Study Paper

On

DIGITAL RIGHTS MANAGEMENT SYSTEM
A Technology for Secured Delivery of Digital Content through the Internet

September 2022

Convergence and Broadcasting Division,
Telecommunication Engineering Centre
Department of Telecommunications
Ministry of Communications
Government of India
K.L. Bhawan, Janpath, New Delhi-01

Table of Contents

Digital Rights Management System

1. Abstract

Security of Television (TV) broadcasting is crucial for safe and secure content transmission. Conditional Access Systems (CAS) are widely used to provide a secure path to Television services such as Cable Television Services (Cable TV), Direct-to-Home (DTH) services, Headend-in-Sky (HITS) services, and terrestrial TV services. However, technology has evolved, and Internet protocol-based services have entered into TV broadcasting services, and the same are widely accepted by many people. To ensure the security of these TV broadcasting services, some mechanism or technology is required. Digital Rights Management System (DRM) is one such technology to address the security aspects of these new IP-based services. This paper presents various aspects of the Digital Rights Management System, including the difference between CAS and DRM, different risks of IPTV content, an overview of DRM, basic principles of DRM technology, the architecture of a DRM system for cable television, use cases of DRM, the requirement of a DRM in content delivery of cable television service and implementation of DRM in IPTV cable distribution.

Disclaimer: The outcomes/conclusions drawn and recommendations made thereof in this study paper are of academic interest only and view of the writers only and should in no case be considered as an official stand or formal view of TEC.

2. Introduction

The terms Conditional access system (CAS) and Digital Rights Management system are frequently used interchangeably, although both have separate roots. Within the converged world of the connected home, they are being integrated into a unified system to shield the rights and revenues of content owners and distributors. CAS and DRM are growing to satisfy this converged world. CAS is supposed to manage the delivery of pay TV, while DRM is supposed to manage the delivery of content through the Internet and mobile. The content should be viewable seamlessly once it reaches the authorized user. Viewers want to time-shift and share content across their many devices. These need a system to safeguard content and supply copy management across the media devices within premises like TV, PCs, mobile phones, laptops, etc. With the convergence of media and distribution formats, the distinction between CAS and DRM is getting lesser. The viewers are looking to a world where they will access content from their set-top boxes (STB) via IPTV, mobile devices, and the web. Further, once they have access to content, they want the power to share it across many media players, from their televisions to handheld devices.

The traditional model utilized by broadcasters for revenue protection has been CAS, designed to manage access to subscription services delivered via cable or satellite. The broadcaster or the multi-service operator scrambles all the pay channels; the key supplied with the set-top box (STB) at the customer end unscrambles only those channels that the viewer has opted to pay for.

The advent of new and latest means to distribute and watch video content has updated the broadcast aspect. The popularity of streaming and progressive download for delivering content to Personal computers/ Mobiles led to the need for something similar to CAS to protect or shield revenue. Unlike the controlled delivery of cable TV and the Set-top box (STB), streaming takes place over an open system, the public Internet.

Cable Television Services, Direct-to-Home services, Internet Protocol Television services, Headend-in-Sky services, and terrestrial TV services are widespread for television broadcasting and distribution services. Internet Protocol-based TV broadcasting is also now available due to technological advancements and convergence. It includes IP linear services and IP video on demand (VoD).

TV broadcasting services are all about transmitting content via one of the above-mentioned methods. But it is not as easy as it seems. Various factors should be kept in consideration while transmitting any data. One such factor is the security of data i.e. how secure the transmission channel is. Nowadays, analog transmissions have been phased out. Digital transmissions offer better efficiency and more opportunities. Like every other system, advancement in modern technology also brings new issues like digital data piracy. In digital systems, not only can one make copies of data quickly and often for free, but it is also easy to do so without being detected.

Therefore, the security of TV broadcasting is crucial for the safe and secure transmission of content. Conventional TV services such as Cable TV, DTH, HITS, and terrestrial TV use the Conditional Access System for controlling and managing the authorized access of content, and

preventing unauthorized access to content. Similar security mechanisms are required for the new IP-based methods for delivering content. One such technology or mechanism that can help us is Digital Rights Management System (DRM).

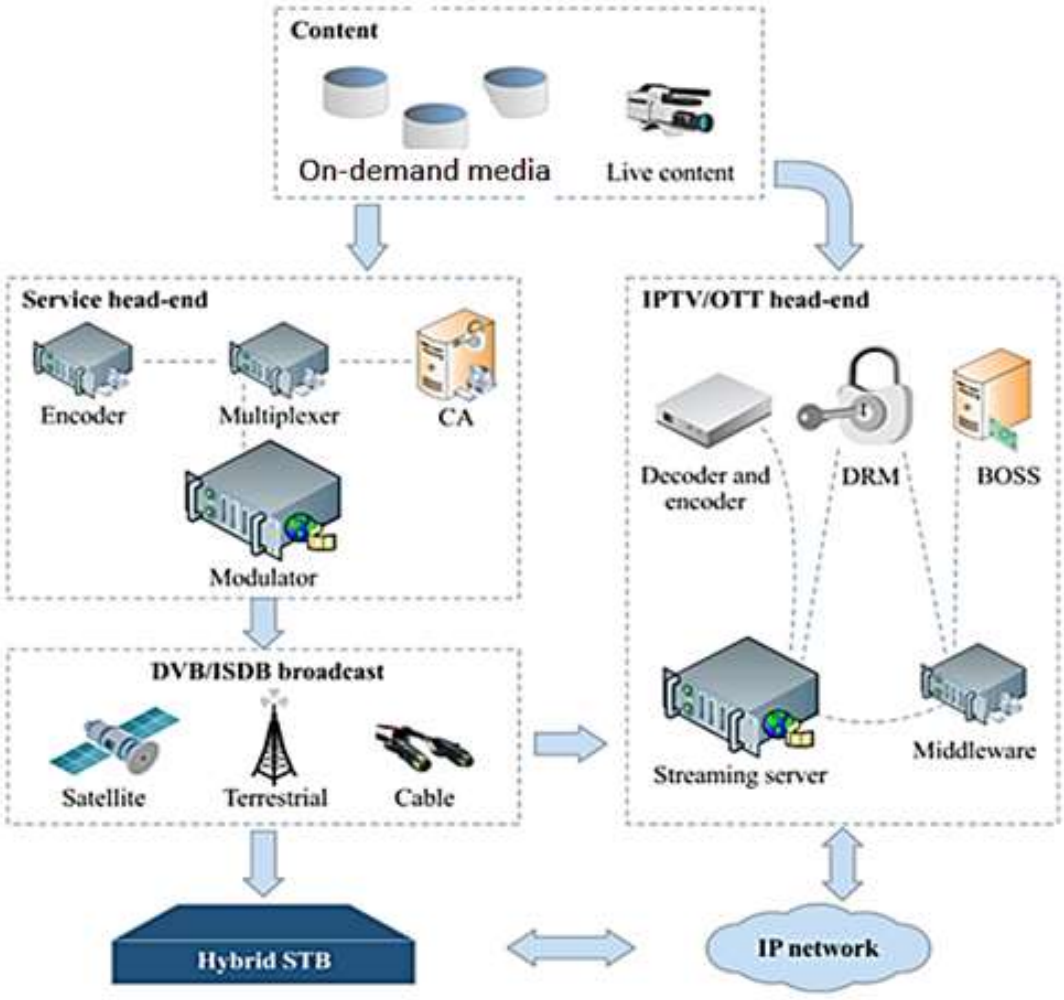

Figure 1 - Hybrid STB video system overview *(Source ITU J.1005(08/2015))*

Digital Rights Management System (DRM) technology is designed to protect the content from unauthorized access based on device authentication. It can only protect IP-type content (IP VOD, IP Linear, etc.) as of now as indicated in the figure-1. To elaborate further, a hybrid set-top box can provide DVB-based services and IP-based services. It requires a Conditional Access System to protect non-IP-based services such as Cable TV or DTH, and a Digital Rights Management System to protect the content of IP-based services such as IP linear and IP video on demand from unauthorized access [2].

3. Difference between CAS and DRM

Increasing concern for the distribution of copyrighted content (such as audio, video, text, data, mixed media, etc.) over a large range of media (e.g., magnetic tapes, magnetic disks, optical disk, satellite, cable, terrestrial), etc.) has led to several other ways of protecting content. Typically, these programs have been designed to safeguard the content during the

transmission and after the content has been received (e.g., in the set-top box, television, personal computer, cell phone, etc.). Two protection systems namely Conditional Access (CA) and Digital Rights Management (DRM) are deployed.

Conditional access systems (CAS) (refer to figure-2) are deployed in broadcast platforms to securely deliver content from a service operator, like a satellite or cable TV provider, to individual recipients like set-top boxes. Most network operators will scramble a minimum of a number of their services to guard their pay-tv operations. Conditional Access Systems use security principles that include the encrypted data along with EMM (Entitled management message) and ECM (Entitled control message) both referred to as Conditional Access Messaging (CAM), which are typically broadcast in the transport stream together with, or in conjunction with, the scrambled program (content). CAM contains two different and independent message streams, one that features a collection of continually updated at irregular intervals encryption keys and the other that has the subscriber rights to watch a particular program (content). Both conditional access messages include the related access conditions.

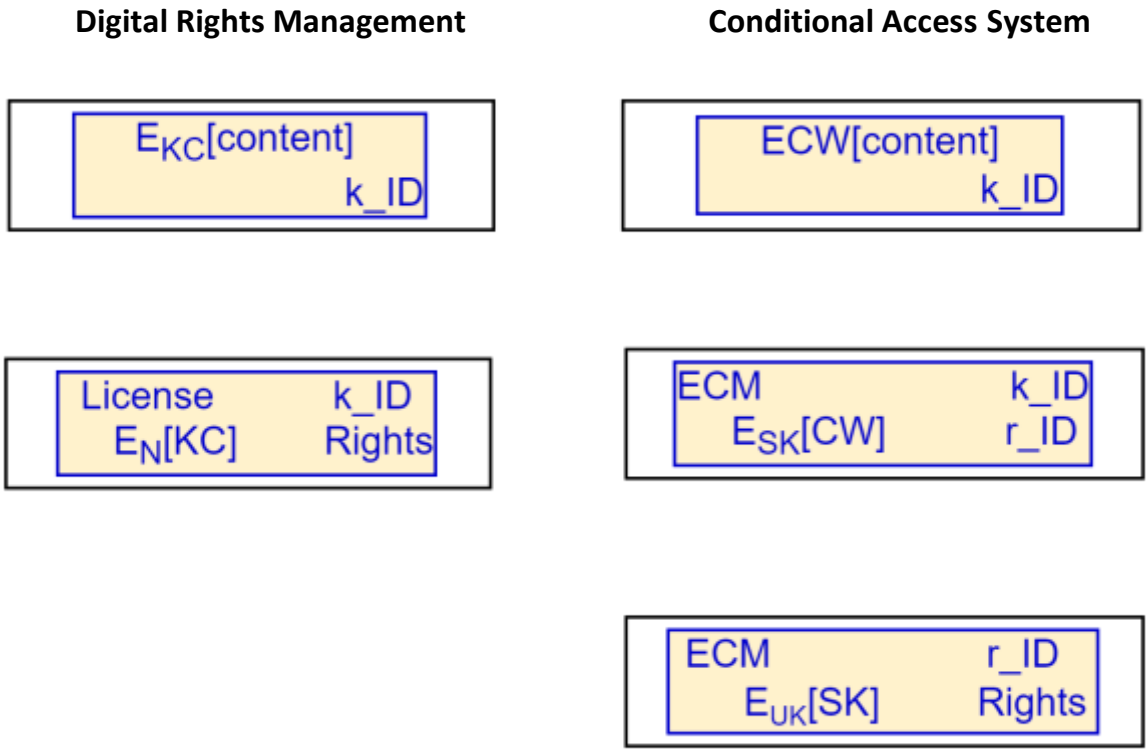

Figure 2: -DRM and Conditional Access System

Unlike Conditional Access Systems (CAS) for the broadcast streaming of content, DRM systems are developed to securely allow the utilization of other sorts of content (e.g., MPEG files, CDs, DVDs, audio/video streams, etc.) on devices like personal computers and other electronic items. With a plethora of periodically updated keys and multi-message streaming utilized in CA Schemes, DRM systems typically use a single license that includes the content usage rights and a decryption key for consuming the protected content. In addition, the

license may be delivered independent of the content, yet bind the content to the license and a particular device or potentially a group of devices.

CA and DRM technologies are developed to shield different kinds of content with different delivery methods, and thus consider different security risks in mind. For instance, conditional access protection systems were developed for pay-tv media that is broadcast to a plurality of devices in a streaming fashion, i.e., real-time playback. Therefore, because the content is broadcast and streamed, continuous updating of the keys and encryption thereof at different times and concealed in various messages) are the key to a strong CAS. On the other side, DRM systems are developed for sending a single piece of content (such as audio, video, files, etc.) (i.e., not necessarily a real-time broadcast but it must be digital data that can be stored and afterward played or consumed) to single device (or small group of devices). Therefore, the binding of the content to a single license and binding the license to a particular device (or group of devices) gives a suitable level of protection that is somewhat tailored to how the content is received and consumed.

Major differences between CAS and DRM are briefly explained in following table: -

CAS (Conditional Access System)	DRM (Digital Rights Management)
• Developed for pay-tv media that is broadcast to a plurality of devices in a streaming fashion, i.e., real-time playback. • CAS is supposed to manage the delivery of pay TV. • The traditional model utilized by broadcasters for revenue protection has been CAS, designed to manage access to subscription services delivered via cable or satellite. • Conventional TV services such as Cable TV, DTH, HITS, and terrestrial TV use the Conditional Access System for controlling and managing the authorized access of content, and preventing unauthorized access to content. • CAS use security principles that include the encrypted data along with EMM and ECM both referred to as Conditional Access Messaging (CAM), which are typically broadcast in the transport stream together with, or in conjunction with, the scrambled program (content).	• Developed for sending a single piece of content (such as audio, video, files, etc.) (i.e., not necessarily a real-time broadcast but it must be digital data that can be stored and afterward played or consumed) to single device (or small group of devices). • Manage the delivery of content through the Internet and mobile. • Designed to protect the content from unauthorized access based on device authentication. • It can only protect IP-type content (IP VOD, IP Linear, etc.) to elaborate further, a hybrid set-top box can provide DVB-based services and IP-based services. • It requires a Conditional Access System to protect non-IP-based services such as Cable TV or DTH, and a Digital Rights Management System to protect the content of IP-based services such as IP linear and IP video on demand from unauthorized access.

Emerging network technologies because of the convergence of technology like home networking, and OTT, however, are setting out to reveal current disadvantages between these alternative content protection methods or schemes. Specifically, the desire and need to make all appliances and other devices within a home capable of communicating with each other, and having the ability to utilize the unique capabilities of every device on any device within the home network, make unifying these two content protection systems advantageous [3].

4. The risk of IPTV content

To effectively protect IPTV content, it is necessary to analyze the risk faced by current IPTV content so that IPTV DRM protection can be effectively implemented. At present, the risk in respect of IPTV content is mainly in the following areas:

a. It is illegal to copy content. It refers to the illegal users cracking the key, copying out from the IPTV digital content, and illegal distribution of such copying content.
b. Content providers mustn't have pirated technology to ensure that IPTV could provide users with the latest, high-quality audio content.
c. Hacker programs are obtained through illegal means. Hackers can easily attack the content library to get non-encrypted content.
d. STB to copy content. As the STB is installed at users' premises, users can easily copy down audio or video content from the analog port or by the camera to display the content preserved. At present, some STB manufacturers are using special chips so that the signal is recorded by interference.

5. Overview of DRM

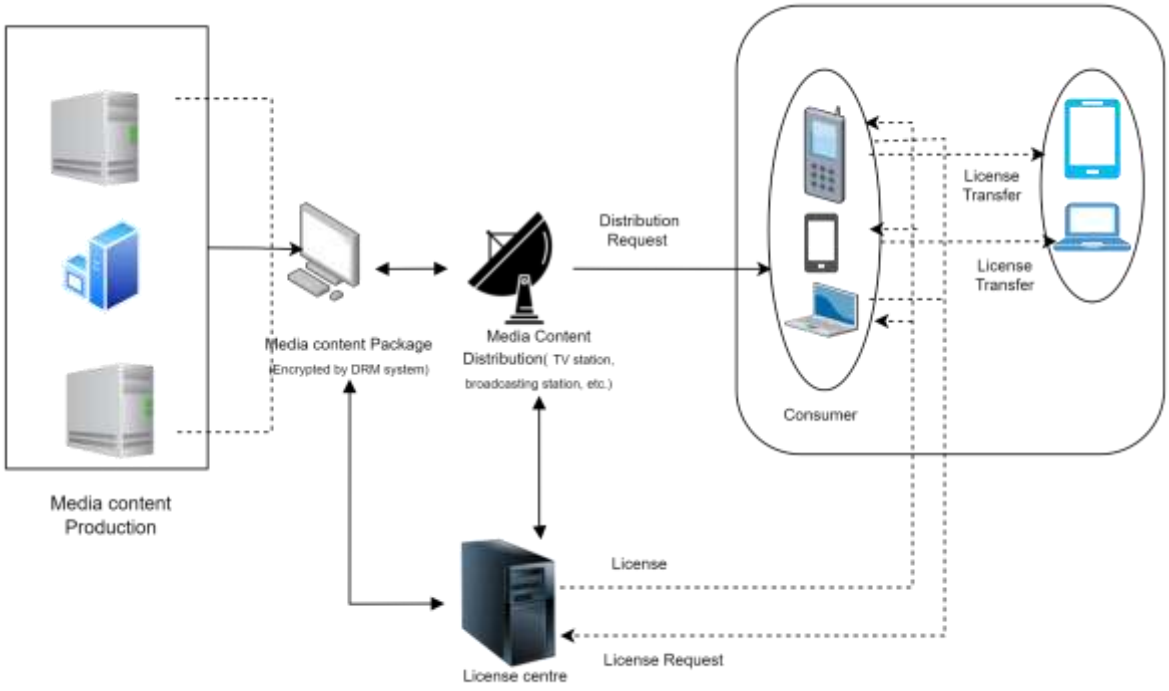

Figure 3: -DRM framework of Digital TV

DRM technology is an important integral mechanism that describes, defines, monitors, and protects the rights of the stakeholders involved in the process of making, broadcasting, and playing digital content. DRM is the chain of software and hardware technologies and services that manages the authorized use of digital content and all the consequences and outcomes of its use throughout the life cycle of the content. Its objective is to ensure the legitimate use through the life cycle of digital content, protect the intellectual property rights of digital content, protect the trade channel of digital content, protect the interests of authors, publishers, and distributors, and also the legitimate rights of end-users. Therefore, finally achieving the goal of keeping the balance of the interests among all parties, stimulating digital content product development and prosperity. The figure-3 shows the common framework of digital TV.

6. Basic Principle of DRM Technology

The principle of DRM technology is to use technical means of digital products, distribution, transmission, and implementation of all regulatory features to make digital products only for authorized use following the licensed duration of use. Following the different implementation mechanisms, digital copyright protection technology is mainly of two kinds:

a. Digital watermarking technology, and
b. The other protection mechanism is based on data encryption and anti-copying DRM technology as the core.

Digital watermarking technology is the use of the hidden tags or kind of marker embedded in the digital and in the basic quality of the original work, without prejudice to the content, to achieve the copyright of digital content protection. These hidden tags are also integral parts of the copyright-related information hidden in the digital content that can be extracted only with dedicated testing tools. However, the current market utilizing digital watermarking technology is not sufficiently mature and liable to be easily damaged or cracked, and the digital watermark method can only be used in evidence after fraudulent detection or tracking and cannot prevent piracy of content in advance.

With data encryption and anti-copying technology as the main parts of the DRM, digital content is encrypted, and only authorized users get the decryption key. The encryption key is bound to the user's hardware information, and the encryption technology combined with hardware-binding technology can effectively achieve the purpose of copyright protection. Most current domestic and international companies and research institutes are implementing DRM systems using this technology [4].

7. The Architecture of the DRM system

Figure 4 shows the architecture of the Digital Rights Management system required for content delivery by cable platforms. The basic requirement of DRM is the content right protection of IP-based services such as IP linear TV and IP VoD.

The DRM system is usually deployed at the cable platform. The raw content, collected from different broadcasters and different resources that are outside of the cable platform, is encoded or transcoded which is further forwarded to the DRM system for encryption upon receiving the request from the DRM client (installed at the user end terminal device). The DRM system encrypts the content and sends the encrypted content along with the license of authorized access and decryption key (required to decrypt the content at the client side) to the DRM client with the help of the content delivery server.

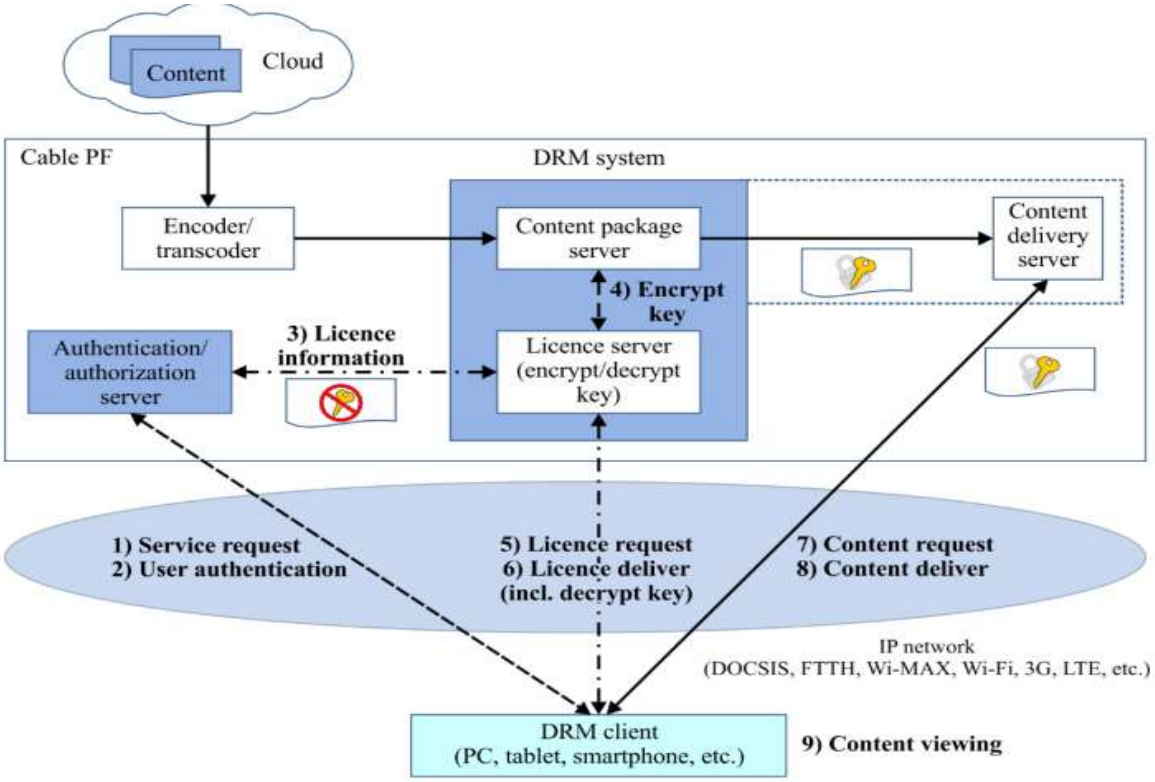

Figure 4 – Model of general DRM system and expected signal flow *(Source ITU J.1005(08/2015))*

Working of the DRM system required for content distribution service is explained in detail as follows:

i. First of all, the subscriber accesses the cable operator's portal site through the DRM client for availing of the services.
ii. The portal site sends the client requests to the authentication/authorization server at the cable platform. At this server, authentication and authorization of the user for accessing content are being carried out.
iii. Service providers decide whether the content may be allowed to deliver to the content delivery network (CDN). On deciding this, DRM license information is exchanged between the license server and the authentication/authorization server.
iv. After exchanging the license between the license server and the authentication/authorization server, an encryption key and license are generated by the license server. The encryption key in turn is sent to the content package server for encrypting the content.
v. Now, the DRM client requests the DRM license from the license server which contains the decryption key and some other things that help to manage authorized usage of the content.

vi. Then, the license server delivers the license to the DRM client for the decryption of content.

vii. After delivery of the license, the user requests the content from the content delivery server.

viii. Upon the request of the DRM client, the content delivery server delivers the encrypted content to the subscriber.

ix. Now, content is decrypted by the DRM client with the help of the decryption key contained in the license and now users can enjoy their content.

7.1. Components and flow

Now, the working of each of the components of the DRM system and the communication flow required to deliver the content at the client end's device are elaborated as follows:-

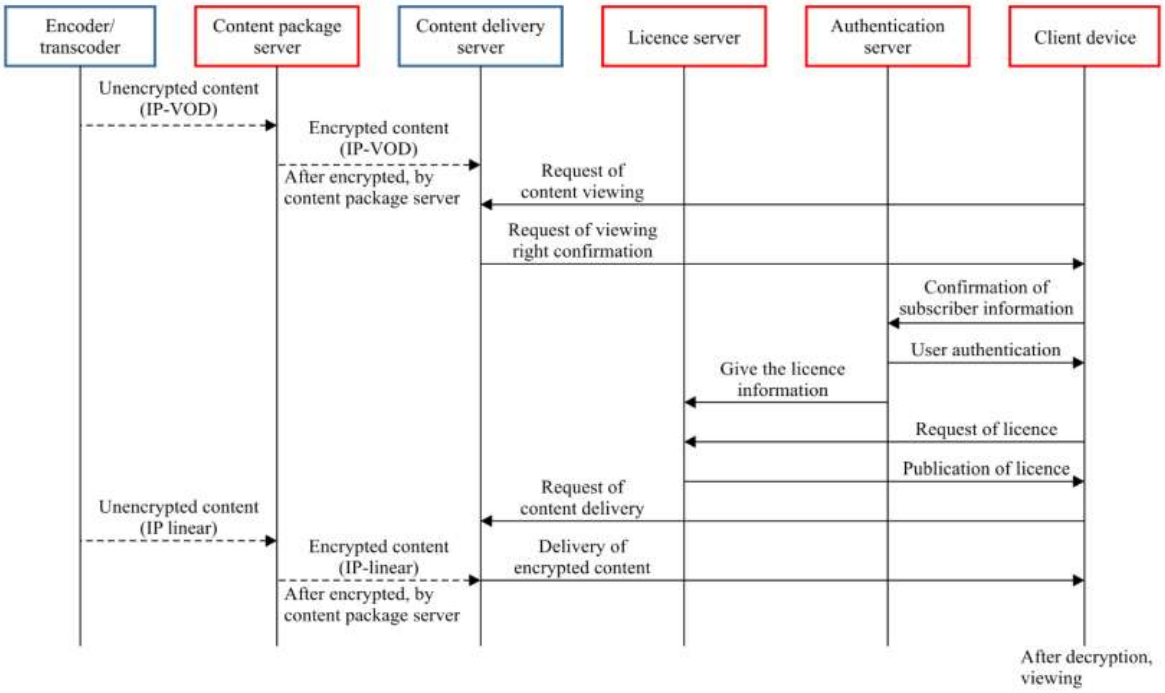

Figure 5 – Example of DRM processing flow

7.2. Encoder / Transcoder

The encoder is used to convert the content into a deliverable format for the network and the transcoder converts the content into receivable format i.e.; it converts the content into an appropriate number of pixels for good quality reception of content. The DRM system should use the MPEG2-TS/MP4 for good quality. It pre-processes the content (such as live stream, encoding of media file, and transforming of the container) before encryption of content.

7.3. Content package server(encryption)

This section of DRM aims to encrypt the content using an international or proprietary specification of encryption in alignment with a content format such as MPEG-2 /MPEG 4/ HEVC etc.

7.4. Content delivery server

The content delivery server aims to deliver the content to the client device by choosing the appropriate delivery method upon request of content viewing and confirmation of session establishment. It is sometimes also known as a content delivery network (CDN).

7.5. License server

It deals with the license issuing and delivering it to the permitted client in synergy with the authentication server i.e.; it gets the user information from the authentication server for delivery of the license and managing it. Usually, a license includes a license use case, license period control, and license delivery method. It is pertinent to mention here that simultaneous viewing of content on STB and non-STB devices is not covered as it requires exclusive controls from the content providers.

7.6. The Domain management server

It deals with limiting the number of devices which can access the content by the single license provided by the license server just like the OTT application which restricts the number of devices by which authentic users can access the content i.e.; it sets the maximum limit to the number of devices by which a user can simultaneously login into that application with a single license. Such a group of devices is known as the domain and the devices bonded in that domain can use the protected content. The user can also add or delete the devices from the domain as long as the total number of devices in the domain does not exceed the limit defined by the service.

7.7. Client device

There should be a client DRM installed on the client's device. The player in the client DRM should be securely embedded in the device because it is responsible for the decryption and display of the content on the client device. The figure-6 shows the structure of client DRM.

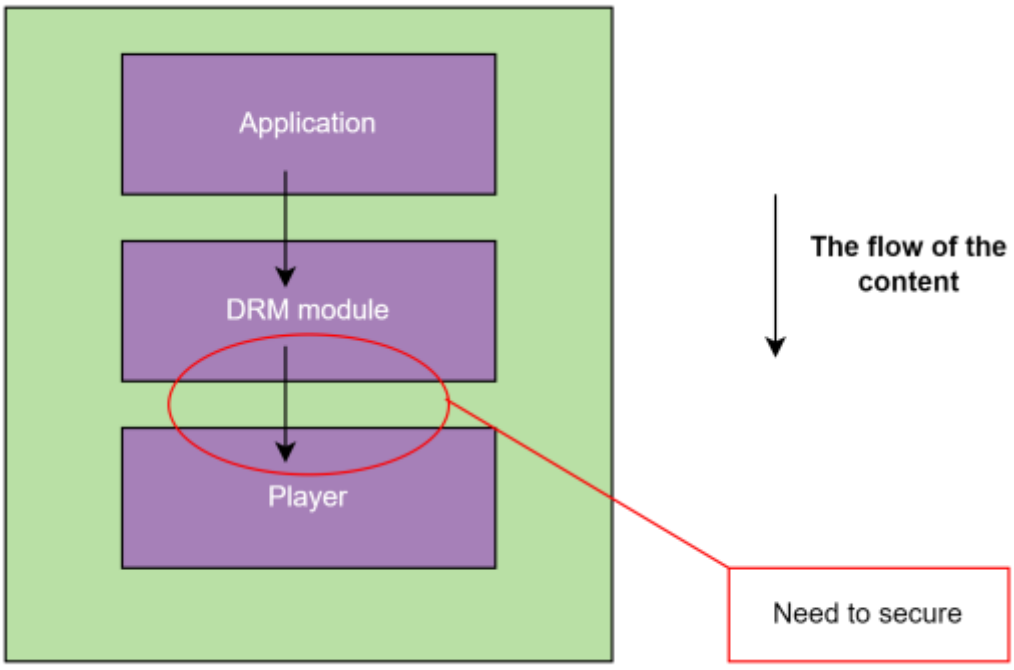

Figure 6 – Structure of client DRM

7.8. Authentication server

It performs an authentication function and does the authorization of the user by verifying the user ID and password stored in the cable operator's subscriber management system (SMS). The authentication server sends this information to the license server for the generation of the license and encryption key and if the user is not authorized then the authentication server terminates that request to itself only [2][3].

8. Use Cases of DRM and Global Best Practices

a. Limit access to files – DRM technology helps writers, filmmakers, artists, and other content creators to prevent unauthorized use of their content. It protects their bottom line and ensures the proper distribution of their products. One of the examples of this case is Apple iTunes. The iTunes Store uses DRM software to limit the number of devices that can access the purchased audio files. In the case of a downloaded song from an iTunes music store, the store collects data of users such as purchase details, usage function, the device used, etc. to limit playing iTunes music on any other unauthorized devices.

b. Keep digital work unaltered – Content creators always want to ensure that their work is not disturbed in any form. DRM technology tries to ensure the originality of the content. For example, browsing through premium stock images, video, or audio can only be played if one has usage rights and licensing.

c. Prevent software tampering – DRM technology prevents your software from running on a device where third-party software is already running. This is important to prevent other software from accessing the contents of your software.
Microsoft software, like windows or office applications, contains a DRM system referred to as Play Ready. This program prevents windows from running on a personal computer device when another software is already in use and hence, it prevents any unauthorized user or bot from crawling the contents of its software.

d. Produce content safely - DRM software embeds a tracking ID for every piece of content to track usage and summarize all the microscopic information within the dashboard.
In the case of running marketing campaigns, DRM software can collect and manage contracts and agreements to induce better information in terms of use and to create content without having to deal with legal issues.

e. Prevent leaking confidential information - DRM also helps in safeguarding important and crucial documents from getting leaked [6].

f. Malaysia, Morocco, Philippines, Canada, Indonesia, China, France, North America, and South Korea are among a few countries that have successfully implemented IPTV using Digital Rights Management (DRM) system as the security and content protection mechanism to protect content from unauthorized access via the internet.

9. DRM in IPTV Cable Distribution

9.1. Cable platform and Place of DRM in cable platform

Protection of content is becoming even more important nowadays due to various emerging content. DRM can be used in the entertainment/ media industry, tech industry, and enterprises to protect content or any kind of data. DRM works by exchanging license information between the DRM system and the customer terminal device. After exchanging license information, a DRM licensed terminal device can decrypt the content that was encrypted in the DRM system at the transmission end of the system before content distribution.

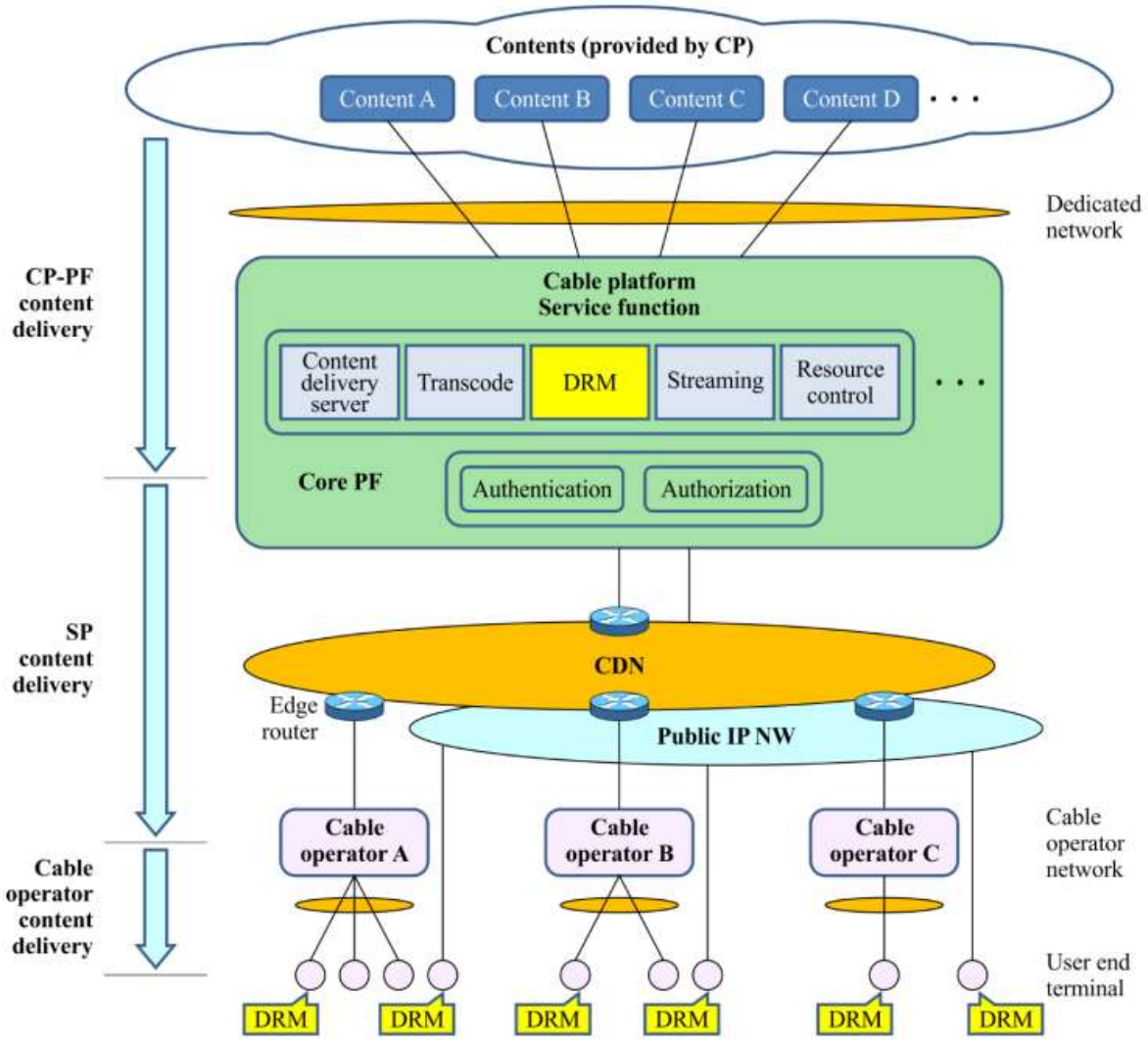

Figure 7 – Cable platform and DRM *(Source ITU J.1005(08/2015))*

The figure-7 shows the basic functional components required in DRM-protected TV broadcasting services. Content providers (CPs) mainly provide the content for transmission, they can be broadcasters or the entity that owns or is licensed to sell content or content assets. Content providers transmit content securely to cable platforms by a dedicated network. A cable platform is a business entity that can manage and operate collective services on a dedicated network of digital broadcasting and is operated mainly by platform providers. To transmit content from cable platforms to cable operator service providers (SPs), a content delivery network (CDN) is used. The cable operator further distributes the content to the customer's end terminal device with the help of its network.

Usually, the function of DRM such as encryption and license distribution is provided in the cable platform, but it can also be done at the stage of the Service provider's server or cable operator's server. Service authorization and user authentication are compulsory before delivering content at the later stages. The service provider then performs the necessary operation required to provide a secure path between the cable platform and cable operator such as confirming the exclusive control of conditions for simultaneous viewing. After performing these tasks, DRM performs encryption and transmits the content to the cable operator's headend system. Further, the cable operator distributes the encrypted content to the subscriber's end terminal devices such as Set-Top-Boxes, smartphones, tablets, etc. with the help of its network. But to decrypt the content received from the cable operator, subscribers require a license of authorized access to the content and that is transmitted by the service provider with the set timing (which can be understood as a subscription) to the subscribers and the method of delivery of that license will be decided by the service provider only. After delivery of the license, content can be decrypted and subscribers can now enjoy their content. There are various DRM scenarios present nowadays in the market which have different methods of providing licenses. In some cases, the license is delivered after the delivery of content. As DRM is required for the protection of content therefore it should be robust and should comply with all safety and security rules required to provide a secure channel for content delivery.

9.2. Service model

The figure-8 shows the expected service model of IP video content delivery protected by the "Digital Rights Management System". IP-based content delivery by this service model can cater to both homes and outdoor services. The cable operator's IP network will be used to deliver content to Set-top boxes and non-set-top box devices and public IP networks will be used if the content is required to be delivered outdoors at non-set-top-box devices.

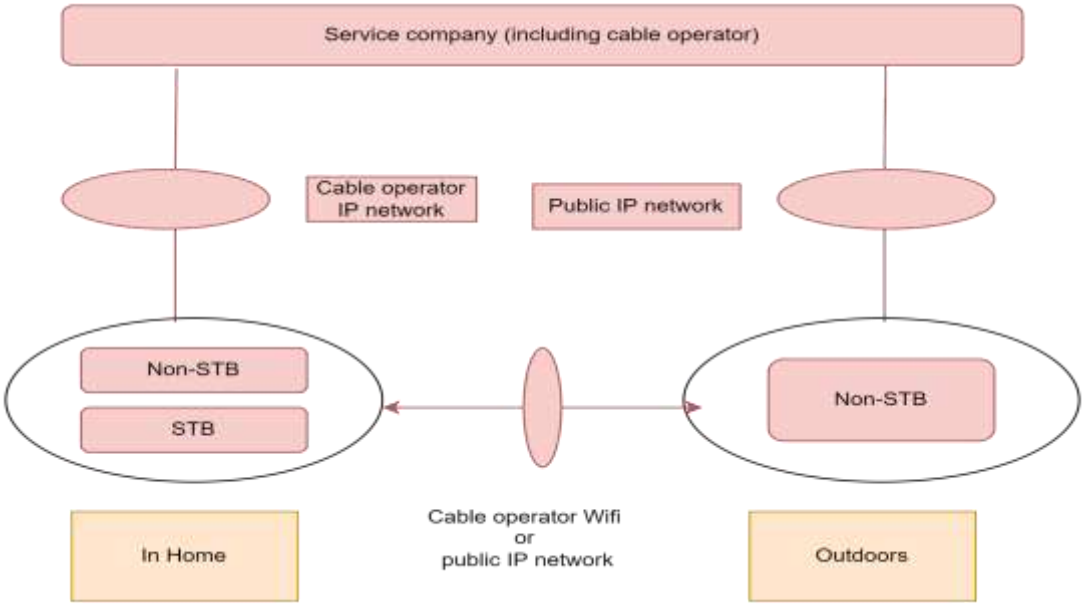

Figure 8 - An expected service model of IP video content delivery

IP-based services include IP linear TV and IP Video on Demand wherein IP linear service can deliver terrestrial broadcast and satellite broadcast content and community broadcast content and IP VoD can deliver videos on demand and stored content either with the help of a cable operator's network or public IP networks.

10. Conclusion

Security Assurance of different types of data/ content is a continuous and evolving process, wherein Digital Rights Management System along with the Conditional Access System plays a pivotal role to ensure the delivery of encrypted content to only authorized users. Earlier, both the technologies, DRM and CAS, used to work separately to protect different types of content/ data but with the convergence of media and distribution formats, the distinction between CA and DRM is lessening to an extent that now both technologies may work in an integrated way to make cable television system more secure and robust from piracy and other risk related to IPTV as discussed in this paper. The broadcasters continue to make it difficult for the pirates to get quality copies through a strong CAS and a robust Internet DRM. A trio of technologies - DRM, CA and copy management - is there to guard the revenue. To address the issue of deployment of non-standard CAS in the television broadcasting sector and to ensure better conformity of standards by CAS, TEC has released the Test Guides for CAS and Subscriber Management System (SMS) that prescribe the various mandatory and desirable functional requirements for CAS. Along similar lines, the appropriate authority may consider preparing the Test Guides/ specifications for DRM that prescribe the various mandatory and desirable functional requirements for DRM.

11. Abbreviations

Abbreviation	Expanded Form
CA	conditional access
CAS	conditional access system
CDN	content delivery network
CP	Content providers
DRM	Digital rights management system
DTH	direct to home
ECM	entitled control message
EMM	entitled management message
HITS	head end-in-sky
IP	internet protocol
IPTV	internet protocol TV
OTT	over the top
SMS	subscriber management system

SP	service providers
STB	set-top box
VoD	video on demand

12. References

1. DRM technology (DRM technology | TV Tech (tvtechnology.com))
2. J.1005(08/2015) Architecture and requirements of digital rights management (DRM) for cable television multi-screen (ITU-T Recommendation database)
3. Conditional access to digital rights management conversion (US20050182931A1 - Conditional access to digital rights management conversion - Google Patents)
4. Architecture Design for DRM System of Digital Television (009-ICCAE2011-A00234.pdf (ipcsit.com))
5. J.1006(10/2016) Specification of IP-VoD DRM for cable television multi-screen system in a multi-DRM environment (ITU-T Recommendation database)
6. 12 Digital Rights Management software in 2022 (12 Digital Rights Management (DRM) Software in 2022 - Geekflare)

****