Digital Rights Management for Forward Lock Content

A dissertation submitted in the partial fulfillment for the award of Degree of
Master of Technology
In
Software Technology

By
NALINAKSHYA NILOTPAL SAHOO
(Roll no. 2K12/SWT/09)

Under the guidance of

Prof. Manoj Kumar

DELHI TECHNOLOGICAL UNIVERSITY

BAWANA ROAD, DELHI

DECLARATION

I hereby want to declare that the thesis entitled "**Digital Rights Management for Forward Lock Content"** which is being submitted to the **Delhi Technological University**, in partial fulfillment of the requirements for the award of degree in **Master of Technology in Software Technology** is an authentic work carried out by me. The material contained in this thesis has not been submitted to any institution or university for the award of any degree.

NALINAKSHYA NILOTPAL SAHOO
Delhi Technological University, Delhi

CERTIFICATE

Delhi Technological University
(Government of Delhi NCR)
Bawana Road, New Delhi-42

This is to certify that the thesis entitled **"Digital Rights Management For Forward Lock Content"** done by **NALINAKSHYA NILOTPAL SAHOO** (Roll Number: **2K12/SWT/09**) for the partial fulfillment of the requirements for the award of degree of **Master of Technology** Degree in **Software Technology** in the **Department of Computer Engineering**, Delhi Technological University, New Delhi is an authentic work carried out by him under my guidance.

Project Guide:
Prof. Manoj Kumar
Associate Professor
Delhi Technological University, Delhi

ACKNOWLEDGEMENT

I take this opportunity to express my deep sense of gratitude and respect towards my guide **Prof. Manoj Kumar Department of Computer Engineering.**

I am very much indebted to him for his generosity, expertise and guidance which I received from him while working on this project. Without his support and timely guidance the completion of the project would have seemed a far –fetched dream. In this respect I find myself lucky to have my guide. He has guided not only with the subject matter, but also taught the proper style and techniques of documentation and presentation.

Besides my guide, I would like to thank entire teaching and non-teaching staff in the Department of Computer Engineering, DTU for all their help during my tenure at DTU.

NALINAKSHYA NLOTPAL SAHOO
M.Tech. Software Technology
2K12/SWT/09

ABSTRACT

In this report, a new approach for DRM forward lock file has been implemented .DRM forward lock content cannot be forwarded to other mobile device due to the restriction as per OMA DRM method.

But a new approach has been implemented for encrypting the forward-locked DRM contents using a unique number of the device, and storing the encrypted forward locked DRM contents. So whenever the user downloads forward lock content, the new file in the device is created which is an encrypted content. If user transfers the content to other device, then content cannot be usable in that device. It can open on the originating device where it was downloaded earlier.

TABLE OF CONTENTS

LIST OF FIGURES

List of Acronyms

DRM	Digital Rights Management
OMA	Open Mobile Alliance
CEK	Content Encryption Key
DRMREL	DRM Rights Expression Language.
DCF	Digital Content Format

CHAPTER 1

INTRODUCTION

The Digital Rights Management (DRM), a framework for ensuring the copyrights of information coursed through the Web or other advanced media by empowering secure appropriation and/or debilitating unlawful dissemination of the information. Commonly, a DRM framework secures protected innovation by either encoding the information so it must be gotten to by approved clients or denoting the substance with a computerized watermark or comparative system so that the substance can't be openly circulated. It works like access control advances that can be utilized by equipment producers, distributers, copyright holders and people to restrain the utilization of computerized substance and gadgets .The perfect DRM framework is adaptable, altogether straightforward to the client and really complex stuff for a computer program to crack. [2]

A digital rights management method operates on three levels:

-- Establishing a copyright

-- Managing the distribution

-- Controlling on consumer

1. DRM Framework

OMA DRM is a Digital Rights Management (DRM) framework developed by the Open Mobile Alliance, whose individuals speak to cell telephone producers, portable framework makers and cellular telephone system administrators. DRM provides a way for content creators to set enforced limits on the use and duplication of their content by customers. The system is implemented on many recent phones. DRM gives an approach to substance inventors to set authorized breaking points on the utilization and duplication of their substance by clients. The framework is executed on numerous late telephones. To date, two variants of OMA DRM have been released: OMA DRM 1.0, OMA DRM 2.0. and OMA DRM 2.1[1].

1.1 Types of DRM

1.1.2 Forward-lock Method

In the forward-lock method the media object is wrapped into a DRM message and delivered to the device. Forward Lock is frequently used for ring tones and wallpaper and can effectively prevent illegal copying of files. In Forward Lock mode, the content is packaged and sent to the mobile terminal as a DRM message. The mobile terminal could use the content, but could not forward it to other devices or modify it. Forward Lock content is not encrypted when it is received or when stored in phone memory. When the .dm file is copied to a PC or memory card, it will be encrypted so as to make sure it cannot be used or transferred from the mobile terminal. The file extension for a Forward Locked file is .dm, which includes the header and the encoded (but not the encrypted) content in it [2].

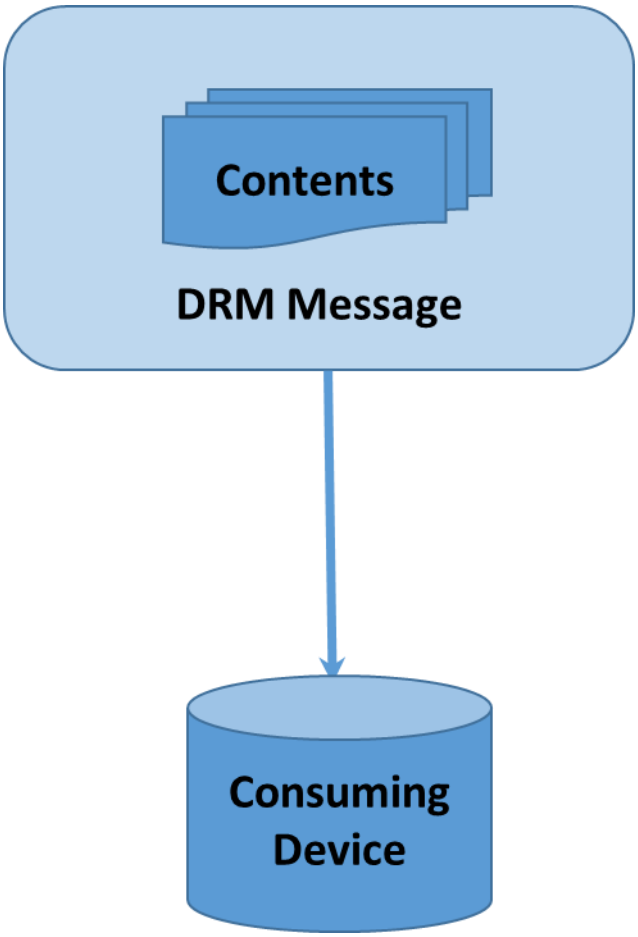

Fig-1 Forward-lock

1.1.3 Combined Delivery Method

If the device supports the “combined delivery” method it MUST also support the “forward-lock” method so Combined Delivery is an extension of Forward Lock. In the combined delivery method digital rights and media object is wrapped into a DRM message and delivered to the device. The user could use the content as defined in the rights object, but could not forward or modify it. The rights object is written in DRMREL and defines the number of times and length of time that the content can be used thus enabling the preview feature. The file extension for a Combined Delivery file is also .dm, which includes the header, the Rights Object and encoded content. [1]

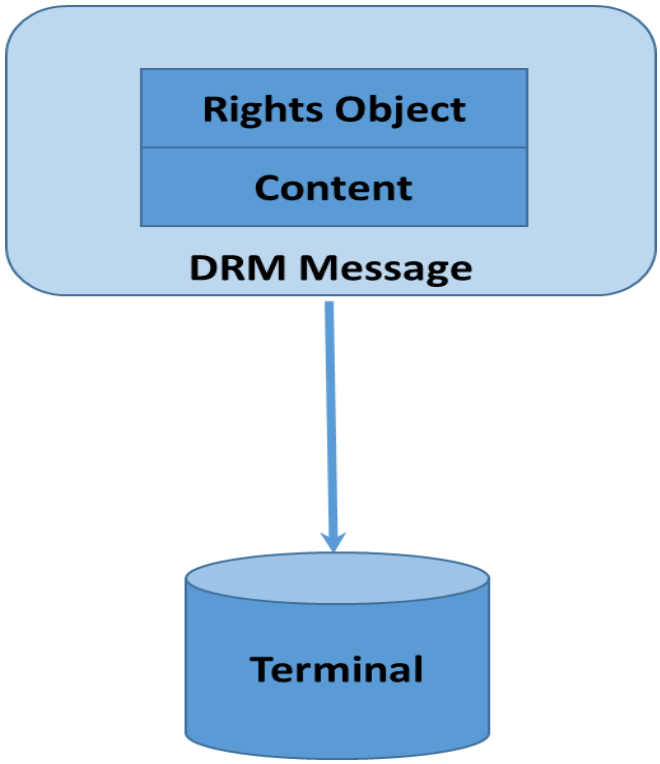

Fig-2 Combined Delivery

1.1.4 Separate Delivery Method:

If the device supports the “separate delivery” method it MUST also support the “combined delivery” and “forward-lock” methods. In the Separate Delivery mode, the content and rights are packaged and delivered separately [1]. The content is encrypted into DRM Content Format (DCF) using a symmetric cryptograph method and can be transferred in an unsafe way such as Bluetooth, IrDA and via Email. [2]The Rights Object and the Content Encryption Key (CEK) are packaged and transferred in a safe way such as an unconfirmed Wireless Application Protocol (WAP) push. The terminal is allowed to forward the content message but not the rights message. In separate delivery, the content is in the format defined in the OMA DRM Content Format specification. The content is encrypted using a symmetric encryption key called content encryption key (CEK). The content can be decrypted only with the same key that has been used for encryption. With separate delivery, the encrypted content is delivered to the device separately from the rights (typically over HTTP download or MMS). The rights object containing the CEK is delivered to the device using connectionless WAP Push over SMS.Super distribution is a part of Separate Delivery application which encourages digital content being transferred freely and is typically distributed over public channels. But the content recipient has to contact the retailer to get the Rights object and CEK to use or preview the content. Once the user had downloaded the encrypted content, the content can be forwarded to any mobile device which supports super distribution. To use that content the destination user needs to get the Rights object from Rights issuer application. The encrypted content file type extension is .dcf (DRM Content Format); the right file extension is .dr or .drc [2].

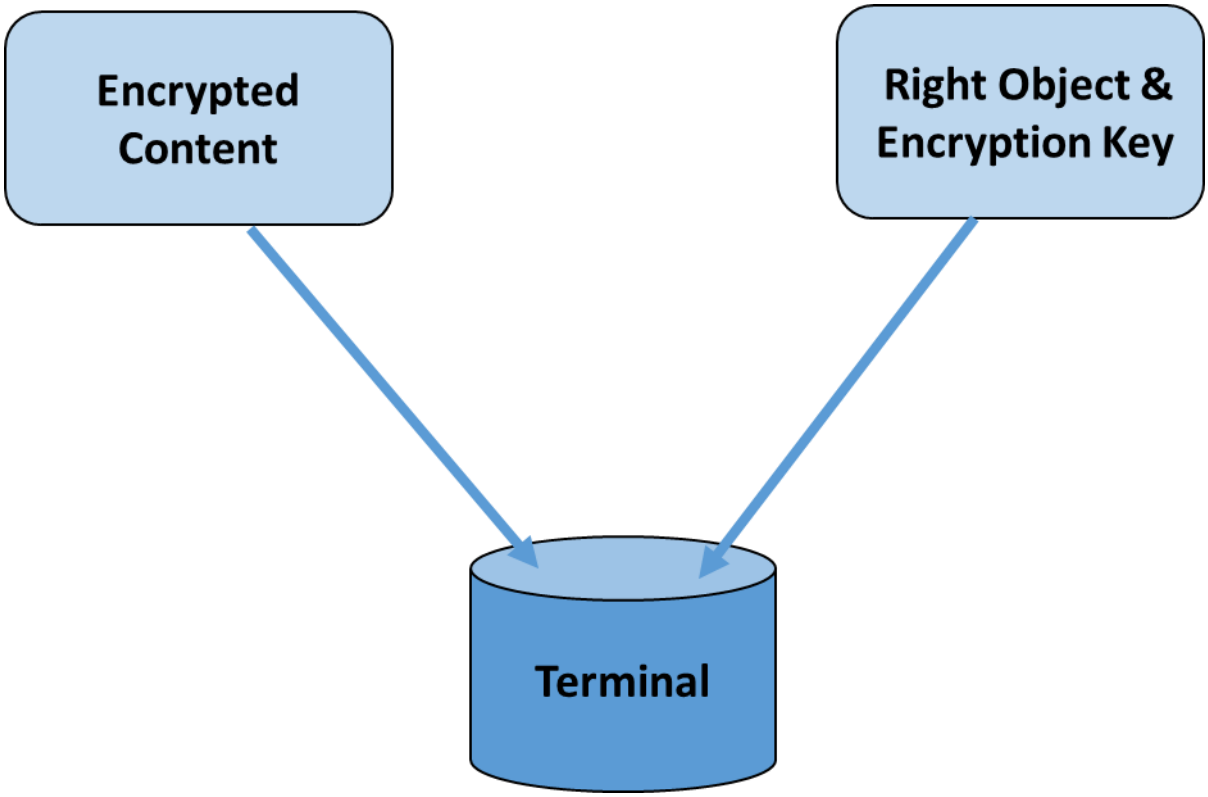

Fig-3 Separate Delivery

1.2. DRM content format

DRM content format (DCF) is used to package and protect discrete media, such as ring tones, applications, and images. The content in DRM content format is encrypted using a symmetric encryption key [3]. The content is then placed as a single content object in the DCF internal structure and layout. The MIME type for objects conforming to the DRM content format is ***application/vnd.oma.drm.content***. It is used in separate delivery where the content is encrypted into the message without the rights. The key used to encrypt the content is sent separately with the rights to the device [3].

The structure of DRM protected content format MUST be according to the table below.

Field Name	Type	Purpose
Version	UINT8	Version Number
Content Type Len	UINT8	Length of contenttype
Content URI Len	UINT8	Length of content URI
Content Type	Content Type Len Octets	Mime type of plaintext
Content URI	Content URI Len Octets	Unique Identier of content
Header Len	Uintvar	Length of header field
Data Len	Uintvar	Length of data field
Headers	Header Len Octets	Additional metadata
Data	Data Len Octets	Encrypted data

Fig-4 DRM Content Format Fields

1.3. Problem with DRM 1.0

The OMA DRM 1.0 model is designed for the mobile industry and is based on the assumption that the mobile terminal is reliable. In the Forward-lock mode and the Combined Delivery mode, the content is not encrypted. In the Separate Delivery mode, the symmetric encryption key is not encrypted. The media content can be stolen if the mobile terminal is hacked or the Right Object message with the CEK is revealed [4].

1.4. OMA DRM 2.0

The OMA DRM 2.0 standard was released in 2006 as an upgrade and extension of version 1.0. It supports many application scenarios like preview, download, Multimedia Messaging Service (MMS), streaming media, super distribution, and unconnected device, making the copyright protection more reliable and flexible [3].

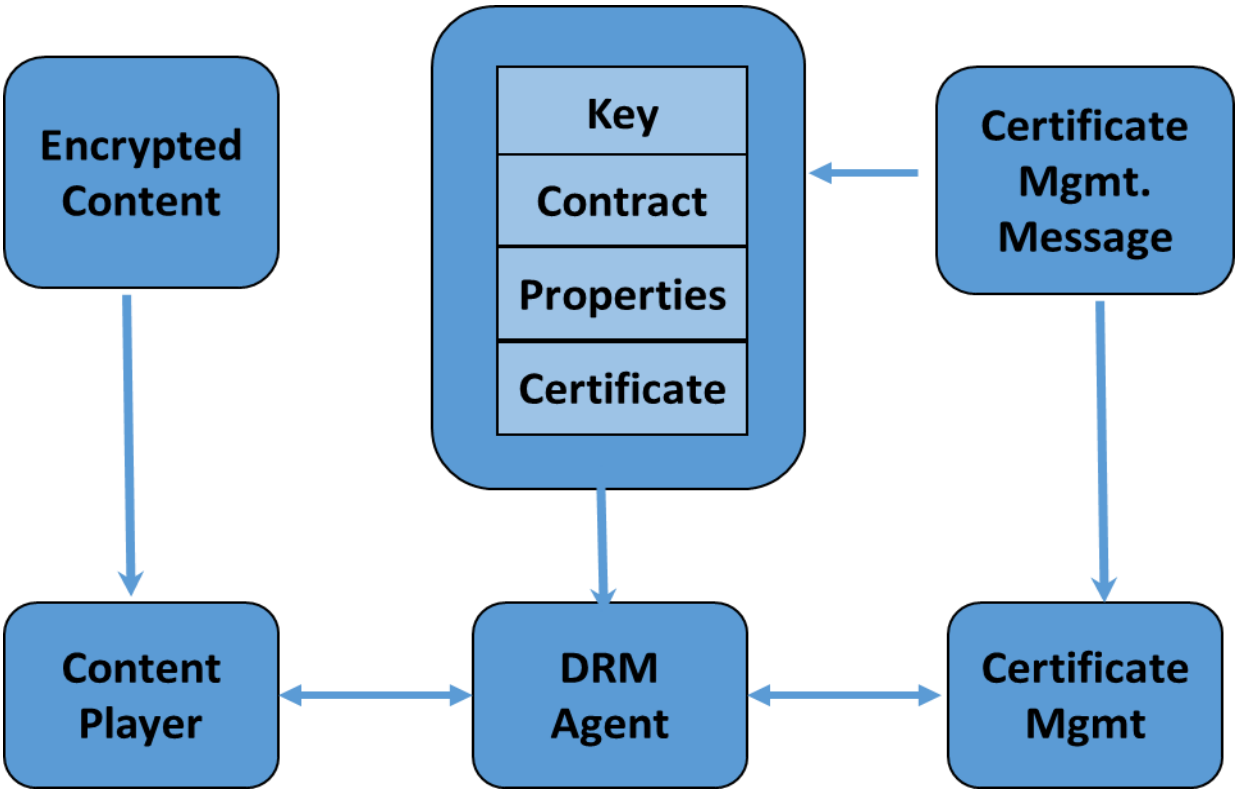

Fig-5 DRM 2.0 procedure

1.5. MOTIVATION

As per to the OMA standard, Forward-locked contents cannot be transmitted to or copied to other portable devices. So if the portable device lacks the in its internal storage, it must delete existing digital contents from the portable device and further download or store new digital contents. So if the conventional portable device needs to store the digital contents only in its internal storage memory then it must extend internal storage medium, which can cause an increase in the cost of the parts [5].

1.6. PROBLEM STATEMENT

Forward lock content is restricted in the device where it's originally downloaded or received. It cannot be forwarded to other devices by any of the unsecured method (EMAIL, MMS, BLUETOOTH, WIFI ETC) .But as we know memory is not much on mobile devices which is quite difficult to keep the large media content .It makes difficulties to user to keep their purchased content for long time.

Forward-locked contents, according to the OMA standard, cannot be transmitted to or copied to other portable devices. So if the portable device lacks the in its internal storage, it must delete existing digital contents from the portable device and further download or store new digital contents. So if the conventional portable device needs to store the digital contents only in its internal storage memory then it must extend internal storage medium, which can cause an increase in the cost of the parts [6].

To resolve such problems, a new method is required to subordinate forward locked DRM contents to the devices and to support an intrinsic function of forward lock content although the contents are stored in a storage medium.

2.1 SCOPE OF THE THESIS

The scope of this thesis is to study the DRM methodologies for forward lock content. In order to provide security for the digital content or being stolen we have introduced some methods which will guard its privacy .So that it can be shared to other user but not violate its properties.

2.2 THESIS ORGANIZATION

Chapter 1 begins with General introduction and related work. It addresses the topics like, Problem Statement, Scope, Related work and thesis organization ,different DRM methodologies and comparison.

Chapter 2 presents the proposed research methodology which explains the detailed model of fuzzy inference system used in correction load of selected similar days.

Chapter 3 shows the implementation of the proposed methodology also the tools used in it.

Chapter 4 concludes the thesis.

CHAPTER 2

LITERATURE REVIEW

Different DRM Systems have different DRM implementation and infrastructure but the DRM process is same which basically consists of three things. Content provider, DRM technology provider, Consumer [5].

Below figure explains simplified diagram of DRM content distribution from content provider to a consumer. The consumer encrypts content using a download mechanism from network. The consumer tries to use encrypted content by sending a request to DRM technology provider through internet for license [5].

The DRM technology provider identifies the request based on policies. For issuing the license a financial transaction may be conducted. The license is packed and transfer to client through Internet .After that it is used on client or consumer device side according to the request.

Tradition goal for a DRM is to prevent an end user to make an unauthorized use of a piece of content basically music or video. For example DRM protection is DRM content purchased from a specific store may require specific device may not be playable on other device. This DRM method prevents illegal digital content sharing, and protects content [5].

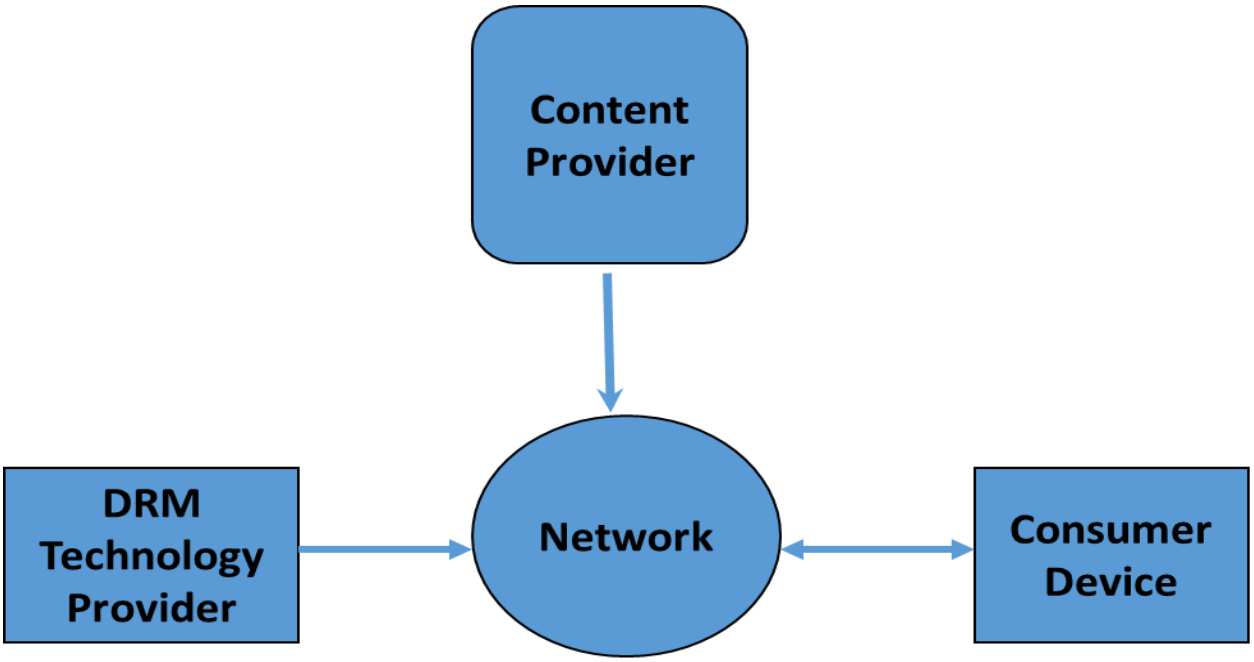

Fig-6 Common system in DRM Infrastructure

Need for storing Forward lock content in memory card.

As we know internal memory of a phone is a big issue. We cannot store more items in the phone as space is limited. But we can't copy too directly forward lock DRM file in memory card too.

What is the solution to overcome above problem? It is possible if a unique identifier can be used for each individual content which can uniquely identify the content in device even if we move the content to memory card .So we encrypting the forward-locked DRM contents using a unique number of the portable device, and storing the Encrypted forward-locked DRM contents [6].

In the DRM forward lock header file, added extra field as IMEI Information, which contains the IMEI number of the phone. Now we can send the forward lock content to other phone. But this content cannot be usable as it will not match with IMEI of other devices. It will check the IMEI number from the header and if it is not match with phone IMEI number then it cannot open the file.

Possible threat: User can edit the IMEI number of the phone by opening the file in an editor.

Solution: If IMEI is encrypted in such a way that the original device can access the content.

3.1 Existing Download Sequence for forward lock content

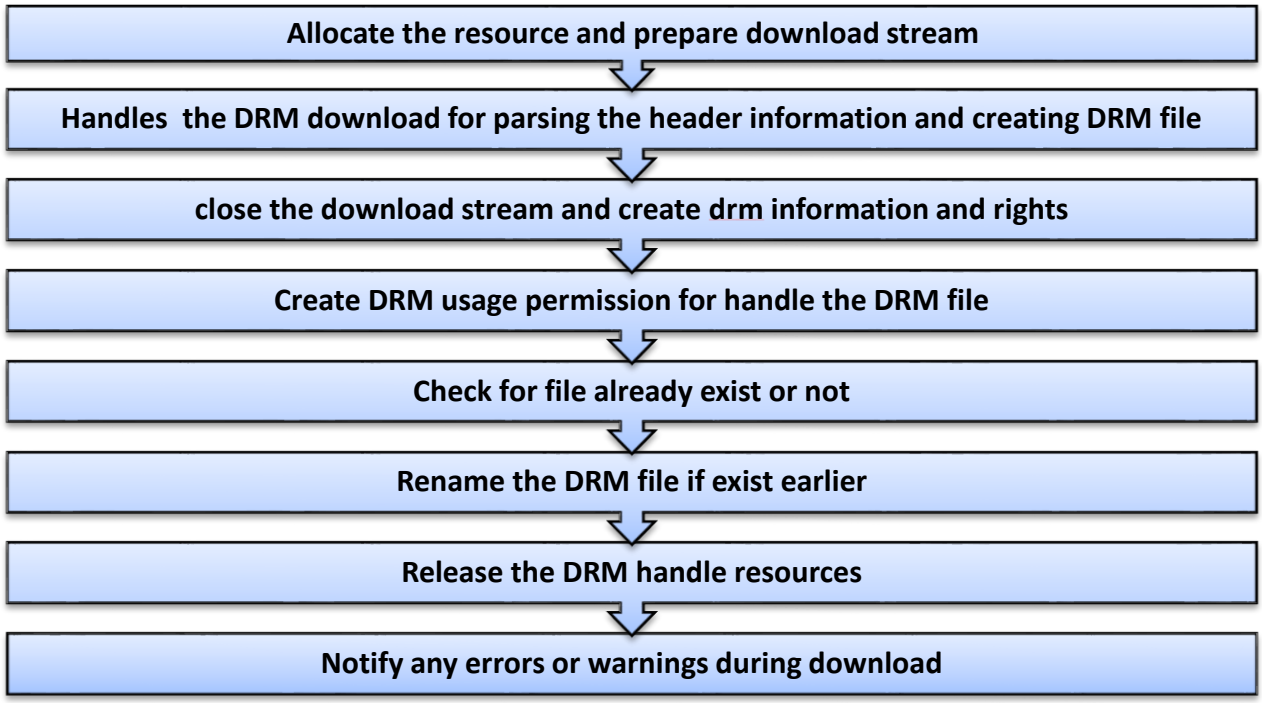

Fig-7 DRM Download Sequence

3.2 Modification of DRM Forward Lock file Content

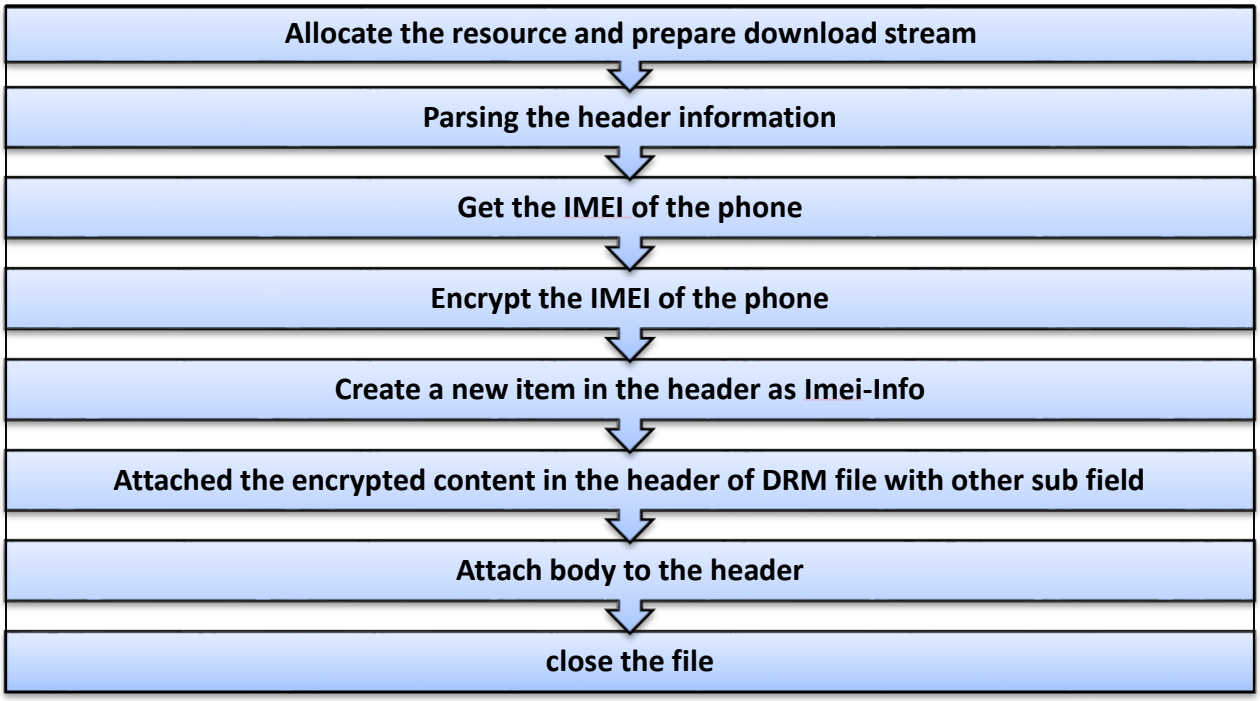

Fig- 8 Modification to earlier Method

Forward Lock Content header format for a digital content:

#video/3gppcid:0000000176229@org.com

padding=RFC2630plaintextlen=378659RightsIssuer:http://wap2.org.com/test/contdowntest/rightissuer.jsp?cid=0000000176229Content-Name:JurrasicFart-h263-15-64-anrnb-12-Content-Vendor: SFC

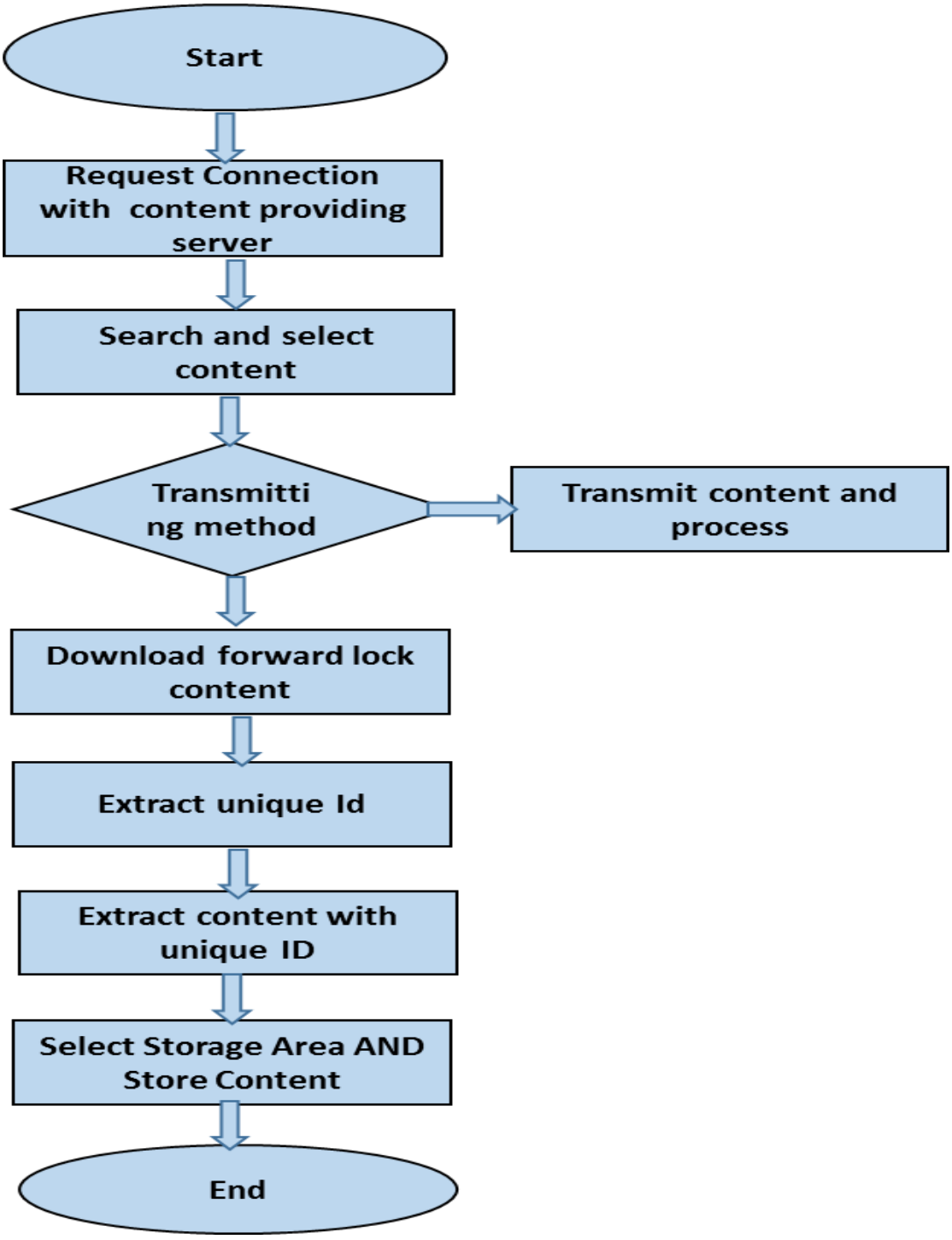

Fig-9 Flowchart for DRM content Parsing in Device

3.1 Accessing the content in device

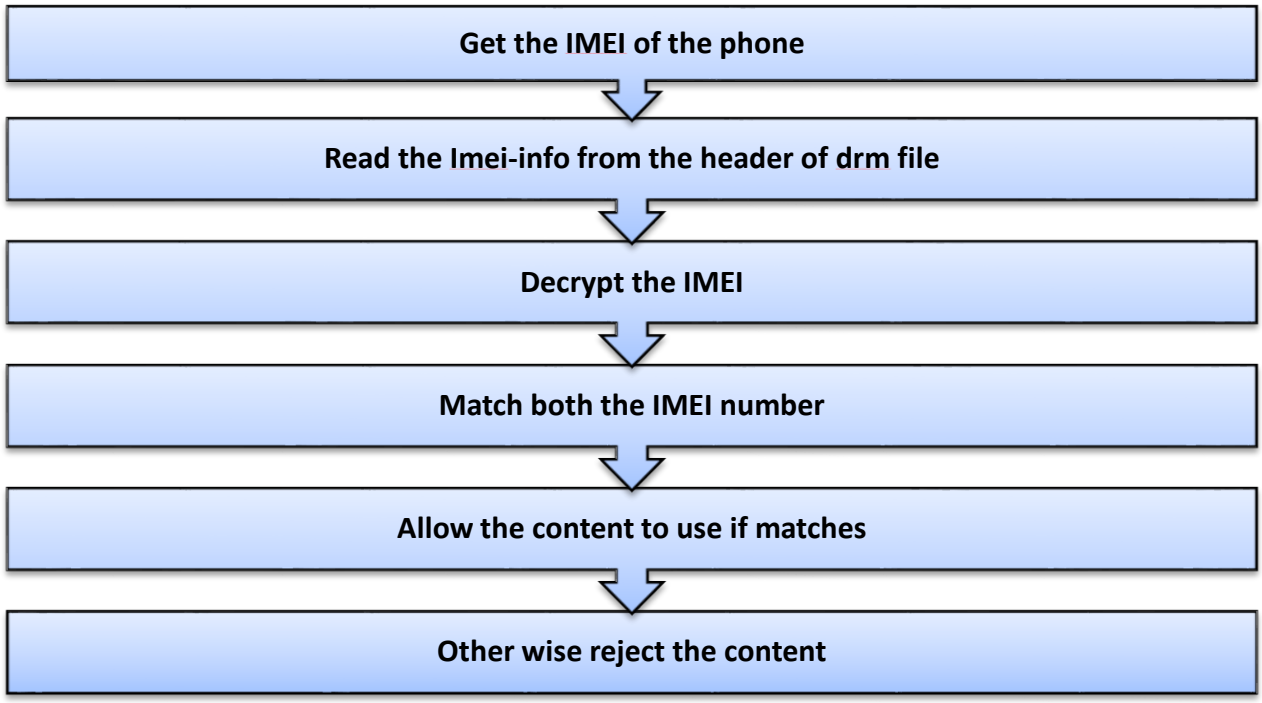

Fig-10 Accessing DRM content in Device

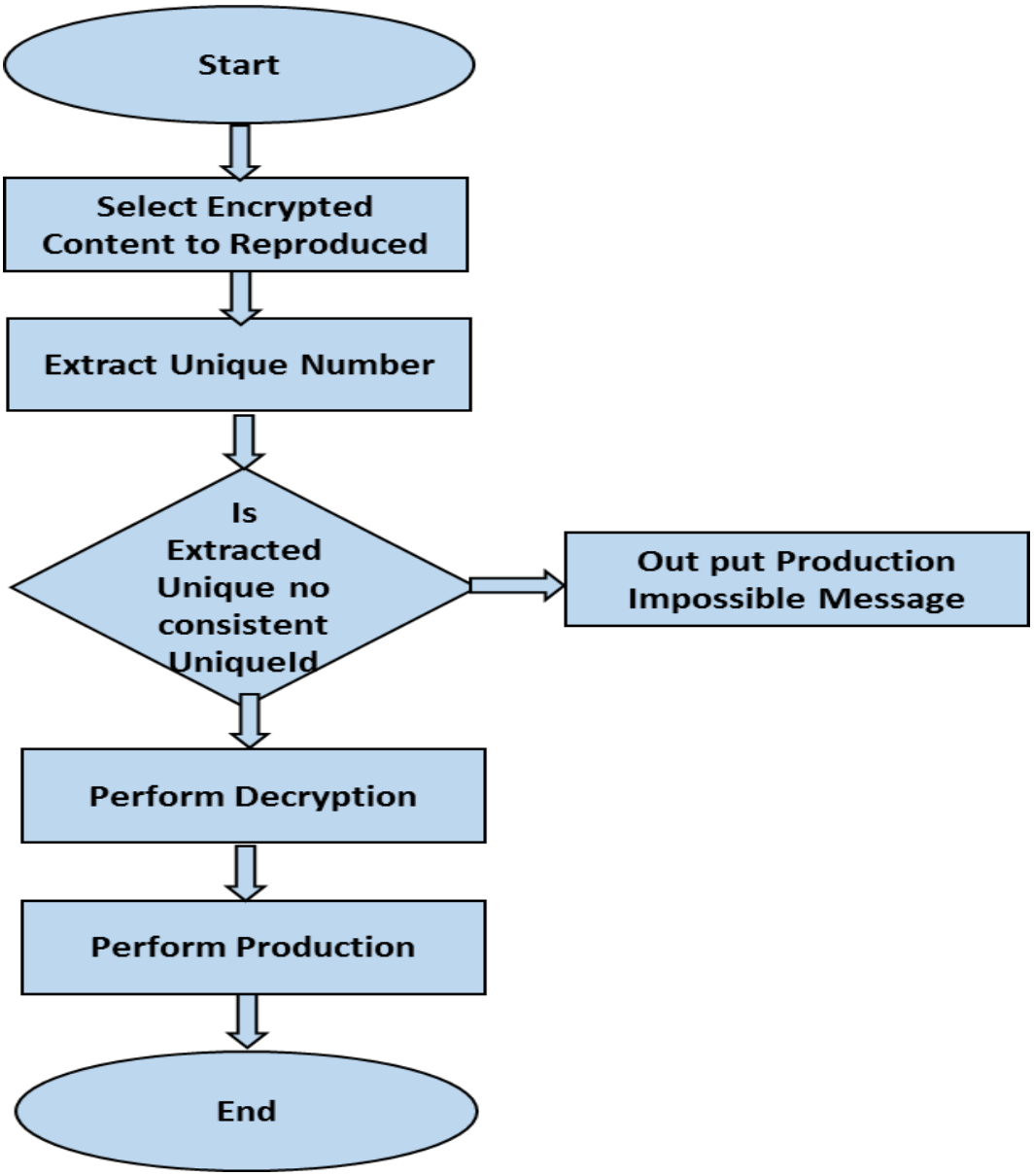

Fig-11 Flowchart for Accessing DRM content in Device

Figure 9 is a flow chart basically explaining a method for downloading and storing a forward-locked DRM content in a portable device based on to an embodiment of the new proposed method and Figure 11 is a flow chart explaining a method for reproducing a forward-locked DRM content and stored in a memory of portable terminal or an internal storage medium connected to a portable terminal, according to an embodiment of the new proposed method the present invention [6].

A portable device establishes a communication channel with a content providing server (500). The portable device searches for and selects a DRM content that can be provided from the content providing server. The portable device transmits a request signal for downloading the selected DRM content to the content providing server. The portable device user selects a providing method for the selected DRM content. That is, one of the forward lock, combined delivery, and separated delivery is selected. In an embodiment of the present invention, it is implemented in such a way that a user selects one of the forward lock, combined delivery, and separated delivery. It should be, however, understood that the content providing method (for example, the forward lock) is previously set between the content providing server and the portable device. Due to the OMA standard, the forward-locked DRM contents cannot be transmitted or copied to the devices other than the portable device that received the forward-locked DRM contents [6].

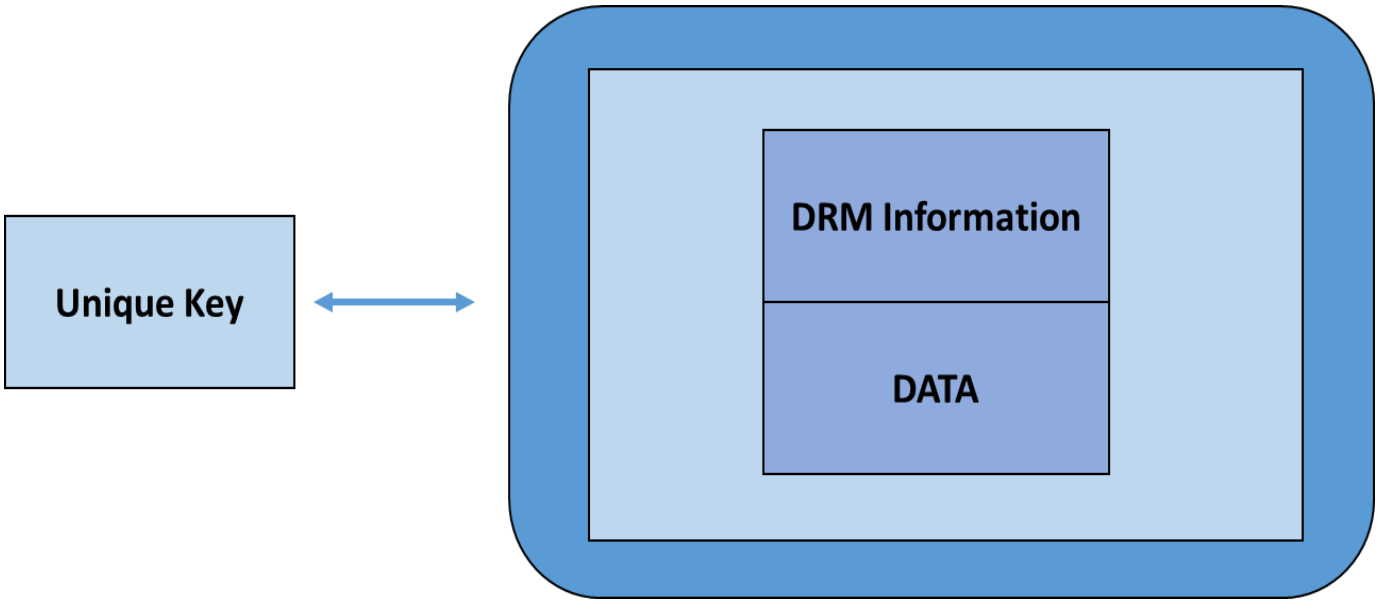

Fig-12 DRM Content with Present Invention

Above figure is a schematic block diagram illustrating a DRM contents providing system according to an embodiment of the present invention. Content providing server is someone which store the digital content based on content id. Content Id represents basically the URI plus mime type. Each content uniquely represents based on this content id in server [6].

CHAPTER 3

METHODOLOGY

4.1 Data Encryption and Decryption using RSA

RSA is one of the public key cryptography is widely used for secure data transmission. It uses encryption key is public and is different from the decryption key which is kept secret. In RSA, asymmetry is based on the factoring product of two large prime numbers and factoring problem [8].

A user of RSA creates and then publishes a public key based on the two large prime numbers along with an auxiliary value. The prime no kept secret. The public key used to encrypt message but with currently published method .If public key is large enough then only who has knowledge with such prime numbers can easily decode message [8].

The RSA algorithm involves following steps:

Key generation.

Encryption.

Decryption.

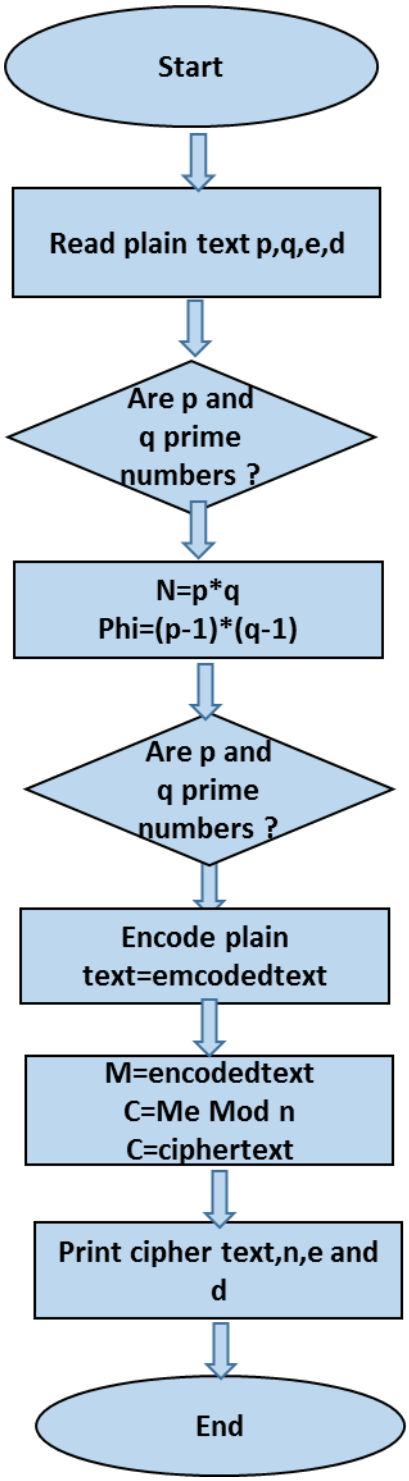

Fig-13 Flowchart for flow chart of the encryption algorithm

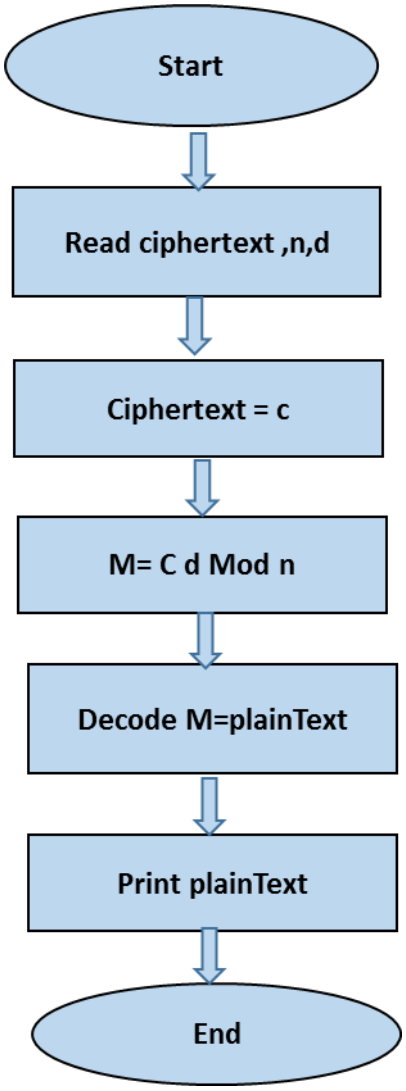

Fig-14 Flowchart for flow chart of the decryption algorithm

In previous method DRM content is encrypted at client side after it has been downloaded, content is parsed through the DRM parser. Header is extracted to identify the content based on the mime type.

Then it has been encrypted using the device IMEI number .But it has the client overhead too each time to encrypt the content .So to avoid this issue we have proposed one more method by which It will smooth the process .

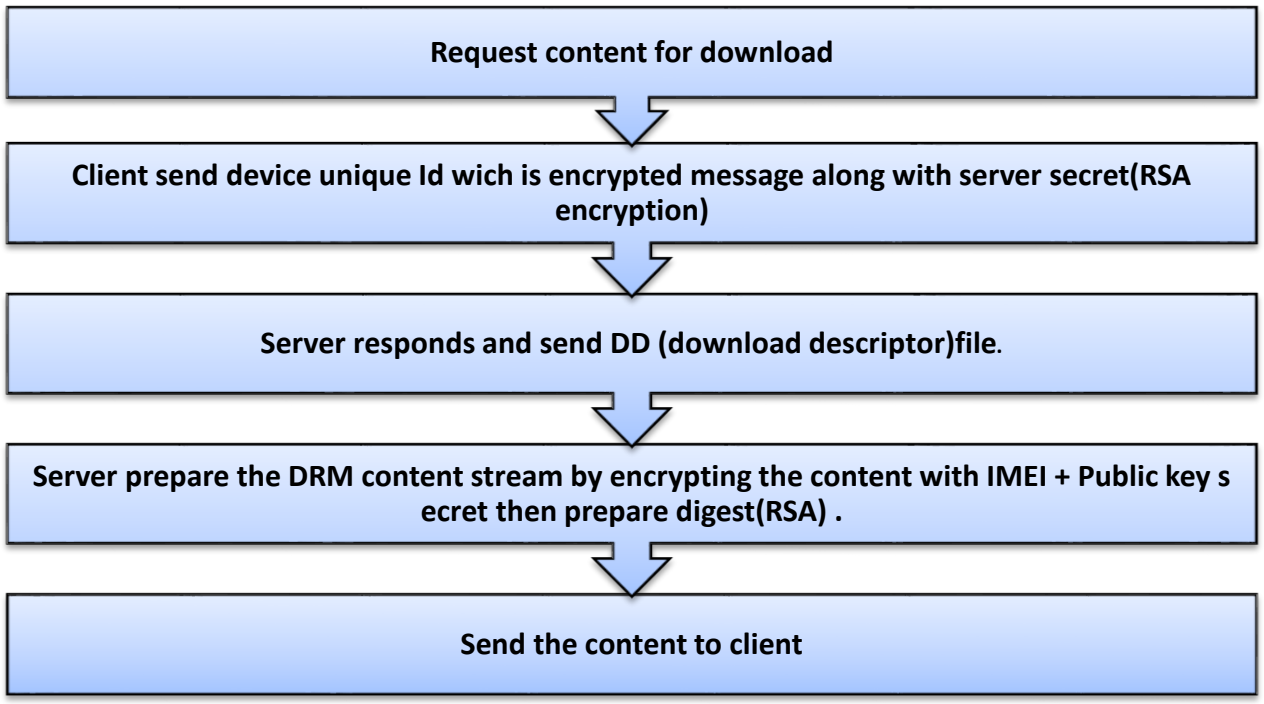

Fig-14 Enhanced Method for DRM content processing at Server

For accessing the content in device, it needs to get the unique I'd like IMEI number of the device from the method and using its private secret key decrypt the content .It authenticate the content based on the IMEI matching after decryption. If it matches allow to open or use the content otherwise discard the content.

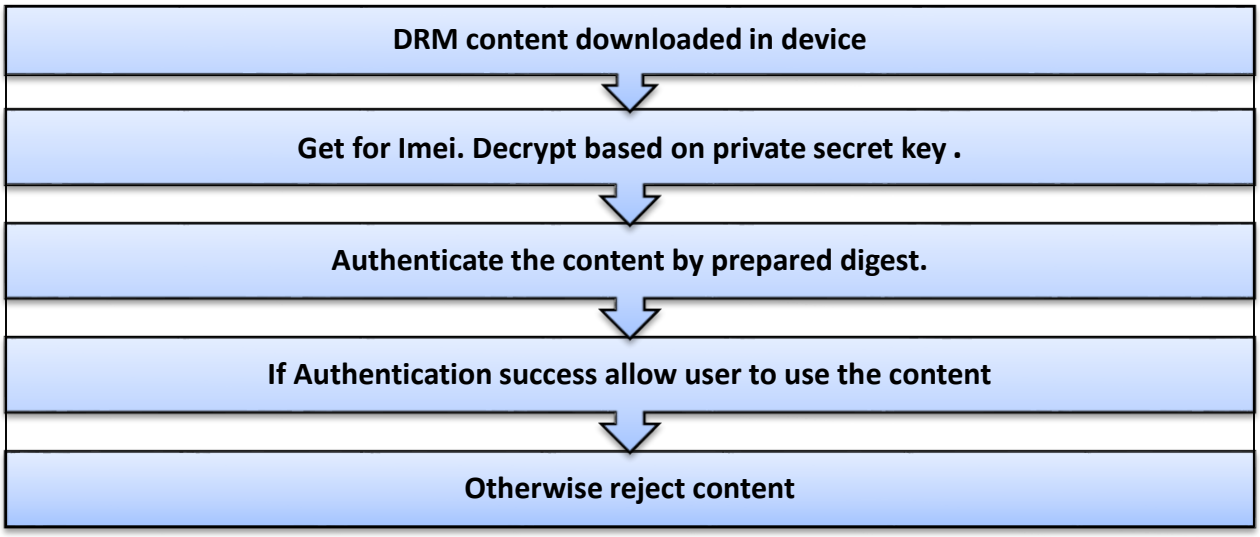

Fig-15 Enhanced Method for DRM content processing at Client

Figure 14 is a flow chart fundamentally clarifying a system for downloading and putting away a forward-locked DRM content a versatile gadget taking into account to an embodiment of the new proposed strategy clarifying a technique for recreating a forward-locked DRM content and put away in a memory of convenient terminal or an internal storage medium associated with a compact terminal, as indicated by an epitome of the new proposed strategy the present innovation [6].

4.2 Tools Used to Develop the Program

This is implemented using two computers .In one computer server runs and other client program runs .We have used socket programming in Linux platform to achieve the Inter process communication in between them. Client and server used File transfer protocol for downloading or uploading of content.

Client create socket and bind the server address. First communicate to the server and share the IMEI number through a secured message. The secured message is IMEI is encrypted along with public key of server.

After receiving the message, server sends acknowledgement. Now it decrypts the message using the private key. It extracts the IMEI number from the message and uses it to preparing the DRM content.

The DRM content is normal content which is a non-encrypted content. Sever parse the header and encrypt it using the IMEI number and send to the client. When client program received the DRM content, it again reparse the header and decrypt the content using its private key and extract the IMEI number from the header. Now this unique ID is stored in its database for identifying the owner of the content.[6]

CHAPTER 4

CONCLUSION & FUTURE WORK

5.1 CONCLUSION:

DRM ensures the worth chain of substance download and other quality included administrations. With DRM, the substance proprietor can be appropriately paid and urged to make more important substance. Offer control to the merchant of computerized substance or gadgets after it has been given to a shopper

Keeping the buyer access, denying the client the capacity to duplicate the substance or changing over it to different organizations. Limiting the customers on what equipment can be utilized with the gadget or what programming can be keep running on it.

So vast mixed media content, now client can download substance and utilization it .So memory issue can be explained with this strategy and which likewise not disregard the DRM idea.[9]

5.2 Future work

This may from the future work on Digital rights management. The method to be followed for protecting or securing the forward lock content is as follows. As the IMEI number is shared via public key encryption this can be hacked by intruder if anyone knows the private key. So the threat is there for hacking of the content in between the transmission.

To overcome this problem, there would be more security or extra level of encryption needs to be provided while transferring the unique ids. This can be achieved by double encryption above the encrypted content.

REFERENCES

[1] OMA DRM - Wikipedia, the free encyclopedia,(DRM) system invented by the Open Mobile Alliance

[2] Basic DRM Concept, A copyright protection for digital media – Wiki page. http://en.wikipedia.org/wiki/Digital rights management

[3] Open Mobile Alliance DRM – Technology, OMA Releases, V1.0. OMA-ERELD-DRM-V1_0-20040625-A.pdf

[4] Victor-Valeriu Patriciu, Ion Bica, Mihai Togan, Stefan-Vladimir Ghita, "A Generalized DRM Architectural Framework", AECE, Volume 11, 2011, page(s): 43 – 48, ISSN: 1582-7445.

[5] N. Dufft, A. Stiehler, D. Vogeley, and T. Wichmann. Digital music usage and drm. http://www.indicare.org/tiki-download file.php? fileId=110, May 2005.

[6] Method and system for processing forward-locked DRM contents, and portable device adapted thereto, Patent Id EP 2178015 A2, July 2008.

[7] S. M¨uller, S. Katzenbeisser, and C. Eckert, "On multiauthority ciphertext-policy attribute-based encryption," Bulletin of the Korean Mathematical Society (B-KMS), vol. 46, no. 4, pp. 803–819, July 2009, to appear.

[8] Research and implementation of RSA algorithm for encryption and decryption Strategic Technology (IFOST), 2011 6th International Forum on 22-24 Aug. 2011.

[9] W. Zeng, H. Yu, and C.-Y. Lin, eds, Multimedia Security Technologies For Digital Rights Management, Elsevier, 2006.