RESEARCH ARTICLE OPEN ACCESS

Design and Implementation of Cloud Based DRM Framework on Android Platform

Ms. Kirti D. Nakhale, Prof S.P. Karmore
(Department of Computer Science, Nagpur University, Nagpur-16
(Department of Computer Science, Nagpur University, Nagpur-16

ABSTRACT -
Digital Rights Management (DRM) aims at protecting digital contents from being abused through regulating their usage. This paper presents a Digital Rights Management (DRM) framework to secure digital content and software applications. Android is one of the popular OSs and application platforms for mobile devices. Unfortunately, to the best of our knowledge, fewer of these DRM schemes are concerned with the cost of the servers in a DRM system when the number of users scales up. To accommodate value-added services such as selling wallpapers, ringtones, applications, and games on Android mobile phone, it is essential to ensure copyright protection on these products. These DRM systems can be used for any content in a wide variety of environments, services, and devices. In our project we would be adding DRM based on cloud, thus each mobile node would act as a DRM provider, and DRM consumer. In addition, the cloud computing is introduced in the scheme to provide more efficient and higher quality services.

Keywords- Android, Digital rights management, open source, content protection, software security

I. INTRODUCTION

The DRM systems can be used for any content in a wide variety of environments, services, and devices. With the fast development and growth in the mobile industry, the acceptable amount of mobile applications and services are offered, which engage Internet scale data collections. Meanwhile, it has a remarkable impact on digital content providers as well as the mobile engineering that a huge number of digital content have been pirated and unlawfully distributed. Android is an open mobile phone platform to accommodate value-added services such as selling wallpapers, ringtones, applications, and games on android mobile phones. It is essential to ensure copyright protection on these products, This paper studies how the Android source code to implement the Open Mobile Alliance (OMA) Digital Right Management (DRM), for software protection.

Digital content can be in the form of documents, e-books, audio, video and games. Digital rights management controls the access to sensitive content by including information about the user rights of the content in the form of a authorization (license). Such rights include information on the duration of the file to be accessed and permissions to read or print the content. A user license to that effect is issued to the client for consumption of the content.

II. BACKGROUND

The objective of the OMA DRM systems is to provide standardized DRM solutions for content services across mobile networks, but in a network and content-agnostic manner. In this digital era, information sharing and unauthorized distribution of high value content has grown multifold. The new wave of social networking sites augmented by handheld gadgets like smart mobile phones, have added to the complexity Content publishers and software vendors find it increasingly difficult to protect their work and copyrights. E-books and multimedia files are freely distributed over internet and software cracks are created to bypass vendor's restrictions. Software vendors are forced to adapt strong anti-piracy enforcement strategies and technologies to prevent such risks and check intellectual property (IP) infringements.

OMA DRM 1.0 is a DRM solution for securing pure and trouble-free mobile content download services, such as ringtones, screensavers and Multimedia Messaging (MMS). OMA DRM 2.0 and 2.1 enables suitable security and quality for full track music and video download and streaming services for equally mobile devices and PCs. OMA DRM 2.x enables for instance subscription and domain based business models, where domain enables the user to bring into play the same content on multiple devices.

The task of the Open Mobile Alliance (OMA) is to smooth the progress of global user acceptance of mobile data services by specifying market focused mobile service enablers that ensure service interoperability across devices, geographies, service providers, operators, and networks, whereas allowing businesses to struggle through innovation and discrimination. OMA's extensive work on DRM has resulted in OMA DRM being the de-facto attribute on any digital content enabled mobile phone in the market these days. Hundreds of millions OMA DRM enabled phones are sold annually wide-reaching. OMA BCAST specifies the solutions for Mobile TV broadcast networks such as DVB-H. OMA BCAST includes two options for overhaul and content fortification, the device centric DRM Profile and SIM card centric Smartcard summary.

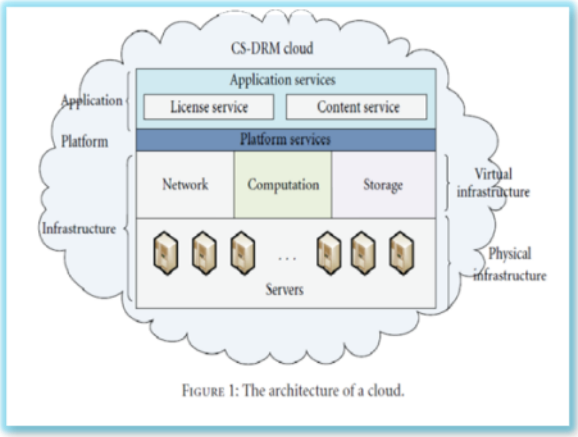


Fig 1.Cloud Architecture

III. COMPARED WITH CONVENTIONAL DRM

All existing ORM system based on CIS mode architecture the encrypted resource only by the CIS mode or P2P mode distribution. Client only downloaded the full resources before they can apply for a certificate, and to decrypt play. On Android mobile phones, the "Home" is a desktop application where a user can click on an icon to launch an application such as contacts, dialer, camera, music, settings or browser. Furthermore, the user can also click on an icon in the status bar at the top of screen to read some notifications, such as download completion, miss call, text message arrival or Wi-Fi connection activation. The new DRM system is designed to provide copyright protection for any type of content.

On the other hand, software licensing solutions are used to control or dictate permissions related to software. A software license may include a time limit for the use of Software. Various control strategies are instilled to hinder unauthorized duplication and use of software. One such approach is to provide a hardware dongle for software interlock.

A. Problem definition

- Digital Rights Management (DRM) is a mechanism which protects digital content from being abused through regulating its usage. In the context of a DRM system, only an authorized user, who has obtained a license, can access the digital content according to the rights information defined in the license.
- Specifically in a DRM system, with the number of active users scaling up ,mass of the data requests and data operations place a heavy burden on the DRM system.
- The existing DRM schemes are still required to purchase huge amount of equipment and perform maintenance, which is a large investment and takes high daily expenses, when the number of user visits increases. The huge capability of computation and storage of the cloud environment makes the cloud one of the best solutions for satisfying performance requirements of the entire DRM system when the number of user visits grows to infinity.

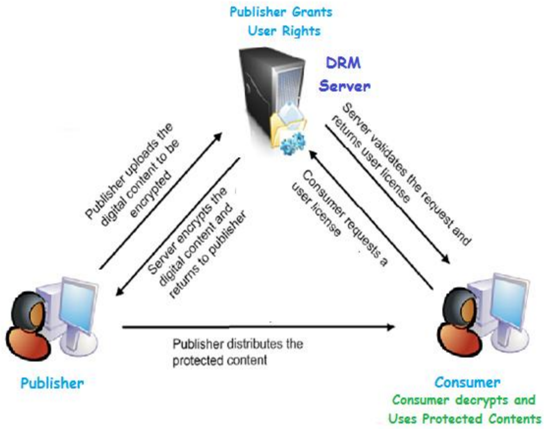

Publisher Grants
User Rights
DRM
Server
Publisher uploads the digital content to be encrypted
Server encrypts the digital content and returns to publisher
Consumer requests a user license
Server validates the request and returns user license
Publisher distributes the protected content
Publisher
Consumer
Consumer decrypts and
Uses Protected Contents

Fig 2. DRM Architecture

B. Objective

The objective of this DRM system is to provide standardized DRM solutions for content services across mobile networks, but in a network and content-agnostic manner

IV. THE RELEVANT CONCEPT

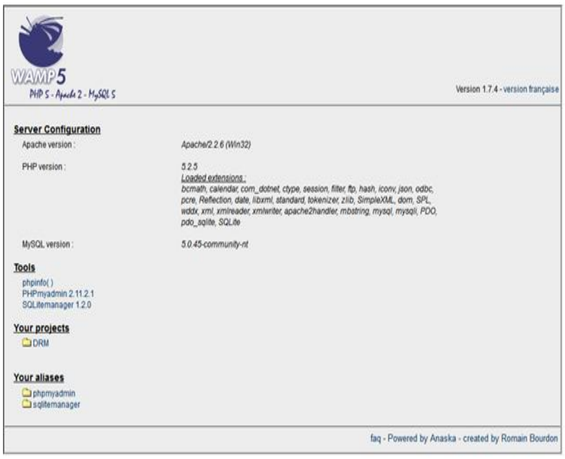
The cloud computing offers services, computation, and storage from a isolated and centralized facility or contractor [10]. In a cloud, data can be easily and all over the place accessed. One of the most essential characteristics of cloud computing is its give as you go manner. It means that users only need to rent corresponding services provided by cloud computing and pay for the actual utilization of services, rather than buy software and physical hardware which users may consider too expensive.

But this traditional DRM's authentication still is C/S mode, media files. It uses digital media server to provide media files have copyright encryption processing and uses authentication server distributed authorization documents. The traditional combination of DRM and P2P networks just used

P2P way to quickly distribute encrypted data and the authentication phase is still C/S mode.

A cloud system is a system implementing cloud computing. Without ambiguity, a cloud system is abbreviated as a cloud in the rest of the paper.

A cloud refers to not only function services delivered in excess of the Internet, but also the hardware and system software in the system. As shown in Figure 1, the typical structural design of a cloud consists of three layers.


WAMP5
PHP 5 - Apache 2 - MySQL 5
Version 1.7.4 - version française

Server Configuration

Apache version : Apache/2.2.6 (Win32)

PHP version : 5.2.5

Loaded extensions :
bcmath, calendar, com_dotnet, ctype, session, filter, ftp, hash, iconv, json, odbc, pcre, Reflection, date, libxml, standard, tokenizer, zlib, SimpleXML, dom, SPL, wddx, xml, xmlreader, xmlwriter, apache2handler, mbstring, mysql, mysqli, PDO, pdo_sqlite, SQLite

MySQL version : 5.0.45-community-nt

Tools
phpinfo()
PHPmyadmin 2.11.2.1
SQLitemanager 1.2.0
Your projects
DRM
Your aliases
phpmyadmin
sqlitemanager
faq - Powered by Anaska - created by Romain Bourdon

Fig 3: Wamp server page

The infrastructure layers take account of the substantial infrastructure and the essential infrastructure. The former is composed of tens of thousands of commercial machines.

In the cloud, the infrastructure can also be seen as a service provided to customers. Some businesses are based on infrastructure services such as Amazon. The DRM architecture supports protection of multiple content formats through customization of content rendering software. The supported types include the following:

- Text
- Image
- Audio
- Video
- Mobile applications and games

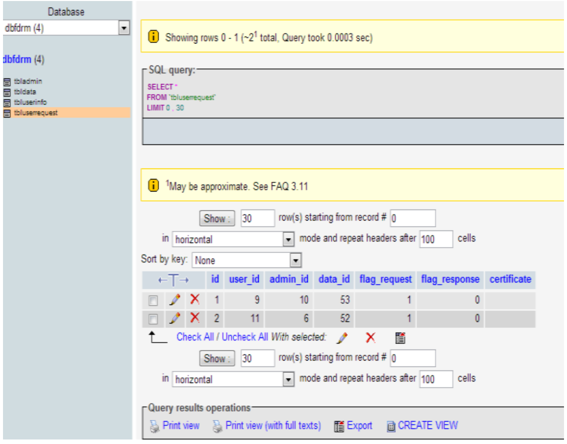
To solve the problem of unauthorized copying and limiting the access to the rightful individuals, the digital content will be initially encrypted by the publisher, with a secret key. The publisher who owns the distribution rights (or the content itself) sets the user's rights. These rights include permissions such as print, view, execute, play and constraints like time limit or number of views. The encrypted content is distributed to users for consumption.

C. Software Protection by Android Market

Android Market [9] developed by Google is not contained in the Android open source and only obtainable on commercial phones with Google's authorize.

The Android Market purpose includes download and installation features. Downloading APK files from Android Market doesn't require an SD card. Therefore, the download difficulty observed in Section III-A is solved. Without any further code, software developers can facilitate the Market safety provided by the Android Market server [10]. After installing an APK file by means of Market protection, the target file is located in -data-app-private folder, where the ADB tool cannot drag from the commercial phones.

However, the Market safety cannot solve the difficulty on a Rooted phone since it allows users to access the whole folder
System including the-/data-app-private folder [11].



Showing rows 0 - 1 (~2[1] total, Query took 0.0003 sec)

SQL query:

```
SELECT *
FROM `tbluserrequest`
LIMIT 0 , 30
```

[1]May be approximate. See FAQ 3.11

Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells
Sort by key: None

	id	user_id	admin_id	data_id	flag_request	flag_response	certificate
□	1	9	10	53	1	0	
□	2	11	6	52	1	0	

Check All / Uncheck All With selected:
Show :
Query results operations
Print view
Print view (with full texts)
Export
CREATE VIEW

Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells

Fig 4:- server view of user req Id

A referee software store Slide Me [12] uses the Android built-in download and installation actions mentioned. This move towards assists the software developers to engage the guard in their code. *Slide Me* provides a Java library *Slide Lock* to make easy the developers in protecting their application. A developer ought to define a *Slide Lock* Key string linked with an application. During implementation time, the application with *Slide Lock* library sends back the Android phone information via an HTTPS connection to the *Slide Me* server. Then the *Slide Me* servers ensure the authority according to the *Slide Lock* Key and the Android phone information [13].

The applications hold and wait for the outcome in the HTTPS response. The Slide Lock does not disrupt the implementation of application when the Slide Me server is unapproachable. One may purposely fail the connection effort on his/her rooted phone by passing on an invalid IP address to the Slide Me server slideme.org in the Linux configuration file /etc/hosts, which is representation link to the read-only /system partition. Rooted phones and our Dream prototype can remount the /system partition to be writable and then amend the /etc/hosts file.

V. RESEARCH METHODOLOGY TO BE EMPLOYED

- Digital rights management is the primary means of supervision and management in the Internet to protect digital intellectual property.

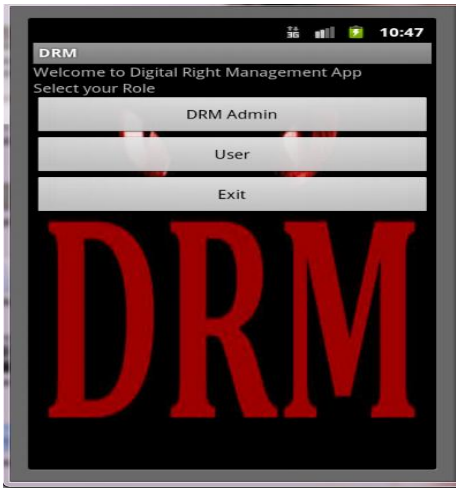

10:47
DRM
Welcome to Digital Right Management App
Select your Role

Fig 5. Android front view

- But the traditional digital rights management is still based on C / S structure.
- In the interim, it has a incredible impact on digital content contributors as well the mobile industry that a great number of digital content have been plagiarized and unlawfully distributed
- All existing DRM system based on C/S mode architecture the encrypted resource only by the C/S mode or P2P mode distribution.
- In a cloud, the content server provides rich and powerful services for handling contents.
- The virtualization technology used above the infrastructure of the cloud guarantees the data security, sharing, and isolation.
- This system combined the principle of the third generation of network structure characteristics with the P2P system, advanced a new digital rights management system and described the structure and working mechanism of the system.[1]

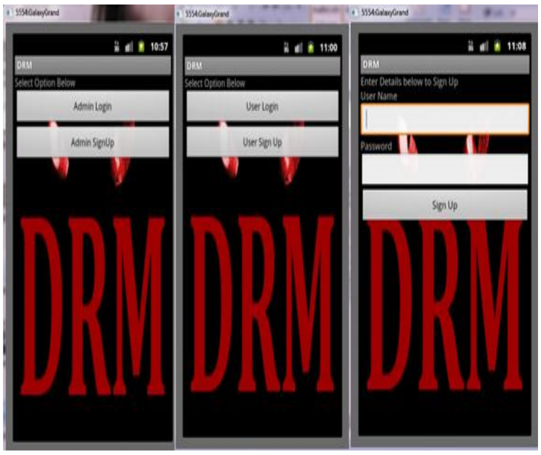
D. Entities involved

The entities involved are:

- End user, who legally obtains the software or digital content for consumption
- Publisher[DRM ADMIN], who distributes the content and is responsible for managing user rights
- DRM ADMIN, which authenticates to DRM server and requests access to specific content or digital object
- DRM server, which holds the content decryption keys and rights information and distributes them to clients in the form of a license.

E. The following are the variables used in our scheme

- U is a registered DRM user
- P is a publisher of the content
- Uid is a registered user id of the DRM
- Upwd is the password corresponding to Uid
- E() is the encryption function
- S() is the signature function
- C is the digital content
- EC is the encrypted content
- Mid is the machine identification name such as MAC id or FQDN of the workstation.
- Upub is the public key of the registered user
- Upriv is the private key of the registered user
- Ucert is the x509 certificate issued to the user
- Urc is the rights assigned to the user on content C
- Mpub is the public key of the workstation


5554:GalaxyGrand
10:57
DRM
Select Option Below

5554:GalaxyGrand
11:00
DRM
Select Option Below

5554:GalaxyGrand
11:08
DRM
Enter Details below to Sign Up
User Name
Password

Fig 6:- front view of admin and user login

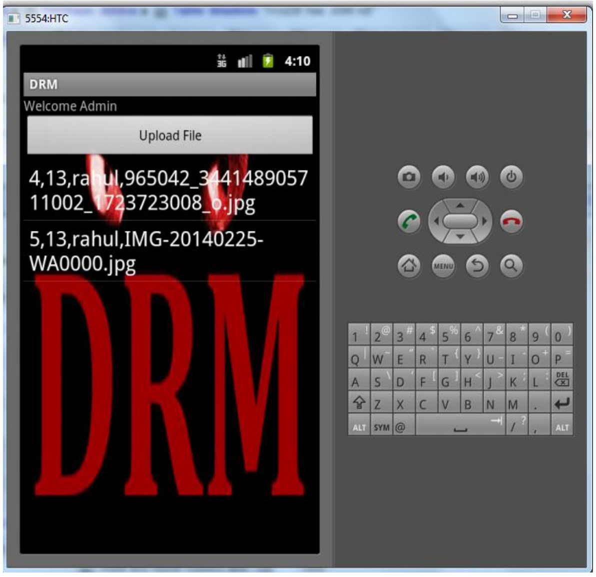
VI. PROPOSED PLAN OF WORK

- We are developing a prototype based on the Android jellybeens4.0 source code and analyzed the DRM for android mobile devices.
- In this project we would be integrating the concept of user based DRM, Where a user would login and see the uploaded contents of various admin.
- When a few other user logs in and checks for DRM checks, then the details of the user who added the DRM would be displayed so that the users can know which party added the DRM
- In our project we would be adding DRM based on cloud, thus each mobile node would act as a DRM provider, and DRM consumer. This would be done using P2P protocol.
- The huge capability of computation and storage of the cloud environment makes the cloud one of

the best solutions for satisfying performance requirements of the entire DRM system, when the number of user visits grows to infinity.

VII. PROPOSED METHODOLOGY

- The above situations call for a new DRM scheme which is low-cost, flexible, secure, efficient, and practicable.
- This system not only rapidly through the P2P network to distribute resources, and certification work completed by the cloud server, to ensure the quality of network transmission.
- This DRM system is designed to provide copyright protection for all digital contents available on internet.
- In addition, the cloud computing is introduced in the scheme to provide more efficient and higher quality services.

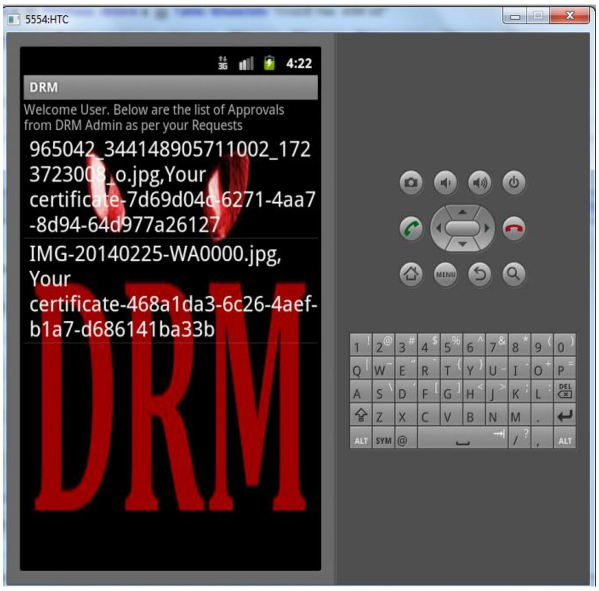


Welcome Admin

4,13,rahul,965042_3441489057 11002_1723723008_o.jpg

5,13,rahul,IMG-20140225-WA0000.jpg

Fig 7 :- user request with id android view



Welcome User. Below are the list of Approvals from DRM Admin as per your Requests

965042_344148905711002_1723723008_o.jpg,Your certificate-7d69d04d-6271-4aa7-8d94-64d977a26127

IMG-20140225-WA0000.jpg, Your certificate-468a1da3-6c26-4aef-b1a7-d686141ba33b

Fig 8:- screen shot of license with file.

VIII. CONCLUSION

In this paper, we presented a DRM framework to protect digital content and software applications. The framework can be extended to support multiple content formats. We are developing a prototype based on the Android jellybeens4.0 source code and analyzed the DRM Forward-Lock protection for any digital contents.

In our project we would be adding DRM based on cloud, thus each mobile node would act as a DRM provider, and DRM consumer. In addition, the cloud computing is introduced in the scheme to provide more efficient and higher quality services.

The huge capability of computation and storage of the cloud environment makes the cloud one of the best solutions for satisfying performance requirements of the entire DRM system, when the number of user visits grows to infinity.

REFERENCES

[1] Xin Zhou , 2Hongwei Chen, 2Chunzhi Wang " A New Digital Rights Management System for P2P Streaming Media" *The 8th International Conference on Computer Science & Education (ICCSE 2013) April 26-28, 2013. Colombo, Sri Lanka 2013 IEEE*

[2] Yuh-Jer Hung, Hsu-Sheng Chang, Chen-Yuan Chuang, "An Inter-Store Transaction Mechanism to Distribute Mobile Applications" *4th IEEE International Workshop on Mobility Management in the Networks of the Future World,2012 .*

[3] Luo Xueming, "Access Control Research Based on Trusted Computing Android Smartphone", *2013 Third International Conference on Intelligent System Design and Engineering Applications, IEEE Transaction 2012.*

[4] X. Su+, M. Chuah*, G. Tan, "Smartphone Dual Defense Protection Framework Detecting malicious applications in Android Markets" *2012 8th International Conference on Mobile Ad-hoc and Sensor Networks.*

[5] Chen-Yuan Chuang,Yu-Chun Wang1 Yi-Bing Lin, "Digital Right Management and Software Protection on Android Mobile phone" *IEEE Transactions On Multimedia, VOL. 15, NO. 4, JUNE 2010.*

[6] Miguel Soriano, Stephan Flake, Juergen Tacken, Frank Bormann, Joan Tomàs, " Mobile Digital Rights Management Security Requirements and Copy Detection Mechanisms" *Proceedings of the 16th International Workshop on Database and*

Expert Systems Applications (DEXA'05)2005 IEEE.

[7] Mejdi Trimeche and Fehmi Chebil,"Digital rights management for visual content in mobile application" *IEEE Transactions On Mobility Management ,Vol.12,april 2004.*

[8] Chaokun Wang, Peng Zou, Zhang Liu, and Jianmin Wang " CS-DRM: A Cloud-Based SIM DRM Scheme for Mobile Internet" *Hindawi Publishing Corporation EURASIP Journal on Wireless Communications and Networking .Reserch article.2011*

[9] Muhammad Hataba Ahmed El-Mahdy "Cloud Protection by Obfuscation: Techniques and Metrics" *2012 Seventh International Conference on P2P, Parallel, Grid, Cloud and Internet Computing,2012 IEEE*

[10] Ravi Sankar Veerubhotla and Ashutosh Saxena, Senior Member, IEEE "A DRM Framework Towards Preventing Digital Piracy, Security & Privacy Lab", *Infosys Labs,Infosys Technologies Limited, Hyderabad, India.2011IEEE*