architecture,” IEEE Trans. Inf. Forens, Dec.2009

[16] M. K. Sun, C. S. Laih, H. Y. Yen, and J. R. Kuo, A Ticket Based Digital Rights Management Model In Proc. CCNC 2009.

[17] P.P.Tsang,M.H.Au, A. Kapadia, and S.W.Smith, PEREA:Towards Practical TTP-free revocation in anonymous authentication in Proc.CCS, Alexandria 2008.

[18] D.J.T.Chongand;R.H.Deng,“Privacy-enhanced superdistribution of layered content with trusted

access control," in Proc. ACM Workshop Digital Rights Management, Alexandria, VA, Oct. 30, 2006

[19] J. Zhang, B. Li, L. Zhao, and S. Yang, License management scheme with anonymous trust for digital rights management In Proc. ICME. 2005

[20] Barsoum, A.; Hasan, A., "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems," Parallel and Distributed Systems, IEEE Transactions, 2012.

[21] Deepti Theng, L. G. Malik, S. U. Nimbhorkar, "Efficient Computational Strategy for Cloud Computing Environment," International Journal of Internet Computing ISSN No: 2231 – 6965, VOL- 1, Page(s): 36-42, ISS- 3 2012.

[22] R. Ahmad and E. Behza, "Internet cash card," inU.S. Patent Application 20020143703. 2002.

[23] Y. Tsiounis, Anonymity & Privacy: The Internet Cash Example [Online]. Available: http://www.internetcash.com/fgo/0,1383,white02,00.

[24] 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.

[25] Y. S. Kim, S. H. Kim, and S. H. Jin, "Accountable privacy based on publicly verifiable secret sharing," in Proc. ICACT, Gangwon-Do, South Korea, 2010, pp. 1583–1586.