International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988Volume 9 (2017) pp. 218-231
© MIR Labs,www.mirlabs.net/ijcisim/index.html

Consumer Privacy Protection in Digital Right Management: A Survey

Amira Mostafa [1*], Tarek Gaber [2*], Ghada Eltaweel [3], and Ajith Abraham[4]

[1]School of Computer Science and Informatics, Suez Canal University, Ismailia, Egypt.
eng5mrmr@hotmail.com,
[2]School of Computer Science and Informatics, Suez Canal University, Ismailia, Egypt.
tarekgaber@ci.suez.edu.eg
[3]School of Computer Science and Informatics, Suez Canal University, Ismailia, Egypt.
ghada@ci.suez.edu.eg
[4]Machine Intelligence Research Labs (MIR Labs), Washington, USA
ajith.abraham@ieee.org

Abstract: **Digital Right Management (*DRM*) is a technology used to manage the usage of the digital contents that distributed through the Internet, and helps the content owners to prevent un-authorized use of their copyrighted content. However, consumer privacy is a growing problem appeared in *DRM* environment. This problem emerged because of the consumers can distribute copies of the digital contents without any consideration of the owners' copyright, which lead to moving the content owners to use *DRM* that allows the consumers to access the content only if they have authenticated by their identity information. Thus, the consumer privacy is violated in *DRM* system. This paper gives a survey about the current consumer's privacy preserving solutions. It analyses their advantages and disadvantages and then highlights some open issues to be addressed.**

Keywords: Digital Rights Management (*DRM*), privacy, consumer privacy, anonymity, accountability.

I. Introduction

Since the rapid growth in the communication technology, It is became fast and easy for the consumers to obtain any digital contents such as: digital music, movies, and e-Books from anywhere through the web sites. These digital contents are available for the consumers without any constraints on the content distribution. Thus, numbers of problems are appeared. Firstly, the consumers are able to distribute these contents acting as the contents owners. Secondly, any consumer can copy and use these contents without buying it. These problems caused a big revenue loss for the content owner [16], [6]. To overcome these problems, digital rights management (*DRM*) technology is becoming one of the available solutions. "The *DRM* is a technology that allows only authorized consumers to access digital contents" [6]. In *DRM* system, a content is encrypted by cryptography techniques and controlled by digital license which contains sets of the usage rights produced by the content owner and the consumer should practice them when using the digital content [10, 6]. By this system, only an authorized consumer can obtain the license and access the required content, and the consumers are required to disclose their identities to the license issuers to obtain the required license. Thus, consumers' identities information is revealed during the license acquisition process, and the consumer preferences could be tracked as we will detail later [10, 4, 37]. Getting access to the required content, and the consumers are required to disclose their identities to the license issuers to obtain the required license. Thus, consumers' identities information is revealed during the license acquisition process, and the consumer preferences could be tracked as we will detail later [10], [4], [37].

A. Our contribution

Clearly, the *DRM* technology overcomes the problems of the content owners and protects their copyright. However, it has not paid much attention to the consumers' right. Thus, in this paper we will discuss the consumer privacy problem in *DRM* systems, and highlight the importance of the consumer's privacy. Then, we outline number of methods used to solve this issue, and present an overview of the existed proposed solutions that address the consumer privacy problem to enhance the public image of *DRM* systems.

The rest of this study is organized as follows. Next Section explains what the *DRM* is. Section III discusses a number of *DRM* open issues. Section IV gives an overview of privacy in *DRM* whereas the requirements of *DRM* Privacy protected in Section V. The techniques used to address the requirements identified in *DRM* consumer privacy problem in Section VI. Section VII gives an overview of the proposed solutions that address the consumer privacy problem whereas we present our proposed solution in Section VIII. The comparison between these solutions in Section IX. Finally, the article is summarized in Section X.

II. DRM Overview

There are different *DRM* models [6], [7],[8],[9], those have different *DRM* functionalities, names and ways to specify the content usage right. However, the basic *DRM* processes are the same in all these models.

We present an overview of modern *DRM* system typically involve distinct four parties: content owner, content provider, license server, consumer, as we shown in the Figure 1.
This system separates between the purchase and delivery of the content, and the license (content decryption key, usage right) delivery, in which each of them are delivered in separated package [44]. The parties of this system are as follows:

- Content Owner (*CO*): is an entity that usually owns the copyright of the contents, and define its usage rights. It responsible to encrypt the digital contents using encryption algorithm and transfer them to the content provider (1), also he transfers the decryption key and the usage rights to the license server to generate the license (2).
- Content Provider (*CP*): is an entity that distribute, advertise the protected digital contents and transfers them to consumer (3), (4). It responsible for checks the consumer authenticity (if he is authorized or not), the payment process (5), and send license details for the license server to generate the required license (6).
- License Server (*LS*): is an entity that is responsible for issuing the required license for content and transfer it to the consumer (7).
- Consumer(*C*): it is an entity in the system that needs to purchase and playback specific DRM- protected digital content on his device. So, he can download the protected content from content provider through his website and obtains the license from the license server. To buy the license, the consumer needs to install DRM client on his device and authenticate himself to the *CP*, and then make payment through gateway (which associated with CP). Once the consumer is authorized, *CP* reports the license server to issue the license. Finally, the consumer can obtain the license from *LS* and access the content according to usage rights that defined in the license.

In the DRM system Firstly, the content owners encrypt their contents using encryption key and define its usage rights. The owner sends the protected content to the content provider to distribute it in the distribution server to be allowed to the consumer for download. And, he sends the decryption key with the usage right to the license server to generate the license for the consumer. When the consumer choose DRM- protected content, They can download it from *CP*' website and request the license from *CP*. *CP* checks consumer authenticity. If the *C* is valid and make a payment, the *CP* report the *LS* to issue the required license. Finally, *LS* sends the license to *C*. Thus, the consumer can play/ view his content accordance to the usage right.

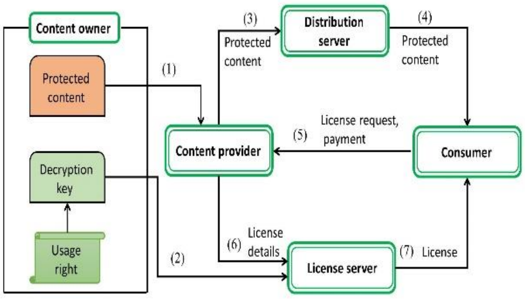

Figure1. A typical modern DRM system architecture

A. Notation

Table 1 denotes the notation we use throughout the remainder of this paper.

III. DRM problems

Now, we give an overview about number of issues that faces the *DRM* system. Such as: consumers' privacy, *DRM* interoperability, *DRM* incompatibility, first-sale doctrine (i.e. license reselling).

A. Consumer privacy

The current *DRM* systems give the content owner most authorities and abilities, neglecting the rights of the consumers [13]. Thus, the content owner feels satisfaction with the *DRM* system that protects his copyright and profit. However, the consumer feels that his privacy is usually overlooked. Such as: the consumers must to register by their real identities with a content owner to be authorized and get the content, also they are required to disclose their identities to license issuer to obtain the content licenses [6]. Moreover, the *DRM* system can track the consumer's playing statistics that violate his privacy [4], e.g. what time you play, which music, how often do you play them, etc.

B. Interoperability

In our current, the companies have several heterogeneous computing devices. Thus, interoperability between these devices are truly necessary for companies to function, where interoperability allows the consumer to use the digital content in multiple ways and multiple devices [12]. However, current *DRM* systems do not have a common *DRM* interoperability scheme led to force the consumers to buy the same digital contents many times to be able to use them on their heterogeneous computer machines [6].

C. Incompatibility

DRM systems require specific software/hardware installed on the consumers' PC or laptop to be render. The incompatibility problem appeared when the required software does not work with the installed operating systems. For examples, adobe digital editions do not work on Linux operating systems [12], and in August 2006, the sales of PDF is stopped in amazon with *DRM* restrictions, and the consumers could not access their files 30 days after that from on line services and on new devices [11].

D. First-sale: License Reselling

Distribution a digital content depends entirely on the license of digital content [6]. Thus, even the consumer obtains digital content from content provider, he cannot access it unless pays to the License issuer for a content license. This license contains the content decryption key and a usage right that is do not permitted to consumer to resell the content or actually resells the license of this content. Under this approach, the *DRM* system does not allow for the consumer to resell the license that he pays his money to obtain it [6, 13].

Table 1. Notation

Notations	Description
DRM	digital right management
C	Consumer
CP	Content provider
Ls	license server
LI	license issuer
CO	content owner
D	Distributor
CC	computing center
TTP	trusted third party
SWP	software provider
CSP	cloud service provider
APS	Anonymous payment scheme
KC	key center
CEC	content execution center
CADs	content access devices
CP-ABE	cipher text-policy attribute based
WMRM	Windows Media Rights Manager

IV. Overview of Privacy

The revolution in the World Wide Web made the individuals interested in electronic means of communications. At this time, privacy concept appeared as an important issue for the electronic community. The famous definition of the privacy as: "The right to be let alone". It means the freedom to do things without other people watching you or knowing what you are doing.

A. Privacy types

Rachel et al. [17], discussed 7 types of a privacy as follow: Consumer privacy, Personal Communication Privacy, Association Privacy, Bodily privacy, privacy of behavior and action, privacy of location and space, privacy of thoughts and feelings

1) Consumer privacy:

It interested about consumer- related information. It gives the consumer the right to control the collection, use and disclosure of their information. such as: the name, address, telephone number, date of birth, e-mail address, ID number, a credit-card number and medical history [15].

2) Personal Communication Privacy:

It means avoiding the breakthrough of communications between consumer and his used machines such as access to e-mail, telephones or mail interception, microphone and illegal recordings. Also, it helps the individuals when communicating with other to avoid monitoring the data that passes between the consumers through communication software.

3) Association Privacy:

It gives the individuals the right to associate with groups or organizations which they choose to belong without being monitored. Such as: political parties, trade unions and religious groups. Thus, the individuals can live in democratic society and they have freedom of political speech and worship.

4) Bodily privacy:

It gives the individuals the right to keep their body function private. It supports a healthy for them (e.g. body examination, medical treatment, avoiding torture or blood transfusion without consent). Also, it helps to prevent revealing any information about individuals' medical conditions.

5) Privacy of behavior and action:

It interested about the individual's activities in private and public space, e.g. personal habits, political activities and religious practices. Where, the individuals can behave in private /public space without any monitoring or control from others.

6) Privacy of location and space:

It gives the individuals the right to move in the public spaces as they want. Such as: walk in the street, live in the home and drive the car. So that the individuals feel they are free without tracking or any objection from the others.

7) Privacy of thoughts and feelings:

It gives the individuals the right to feels as they like and keeps their feeling and thoughts from the others. Also it gives them creative freedom that beneficial to the whole community.

B. Consumer Privacy in DRM

The consumer privacy has a lower priority in *DRM* systems and it's has been violated in some process as follow:

- Authentication process: it is an essential process that allows the consumer to be authorized in the *DRM* system. The consumer is authenticated by his/ her information identity with the content owner or the content provider to obtain the protected content. But he did not know who can see this information and where the system stored it. Also, the consumer authenticates himself to the license issuer to obtain the license [6, 14]. This process not only creates the threat of disclosure of a customer's information, but also may be provide this information to other company's opponents of the consumer by simply selling this information. [15]
- License acquisition: usually the license in *DRM* system is tied with the consumer identity. Thus, the license issuer can reveal the consumer preferences for specific types of content [19] and determine information about other content which the consumer is running in conjunction with licensed contents [15]. This information can be used for improving the service or marketing to attract the other consumers to trust on the contents.

V. Requirements of privacy-preserving DRM

The *DRM* systems need to strike a balance between protection of copyright for the content owners and protection of privacy for the consumers. There for, the *DRM* should satisfy following objectives:

A. Consumer Anonymity:

the consumer's individual information should not be identified by any party in the *DRM* system such as, *CP* or *LI*. Thus, no party can find who buys and access the content [42], [20].

B. Profile Building Prevention:

The *DRM* system should prevent any party to build Profile about their consumers such as: trace the consumer's actions, link these action to certain pseudonyms which is related to a certain consumer and knows the accessed content [42],[3]. Thus, any party cannot be able to de-anonymize the consumer and violate his privacy.

C. Consumer Traceability:

The *DRM* system needs to trace the consumers for any misuse of their purchased contents/licenses. [13], [8].

D. Collusion-Resistance:

The *DRM* system is essential to resist any collusion of the *DRM* servers such as the content owner and the content provider. Because of, they can associate a consumer's transactions with his real identity [41], [2] and violate his/her privacy.

E. No Reliance on Trusted Third Party (TTP):

TTP means that a broker between two parties who both trust him to facilitate the transactions between them. The *DRM* system should not reliance on *TTP* based on suggestions from Win et.al in [2] because of in the real life, a *TTP* can become untrusted and disclose the personal information about the consumer and increase the cost on the consumer.

VI. Methods or Technique Used To Solve the Requirement Identified In DRM Consumer Privacy Problem

This section presents number of methods to address the consumer's privacy problem such as:

A. Anonymity:

It a property allows the consumer to communicate anonymously with any party in the system [9], [18], where the consumer's identity still hidden in all system's process.

B. Pseudonymity:

It a process identifying each consumer by pseudonym instead of his real identity. Thus, the consumer can access a content or a service without his real identity revealed [6].

C. Unlinkability:

It means that a consumer can communicate with the *CP* or *LI* without links a consumer's transactions to his identity or link these transactions to each other. Except in case the consumer is acting illegitimately, an authority be able to revoke the unlinkability [9].

D. TTP:

Is an entity make the consumer doesn't communicate directly with *CP* or *LI* and preserves his identity from them [6], [1].

E. Smart-Card:

It a method to preserve the consumer privacy by smart card that can use on any compliant device and used as consumer's unique identifier instead of his real identity during authentication process [3].

VII. The proposed solutions to solve the consumer privacy problem

DRM systems are proposed to address the consumer privacy problem. On the basis of their solution, we categorize these research works into three classes and some branches as we shown in the Figure 2.

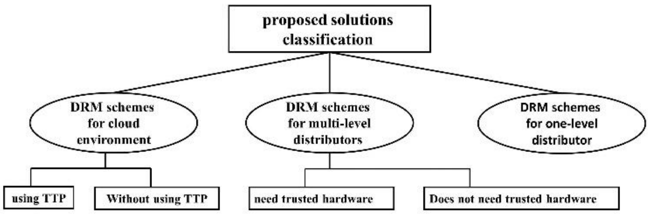
proposed solutions classification
DRM schemes for cloud environment
DRM schemes for multi-level distributors
DRM schemes for one-level distributor
using TTP
Without using TTP
need trusted hardware
Does not need trusted hardware

Figure 2. The classification of the proposed solution

A. DRM schemes for cloud environment

Cloud computing is an Internet-based computing technology which allows to store and access large amount of data and programs from different sources and countries over the Internet instead of your computer's hard drive [32].

1) Using TTP:

We will submit a system using *TTP* that reviews all registration, deals and transaction communications between all the parties in the system.

Joshi et al [1] proposed *DRM*-privacy preserving system for cloud environment using *TTP*. It uses number of cryptographic primitives such as ring signatures with an anonymous recipient scheme [40]. This system permits for the consumer to purchase the software license anonymously and execute it in any computing center through *TTP* that cannot find out which software the consumer has bought and from whom. Where, *TTP* gives the consumer token to execute the software at the computing center without revealing any information about him.

This system consists of four participants with different roles as we shown in the Figure 3, and it consists of four phases as follow:

license acquisition, the consumer anonymously send a license request with software ID to *SWP* using anonymization network such as 'Tor' [21], then he anonymously pays *SWP* for the license using anonymous payment scheme [22]. After that, the (*SWP*) generate the license and send it to consumer.

Token request process, the consumer sends a token request with his license to *TTP*. *TTP* verifies the license by checking the signature of *SWP* and the terms of the license, and use the C's re-encryption key to re-encrypt the encrypted software ID under the public key of the *CC*. Then, *TTP* create a token and send it to the consumer. This token is signed by *TTP* and contains timestamp, re-encrypted software ID and encrypted Metadata by *SWP* public key.

Content execution process, C anonymously submits the token to *CC* using Tor. *CC* validates the token by check *TTP*'s signature and its timestamp then decrypt re-encrypted software ID and allows consumer to execute the software specified by the ID. *CC* kept the tokens for certain period of time and removes the timestamps then sends them to the *SWP*.

Consumer revocation, the malicious consumer who exceeds the execution limit can be tracked by *SWP* using secret- sharing scheme [23]. This scheme allows the software provider to expose the malicious consumer's identity through his token, and allows *TTP* to assign the consumer a pseudonym (p) in each token. When *SWP* detect the license violation, he reveals C's pseudonym from the token and contacting with *TTP* to reveal the mapping from C's pseudonym to identity.

Advantages of Joshi's System: Joshi's solution is being able to protect the consumer privacy on cloud environment and preserve the business secrecy as well. So it addresses the following issues:

- Consumer anonymity: it is preserved where, neither software provider nor computing center obtain any Personal information of the consumer.
- Profile building (under a pseudonym): all the parties in Joshi's system cannot build a usage profile under a pseudonym. Where *TTP* cannot find out which software is used by consumer because the license is tie up with encrypted software ID instead of the original software ID. And the consumer submit new execution token to *CC* for each software execution. These tokens do not contain any information that would allow *CC* to link multiple execution of the same software by the consumer to one another. Moreover, the consumer creates a new temporary public key for each purchase, so *SWP* cannot link the purchases of *C* to each other based on the public keys.

- Consumer traceability: As we show above, the software provider can trace the malicious consumers.
- Flexibility in choosing a license model, *SWP* in this system presents flexible license models allowing differentiated pricing for software providers.

Limitations of Joshi's System

- Reliance on *TTP*: the consumer registers by his/her identity with *TTP*, and in the real life it may be untrusted and disclose the consumers' identities.
- Adding cost to consumers: using *TTP* need money to do the service thus existing *TTP* increase the cost imposed on the consumers.
- Resistant to collision of *DRM* servers: the anonymity of the consumer is not preserved under collusion of the software provider and *TTP*. Where, secret sharing allows the disclosure of consumer identities in case of fraud and *TTP* knows these identities and can reveals it to the software provider.

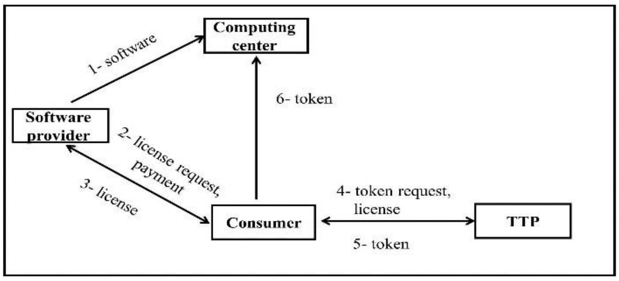

Figure 3. Basic approach of DRM concept in Joshi et al [1]

2) Without TTP:

In the real life *TTP* may be untrusted and became malicious, thus many schemes are proposed do not reliance on *TTP* such as:

Petrlic et al. [34] proposed privacy-preserving *DRM* scheme for cloud environment without using any *TTP*. It based on use of a combination of cipher text-policy attribute-based encryption (*CP*-ABE) scheme [35] with an anonymous payment (*APS*) scheme [36]. Thus, the consumers are able to anonymously buy content from content providers and anonymously execute it at any content execution centers.

This system consists of five participants the bank, content provider, key center (*KC*), content execution center (CEC) and the consumer. The bank anonymously issues two digital coin i.e. payment tokens $(PT_{1,}PT_2)$ for the consumer. These tokens used to allow the consumer to purchase the encrypted content from the *CP* anonymously, pays for the execution at CEC and used as authorization credential by the CEC towards the *KC*. Where the *KC* generates a private key needed for content decryption without reveals the consumers identities. This system consists of four phases as follow:

Payment token retrieval, the bank anonymously using communication channel e.g. TLS [25] issues payment tokens PTs for the consumer worth the specified values and draws the amount from the consumer's account. Each token PT of them is defined by $PT\ 's$ ID [acc] and contains account information signed by bank's public key.

Content purchasing process: the consumer sends the content ID to *CP* anonymously using TLS and pays for the content with PT_1. Then, PT_1 is checked whether it is worth the price of the content, and a payment transcript is generated during the payment and kept on *CP*. After that, *CP* checks whether PT_2 is a valid payment token by checks the bank's signature. If the check succeeds, *CP* generate a license include the *CP*'s terms, $(PT_2 - acc)$. Finally, *CP* encrypts the content key by (*CP* -ABE) scheme under the license as cipher text- policy during the encryption, and the encrypted content key is forwarded to the consumer.

Content execution: C chooses CEC to execute the content, and communicates with it using TLS, and he pays for the execution with PT_2. CEC checks PT_2's validity, and the payment transcript is generated during the payment and kept on CEC. Then C submitted the encrypted content key to CEC and tells it the content ID of the content to execute and from any *CP* get it. CEC retrieves the content identified by this content ID from *CP* and contact with *KC* via TLS to obtain the private key to decrypt the content key. CEC submits PT_2 , it is credentials and the license to *KC*. *KC* checks bank's signature in PT_2 and CEC's credentials validity. If the checks succeed, *KC* generates the private key identified by the attribute set and returns it to CEC. Finally, CEC decrypts the content key which is used to decrypt the content. This content is executed and the result sent to the consumer.

Clearing and Fraud Detection: both *CP* and CEC send PT 's component and the payment transcript to the bank via TLS to get their money. The bank checks the PT 's signature. If the check succeeds, the bank books the $PT\ 's$ value to the party's account. Then the bank stores $PT\ 's[acc]$ and the payment transcript in it is deposits database. When a new entry is stored in deposits database, the bank checked whether the same $PT\ 's[acc]$ component is stored already or not. In case of that PT was spent twice, the *APS* allows the bank to reveal the malicious consumer's identity.

Advantages of Petrlic's System:

- Consumer anonymity: it is preserved where, neither the content providers nor the content execution center are able to obtain any information about the consumer.
- No reliance on *TTP*: this solution doesn't need any *TTP* in their transactions.
- Profile building (under a pseudonym): all parties in the system cannot build profile about the consumer, where the CEC cannot link content executions to each other. It learns PT_2's component that includes the hidden account information. However, this component does not allow for a linkage with other $PT\ 's$. And, the *CP* cannot link license retrievals by consumers to each other although he knows $(PT_{1,}PT_2)$ because of neither the $PT\ s'$ components nor the performed payments are linkable to each other. Thus, the licenses are unlinkable to each other. Also, *KC* cannot link several executions during key retrievals to each other, because the $PT\ s'$ components are unlikable to each other. Moreover, using *APS* scheme the bank cannot link a PT that it issued to a consumer during payment token retrieval to a consumer when *CP*/CEC deposits PT at the bank to cash the money.
- Consumer traceability: as shown above, the double spending prevention of *APS*s is used to detect

license fraud.

- Resistant to collision of *DRM* servers, the consumer privacy preserved under collusion of the CEC and *KC*, whereas neither *KC* nor CEC learns any more about the consumer and content to allow them to break the consumer privacy.
- Flexibility in choosing a license model, the pay-per-execute model is presented in this system.

Limitation of Petrlic's System

- Limited solution: the used digital coin is not used in the worldwide and many people are still unaware of digital currencies.
- Adding cost to consumers: as shown above, the consumer requires spending his/her money twice, one to obtain the content and other to execute it and obtain the private key. That introduces an additional cost to the consumers.

Huang et al. [41] proposed privacy-preserving *DRM* scheme for cloud environment. It makes combining the techniques of cipher text-policy attribute-based encryption (*CP*-ABE) and proxy re-encryption (PRE). By this scheme, the content encryption key divided into two parts, content master key and assistant key. The content master key is protected by access policy over attributes.

The consumers only have a set of attributes satisfying this access policy can recover the content master key, and then obtain assistant key and decrypt the content.

This system consists of the following entities: content provider, cloud service provider, license server, key server, attribute authority and the consumer.

The content provider and the consumer are registered with the cloud service provide *CSP* via secured channel. Where, the *CP* outsource the contents to cloud storage through *CSP*, also *CSP* distribute the license that generated by the license server to the consumers. The key server generate public key and secret key for *CP* and C, and the attribute authority assigns a set of attributes A_U to the consumer, and then generates a set of consumer attribute secret keys ASK_U.

This system consists of four phases as follow:

Content encryption: *CP* generates the content encryption key (CEK) that consists of random content master key (CMK) and random assistant key (AS). The *CP* encrypts the contents by this key and sends it to *CSP*. Then *CP* defines the attribute-based access structure AS for the content, and encrypts CMK with AS using ABE scheme, encrypts the AK with the public key and then sends them to the key server through *CSP*.

License acquisition: the consumer chooses the content from the *CSP*, and pays the chosen content. After that, *CSP* sends the license acquisition request including the consumer's usage rights UR to the license server. The license server acquires the encrypted content master key from the key server and generates the license then sends it to the consumer through *CSP* anonymously. This license includes the encrypted content master key, the usage rights UR, and the license's signature. Once the consumer receiving the license, he verifies the signature and keeps the license.

Content decryption: when the consumer's attributes satisfy the access structure of the content and he has effective usage rights in the license, they can acquire the assistant key anonymously from the key server to access the content. And if the consumer and his attributes not revoked, the key server re-encrypts the encrypted assistant key and sends it to the consumer. The consumer recovers the assistant key AK with his private key, and then recovers the content master key CMK from the license. Finally, the consumer generates the content encryption key and decrypts the content with the CEK.

Revocation Scheme: when the consumer's attributes not satisfy the access structure of the content or found any malicious consumer, the attribute authority delegates the key server to perform the attribute revocation and consumer revocation. Thus, in both cases the key server refuses to re-encrypt the assistant key for the consumer without disclosing it, and the consumer cannot access the content.

Advantages of Huang's System

- This system can achieve consumer anonymity, consumer traceability and Content confidentiality and doesn't reliance on *TTP*.
- Cipher text- policy attribute-based encryption technology support: the content confidentiality is preserved under the collusion of multiple consumers whose combining their attributes to decrypt the encrypted content if each one cannot decrypt the content alone. So, the key is dividing under this technology as we show above.

Limitation of Huang's System

- Flexibility in choosing a license model: this system limited support for different license model.

Petrlic et al. [42] proposed privacy-preserving *DRM* scheme for cloud environment. It use the homomorphic encryption scheme [43] based on secret sharing scheme and combined with the software re-encryption scheme to achieve the consumer privacy protection.

This system consists of four participants, the service provider, computing centers, software providers and the consumer the consumers buy the software from a software provider and execute it at a computing center through the service provider which acts as proxy between the consumer and software provider/computing center. These the involved parties are certificated by a public key infrastructure (PKI) that issue each participant by public and private key.

This system consists of three phases as follow:

Software buying: the consumer sends the required software and payment token in encrypted message with its signature to the service provider. Then, the service provider verifies the signature and forwards the encrypted message without the signature to the software provider to obtain the software via a secure channel.

Software and license retrieval: based on the secret sharing scheme, the decryption key is subdivided into two parts between the consumer and the service provider to prevent the consumer to share it with the others. Thus, *SWP* provides SP's with the encrypted software and the license that contain SP's share of decryption key. Then the *SWP* send to the consumer encrypted share of decryption key through SP' as a secure channel.

Software execution: *C* send encrypted message to *SP* contain payment token for the software execution and modification vector that chosen randomly. Then, *C* adds modification vector to his share value and encrypts them by its homomorphic key and send them to *CC*. The *SP* checks the license, then re-encrypt the software and adding modification vector to it, and then generate aggregated homomorphic key K_{aggrh} that is unique for each transaction. This key used by the computing center to decrypt the software decryption key. Then, SP send the re-encrypted software, K_{aggrh}, his share values, and payment token towards the *CC*. Finally, *CC* retrieves the software decryption key by decrypting the aggregation of the encrypted share with K_{aggrh}, and then *CC* executes the software, receives input data from the consumer, and returns the computation result to the consumer.

Advantages of Petrlic's System

- This system can achieve consumer anonymity,

unlinkability of content execution, flexibility in choosing a license model and doesn't reliance on *TTP*.
- Consumer traceability: the license is checked before every software execution. Thus, in case of fraud from the consumer, PKI can disclose the relation between the consumer's public key and its identity.

Limitation of Petrlic's System

- Resistant to collision of *DRM* servers: profile building not preserved under collusion between the service provider with the software provider or the computing center.
- Adding cost to consumers the consumer pays twice, one to obtain the software and other to execute it. So, this system increase the cost imposed on the consumers.

Gourkhede et al. [30] proposed privacy-preserving enhanced *DRM* scheme for cloud environment without using any *TTP*. It makes number of cryptographic primitives such as blind decryption and hash chain to avoid the *TTP*. And preserve the consumer privacy based on anonymous token sets, where the consumer uses them for his/her transactions instead of their real identities.

In the proposed system there are three parties: a data owner, a cloud service provider (*CSP*) and the consumer. A data owner who generates the anonymous token sets in the system. These token sets obtained only for the registered consumer and after he paid the required amount for service using anonymous payment scheme [27]. Then, the consumer performs the blind decryption protocol [28] to get the decryption key that decrypt the token sets and get list of the tokens. Finally, the consumer obtains the required license from the cloud service provider and access the protected content that he downloads it from the cloud. This system consists of three phases as follow:

Content packaging: the data owner stores the content in the cloud, and defines the usage attribute such as (age, country, and city) for each content separately. The data owner encrypts the contents with the content encryption key (CEK) based on the usage attribute and creates the license with the usage key that decrypt the protected content. Thus, only the consumer who has the required usage attribute can access and download the content he prefers from the cloud.

License acquisition: the registered consumer sends encrypted license request with token for authentication to *CSP* to obtain the content license. *CSP* decrypts this request and checks the expiry time of the token, verifies the signature on the encrypted ID of the token and checks whether this token belongs to the revocation list/used token. If the verification success, *CSP* send the license to the consumer to decrypts and access the protected content.

Consumer revocation: the malicious consumer who violates the license can be revoked by the owner. The *CSP* can monitor a content usage of the consumer via his/her token that used in the license acquisition. Then the *CSP* sends this token linked to violated license to the data owner for revocation. The data owner decrypts token ID of this token and recover all token IDs of the anonymous token set and add this token set to revocation list without revealing the consumer's identity.

Advantage of Gourkhede's System

- This system doesn't reliance on *TTP*, can resistant to collision of *DRM* servers and achieves Consumer traceability.

Limitations of Gourkhede's System

- Non-anonymous consumer authentication: the consumer register with the data owner by it is identity information that is violating the consumer privacy.
- Profile building: All the content usage of a consumer is tracked by the *CSP*. *CSP* are able to build usage profiles of content executions under a pseudonym.
- Flexibility in choosing a license model, this system limited support for license model that allowing differentiated price.

B. DRM schemes for multi-level distributors

The multiparty *DRM* system consists of multiple levels of distributors between the owner and the consumers as we show in the figure [4]. This system sufficient to provide proper business strategies for all regions, and have flexibility of packaging multiple contents together in regional manner. Now, we present different schemes for multi-level distributors system. All of these schemes do not reliance on *TTP*. However, some of them needed trusted hardware involved in their system and other does not need trusted hardware.

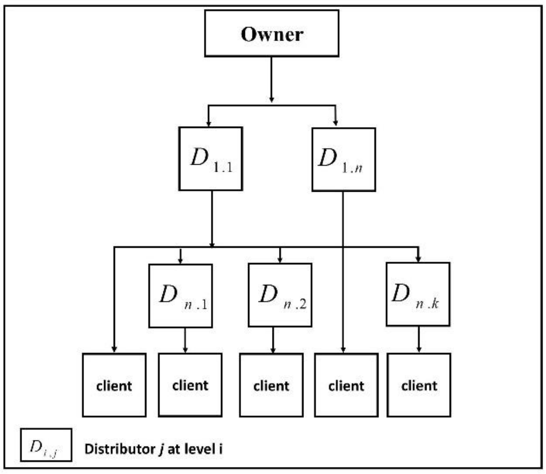

Figure 4. Multi-level distribution architecture

1) Need trusted-hardware

Win et al. [2], proposed a privacy-preserving multiparty *DRM* system without relying on *TTP* assumption. It makes number of cryptographic primitives such as blind decryption and hash chain to avoid the *TTP*. And preserve the consumer privacy based on anonymous token sets, where the consumer uses them for his/her transactions instead of their real identities. This system consists of owner, multiple levels of content providers and consumers, where the owner generates anonymous token sets for the consumer and the content providers performs the content purchase transactions with the consumers. The consumer gets the anonymous token set from the owner anonymously after he pays for the service using anonymous payment scheme [27]. These anonymous token set is encrypted, Thus the consumer register with the owner by his identity information to request the decryption key for these encrypted token sets using blind decryption protocol [28]. All the tokens in anonymous token Set are securely stored at the consumer side. And protected by The Trusted Platform Module (TPM) of the consumer device that encrypts all the tokens to prevent them from stealing/loosing. This system consists of three phases as follow:

Content packaging: the owner specifies the required attributes for each contents separately, and each consumer gets their attribute keys according to his/her information on the registration process. Then the owner encrypts the content with content encryption key based on the consumer attribute key set, and stores the encrypted content and it is information in the content server. The consumer can download the encrypted content if he applies the required attributes for the content.

License acquisition: *C* presents token to *CP* for authentication. Then, the *C* send encrypted message to the *CP* contains secret key, token and license request. The *CP* decrypts the message and Checks the expiry time of the token, verify the signature on the encrypted ID of the token and checks whether the token is revoked/used token. If verification success and the consumer makes payment for the license using anonymous payment scheme. The content provider encrypts the license with the secret key and send it to the consumer. The consumer decrypts the encrypted license and obtain the license. Then, the *CP* store the token in it is database.

Consumer revocation: the malicious consumer can be tracked by the content provider using the anonymous token which the consumer used in license acquisition. The *CP* can monitor a content usage of the consumer if his license violated or any misused from him. The *CP* retrieves the token from it is database and sends to the owner for revocation. The owner obtains the token ID from the token and decrypts it, and then he recovers all the token IDs of the anonymous token set. Thus, the owner can decrypt and compute the anonymous token set and add this set to revocation list without revealing consumer identity and inform all the content providers about the updated revocation list.

Advantages of Win's System

- This system preserves the consumer privacy in License acquisition without reliance on *TTP*, can achieve consumer traceability, and resistant to collision of *DRM* servers, where the owner and the content providers cannot link a transaction with the real identity of a consumer even if they collude, thus the consumer anonymity is preserved under collision of them.

Limitation of Win's System

- Non-anonymous consumer authentication: The consumer has been authenticated by its real identity with content owner that violate his privacy.
- Profile building: *CSP* can be able to track a content usage of the consumer even if they do not violate the license.

Petrlic et al [3], proposed a privacy-preserving multiparty *DRM* system. It based on a re-encryption scheme [33] that runs on any mobile Android device that involves a smart card which used as instead of collaborating with a *TTP*. This smart card used to check the licenses and determine the consumer is still allowed to access the content or not. Thus, the consumer is able to anonymously buy content and anonymously playback the content. This multiparty *DRM* system consists of multiple content providers, content distributors and consumers. Where a content provider provides it is protected content to consumer via a number of different content distributors after he/she purchased the license from a *CP* before. This system consists of three phases as follow:

System initialization: such system is allowed to any devices have different hardware trust anchors. However, it focuses on mobile consumers with different content access devices (CADs) accessing the content, e.g. smart phones, tablets, any computer have trusted platform modules (TPMs). Where every consumer will employ a smart card in his device that has been provided to him/her. This smart card is programmed before shipping by a private key $[Sk_{sc}]$ and digital certificate $[cert_{sc}]$ that can be used for anonymous authentication with *CP* during license purchasing process to preserve consumer anonymity.

License purchasing process: the consumer purchases the license from *CP* via his/her (CAD) i.e. mobile phone from *CP*, where the consumer and the *CP* are communicated using an anonymization network such as Tor [21]. The consumer's CAD initiates the TLS handshake [25] with the *CP*. Then CAD send smart card certificate, it is signature, it is public key with the content-idi of the required content and payment token PT to *CP*. The consumer gets this payment token by set up an anonymous payment scheme [24] with his/her bank. Then *CP* checking the signature and creates the license that encrypted under the smart card's key for content i. Finally, *CP* forward the license, it is signature, the content-idi and the encrypted content key to the CAD. The CAD stores this encrypted content key and forwards the license and it is signature to the smart card. The smart card verifies the license's signature and decrypts the license with it is key. And then it checks whether the id was not used before and check whether the consumer is still allowed to access the content. Then the license is stored under the content- idi on the smart card. Content execution, the consumer first selects a CD of his/her choice dependent of the region he currently is in. where the consumer and the CD are communicated using Tor. Then the CAD establishes a TLS connection with the CD. The CD authenticates towards the CAD with it is new certificate. And then, the smart card forwards the list of available content-ids, i.e. music/film to the CAD. The consumer chooses the content-idi to be executed and forwards it together with CD's certificate to the smart card. The smart card verifies the CD's certificate and checks whether the license terms still allow the consumer to access the content. Then The CAD re-encrypts the encrypted content key by the CD's public key and forwards it to the CD. Finally CD decrypts it with it is private key to obtain the content key $[CK_i]$. Then CD decrypts the content retrieved from *CP* using $[CK_i]$. And this content streamed to the consumer's CAD.

Advantages of Petrlic's System

- This system preserve consumer anonymity, doesn't reliance on *TTP*, preserve the consumer privacy in License acquisition and resistant to collision of *DRM* servers
- profile building (under a pseudonym): all parties in the system cannot build profile about the consumer, where the *CP* cannot link different purchases made with the same smart card that use same certificate for anonymous authentication towards the *CP*.

Limitation of Petrlic's System

- Limited solution: Petrlic's solution is limited to specific devices such as smart phones, tablets, etc.
- Adding cost to consumers: As shown above, using of smart card to protect the consumer usually introduce an additional cost to the consumers.
- Consumer traceability: This system does not address how to treat with the malicious consumer which tries to execute content without having a license.

2) Does not need trusted-hardware

Mishra et. al [19], proposed a privacy-preserving multiparty *DRM* system. It based on the key management scheme based on secret sharing scheme [23, 29], where no party has a complete share of the decryption key. Thus, the key is protected from the consumers and the involved parties such as the distributor and the license server. It achieves the consumer privacy based on anonymity of contents' identity and conceals consumer's preferences from the license server and distributor.

This system consists of: owner, multiple levels of distributors $D_{i,j}$, license server and consumer. As we shown in the Figure 4, the owner provides it is protected content for free to consumer via a number of different content distributors where *C* is mobile and move from one region to another. The owner handles the consumer's registration and assigns a unique registration identity ID_C to him, and then the consumer can buy the content licenses from a license server.

This system consists of four phases as follow:

The content packing: the contents are encrypted using unique key for each content, and all content identities encrypted using the same key S. These encrypted contents, their encrypted identities and the content information are sent to D. The encrypted contents are kept on media server and identified only by their encrypted identities rather than it is original identities, and the content details displayed on their website. After the content encryption finished, the key shares are generated using threshold scheme (t, n). It divides the shared key t into n parties in such a way that the key cannot be retrieved unless authorized shares are collected. These key shares are sending to the *Ds*, *LS*, and *O* respectively, and D, *LS* store their key share corresponding to their encrypted identities.

Content download: the consumer with the help of encrypted content identity that obtained from the D, he can download the protected content they want. The consumer performs the name mapping mechanism between content identity and content encrypted identity with distributor to obtain the encrypted content identity for his required content, whereas protect anonymity of contents' identity and conceals consumer's preferences from the distributor.

The license acquisition: the consumer chooses D and submits the license request with encrypted content identity to him. D verifies the consumer's authenticity. If verification success, D encrypt his key share by consumer public key and generates it is signature and send them with encrypted content identity and consumer identity ID_C to *LS*. Then *LS* verifies the signature of D. If verification success and on receiving the payment, *LS* encrypt his key share by consumer public key and generates it is signature. Then, *LS* issues license containing, his key share with it is signature, D's key share with it is signature, rights and constraints. And *LS* associates the license with encrypted C's identity and sends it to C. C verifies the *LS*'s signature. If verification succeeds, C decrypts key shares of (*Ls*, D), extracts them, and recovers the secret key.

Consumer revocation: the owner can catch the malicious consumer, if the right is violated. The owner retrieves the encrypted consumer identity from the license and sends it to the license server. License server decrypts it and gets the original consumer identity ID_C and sends it to the owner. The owner adds this malicious consumer to his revocation list and inform to all the distributors about him without disclosing any information about the consumer.

Advantage of Mishra's System

- Consumer privacy protected in license acquisition without reliance on *TTP*, consumer anonymity is preserved, consumer traceability and resistant to collision of *DRM* servers, and no party can build profile about the consumer.

Limitation of Mishra's System

- Limited solution: This system allowed only for the mobile consumer.
- Non-anonymous authentication, the distributor verifies the authenticity of consumer and this verification disclose consumer's identity.

C. DRM schemes for one-level distributor

The two party systems mean that only one-level distributor involved in these systems (seller and buyer). Now we present three schemes proposed for the two party systems as follow:

Feng et al [4], proposed *DRM* system to protect consumer's privacy during a license acquisition. It makes number of cryptographic primitives such as (partially) blind signatures [26] that generate signature for content key ID, thus prevent the license server to know what is content that the consumer has requested license for.

In the proposed system there are four parties: content packaging server, license server, payment server, and the consumer. The contents are placed in the content packaging server, and the consumer can obtain the content license from license server after he pays for it through the payment server.

This system consists of two phases as follow:

Content packaging: the contents are classified into different groups according to their prices. The content packaging server generates a unique key $ID(k_{ID})$ for the content and finds the group $ID(g)$ the content belongs to. These contents packaged in encrypted form using symmetric encryption which the encryption and decryption keys are the same and be ready in content packaging server. The content encryption key (K) is identified by it is key ID (ID) by the following equation: $k = \mathrm{sgn}_g(KID)$ (1)

Both (k_{ID}) and (g) are stored into an unencrypted header of the content and extracted from content and sent to the license server to obtain the decryption key in license acquisition.

The license acquisition: as we shown in the Figure 5, after the consumer pays to obtain a license in payment server clarified the content group only (g) and receive payment token, the consumer submits to the license server the payment token, group $ID(g)$, blinded content key ID (k_{ID}) with random number r as: $Mb = Bg(r, KID)$ (2)

Then *LS* verifies the token. If the verification success, *LS* signs Mb with stable (partially) blind signature algorithm:

$$Sb = Sgn_g(Mb) \tag{3}$$

And encrypts it with C's public key. Finally, *LS* returns a license to the consumer with the acquired rights and his signature. Then C's *DRM* module checks *LS*' signature and the rights to see if the consumer has the rights to access the content. If verification success, C's *DRM* module decrypts (Sb) with C's private key to extract (Sb). And then use random number r to unbind (Sb) to get

$$Sgn_g(K_{ID}) = Bg^{-1}(r, Sb) \tag{4}$$

The resulting signature $(Sgn_g(k_{ID}))$ is the encryption key where, $k = \mathrm{sgn}_g(k_{ID})$. Thus, this key used to decrypt the protected content, where the content decryption key and the content encryption key is the same.

Advantage of Feng's System

- Consumer anonymity, reliance on *TTP*, The license acquisition and Resistant to collision of *DRM* servers

Limitation of Feng's System

- Consumer traceability: This system does not address how the content owner could trace and revoke malicious consumer.

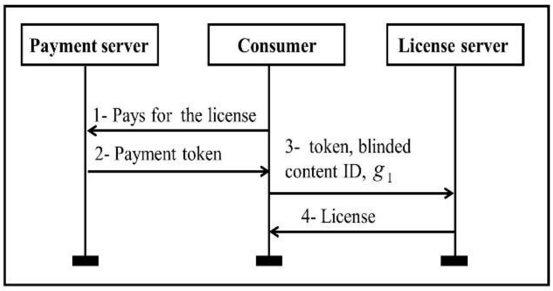

Figure 5. License acquisition process

Yao et.al [5], proposed *DRM* system preserving consumer's privacy. It based on the key management scheme with multiple encryption and decryption keys for the content with the same level. Multiple encryption keys protect the content in case that a content encryption key is disclosed, and multiple decryption keys that allows the consumer to hold an individual decryption key from the license server and decrypt all contents in the same level.

In this system there are five servers, as we show in Figure 6, and it consists of four phases as follow:

Content packaging: according the content classification mechanism and super distribution mechanism [31], the content provider classifies all the contents into many levels, encrypts these classified contents, places them on the content server and distributing these contents publicly available for free download in encrypted form. When a consumer is interested in the certain content in the content server, he can download this content to his/her devices. Thus, the consumer does not disclosure any information about him/her in this process.

Authentication process: the consumer sends an authentication request to the authentication server to get the license and the decryption key. The authentication server checks the consumer's identity certificate, inquiries about the consumer's former payment information through the charging server. If either the consumer is in revocation list or has some unpaid bills, the authentication server will reject this request. If verification passes, the authentication server selects a random transaction ID and sends it with approval information to the consumer. Thus, the consumer uses this transaction ID for his transaction instead of his real name.

License acquisition: the consumer submits his ID, the approval information and the content level to the license server. After the verification, the license server sends unique decryption key and the license to the consumer. Then the consumer can decrypt the required content. And *DRM* client in his/her device monitors the content consumption to make sure that all activities are under the permission of the license.

Consumer revocation: this system depends on the multiple decryption keys mechanism to trace the malicious consumer. Thus, the license server gives each consumer a unique decryption key to become easy to identify the traitor who gives his key to others.

Advantage of Yao's System

- This system protects consumer privacy in license acquisition and doesn't reliance on *TTP*.
- Super distribution technology support: by this technology, the consumers do not need to contact with content provider directly or leave their personal information in the content server.
- Consumer traceability: As we show above this system can trace the malicious consumer. However, this solution does not address how the content owner how revokes any malicious consumer who misuse the content/ decryption key.

Limitation of Yao's System

- Non-anonymous authentication: authentication server knows the consumer identity and can link all transaction IDs to the consumer's identities.
- Profile building: the charging server knows the consumer name and his bill. Thus, this participant can build profile about the consumer.
- Resistant to collision of *DRM* servers: the consumer anonymity in not preserved under the collusion of authentication server and the license server whereas they can link the consumer's transaction ID to his real identity.

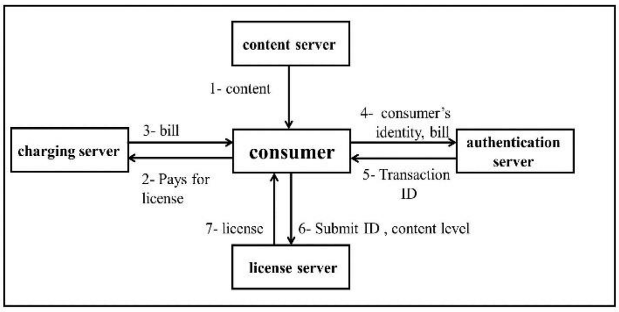

Figure 6. The proposed solution in Yao et al [5]

Yuan et al. [37] proposed *DRM* system preserving the consumer's privacy. It based on a blind signature scheme [38] and then designed two content key acquisition protocols one based on RSA algorithm [39] and the other is based on El Gamal algorithm [40]. Thus, license server generates the content key without knowing anything about the content hides the usage information in the system and protect the consumer privacy.

This system consists of three phases as follow:

Analysis of the WMRM *DRM* system: WMRM is bound to Windows Media Player that is the most widely used commercial *DRM* system. The WMRM *DRM* system applies the symmetric technology which the encryption key and the decryption key is the same, and generates the license by the license server that consists of 5 objects as we shown in the Figure 7. In this license generation process, the license server should know the Key ID to generate the decryption key for the consumer. Thus, the license server can find the content associated with the Key ID easily and track the usage information.

In this license generation process, the license server should know the Key ID to generate the decryption key for the consumer. Thus, the license server can find the content associated with the Key ID easily and track the usage information. Content key acquisition scheme, by this scheme, the license server can generate the decryption key in the WMRM *DRM* system without knowing any information about the Key ID. It is started as follow: the consumer playbacks the content in the Windows Media Player and send license request with the blinded key ID to the license server. Whereas, both of them authenticate with each other via a secure channel. The license server retrieves the Blind (Key ID) from Object WMRM Header, and sign it to get the signature of the Blind (Key ID). Then the license server generates the license and sends it to the consumer with the Key clue which is the relative information to generate the

Figure 7: the license generation of the WMRM *DRM* system

Key. The consumer checks the signature of the Blind (Key ID), unblinds the Key ID and obtains it is signature. This signature used as the content key and the consumer can use it to decrypt the protected content in the Windows Media Player. Content key acquisition protocols, there are two content key acquisition protocols, one based on RSA algorithm and the other is based on ElGamal algorithm. They are designed independently and perform some procedures in the content key acquisition such as: blind the key ID by the consumer, sign the key ID by the license server and checks the signature and unblinds the key ID by the consumer to obtain the content key. In RSA-based key acquisition protocols, this system became easy to understand, and be secure against most attacks. However, the computation speed of the key is slow. In ElGamal-based key acquisition protocols, the system be best secure against the reply attack, because of the signature of the same message with the same key is different from each other for the random parameter changing every time.

Advantage of Yuan's System

- Consumer anonymity: the consumer anonymity is preserved, No reliance on *TTP*, privacy in license acquisition:

Limitation of Yuan's System

- Consumer traceability: This system does not address how the content owner could trace and revoke the malicious consumer.

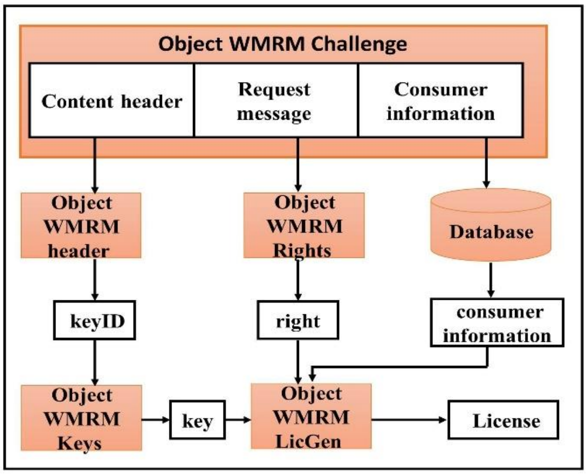

Figure 7. The license generation of the WMRM DRM system

VIII. Our Proposed scheme

Various *DRM* schemes are discussed in the previous section. In this section we focus on enhanced scheme which overcomes some drawbacks of multi-distributor schemes. We will propose *DRM* scheme preserve the consumer anonymity and unlinkability. It does not rely on *TTP* assumption, and support both of the consumer privacy and accountability. Also, we provide our scheme by a privacy preserving revocation mechanism to detect the scammer's consumers in the system and preserve the copyright.

IX. Comparison to related work

The comparison between the proposed solutions schemes is given in Tables 2 and 3. Where "Y" denotes "Yes/Supported," "N" denotes "No/Not Supported," and "N/A" denotes "Not Applicable.". We verify the schemes in the different scenarios where privacy can be threatened.

*Table 2***.** Comparison of cloud schemes in *DRM*

Properties	[1]	[34]	[41]	[42]	[30]
Consumer anonymity	Y	Y	Y	Y	N
Reliance on *TTP*	Y	N	N	N	N
Traitor tracing	Y	Y	Y	Y	Y
Flexibility in choosing license model	Y	Y	N	Y	N
Unlinkability of content executions	Y	Y	N/A	Y	N
Resistant to collision of *DRM* servers	N	Y	N/A	N	Y
Adding cost to consumers	Y	Y	N/A	Y	N/A

Table 3. Comparison of multi/one-distributor

Properties	[2]	[3]	[19]	[4]	[5]	[37]
Consumer anonymity	N	Y	N	Y	N	Y
Reliance on *TTP*	N	N	N	N	N	N
Traitor tracing	Y	N	Y	N	N/A	N
Consumer privacy in license acquisition	Y	Y	Y	Y	Y	Y
Need for trusted hardware	Y	Y	N	N	Y	N
Resistant to collision of *DRM* servers	Y	Y	Y	Y	N	N/A

X. Conclusions

In this paper, we present a brief description of the various schemes of digital rights management, and a comparative analysis of these schemes is given based on their features to achieve a balance between the *DRM* system and the consumer privacy. As evident from the analysis, we can design *DRM* scheme that overcomes the limitations of other schemes, preserving the consumer privacy without reliance on *TTP* and achieving the accountability.

References

[1] N.Joshi, R.Petrlic."Towards practical privacy-preserving digital rights management for cloud computing". In *Proceedings of the IEEE International Conference on Consumer Communications and Networking Conference (CCNC)*, pp. 265–270, 2013.

[2] L.Win, T.Thomas, S.Emmanuel. "Privacy enabled digital rights management without trusted third party assumption", *Multimedia, IEEE Transactions on*, 14(3), pp.546–554, 2012.

[3] R.Petrlic , S.Sekula. "Unlinkable content playbacks in a multiparty drm system". In *Proceedings of the Data and Applications Security and Privacy XXVII, Volume 7964*, Springer, pp 289–296, 2013.

[4] M.Feng, B.Zhu. "ADRM system protecting consumer privacy". In *Proceedings of the IEEE International Conference on Consumer*

Communications and Networking Conference (CCNC), pp.1075–1079, 2008.

[5] J.Yao, S.Lee, S.Nam. "Privacy preserving DRM solution with content classification and superdistribution". In *Proceedings of the IEEE International Conference on Consumer Communications and Networking Conference (CCNC)*, pp. 1–5, 2009.

[6] T. Gaber. "Digital rights management: Open issues to support e-commerce", in *E-Marketing in Developed and Developing Countries: Emerging Practices*, H. E-Gohary and R.Eid (eds.) , IGI Global,USA, pp.69–87, 2013.

[7] E.Wu, SH.Chuang, CH.Shih, H.Hsueh, SH.Huang, H.Huang. "A flexible and lightweight user-demand DRM system for multimedia contents over multiple portable device platforms", *Software: Practice and Experience*. pp. 1-25, 2017.

[8] C. Yen, H. Liaw, N. Lo. "Digital rights management system with user privacy, usage transparency, and superdistribution support", *International Journal of Communication Systems*, 27(10), pp.1714–1730, 2014.

[9] D.Mishra. "An Accountable privacy architecture for digital rights management system". In *Proceedings of the 6th International Conference on Computer and Communication Technology, ACM*, pp. 328–332, 2015.

[10] D. Mishra and S. Mukhopadhyay. "Secure content delivery in DRM system with consumer privacy". In *Proceedings of the springer conference on Information Security Practice and Experience*, Volume 7863, pp. 321–335, 2013.

[11] X. Zhang. "A survey of digital rights management technologies", *last modified:Nov*, 28, pp.1–10, 2011.

[12] C. Loebbecke, P. Bartscher, T. Weiss, S. Weniger. "Consumers'attitudes to digital rights management (DRM) in the german trade ebook market". In *Proceedings of the IEEE International Conference on Mobile Business (ICMB) and Global Mobility Roundtable (GMR)*, Athens, Greece, June, pp.337–344, 2010.

[13] T.Gaber, N.Zhang, AE.Hassanien."A novel approach to allow multiple resales of DRM-protected contents". In the *proceedings of IEEE 8th International Conference on Computer Engineering & Systems(ICCES)*, pp. 86-91,2013.

[14] MS.Ugale, A.Mune, HR.Deshmukh. "Digital Rights Management by Using Cloud Computing", *International Journal of Computer Science Trends and Technology (IJCST)*, 5(2), pp. 1–7, 2017.

[15] A.Osothongs, V.Suppakitpaisarn, N. Sonehara. "Privacy Disclosure Adaptation for Trading between Personal Attribute and Incentives", *Journal of Information Processing*, 25, pp.2-11, 2017.

[16] MA.Deshmukh, VB.Gadicha. "An approach towards digital rights management system using blind decryption algorithm", *International Journal of Advanced Research in Computer Engineering and Technology*, 5(5), pp.1333–1338, 2016.

[17] R. Finn, D. Wright, M. Friedewald. "Seven types of privacy", in *European data protection: coming of age*, S.Gutwirth, R.Leenes, P.de Hert, Y.Poullet (eds.), Springer, Dordrecht, pp. 3–32, 2013.

[18] M. Brusó, K. Chatzikokolakis, S. Etalle, J. Hartog. "Linking unlinkability", in *Trustworthy Global Computing*, C.Palamidessi, M.D.Ryan (eds.), Springer, Berlin, Heidelberg, volume 8191, pp. 129–144, 2013.

[19] D. Mishra, S. Mukhopadhyay. "Towards a secure, transparent and privacy preserving DRM system". In *Proceedings of the springer conference on Recent Trends in Computer Networks and Distributed Systems Security*, Volume 335, pp. 304–313, 2012.

[20] Q. HUANG, Z. MA, Y. YANG, J. FU, X. NIU. "Secure and privacy-preserving DRM scheme using homomorphic encryption in cloud computing", *The Journal of China Universities of Posts and Telecommunications*, 20(6), pp.88–95, 2013.

[21] R.Dingledine, N.Mathewson, P.Syverson. "Tor: The second-generation onion router". *Technical report*, Naval Research Lab Washington DC, USA, 2004.

[22] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete", *Communications of the ACM*, 28(10), pp.1030–1044, 1985.***

[23] A.Shamir, "How to share a secret", *Communications of the ACM*, 22(11), pp.612–613, 1979.

[24] H. Tewari, D. O'Mahony, M. Peirce. "Reusable off-line electronic cash using secret splitting", *Networks & Telecommunications Research Group, Computer Science Department, Trinity College, Dublin*, 2, pp.1–15, 1998.

[25] T. Dierks and E. Rescorla. "The transport layer security (TLS) protocol", *Version 1.2, Internet Engineering Task Force (IETF) Request For Comment (RFC) 5246*, pp. 1–104, Aug.2008.

[26] M. Abe and E. Fujisaki. "How to date blind signatures". In *Proceedings of the springer on Advances in Cryptology—ASIACRYPT*, Volume 1163, pp. 244–251, 1996.

[27] A. Razvan, B. Erfani. "Internet cash card", in U.S Patent application 20020143703, 2002.

[28] K. Sakurai, Y. Yamane. "Blind decoding, blind undeniable signatures, and their applications to privacy protection". In *proceeding of the International Workshop on Information Hiding, Springer*, volume 1174, pp.257–264, 1996.

[29] G. Blakley. "Safeguarding cryptographic keys". In *Proceedings of the National Computer Conference*, volume 48, pp. 313–317, 1979.

[30] M.Gourkhede, D.Theng. "Preserving privacy and illegal content distribution for cloud environment", *International Journal of Computing and Technology*, 1(3), pp.1–7, 2014.

[31] M. Kawahara. "Superdistribution: the concept and the architecture", *IEICE TRANSACTIONS (1976-1990)*, 73(7), pp.1133–1146, 1990.

[32] M. Gourkhede, D. Theng. "Analysing security and privacy management for cloud computing environment". In *Proceedings of the IEEE Fourth International Conference on the Communication Systems and Network Technologies (CSNT)*, pp. 677–680, 2014.

[33] G. Ateniese, K. Fu, M. Green, S. Hohenberger. "Improved proxy re-encryption schemes with

applications to secure distributed storage", *ACM Transactions on Information and System Security (TISSEC)*, 9(1), pp.1–30, 2006.

[34] R.Petrlic, CH.Sorge. "Privacy-preserving digital rights management based on attribute-based encryption". In *Proceedings of the IEEE 6th International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–5, 2014.

[35] J. Bethencourt, A. Sahai, B. Waters. "Ciphertext-policy attribute-based encryption". In *Proceedings of the IEEE Security and Privacy*, pp. 321–334., 2007.

[36] D. Chaum, A. Fiat,M. Naor. "Untraceable electronic cash". In *Proceedings of the* CRYPTO '88 *on Advances in Cryptology*, Volume 403, Springer, pp. 319–327,1990.

[37] J.Yuan, W.Zhang, F.Zhao. "Content key acquisition protocols hiding the usage information in DRM system". In *Proceedings of the IEEE 15th International Symposium on Consumer Electronics (ISCE)*, pp. 313–317, 2011.

[38] D. Chaum. "Blind signatures for untraceable payments". In *Proceedings of CRYPTO 82 on Advances in cryptology*, Springer, pp.199–203,1983.

[39] R.Rivest, A.Shamir, L.Adleman. "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, 21(2), pp.120–126, 1978.

[40] T. ElGamal. "A public key cryptosystem and a signature scheme based on discrete logarithms". In *Proceedings of CRYPTO 84 on Advances in cryptology*, Volume 196, pp. 10–18, Springer, 1985.

[41] Q.Huang, Z.Ma, J.Fu, X.Niu, Y.Yang. "Attribute based DRM scheme with efficient revocation in cloud computing", *Journal of Computers*, 8(11), pp.2776–2781, 2013.

[42] R.Petrlic, CH.Sorge. "Privacy-preserving DRM for cloud computing". In *Proceedings of the IEEE 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pp. 1286–1291, 2012.

[43] C. Castelluccia, E. Mykletun, G. Tsudik. "Efficient aggregation of encrypted data in wireless sensor networks", In *Proceedings of The IEEE Second Annual International Conference on the Mobile and Ubiquitous Systems: Networking and Services*, MobiQuitous, pp. 109–117, 2005.

[44] M.Den. "Privacy preserving content protection", *PhD thesis, Doctoral dissertation*, Katholieke Universiteit Leuven, 2010.

Author Biographies

Amira Mostafa was born in Ismailia on April 10th, 1987. Received the Bachelor degree in computer science from Suez Canal University, Ismailia, Egypt, in 2008. Her current research interests in software security, digital rights management (DRM) systems, consumer privacy techniques for DRM.

Tarek Gaber received a PhD degree from the University of Manchester in Computer Science in 2012. He has worked as an Assistant Lecturer at many universities including Faculty of Computers and Information Sciences, Ain Shams University, and the School of Computer Science, University of Manchester, Manchester, UK. He had a Postdoctoral Fellow at Faculty of Electrical Engineering and Computer Science, VSB Technical University of Ostrava, Czech Republic. Currently, he is an Assistant Professor at the Faculty of Computers and Informatics, Suez Canal University, Ismailia, Egypt. He is also IEEE member and a member of The Scientific Research Group in Egypt (SRGE) www.egyptscience.net. He participated in the organization (co-chairing) of many international conferences and organized a number of Workshops and Special Sessions at other international conferences. He also served as a Session Chair, PC Member at many international conferences, and a reviewer at a number on international journals. Dr. Tarek has authored/coauthored over 35 research publications in peer-reviewed reputed journals and conference proceedings and he has 2 books in the topics of image processing, data mining and machine learning. Tarek's major research interests include image processing, pattern recognition, information security, machine learning, wireless sensor network, and biometric authentication and identification.

Ghada Eltaweel received B.S., M.S., in computer Sciences and Ph.D. degree in Information technology from Cairo University in 1996, Helwan University in 2000, and Cairo University 2005 respectively. She is currently Professor in Suez Canal University, Ismailia, Egypt, since November 2016, Her research interests include image classification, DNA, image fusion, and image security.

Ajith Abraham is the Director of Machine Intelligence Research Labs (MIR Labs), a Not-for-Profit Scientific Network for Innovation and Research Excellence connecting Industry and Academia. The Network with Headquarters in Seattle, USA has currently more than 1,000 scientific members from over 100 countries. As an Investigator / Co-Investigator, he has won research grants worth over 100+ Million US$ from Australia, USA, EU, Italy, Czech Republic, France, Malaysia and China. Dr. Abraham works in a multi-disciplinary environment involving machine intelligence, cyber-physical systems, Internet of things, network security, sensor networks, Web intelligence, Web services, data mining and applied to various real world problems. In these areas he has authored / coauthored more than 1,000+ research publications out of which there are 100+ books covering various aspects of Computer Science. One of his books was translated to Japanese and few other articles were translated to Russian and Chinese. About 900+ publications are indexed by Scopus and over 700+ are indexed by Thomson ISI Web of Science. Some of the articles are available in the ScienceDirect Top 25 hottest articles. He has 700+ co-authors originating from 40+ countries. Dr. Abraham has more than 25,000+ academic citations (h-index of 78 as per google scholar). He has given more than 100 plenary lectures and conference tutorials (in 20+ countries). For his research, he has won seven best paper awards at prestigious International conferences held in Belgium, Canada Bahrain, Czech Republic, China and India. Since 2008, Dr. Abraham is the Chair of IEEE Systems Man and Cybernetics Society Technical Committee on Soft Computing (which has over 200+ members) and served as a

Distinguished Lecturer of IEEE Computer Society representing Europe (2011-201)3. Under his direct academic supervision, 12 students received Ph.D. degrees and is currently supervising 12 Ph.D. students in different Universities in Europe, USA, Africa and India. He has examined over 100 Ph.D. theses. Currently Dr. Abraham is the editor-in-chief of Engineering Applications of Artificial Intelligence (EAAI) and serves/served the editorial board of over 15 International Journals indexed by Thomson ISI. He is actively involved in the organization of several academic conferences, and some of them are now annual events. Dr. Abraham received Ph.D. degree in Computer Science from Monash University, Melbourne, Australia (2001) and a Master of Science Degree from Nanyang Technological University, Singapore (1998). More information at: http://www.softcomputing.net/