Privacy in a Multiparty Multilevel DRM Architecture Based on commutative encryption

January 5, 2012

Abstract

We consider the question of protecting the privacy of the user in multiparty multilevel digital right management (DRM) system. DRM technology is widely used to protect digital contents from illegal use but generally consumer privacy sacrificed. Current DRM working architecture support only two party system, consist content owner and user [18]. However, for scalable business there is a need of additional levels of distributors, a multiparty multilevel DRM architecture is the solution of this problem [12]. But traditional digital content super-distribution approach does not address the user privacy issue efficiently and pose serious threat to user privacy. It is commonly acknowledge that user privacy in DRM system should be well protected. Many research efforts have been devoted to prevent users' privacy. In this paper, we propose and analyze a privacy right management scheme for multiparty multilevel DRM architecture. The scheme use cryptography specially commutative encryption to protect user privacy during content download and licence acquisition. Proposed scheme deals efficiently the issue of users' privacy, and also provide the way to track the malicious user responsible for license violation.

1 Introduction

The widespread use, and great improvement in network technology has greatly facilitated the distribution and exchange of information at low cost. Immediate access and cheap mode of multimedia content distribution, is one of the new benefits this internet-based distribution brings for e-comers. However, digital content by nature is highly vulnerable to unauthorized use and illegal redistribution. This raises serious threat to intellectual property rights and copyright protection . In general, after content distribution, no further protection is provided and malicious user get the chance of copying and redistribution. While these new technologies have the potential to open up new markets that will protect digital content persistently after distribution also. Digital Rights Management (DRM) is the technologies that ensure the protection of digital content after distribution also [14, 18]. The goal of DRM technology is to distribute digital contents in a manner that can protect and manage the rights of all parties involved in the system. DRM is a complex information systems in the sense that they highly involve technological, business, economical and most importantly, social factors.

DRM involves many diverse areas such as cryptography, signal processing and information theory,business modeling, e-commerce, law, legal and social aspects, etc. The core concept in DRM is the use of digital licenses. The consumer buys a digital license, getting certain rights to him instead of buying the digital content. A License constraints may include expiration date, available regional zone, software security requirements, hardware security requirements, and watermarking requirements.

The goal of DRM system is to protect the digital content and enforce of rights attached with the license in a DRM system to comple te this copyright enforcement goal of owners and distributors usually user privacy sacrificed and a curious operator normally identifies user's preferences. In general, DRM system are almost privacy encroaching and violating the users' privacy rights in many times. DRM system usually involve tracking of the sold digital content in order to check violation detection and easily access information (such as user identity, digital content identity and IP address, etc.) are potentially destructive of user privacy. Because of data collection by distributors and network operators, privacy usually compromised. Because of the primary focus of DRM, protection of intellectual property right, creating serious threat to user's privacy [13].

As privacy is becoming increasingly important part of digital contents business, privacy is emerge as a greater concern in DRM. Preserving the user Privacy in DRM may refer the problem, what digital content user is purchasing, without disclosing the content details to the owner/distributor. In the perfect privacy scenario, user can enjoy full content hiding and is able to buy digital content or services without reveling any information about digital content to any involve parties [8]. We propose a approach to provide privacy protection in DRM system. Our approach, based on cryptography. In this approach, neither license server get information, for what content, he is issuing license nor distribution server come to know which protected content user is downloading. For example when a user access any movie then a curious operator can know, which movie type of movies user watch and easily know the user's preference. That means a distributors may collect the users' personal information and hand over to others for business purpose. Some privacy related issues are, Who is purchasing what items, How frequently user is buying, When a user is purchasing the content. How much money a user is spending over digital content. Here we are providing the privacy by hiding the content information from distributor as well as license servers.

Consumer privacy in digital content distribution is emerge as a serious concern from users point of view. Some of DRM systems have taken users' privacy seriously and have designed architecture to protect privacy. There are papers [2, 5, 6, 22, 19, 8, 24, 26] that proposed solution related user privacy in e-commeres. Most of the architecture that fulfil privacy requirement fail to track violation detection. Some architecture that can track the malicious user, need to trust over third party. Trusted third parties are not a very practical concept in multiparty multilevel DRM. Because this system involve large number of distributor sub distributers and the purpose of this system is to make architecture flexible so that help in handling different price structure of media in different countries. But by including one more authority will increase lot of workload for the users because before every transaction he has to contact to many parties like distributor for content download, third party for payment token and finally to license server for license. After all there workout, still user privacy depends on third part. There for a working architecture is needed for multiparty multilevel DRM that fulfill the requirement of security, privacy, authenticity and violation detection

and such that architecture does not loose flexibility and robustness .

Liu et al [18] have present review of current state of DRM, also raise the privacy related issue in DRM system. A number of schemes have been proposed to protect user privacy issue. However, do not tackle all the privacy concerns, some architecture gives strong privacy but not able to handle violation detection [2, 5]. The scheme proposed by Bao et al. [2] and Chen et al. [5] both have introduced efficient scheme that prevent the owner from finding out which specific digital content User is purchasing. These scheme effectively protect user privacy but for the implementation of these schemes, all content should have similar financial value, that is more unlikely in practical scenario. Also these schemes are not able to handle the problem of violation detection. In [6] Chong et al. have extend the technique given in [2, 27] and proposed privacy enhanced super-distribution of layered content with trusted access control. But this hash function based super-distribution architecture issued the same key to all users. This make difficult to detect violation in the system. Feng et al. in [13] have proposed a system to protect consumer privacy through a key ID. They have used associated key ID with decryption key instead of content ID. Since key ID is easily retrieve from the protected content, any body can retrieve the key ID and know "which key ID is associated to which content". It provides the way to curious operator to learn content ID corresponding to key ID and create serious threat to user privacy, also does not provide privacy during protected content download. In [26] the user need to trust to third party, to get an anonymity ID also during license acquisition operator can identify the ip address and get user information.

In this paper to overcome the aforesaid user's privacy, we design an efficient and practical scheme to enhance privacy protection for user in multiparty multilevel DRM system without the need of trusted third party and also achieve accountability. Although the architecture of privacy protection is based on commutativity in cryptography. Consider the scenario when a user want to buy digital contents from the owner/distributer without disclosing any information that what user is buying. But when things come to physical goods, its inherently difficult to hide from the seller, what, when, whom, and how much he is selling. Because in physical items seller has to track his inventory so that he will not loose goodwill because of limited inventory of goods. In viceversa, there is no such a concerns of inventory in digital goods. So digital goods provide a way towards the privacy of users' preferences. For the Privacy of a user content provider should be learn nothing except what must inescapable be acquire to achieve for the accountability. In particular, involve parties should be unable to know what the item a user have buy, but they should be able to check the user authenticity and payment details.

Remaining of the paper is organize as follows. In section 2 preliminary are given. In section 3, we propose our multiparty multilevel privacy enhancing DRM architecture. In section 4, we will discuss the related issue with the architecture like authentication, violation detection and payment. Finally we will conclude in section 5.

2 Preliminaries

A general DRM architecture [18] involve four core component content owner, license server, distributor and user. Each involve parties have own concern and requirements that need to

be satisfies in the architecture for smooth running of business. Each component of DRM is the collection of some servers, logical devices and applications. A component interact with other component using predefined interfaces or ports. A interface is determined by a set of methods and connected with its component using cable. At the application level, need to have a complete DRM system. We identify three key DRM services with respect to content consumer: Content owner, License server, and Distributer. Identifying the multiple roles of components in a DRM system is crucial. Below, we are describing the concern and requirement of involve parties in an architecture.

Content owner: Content owner holds the digital rights of the content and want to protect these rights. Owner is concern about unauthorized use and illegal redistribution of contents. Owner concern for unauthorized use of content is resolved by encrypting the content with symmetric key algorithm. Symmetric key is usually used to encrypt the content for high performance of computation and for each digital content, a different symmetric key is used.

Content owner consist of different applications and servers, with inter operability feature. Owner include packager, financial clearing house, usage clearing house, tracking server, registration authority and monitoring server. Owner provide unprotected content to the packager; packager encrypt these content by using symmetric encryption algorithm. After encryption packager send content key to the license server and protected content to the distributor.

Distribution Server: The distribution server provides the encrypted content, trailer of content and content information to the user without asking any information and payment to him. The distributor keeps a data base of content ID and details of products on there website. Contents price structure is based on usage rules associated with contents.

Distribution server have different component, with each component some tasks are associated. Distribution server has a media server and setup a website presenting the protected content and content information. Tracking server also remain associated with distributor to track license violation in his zone. Interoperability unit of distributor check the devices of customer and provides the files format and player according to compatibility of user device. Distributor also has costumer care unit to solve the problem related to user query.

License Server: License server is responsible for license distribution as well as for payment and users' authentication. License server receives the rights and contracts, and the content encryption key corresponding to encrypted content ID from the content owner, and output the license including usage rule to the user based over the his demand after the verification and payment. Digital licenses content different permission, usage rules and contracts, which may be interpreted by the plug-in. License server maintain autharization and authentication server to check user authenticity and also have finincial clearing house to take care the payment related issue. License server also maintain a data base content that content information that which license is issued to which user.

User: User in the DRM system is concern about easy to access of the content, easy to use, and his own privacy. User wants to consume protected content in a user friendly way and wishes to browse the content catalog where the contains and offers can be selected of his choice. Since a Customers also require a license to consume protected content, they must be able to select license type associated with usage rules. Also Several devices may be associated with a user, so rights should be associated with users, instead of with devices. There should be a general support for multiple devices.

User select a content from the distribution server's website and download the protected

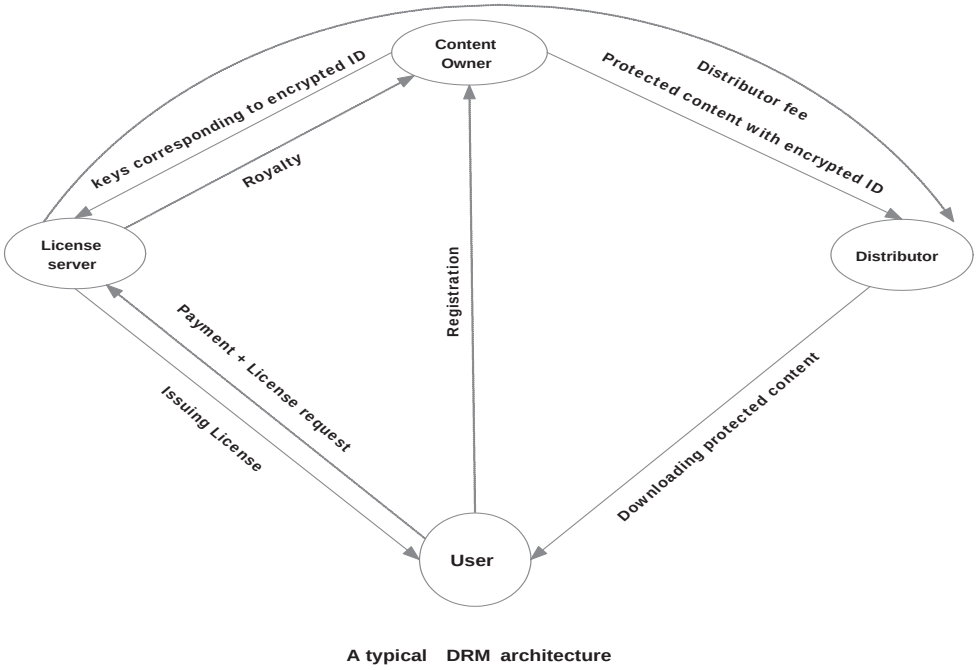

Figure 1: A typical DRM architecture

content from the media server and by paying license fee to the license server get the license file. Finally, Customer wants to consume the protected content, according to the usages rule associated with corresponding license to his all devices.

2.1 Multiparty Multilevel DRM Architecture

A two party DRM model may not be sufficient to handle present business scalability. Present working models are not very flexible to make proper business strategies according to geographical regions. Therefore, a architecture is needed that can cover all world market and the different strategy for different region or countries can be implemented in the same architecture. A multiparty multilevel DRM architecture is the solution of this problem [12]. Because a distributor at lower level that is a local distributors can take care of the local market in a better and make strategy according to market demand. Also there is a need to have flexible architecture to support existing business strategy and extensible to adapt the future business strategies. All these things ask for the need of a innovative and scalable business models which have the flexibility of making strategies and policies according to local market. It is necessary to have a more flexible and herbarial distribution system. Therefore, a multiparty, multilevel DRM architecture comes in picture, which can involve multiple level of distributer, sub-distributer at lower level in additions to the owner and consumer. A local distributor can better handle and explore potentially known market by making strategies according to the local customer demand and their preferences. With the help on sub-distributers, owner can also handel different price structure in different countries or geographical regions.

Our multiparty multilevel digital right management architecture providers flexibility to

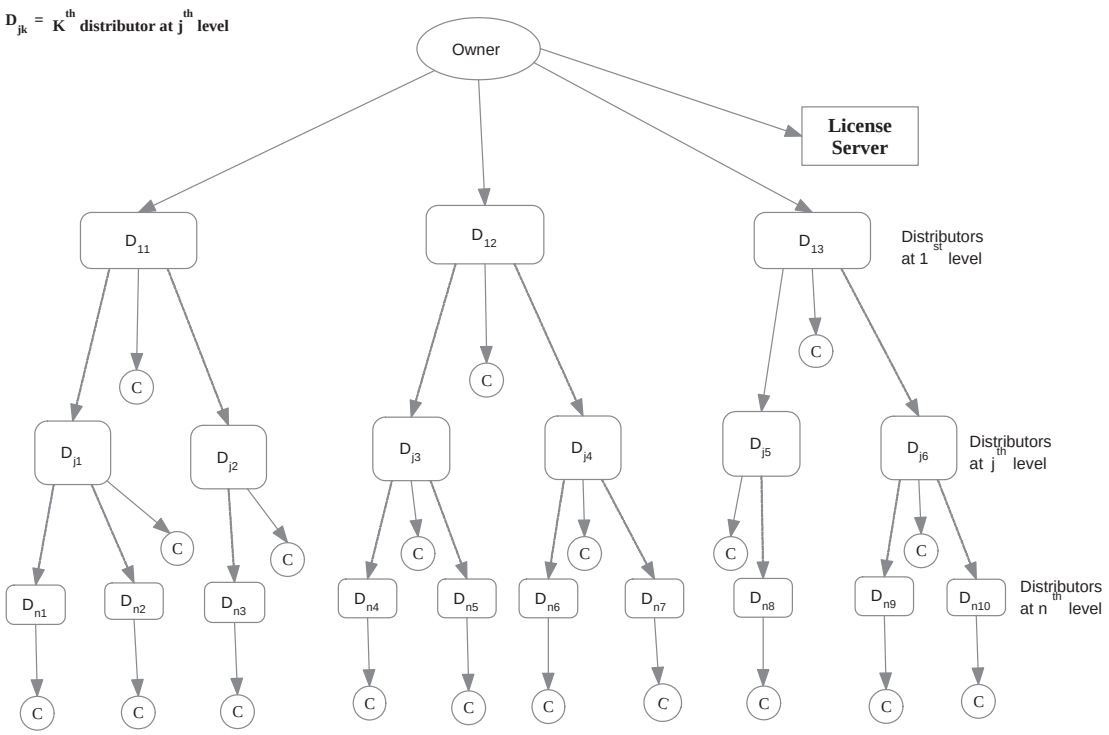

Figure 2: Multiparty multilevel DRM framework

handle a local market that are usually unknown to the content owner. In this architecture distributor have the authority to create offers over the recommendation of owner. This model allow more to make more innovative and scalable business strategies. in [14] they considered the distributor as a trusted authority, and hence distributor can posses content key. But this model restrict the number of distributors because to find large number of trusted distributors is very difficult in practice. But in our architecture distributer do not have the rights of key distribution this point allow the participation of more number of distributors and sub distributors. This architecture also give freedom to the user to select the distributor of his choice or the distributor of nearest reach.

2.2 Commutativity in Cryptography

Commutativity implies that the order in which the various operations like content encryption or decryption perform, does not effect the final output. This commutative algorithm enables the two parties two proceed independently without sharing any key to each other through different different paths and finally compute the secret content [23]. That is, when two encryption operation apply on a content, the encryption sequence does not change effect the decryption sequence. In general, commutative encryption property holds for finite number of encryption algorithms and the simplest example is XOR stream cipher. If CE is a commutative encryption algorithm with message M and keys S_1 and S_2 then,

$$CE(CE(M|S_1)|S_2) = CE(CE(M|S_2)|S_1)$$

Some cryptographic strong family of encryption functions discussed in [23, 11]. Commutative property has been used in many schemes, to name a few, privacy protection in e-commerce [2, 5], privacy protection in drm [6], watermarking [16, 15], oblivious information sharing [1], and wireless sensor network [17, 25].

2.3 Identity Based Encryption (IBE)

In 1984 Shamir [20] has motivate the concept of identity-based cryptosystem. This is a public key encryption scheme in which the public key is an easily calculated function of user identity, such as his email address, while a user's private key can be calculated for him by a trusted authority, called Private Key Generator (PKG). The identity-based public key cryptosystem can be an alternative for certificate-based PKI, especially when efficient key management and moderate security are required. In this scheme there are four algorithms: (1) Setup: This is a randomized algorithm that takes no input other than the implicit security parameter, generate global system parameters and a master key. (2) Key Generation: This is a randomized algorithm that takes public key string and generate the private key using the master key. (3) Encryption: This is a randomized algorithm that takes plain text and public key ID as input and out put encrypted message. (4) Decryption: This algorithm takes input as ciphertext and private key and output original message.

In identity-based public key encryption, the public key distribution problem is eliminated by making each user's public key derivable from some known aspect of his identity, such as user's email address. When Alice wants to send a message to Bob, she simply encrypts her message using Bob's public identity (such as bob's email address). Bob receives encrypted message, and obtain his private key by submiting his public key to the private key generater(PKG), after verification of bob's authenticity, PKG generate private key to bob and then bob decrypt the message. The private key that PKG generates on Bob's query is a function of its master key and Bob's public identity (public key of bob).

Shamir [20] introduced this concept of identity-based cryptosystem to simplify key management procedures in certificate-based public key infrastructure. After Shamir proposal in 1984 there have been several proposal for Identity based encryption (IBE). The first identity-based Encryption (IBE) was proposed by Boneh and Franklin in 2001 [3], this scheme is based on bilinear pairing. After Boneh and Franklin many IBE protocols were proposed and is still a very active area of research.The identity-based public key cryptosystem can be an alternative for certificate-based PKI, especially when efficient key management and moderate security are required.

2.4 Notations and Definitions

Table 1 explains the meaning of symbols used throughout the paper.

Name	Description
O	Content owner
$D_{i,j}$	j-th distribution server in the i-th level
L	license server
U	DRM User
M	Digital content
MK	Master Key
ID_O	public identity of owner O
SK_U	private key of owner O
ID_U	public identity of user U
ID_L	public identity of license server L
SK_L	private key of license server L
SK_U	private key of user U associated with ID_U
$\mathsf{ID}_{D_{i,j}}$	public identity of distributor $D_{i,j}$
$\mathsf{S}_{D_{i,j}}$	private key of distributor $D_{i,j}$
PKG	private key generator
Sig	signature generation algorithm
Ver	signature verification algorithm
V_M	The value of item M
$\mathsf{CE}(.\|.)$	Commutative encryption algorithm
$\mathsf{D_pub}(.\|.)$	public key decryption algorithm
$\mathsf{E_pub}(.\|.)$	public key encryption algorithm
$\mathsf{D}(.\|.)$	symmetric key decryption algorithm
$\mathsf{E}(.\|.)$	symmetric key encryption algorithm
$A\|B$	concatenation of A and B

Table 1: Notations

Public key algorithm Public-key cryptography is a cryptographic system that requires two separate keys for encryption and decryption, one to encrypt the plaintext say public key, and one to decrypt the cyphertext say private key. Cryptography is generally acknowledged as the best method of data protection against passive and active attack. Here we use public key encryption algorithm to key distribution in the architecture. The keys are delivered using public key encryption to the license server L such a way that neither the neither any involve party nor the attacker can decrypt with out the private key corresponding public key. Public key algorithm is also used to encrypt the digital license containing the protected content decryption keys using the public key of the receiver, thereby enabling only the party holding the matching private key to extract the partial content keys. The components of our proposed DRM system which have a content decryption key are the content owner O and the DRM client C with a valid license. It is very difficult to authenticate a purchaser. Purchasers are concerned about their privacy and anonymity. They simply need to pay a fee to watch a movie. Instead, the DRM client C is a service provider to purchaser and should be authenticated by the License server L. In our public key distribution, we use the setup of Identity-Based Encryption (IBE) [20] instead of certificate-based setup to simplify certificate management and verification. A trusted authority like private key generater (PKG) generates the private key of a server upon receiving its public identity (which may be some known

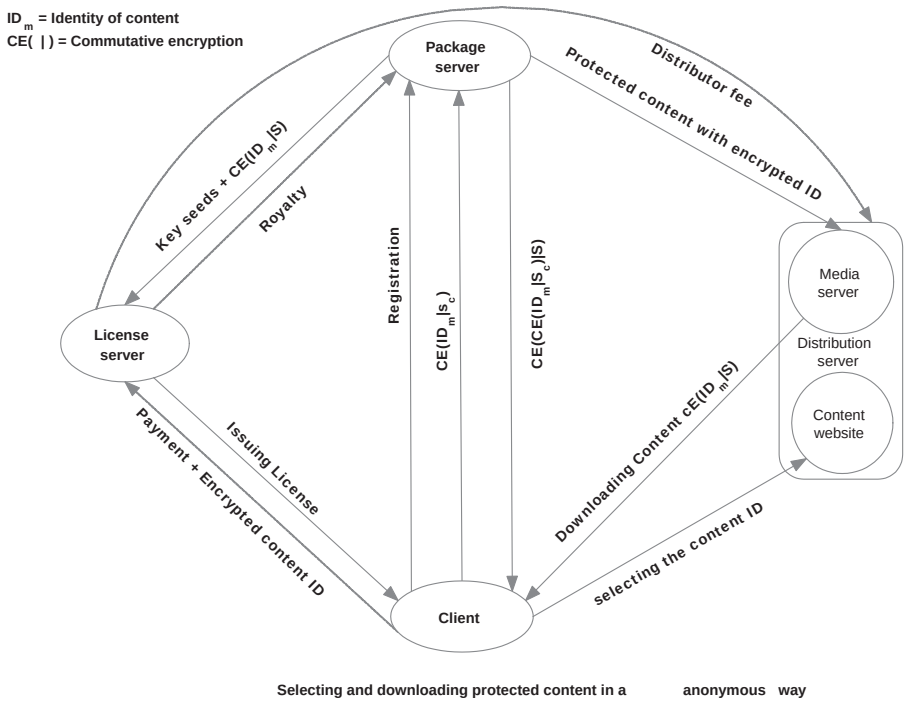

Figure 3: License acquisition in multiparty multilevel DRM

aspect of its identity, such as its e-mail address). We use the private/public key pair thus generated for each entity in the system as the respective signing/verification key pair of the corresponding entity [9].

3 DRM Solution to Privacy Rights Management

We now discuss our user privacy protection scheme which consist multiple parties and multiple distributors. The parties involve in this architecture are Content owner O, license server L, distributers $D_{i,j}, 1 \leq i \leq nand1 \leq j \leq m$ here i denote the level of distributor, and DRM user U.

Key Setup The content owner O, the distribution servers D_i, $1 \leq i \leq n$ and the license server L submit their public identities to PKG and obtain the corresponding private keys S_O, S_{D_i}, $1 \leq i \leq n$ and S_L respectively through a secure communication channel. PKG uses its master key MK to generate the principals' private keys after verifying the validity of the principals' public identities submitted to PKG. The DRM User U submits its public identity ID_U to the content owner O and obtains the corresponding private key S_U through a secure communication channel. O uses its own private key S_O issued by PKG to generate the private key for user after verifying the validity of user's public identity ID_U submitted to O.

3.1 Encryption of digital Contents and their IDs

The content owner generates r distinct secret keys $K_i, 1 \leq i \leq r$ to encrypt the r number of digital content $M_i, i \leq i \leq r$ using symmetric encryption algorithm.

$$E(M_i|K_i), for 1 \leq i \leq r$$

To encrypt unprotected content owner use different symmetric key for each encrypt each digital content. Owner also generate another secret key S to encrypt the IDs of protected content by using commutative encryption algorithm.

$$CH(ID_{M_i}|S) \text{ for } 1 \leq i \leq r$$

To encrypt all the IDs of protected contents, owner use the same key S while to protect the content using distinct keys.

3.2 Secure Delivery of protected Content and Key Seeds

Protected digital content decryption key securely deliver to the license server and protected contents to the distributers with content detail in multiparty multilevel DRM architecture by using simple cryptographic mechanisms as discussed in [12].

Owner generates his signature by using his own public key and send signed protected content $Sig(E(M_i, K_i)|S_O), 1 \leq i \leq n$ and the contents details to the distributers $D_{1,j}, 1 \leq i \leq m$ of level one. When the distributer receives these protected content with encrypted content ID and contents details, He verify the signature of the owner, using owner's public key. If verification succeeds, distributer keeps the protected content over his media server and display contents details on his web site. The protected contents from media server are allowed to download freely and anonymously. This architecture follow hierarchical distribution system of protected content. Distributor of level one provide the content and content information to the distributor of level two, distributor of level 2 to distributor of level 3 and so on. It means, Once distributor of level one receives the protected content and content details from the content owner, they also follow the same procedure and send protected content and details of contents to the distributor of level two. In the same way distributor of level two to distributor of level three and so on.

Owner encrypt the protected contents decryption keys $E_{pub_{L_i}}(K_i|P_L), 1 \leq i \leq r$, using license server L public keyP_L and create tuples $T_i = (E_{pub_{L_i}}(K_i|P_L), CH(ID_{M_i}|S)), V_{M_i}$ for $1 \leq i \leq r$. Owner generate his signature using his own private key $\sigma(T_i) = Sig(T_i|S_O)$ and send the tuples $T_i, \sigma(T_i)$ with usage rules to the license server. When license server receives the content he verifies the signature of the owner, using owner's public key and if verification succeed

$$Ver(E_{pub_{L_i}}(K_i|P_L), CH(ID_{M_i}|S)), V_{M_i}) = true$$

License server decrypt the key seeds using its own private key and store in a safe place corresponding to encrypted IDs of the content.

3.3 Privacy Preserving Digital Content Download

Secure download of digital without information to any third what content user is downloading based on commutative encryption [20]. Here user download the protected content and third party never come to know what content user have downloaded. the things take place in following manner.

Initially user registrar himself to the owner. Owner check the authenticity of the user and provide a unique session ID say (RID_U) at the time of registration for some time duration (say for a year of two year). This unique ID does not reveal any information about the user except the user is authentic user and a part of DRM. User useded this unique Id during commination with the other parties involve in DRM system.

User visit the distributor web site and select the ID of some content that he want to play. User generates a key (a) based on commutative cryptosystem CE and encrypt the selected content ID $CE(ID_{M_t}|a)$. After encrypting the content ID using commutative encryption, user send $CE(ID_{M_t}|a)$ to content owner. When owner receives some request he check whether whether the user is registered user or not, If not Owner ask him for registration otherwise encrypt the user message by his secret S using commutative encryption and generates his signature and send the tuple to user.

$$(CE(CE(ID_{M_t}|S_C)|S), Sig(CE(CE(ID_{M_t}|S_C)|S)|P_O)$$

When user receive the message from the owner, User verifies the signature if

$$Ver((CE(CE(ID_{M_t}|S_C)|S), Sig(CE(CE(ID_{M_t}|S_C)|S)|P_O))) = \text{true}.$$

Then decrypt the message using his decryption key and get $CE(ID_{M_t}|S)$.

Media server keeps the protected content corresponding to encrypted content ID. So the digital content will be identified only by the encrypted ID not by original ID of content that encryption key is only with content owner not with distributor. When a user gets encrypted ID information with the help of owner, He can download the content from media without giving any information about content to the distributor.

3.4 Privacy during License Acquisition

Once a user know $CE(ID_{M_t}|S)$ encrypted content ID of content M_t with the help of content owner. User download the protected content from the media server without knowing to any third party. Since content are protected so user need the license file to play $E(M_t|K_t)$. To acquire the license, user send his license request to the license server corresponding to encrypted content ID $CE(ID_{M_t}|S)$. Since license server does not know about the original ID of the content. That is license server does only know that key K_i is the key of

$$CE(ID_{M_i}|S)$$

, for $1 \leq i \leq r$ and the value associated with these encrypted content IDs. License server does not know the original content of which decryption keys are associated. User gets encrypted

content ID information through owner. With the help of $CE(ID_{M_t}|S)$ user proceed and send license request to the license server.

Suppose a user U wants to acquire the license for a certain content M_t. User send encrypted ID of the content $CE(ID_{M_t}|S)$ with the request of license to the license server.

When license server receives the request from the user, he check the whether a user is register user or not. If user is not a register user, he asks to register. If user is a register user, check authenticity of the user also verify user's registration ID, If user is not authentic user, license server denied the request otherwise proceed. If user is authorized used, license server asks the payment from the user. Once license server receives payment corresponding to requested license file of $CE(ID_{M_t}|S)$, issued the license for the content corresponding to encrypted ID of content $CE(ID_{M_t}|S)$, also associate user ID with the license file. License authority encrypt the license using the public key of user and generate his signature using his own private key and send encrypted license with license server signature to the user.

When user receives encrypted license file from the license server, he verifies the signature of license server using license server public key. If verification succeeds, User encrypt the license using its own private key and get the license. With the help of license user can play the content and enjoy according to the usage rule and permissions associate with license.

4 Some Other Issues

4.1 Payment Privacy

Usually, payment can be of two types in our DRM architecture. First one is the membership, user deposita initial prepayment to the license server. After making initial payment, the user can be able to engage in a virtually finite number of interaction with the license server in order to get the license at the total cost which does not exceed the deposita amount. A user can continue his transaction with license server until the total cost, does not exceed its initial deposita amount. When the user balance become less then the content price, license server deny the request for license and ask to deposita additional payment, after getting payment resume the services. Here license server always know what the user current balance is. The second option pay per item. In this way user need not to deposit initial amount, when user make request for license of some digital content at he same time he make the payment to the license server and license server issue license.

If all the content have different price then it will be difficult to guaranteed the content privacy. When license server receives the payment, he can easily know, what content payment is it. In general, DRM system keep a large data base of digital content with different category. Price of two item in the same category may distinct, also price of two different category items may same. Here, we classified the digital content into different groups according to their prices and the digital content in the same group may have the item from different categories but of the similar financial value. Digital contents from the same group are charged with same price. At the time of payment for the license, user pays for certain rights for a content in the group. If a group content large number of digital content from different category, It will be almost difficult to know about the content for the license server on the basis of

payment and the information, for what content user is making payment in both the cases remain hidden.

4.2 Authentication

In DRM system authentication is an essential process to verify whether the user is authentic user of illegitimate user and to make sure that the authority is issuing the license to right and registered authority. Authentication is very essential to control over the digital content after the distribution. Authentication helps letter in violation detection and to catch the perpetrator responsible for illegal copying or redistribution. Our architecture support authentication check up of a user before issuing the license. In this architecture authentication part is divided in two parts first registration and second verification of authenticity. Registration part is taken care by the owner without charging any fee to the user and user needs to register only once that is in the starting. After registration and successful vermination of user identity, authority issue registration ID to the user. When user request for the license to the authority, authority verify the registration ID of the user, after authentication success, issued the license.

4.3 Violation Detection

Violation detection is the essential in DRM system for copyright protectection. However, its very difficult problem from implementation as well as technology view point. So for there is no satisfactory or workable system that will take care copyright protection and user privacy simultaneously. Lot of technology have proposed and study the copyright protection of multimedia content, which aim is to track and catch malicious user responsible for license violation, copying or redistribution. This Privacy protection architecture also provides the way to track violation of license in the system. Summery of the procedure is as below:

When License server issued the license to the user after authentication success and payment. License server associate user registration ID with the license and store in his data base that which license file is issued to which registered user ID. when tracking server detect some violation in the system, it retrieve the license ID from the license file and send the license ID to the license server. When license server receives the license ID, he check its data base and extract to which user ID this license file has issued and send that user ID to the content owner who has issued this ID to registered user. Owner come to know who is responsible for license violation with the help of registration ID of user. Letter Owner block the user in the system and user no longer eligible to make content transaction with the content provider. Owner also proceeds to take legal action against the malicious users.

5 Concluding Remarks

In this paper, solution provides an efficient and practical scheme that protect users' privacy in multiparty multilevel DRM architecture, which is based on commutativity in cryptography. In this scheme neither distributor get information about the content that a user download from the media server nor license come to know for which content license user is requesting.

With the help of commutative encryption user can easily retrieve the encrypted content ID corresponding to content ID without knowing to any third party that what information he is retrieving. Since distributor also don't have the information about the content so the distributor only the information get that some content is downloading by user but never come to know what the content download record can help to make business better with out creating threat to user privacy in this system. This feature facilitate the privacy during content download without using anonymous IP. Since in this system license server and can maintain the record of what content license he is issuing how many time without knowing the actually content identity. Letter owner can access this information and make his business better. Since license server and distributor have only information that how frequently and how many costumer are downloading but they don't know what content license issuing and what content user is downloading. Since they don't have the information about the really ID of content so that can not use or sell this information, only the owner can use this information and make his business better. In this architecture license server check the authenticity of the costumer and make sure that he is issuing the license for a register ID. Also by making recording of license issuing file with license ID corresponding to user ID to whom this license is issued, help to catch malicious user in the system responsible. This scheme take care of user privacy, authenticity and violation detection simultaneously.

References

[1] Agrawal, R. and Evfimievski, A. and Srikant, R. *Information sharing across private databases.* Proceedings of the 2003 ACM SIGMOD international conference on Management of data, pp 86-97, 2003.

[2] F. Bao, R. Deng, and P. Feng. *An efficient and practical scheme for privacy protection in the e-commerce of digital goods.* Information Security and CryptologyICISC 2000. pp. 162–170, 2001.

[3] D. Boneh and M. Franklin. *Identity-Based Encryption from Weil Pairing.* In proceedings of Crypto 2001, LNCS 2139, pages 213-229, Springer-Verlag, 2001.

[4] C. Conrado, F Kamperman, G.J. Schrijen, and W. Jonker.*Privacy in an Identity-based DRM System.* IEEE Computer Society, 2003.

[5] Chen, S. and Chen, S. and Guo, H. and Shen, B. and Jajodia, S. *Efficient proxy-based internet media distribution control and privacy protection infrastructure.* 14th IEEE International Workshop on Quality of Service, 2006, IWQoS 2006. pp. 209-218, 2006.

[6] Chong, D.J.T. and Deng, R.H. *Privacy-enhanced superdistribution of layered content with trusted access control.* Proceedings of the ACM workshop on Digital rights management, pp 37-44, 2006.

[7] Conrado, C. and Kamperman, F. and Schrijen, G.J. and Jonker, W. *Privacy in an Identity-based DRM System.* Proceedings. 14th International Workshop on Database and Expert Systems Applications, 2003. pp. 389–395, 2003.

[8] Conrado, C. and Petković, M. and Jonker, W. *Privacy-preserving digital rights management.* Secure Data Management. pp. 279-294, 2004.

[9] R. Dutta, R. Barua and P. Sarkar. *Pairing Based Cryptographic Protocols : A Survey.* Manuscript 2004. Available at http://eprint.iacr.org/2004/064.

[10] R. Dutta, D. Mishra, S. Mukhopadhya, *Vector Space Access Structure and ID Based Distributed DRM Key Management.* Advances in Computing and Communications, pp. 223-232, 2011.

[11] Diffie, W. and Hellman, M. *New directions in cryptography.* IEEE Transactions on Information Theory, pp 644-654, 1976.

[12] R. Dutta, and D. Mishra, and S. Mukhopadhyay, *Vector Space Access Structure and ID Based Distributed DRM Key Management.* Advances in Computing and Communications, Springer, pp 223-232, 2012.

[13] M. Feng, and B. Zhu, *A DRM system protecting consumer privacy.* Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE, pp 1075-1079, 2008.

[14] S. O. Hwang, K. S. Yoon, K. P. Jun, K. H. Lee. *Modeling and implementation of digital rights.* Journal of Systems and Software, 73 (3), pp. 533-549, 2004.

[15] Lian, S. *Quasi-commutative watermarking and encryption for secure media content distribution.* Multimedia Tools and Applications, pp 91-107, 2009.

[16] Lian, S. and Liu, Z. and Ren, Z. and Wang, H. *Commutative encryption and watermarking in video compression.* IEEE Transactions on Circuits and Systems for Video Technology, pp 774-778, 2007.

[17] Lee, H.Y. and Moon, S.Y. and Cho, T.H. *Adaptive False Data Filtering Method for Sensor Networks Based on Fuzzy Logic and Commutative Cipher.* International Conference on Computer and Electrical Engineering, pp 228-232, 2008.

[18] Q. Liu, R. Safavi-Naini, and N. P. Sheppard. *Digital Rights Management for Content Distribution.* Proceedings of Australasian Information Security Workshop Conference on ACSW Frontiers 2003, vol. 21, Jan 2003.

[19] Perlman, R. and Kaufman, C. and Perlner, R. *Privacy-preserving DRM.* Proceedings of the 9th Symposium on Identity and Trust on the Internet. pp 69-83, 2010.

[20] A. Shamir. *Identity-based Cryptosystems and Signature Schemes.* In proceedings of Crypto 1984, LNCS 196, pp. 47-53, Springer, 1984.

[21] J. Zhang, N Wu, J. Luo, and S.Yang. *A scalable Digital Rights Man- agement Framework for Large Scale Content Distribution.* pp. 761-764, ISPACS, 2005.

[22] A. Sachan, S. Emmanuel, A. Das, M. S. Kankanhalli. *Privacy Preserving Multiparty Multilevel DRM Architecture*. IEEE Consumer Communications and Networking Conference, 2009 (CCNC 2009). pp. 1-5, 2009.

[23] Shamir, A. *On the power of commutativity in cryptography*. title=On the power of commutativity in cryptography. Automata, Languages and Programming, pp 582-595, 1980.

[24] Win, L.L. and Thomas, T. and Emmanuel, S. *A privacy preserving content distribution mechanism for drm without trusted third parties*. IEEE International Conference on Multimedia and Expo (ICME), 2011. pp. 1-6, 2011.

[25] Yang, H. and Lu, S. *Commutative cipher based en-route filtering in wireless sensor networks*. IEEE 60th Vehicular Technology Conference, pp 1223-1227, 2004.

[26] Yao, J. and Lee, S. and Nam, S. *Privacy preserving DRM solution with content classification and superdistribution*. Consumer Communications and Networking Conference, 2009. CCNC 2009. pp. 1-5, 2009.

[27] B.B. Zhu, and M. Feng, and S. Li, *An efficient key scheme for layered access control of MPEG-4 FGS video*. IEEE International Conference on Multimedia and Expo, 2004. ICME'04, pp 443-446, 2004.