Digital Right Management in Internet Communication and Information Transfer

Francisca Nonyelum Ogwueleka
Department of Computer Science
Federal University Wukari, Nigeria
234(0)7035653127
ogwuelekafn@gmail.com

Aniche Delight Aniche
Department of Computer Science
Gregory University Uturu, Nigeria
234(0)7035653127
delight.aniche@gmail.com

ABSTRACT

The result of the lack of operational proficient digital copyright protection include booming piracy market, lack of motivation for quality creative work and huge revenue loss. This research evaluates encryption based digital right management in internet communication and information transfer and identified major factors contributing to the incompetence of existing digital right management schemes. Data from the Nigeria Communication Commission and other sources were used to study the viability of applying mobile phone communication in digital right transactions. The research sought solution for digital copyright protection in Nigeria that will use the universal mobile phone, recharge cards and public key encryption. The proposed solution changed digital copyright protection from copyright content usage protection to copyright content redistribution protection and used short message service (SMS) of mobile phone service providers as means of communication and public key cryptography for content and transaction security. The solution reduced the required usage skill level and satisfied the Fair Use Policy enabling artists and authors to reach wider market with their products effectually without losing their revenue.

CCS Concepts

• Social and professional topics →Computing / technology policy →Privacy policy

Keywords

Digital copyright protection, digital right management, short message service, mobile phones, public key cryptography, fair use policy

1. INTRODUCTION

Billons of dollar have been lost in copyright infringement from software products to academic products and resources, movies, music, news etc. that has gained momentum with the advent of computer and internet. People can now go online and download thousands of dollars' worth of copyrighted products without paying a dime and go ahead to pirate it and make more millions of dollars from it at a great loss to the Copyright Holder. Techniques that combine data encryption or other data scrambling mechanism, internet communication and information transfer called digital right management (DRM) have been postulated to provide a means to protect the copyright industry. However, none of these schemes have been able to meet this goal considerably as huge compromises in consumers' security and satisfaction resulting from the payment system requirement and the very constrained access to content trails each and every one of them. There are gaps in the use of data encryption in the protection of information both in internet communication and in information transfer especially in the area of copyright protection which has caused consumers and copyright holders dissatisfaction hence the great need for this research to propose a scheme that will satisfy consumers' security and access to copyrighted contents even while offline and the copyright holders in getting the revenue they need and not losing it to pirates.

The aim of this study is to proffer a functional solution to the problem of copyright infringement in the Nigerian context using encryption and communication techniques; objectively proposing a scheme that uses the limited infrastructure and computer literacy in Nigeria to protect copyrighted information in the internet and off the internet; and find the best channel of communication between consumers and copyright holder that will encourage wider consumer base participation and easy, efficient and secure transaction in the purchase and use of copyrighted materials while obtaining/keeping little or no information about the customer.

The significance of this research is in finding a way to use data encryption and the available communication and information transfer techniques to effectively protect copyrighted contents in Nigeria without compromising consumers' security and satisfaction or copyright holders control and revenue. Such scheme will be very beneficial to the copyright industry and the Nigeria economy.

This research focused on the use of data encryption and communication technique (internet communication and information transfer) in the protection of copyrights. We looked at various Digital Right Management (DRM) schemes based on data encryption and the commonly used form of communication in Nigeria and proposed a model that will satisfy the need of consumers and copyright holders considering the limited information infrastructure and computer literacy in Nigeria as a case study for developing countries.

2. REVIEW OF RELATED STUDIES

In the general scene of cryptography, internet communication and information transfer, the last three decades have witnessed volumes of researches and studies. Fagin et al [1] in their study stated that there is good progress in the area of dismantling the skepticism surrounding cryptography. Callas [2] in his study of the social expectations of data encryption indicated that

CoRI'16, Sept 7–9, 2016, Ibadan, Nigeria.
Copyright © 2016 Ibadan ACM Chapter 1-0002-0240-16-01/23/15

cryptography has a future largely dependent on how society uses it, which in turn depends on the current laws, regulations, customs and what the society anticipate cryptography to do. Floyd [3] in his own study proposed a solution based of cryptography for securing wireless mobile ad-hoc networks, which are especially vulnerable given their no clear line of defense. His proposed solution called Mobile Application Security System (MASS) foil unauthorized modifications of mobile applications by other running applications and other hosts on the wireless network, by guaranteeing the authenticity and authority of the mobile code.

Given the central role of encryption in the security of consumer data especially in the area of today ecommerce, Toubba [4] noted in his work the importance of strong encryption key management and granular access control to Web-based applications. Young [5] illustrated the limitations that exist in computer platform security in the use of cryptography in his study. It presented the experimental results of initiation a crypto-viral payload attack on the Microsoft Windows platform, specifically on the Microsoft Cryptographic API. Li. et al [6] in their study of the significance of the application of strong cryptography in voice communication developed a new Hierarchical Data Security Protection (HDSP) scheme using secret chaotic bit sequence. Fortifying data encryption and authentication of corporate networks through cryptosystems was evaluated in a study conducted by Harris [7]. He studied the feasibility of generating biometric key encryption and the experimental analysis of the study holds optimistic prospects for its use in modern cryptosystems.

Today, systems embedded in various chips depend on the same technologies upon which corporate IT depends. These technologies involve Ethernet, TCP/IP, and operating systems. This shows that embedded systems, like mobile phones, automobiles, military weapons and other sensitive life dependent devices are as susceptible to similar security challenges as corporate IT systems [8]. The use of strong cryptography is critical in protecting embedded systems that use wireless technology, such as Bluetooth, Blackberry, RFID etc. from attacks. Lovoshynovskiy et al [9] in their study concluded that recent progress in data-hiding technologies have indicated that network security, Quality of Service (QoS) and secure data communications over public networks can greatly leverage theoretical data-hiding technologies. Zanin et al [10] in their study devised a distributed signature protocol based on the RSA algorithm that can be implemented in large-scale ad-hoc networks. The signature protocol is distributed, adaptive, and robust yet subject to tight security and architectural constraints.

3. CURRENT EXISTING SYSTEM AND ITS LIMITATIONS

There are a number of digital right management schemes in the market with various restriction enforcement techniques, activation means and business models that can grants usage permission based on; content availability, restriction of redistribution of content between devices, the number of devices content can be viewed on, the number of times content can be viewed, how long it is available for and so on. However, none of these schemes have satisfied the various expectations of the consumers and the copyright holders. This has caused an imbalance that has brought dissatisfaction to the consumers, hence the motivation for consumers to circumvent the scheme, that is, pirate the content. This imbalance has also increased the woes of the copyright holders via low return on the investment on DRM due to lack of consumers' patronage and the consumers' renewed motivation to circumvent the schemes that many copyright holder are beginning to wonder if DRM is the required solution to their problem.

3.1 DRM Requirements

DRM system need persistent content protection that implies that protection must stay with the content even after delivery to the consumer. For instance, a digital movie delivered securely over to a recipient can save and copied unrestrictedly and an unprotected copy may be uploaded onto the Internet where many people can download and use it without reduction in quality. The DRM trust model is different from the simple cryptographic model where two parties that trust each other can own a key pair or share a secret key exchange encrypted message while an outside attacker tries to intercept and recover the data [11]. In DRM, one communicating party (the end users) cannot be trusted with a shared secret key or even unencrypted data. Malicious users may break the security system to make a profit through selling cracked software and digital assets. Once the protected content is delivered to the user, an attacker has a chance to break the system with unlimited time and resource [11]. Even though an average consumer may not have the skill, interest or time to attack the system especially when they are affordable, one hostile consumer/hacker with enough motivation and skills can considerably flaw the effectiveness of the system. If such attacker encode his break into software and publish it on the Internet, anyone can get access to the tool and defeat the protection scheme [11]. Perhaps, quite a number of techniques can be employed in chains to fortify the protection. The techniques include; encryption, digital signature and hash functions, digital certificate, individualization, watermarking, tamper resistance, hardware and software based techniques, self protecting container etc [12].

Despite these techniques, currently DRM can best be described as a failure as the schemes are always broken, consumers' patronage is low and there is still great motivation for the high volume consumption of pirated content. A number of factors have conspired to elicit such result.

The central limitation of the DRM technology arose from the misplacement of copyright philosophy obtainable in the traditional copyright protection in digital implementation. The copyright philosophy does not restrict access to copyright content but to its distribution. In summary, DRMs would have been huge success if they had focus on copyright protection in the same way the traditional copyright protection did by restricting access to redistribution than restricting access to usage. If one can access content in a public domain and is, only able to consume it in that domain he/she will not bother to crack the content to obtain a personal copy especially when the content is fairly priced given that the consumer is almost only paying for the distribution cost of his/her personal copy. Therefore, the schemes presented in this study consider a paradigm shift from usage right to distribution or redistribution right.

The second limitation of the schemes is in the neglect of some stakeholders in the distribution chain. Unlike the traditional copyright protection where everybody in the distribution chain gets something – from the artist to the producer, the promoter and to the retailer, digital copyright protection neglects the core interface to the consumers. The third limitation with the schemes is in consumer identification required to access their payment.

People like privacy. Not many people would like a third party to always keep track of the type of content they consume at least for the sake of security. The fourth limitation in the approach of the schemes is in the requirement to be online before one can activate the use of content. People would prefer it that they have the choice to choose a content while strolling or doing any other thing with a friend that has it and be able to consume it without having to first of all go online especially when such a consumer does not have such means. The fifth limitation is in the payment infrastructure requirement, which is obviously not at the reach of everyone that would like to consume content. This also extends to the choice of communication channel, which can only accommodate a minority class. In Nigeria, not every bus driver in the bus garage that would like to listen to a favourite track can afford internet access. The schemes do not have any place for fair use at all. Fair use implies the exceptions to copyright protection like the use of a copyrighted content for academic purpose.

3.2 Validation of the system

The DRM model called "Free Use/Use and Get Paid DRM model" is based on the principle of redistribution right protection that is, protecting copying-right. With this paradigm change in priorities, the copyright philosophy for digital right management schemes can be redefined to meet the consumers' satisfaction and the right holders' expectations. The model approaches copyright protection from the angle of free content consumption wherever you can access it. This means that a consumer has the right to consume all he/she can of a content he/she finds online or in a friend's device or in the library but does not have the right to redistribute it by making a personal copy without a license. With this approach, fair use requirement is fully met as scholars or critics can access and consume contents in public domains. It also wilts down the motivation to attempt to go the whole hug of circumventing the protection scheme when the usage of the content is free in the public domain.

The use of public key cryptography makes offline redistribution right acquisition possible, thereby granting consumers the freedom to consume their favourite content offline and on the go.
The model uses the mobile telecommunication service providers and text message as the mode of communication for the purpose of obtaining redistribution right instead of internet. Given that more people have access to mobile phone at more periods of time and location, consumer base is astronomically increased. Besides, most people would find better motivation to crack a content that requires them to have an internet connection than one that only requires them to just send a text message, especially when they are use to using their phones as most people are.

The use of the mobile telecommunication service providers can make paying for rights with airtime credit possible than the stress of authenticating and paying from one's bank account especially when all that needs to be paid is often less than the service charge for using the online payment system. This method of payment also encourage anonymity which give the consumer a sense of privacy and security as nothing is known about the consumer beyond the phone number. It also solves the problem of the lack of payment infrastructure.

The proposed model takes into account the role of every stakeholder in the distribution chain and disburses as much as 20% of every redistribution right purchased to stakeholders in the downstream distribution chain.

4. METHODOLOGY

In this research, we studied the existing Digital Right Management systems using internet research tool and observed the Nigerian market environment noting the booming piracy market, which beckoned for new DRM system that can meet the market demand. In our research, we realized that the very limited information infrastructure that can support the existing DRM systems is a major factor in the booming of piracy in Nigeria. Using statistics from the Nigerian Communication Commission we established that up to 67% of the 150 million Nigerians have access to mobile phone hence we started developing a model that can use mobile phone communication access as alternative to internet in transacting for content right. The Free Use/Use and Get Paid DRM Model achieves copyright protection by restricting redistribution right, that is, the right to copy a content from one device to another without the appropriate permission while the usage right is free. The model uses two sets of public/private key pair with key lengths of about 64 bits and the NTRU or XTR encryption algorithm to ensure secure offline delivery of license. The content, for example, an electronic book, is packaged by the content distributor in a self-encrypting and protecting container, which allows reading the book using a Universal Usage Key (KUU) resident in the plug-ins that helps the consumption action but not copying action. The distributor packages the content and its reference in the metadata into some temper proof self-protective program using encryption and place the content in the server and in every public domain like facebook, so that people can read but not copy. Figure 1 illustrates the proposed DRM model.

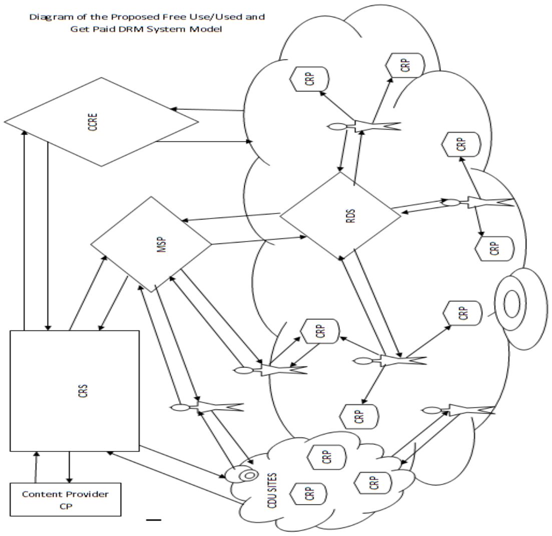

Figure 1. A diagram of the Free Use/Use and Get Paid DRM system model

When a consumer requests to copy content, by clicking copy, a message box pops up and informs the consumer of his lack of redistribution right and asks him/her to click "Ok" to get a right. When the consumer clicks Ok, a form is returned to him into which he/she specifies 'how many redistribution right to purchase', 'the type of copy', whether the consumer is to purchase a Private Parent, a Business Parent or a Child Copy. Upon submitting the form, the program generates a random number corresponding to the state of the randomized storage locations of the byte units of the content inside the self protecting container. To this random number it attaches its Content ID (CID), a nonce which is a part of the random number for that transaction session, a flag specifying the type of copy and the number of copy. The program encrypts this group of information with the Content Redistribution Subsystem (CRS) server Public Key called the Server Business Key (KSB) and returns a string of codes known as the Redistribution Right Request Code (RRRC) to the consumer. The consumer sends the RRRC code as a text message along with his/her Transaction Authorization Password (TAP) in a given format to the Content Redistribution Subsystem (CRS) via the mobile telecommunication service provider. The Mobile Service Provider (MSP) back end scans the message for a valid TAP which the consumer must have set up with the MSP prior to the transaction. If none is found, the service drops the message but if any is found, it forwards the message to the Content Redistribution Subsystem (CRS) for further processing.

At the CRS subsystem, the Encryption Decryption Sub-Unit (EDU) in the Redistribution Transaction Unit (RTU) decrypts the message using the CRS private key called the Server Private Key (KSP) and the Content ID (CID) extracted along with other information. The Content Reference Sub-Unit (CRU) manager in the Content Packaging Unit (CPU) locates the required content and the redistribution rate plus other information regarding the content in its reference database using the CID. The Account Management Sub-Unit (AMU) of the RTU unit calculates the cost to satisfy the number and type of redistribution copy requested then sends an Account Deduction Request (ADR) to the MSP. The Account Deduction and Transfer Unit (ADT) of the MSP confirms the availability of the required cost in the consumers account. If the fund is not sufficient, it sends an Insufficient Balance Message (IBM) back to the consumer and an Abort Transaction Message (ATM) back to the CRS server and the transaction is aborted. But if the fund is sufficient, it deducts the costs from the consumer’s account and credits the CRS server account and sends a Verifiable Digital Receipt (VDR) to the AMU sub-unit of the RTU unit so it can go ahead with the transaction and forward a transaction alert to the consumer. Upon receipt of the VDR, the RTU coordinating with the Packaging Sub-Unit (PU) of the CPU calculates and generates three (3) sets of strings. The first string is about eight bit which when ORed with a predetermined set of string in the content and added to the second string generated by the server yields the key to order and un-steg the randomized locations of the content byte units address in the self protecting container. The third string is the Content Business Key (KCB) of the new copy to be produced.

The RTU working with the PU sub-unit extracts the transaction session nonce contained in the random number and sets the flag for the number of redistribution permission granted and the flag of the type of the redistribution copy. It arrange the information in a predetermined format and encrypt them using the Content Private Key (KCP) which is unique to every copy of the content produced by the server and never gets transmitted. The server forwards the encrypted information known as Redistribution Right Code (RRC) back to the consumer via the MSP. The MSP closes the transaction section and generates a report for audit purposes. Upon receipt of the message, the consumer inputs the RRC code into the RRC code input field of the content. The program decrypts the code using the Content Business Key (KCB) and verifies the nonce. If the nonce does not check out, the process is aborted and the consumer notified but if otherwise, the program ORs its fixed string with the first string in the received RRC code and adds the result to the second string to generate the Redistribution Key (KR). With the KR, the program orders and un-stegs the byte units address locations in the protecting container and prepares the new copy to be copied by generating a new and unique CID comprising of a portion of the parent CID, the session nonce, the time and date of when it is produced and a unique identifier. It also assigns the new KCB sent from the CRS server and the general KSB to the new copy. After the copy is made according to the copy type, the permission counter is decreased by one.

At the CRS server end, about 20% of the revenue is designated and shared in line with a predetermined percentage of distribution by the Account and Audit Unit (AAU) among the downstream stakeholders in the distribution chain with the Transacting Copy or Content (TC) getting up to 10%, the next from the bottom 4%, 2%, 1% and so on. The AAU working with the CRS credits these accounts accordingly and also disburses the shares of each stakeholder at the upstream distribution chain at the end of every business day.

The various types of redistribution copies that can be made include Child Copy (CC) – this copy cannot be used for redistribution i.e. no new copy can be made from it. It is the type intended for use on CDs and DVDs. Private Parent Copy (PPC) – this is the standard copy for private use with no adverts on it. Other copies can be made from it and is the only copy that can produce a Business Parent Copy (BPC). Each PPC can only produce one BPC. Redistribution copies or sales made from the PPC are not rewarded. Business Parent Copy (BPC) – this is the standard redistribution copy that is rewarded for every single copy made from them. However, a BPC cannot produce another BPC but it can only produce PPC and CC copies. PPCs are jumped anywhere there are found in the distribution chain when distributing reward. If a PPC is the TC, the nearest BPC in the chain takes the reward.

Consumers can access and consume contents anywhere they find it but cannot redistribute it without license. The Content Distribution Service (CDS) places the content freely in every public domain they can find like facebook, libraries, portals, radio/TV houses etc. so that consumers can consume and maybe desire a personal copy in which case they will require a redistribution right. Consumers, who have bought BPC copy, can also advertise them on their own in various public domains or to friends/family and get rewarded whenever anybody transacts redistribution permission from their BPC copy. This means for games for instance, consumers can play the game online or in the public domain or in a friends device with limited features and adverts without cost but cannot redistribute a private copy to their own personal device at home or anywhere to be played at their convenience. For books, the consumer can consume the much he/she can in the public domain where it is advertised without cost but will need a redistribution license for a personal copy redistribution. Same goes for music, they can be consumed anywhere they are advertised or played, like radio, occasions, a friend’s house, in the street etc but a redistribution license will be required for redistributing a personal copy to a private domain to be enjoyed at will.

The Free Use/Use and Get Paid DRM system model can be realized in the following four subsystems:

1. Content Redistribution and Plug-in Subsystem (CRPS): This subsystem consist of the Content Redistribution Program (CRP) and the Content Plug-In (CPI). These two units reside with the content at the point of content consumption. The CRP is bonded to each content at the time of packaging by the Content Packaging Unit (CPU) that resides in the Content Redistribution Subsystem (CRS). The CRP is the tamper resistant, protective container that uses different techniques (e.g. encryption, watermarks, steganography) to keep the content safe. The CPI, is a downloadable plug-in that extends the functionalities of existing content readers or players to be able to play contents using the Free Use DRM. Each downloaded copy of plug-in locks to the CPU during installation and becomes a protective repository for Free Use contents in that device. Every consumer intending to consumer a Free Use DRM content must do a one-time per device download and installation of the plug-in and the CPI is upgradeable.
2. Consumer and Consumer Requesting Device Subsystem (CCRD): This subsystem consist of the Consumer and the Consumer Requesting Device (CRD). The consumer uses the CRD device to make content redistribution right request by sending a Redistribution Right Request Code (RRRC), given by the CRPS subsystem at the instant of attempting to copy the content, to the Content Redistribution Subsystem (CRS) through the Mobile Service Provider (MSP) of his/her mobile phone network. This CRD device also receiver back a Redistribution Right Code (RRC) from the CRS subsystem via the MSP subsystem for the consumer if the RRRC request met the Redistribution Right Requirement (RRR) for that content or an Insufficient Balance Message (IBM) or an Invalid Transaction Authorization (ITA) message if the RRR was not met.
3. Mobile Service Provider (MSP): This subsystem consist of three units – the Message Handling Unit (MHU), the Account Deduction and Transfer Unit (ADT) and the Report Generation and Sending Unit (RGS). The MHU handle the messages that are send back and forth between the consumer and the CRS subsystem. The ADT handles the consumer account deduction process prior to the RRC generation by the CRS. The RGS handles the generation and sending of all necessary report regarding the success or failure of each transaction via the MHU.
4. Content Redistribution Subsystem (CRS): This subsystem is the main subsystem providing the DRM and content distribution service to the public. It consists of four major units with several sub-units. They include – the Redistribution Transaction Unit (RTU), the Content Packaging Unit (CPU), the Content Distribution Unit (CDU) and the Account and Audit Unit (AAU).

Figure 2 presents a diagrammatic representation of these primary subsystems and their units with a pictorial depiction of information flow. However, the secondary subsystems that are not primarily required for the operation of this DRM model are not included in the diagram like the Reward Distribution Subsystem (RDS) and the Consumer Content Redistribution Effort Subsystem (CCRE).

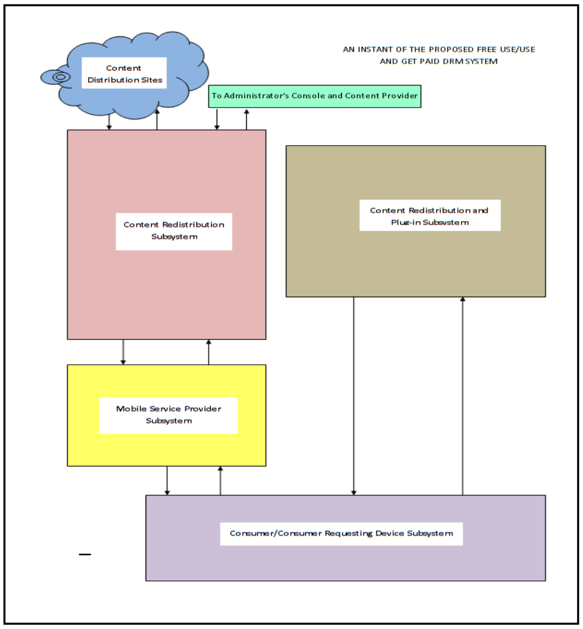
AN INSTANT OF THE PROPOSED FREE USE/USE AND GET PAID DRM SYSTEM
Content Distribution Sites
To Administrator's Console and Content Provider
Content Redistribution Subsystem
Content Redistribution and Plug-in Subsystem
Mobile Service Provider Subsystem
Consumer/Consumer Requesting Device Subsystem

Figure 2: The system structure

4.1 Architecture of the System Design

The Free Use/Use and Get Paid DRM have the architecture shown in Figure 3. The system can be broken down into many subsystems undertaking different functions. There are four subsystems primary to the operation of this proposed system and each composed of a number of unit and sub-unit. Logically related functions carried out by physically related system devices are grouped into subsystems to ease the understanding of the operation of the system. Logically close functions performed in the same subsystem by a group of subsystem devices are co-located to form sub-units. The two inputs to the system are the request from the consumer and the content input and configuration command from the administrator's console. The rest of the other system processes involve the transformation and packaging of the input content to become deliverables. The two outputs of the system are deliverables consumed by the consumer in form of music, movie, software, game, ebooks and news etc and payment instructions/reports. A careful survey of the figure also highlights the sub-units, units and subsystems interactions and the flow of information as well as command within the system.

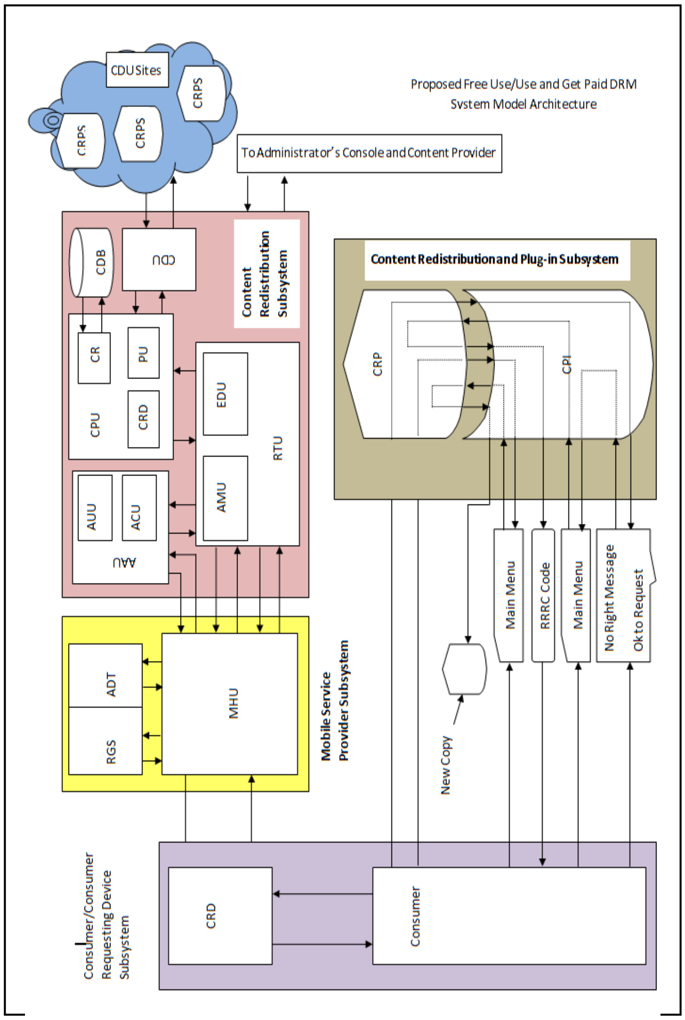

Figure 3. The Free Use/Use and Get Paid DRM system architecture

4.2 The Database Input Interface

The Database Input Interface is the interface through which the database administrator inputs content into the CRS subsystem for further processing like packaging and distribution. The administrator copies the contents into a folder or a volume connected to the CRS subsystem. Through the Content Location Input Field, the administrator browses the drop down list and locates the content file or folder or perhaps types it in. Next, the administrator selects the content type from the drop down list of the Content Type Input Field. The content types can include Music, Movies, Games, Softwares and Ebooks etc. The next field requires the administrator to more clearly describe the content by selecting the class to which the content belong in the content type selected. For instance, if the content is of the type "Music", the administrator selects "Music" in the Content Type Input Field but will need to select the class of music the content belongs to. For the selected type "Music" the content can belong to any of the classes like Jazz, Disco, Reggae, Blues, Hip-hop e.t.c. Next, the administrator specifies the Author or Artist of the content in the Author/Artist Input Field, the Producer or Publisher of the content in the Producer/Publisher Input Field, the Date of Production or Publication of the content in the Date of Production/Publication Input Field, the Album or Series to which the content belong (if any) in the Album/Series Input Field, the content title in the Content Title Input Field, the content format (if known) in the Content Format Input Field, the content provider or copyright holder in the Content Provider/Copyright Holder Input Field by selection from the drop down list of the Providers or Copyright Holders in contract with that Distributor. The administrator can then specify the charges for private parent redistribution right and a business parent redistribution right in the Private Parent Charge Input Field and the Business Parent Charge Input Field respectively. The Advanced Setting yields further functionality to the administrator in managing content input. Functionalities like excluding one or more contents in a folder, binding two or more contents together, specifying content reference marker of the administrator's choice or any other rule the administrator want the content to obey using Right Expression Language (REL). The system administrator (not the Database Administrator) uses the System Configuration Interface to configure the items that appear or are active in the drop down lists in particular and the interface in general. The System Configuration Interface is used in the technical system configuration like specifying what encryption algorithm, Key range, MSP, RDS CCRE subsystems locations etc.

4.3 The Database Output Interface

The Database Output Interface provides a means for the Database Administrator to search the database. Every content input through the Database Input Interface is processed (packaged and organized by the CPU) and stored in one of the virtual volumes in the CDB with their references in the CRU. A search of the database through the Database Output Interface primarily sorts the content reference list in the Content Reference Unit (CRU) to return a list of the required contents to the interface. The administrator selects the type of content he/she is looking for by selecting one of the types in the drop down list of the Content Type Input Field. Next he/she checks one of the radio buttons in the "Search Content by" field to select the search parameter he will like to use in searching for the content. Next, he/she will select the first letter in the name he wants to use. This selection produce a drop down list of all the content of the selected type and class whose selected parameter's first letter match the selected first letter. When he/she chooses from this list, all the contents will appear in the List of Content below. Let us illustrate this with an example. If the administrator chose ebook as the content type, if he chooses to search for this book by Author, he will be require to choose the first letter of the author(s)' name. Assuming he is looking for a book written by Ogwueleka F.N, it follows he will have to choose the letter "O" as the author's name first letter. This action will produce a drop down list of all authors whose name starts with the letter "O". When the administrator selects Ogwueleka F.N. from the list, the List of Content field below will be populated with all the books by Ogwueleka F.N. in the CDB from which the administrator will then select the particular one he wants. This interface is also used at the CDU sites by users to search the database for content. However, while the administrator's interface at the CRS subsystem is equipped with many more features that help the manipulation of contents, the users' interface at the CDU sites can be equipped with shopping carts to enable the user select and organized a list of contents he/she wish to request.

4.4 The Graphical User Interface Visualization

The consumer uses the graphical user interface interacts with system through the CRPS subsystem when redistributing contents in the public or private domain. At the instant of clicking copy to copy the content, the CPI presents the consumer with the No Right Message Box that tells the consumer of his/her lack of Redistribution Right on the content and asks him/her to click OK to request or input right or CLOSE to close the message box and terminate the process. When consumer clicks Ok, a request form, the User Main Menu is returned into which the user indicates the number of redistribution right he/she is requesting and the type of Content Copy he/she wants to redistribute. Perhaps, he selects one of the two types of copy (Private Parent, Child Copy) from a drop down list and click Ok. If the consumer wants a Business Parent Copy which only one copy can be made from any Private Parent Copy, he/she will not need to select from the drop down list but check the Radio Button below before clicking Ok. The Business Parent Option grades-out whenever a Business Parent Copy is made of the content. However, if the consumer has an RRC code, he/she simply inputs it in the ‘Input RRC code here’ input field and then clicking Ok to proceed. If the first explanation is the case, an RRRC code Output Message Box is presented from which the consumer is requested to copy the RRRC code and SMS to the CRR server through a given sms code or CALL a given phone number for more information. If the second explanation was the case, the consumer is presented with a Process In Progress Counter showing the progress of the copy operation and a series of other input window through which the consumer control and contributes to the copy process. At the end of the process, the consumer has a new copy of the content in the location specified by him/her.

The system main menu shown in Figure 4 provide control access and use access to the proposed Free Use/Use and Get Paid DRM system from the distributor’s back end.

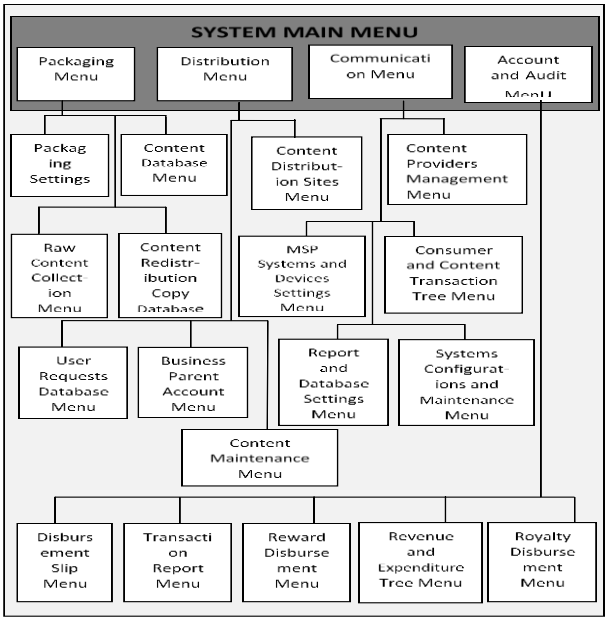
SYSTEM MAIN MENU
Packaging Menu
Distribution Menu
Communication Menu
Account and Audit MenU
Packaging Settings
Content Database Menu
Content Distribut-ion Sites Menu
Content Providers Management Menu
Raw Content Collect-ion Menu
Content Redistr-ibution Copy Database
MSP Systems and Devices Settings Menu
Consumer and Content Transaction Tree Menu
User Requests Database Menu
Business Parent Account Menu
Report and Database Settings Menu
Systems Configurat-ions and Maintenance Menu
Content Maintenance Menu
Disbursement Slip Menu
Transaction Report Menu
Reward Disbursement Menu
Revenue and Expenditure Tree Menu
Royalty Disbursement Menu

Figure 4. The free use/use and get paid DRM system main menu

5. RESULT AND DISCUSSION

The Free Use/Use and Get Paid DRM System Model deals with content packaging, distribution and redistribution, consumer request servicing, content maintenance and royalty disbursement to both distributing consumers and the copyright holders as a result, there are lots of database involved in the operation of this system. The very prominent among them include; the Raw Content Database, the Content Database, the Content Redistribution Copy Database, the Transaction Report Database, the Content Distribution and Distribution Sites Database, the Copyright Holders/Provider Database, the Revenue and Expenditure Database and the Royalty Disbursement Database. The database design of this system is still primitive but must contain the following schema as shown in Table 1 to identify content.

Table 1: Database Schema for Content Identification and Referencing

Content Title	The name of the content file
Date/Time of Upload	The date/time when such content was uploaded in to the distributor’s system
Date/Time of Packaging	The date/time when it was finally packaged or the market
Reference Code	The reference ID recorded in the database that refers to the content or the content copy
Content Type	The type of content e.g. ebook, music, movies etc
Content Class	The class of content which is a sub category of the content type. E.g. classes under music may include hip-hop, reggae, blues etc.
Author/Artist	The name of the author or artist
Producer/Publisher	The content producer or publisher
Date of Production/Publication	The date the content was produced or published
Album/Series	The album or series to which the content belong
Format	The format the content came with and the one it was converted to
Content Provider/Copyright Holder	The person(s) that holds the copyright of a digital content
Private Parent Charge	The amount charged per private parent license
Business Parent Charge	The amount charged per business parent license
Content Business Key (KCB)	The public key of the unique content encryption key pair
Content Private Key (KCP)	The private key of the unique content encryption key pair
Content Parent Copy	The copy from which the transacting copy was made from
Content Offsprings	The copy(s) that where made from the content copy in question

The content's history of transaction is also maintain and used in plotting the content lineage tree. To do that, some of the databases will require maintaining additional information about the content transaction history, which may include the following schema as listed in Table 2.

Table 2: Additional Schema for Maintaining Content Transaction History

Date/Time of Transaction	Date/time of when the license transaction of the new copy was made
Requesting Device	The consumer phone or other mobile devices with which he/her send the RRRC code to the CPS subsystem
No. of Rights	The number of rights the consumer wish to purchase
Type of Right	The type of content copy the consumer wish to make with the license
Transaction Nonce	The unique transaction identifier generated by the CRPS
RRRC code	The redistribution right request code which is generated by the CRPS subsystem and sent by text message to the CPS
RRC code	The redistribution right code generated in response to the RRRC code sent from the transacting content that can unlock the content and allow the number of copies specified to be made
New KCB	The public encryption key of the new content key pair
New KCP	The private encryption key of the new content key pair

The activity of report generation is not concentrated in any particular subsystem or designed to stand alone but is dispersed in the various subsystems. However, the report generation functions of the RGS unit in the MSP subsystem and report generation and cataloging ability of the AUU sub-unit is central to the smooth running of the entire system. The activity of the MSP subsystem is report based as that particular subsystem is central to the transaction of all the consumers with the CRS and yet is located outside the distributor's domain. Besides, being the channel of communication between the consumer and the distributor, each of the two parties depend on the report coming from this subsystem to know what is happening with the transaction at each other's end. Therefore, the RGS is a unit whose function is to monitor the activities in the two other units in the MSP subsystem and generate an appropriate report about them and send to the appropriate parties or device e.g. IBM message to the Consumer, VDR message to the AMU sub-unit in the RTU unit and the CRA server. The AUU as well as the ACU sub-units of the AAU unit directly monitors activities in the MSP subsystem and at the RTU, CPU and CDU units for the purpose of auditing and accounting respectively.

The query functionality like the report generation activity is spread across the various units in the system and imbedded in the different output interfaces e.g. the Business Parent Account (BPA) which enables the Business Consumer to query the system about his redistribution efforts or reward status or the Business Parent Account Menu which enables the administrator to query the system to access and manage the various BPAs. A more robust use of it is made through the database output interface, which the administrator or the consumer can use to search the system's content database for a content of choice.

The Free Use/Use and Get Paid DRM Model is a robust, distributed copyright protection model with a distributor's end (Content Redistribution Subsystem) that package the contents and place them in the public domains and also service consumer request sent over the mobile service provider network and a detached consumer end consisting of the content packaged into some protective program and plug-in program that helps the consumption of the content by the consumer. This implies that a number of languages like PHP for the distributors online database system and Java for content packaging etc will be used for the implementation of the system model. In this research study, we have used the Unified Modeling Language UML to model this system from different perspectives such as the system interaction with the environment using Used Case Diagram and the sequence of operation that take place in the system using Sequence Diagram etc. We also implemented part of this model using Java and PHP programming languages on JBox and MySQL server.

The system was implemented using the drivers in three major decentralized locations, the Content Redistribution Subsystem (CRS), the Mobile Service Provider (MSP) and the Content Redistribution and Plug-in Subsystem (CRPS). The CRS subsystem is integrated in a specialized computer server and has both stand alone and web interfaces integrated together and linked with the MSP subsystem. The MSP subsystem is integrated with mobile service provider(s) system and provides the payment infrastructure and the offline link between the CRS and the CRPS through the use of mobile phone and recharge cards. The CRPS subsystem is the consumable digital content and the plug-in that helps their consumption resident in standalone or networked devices. Any attempt to redistribute a content bundled in the CRPS without license is denied.

When an attempt to redistribute a content is denied, a form is presented with which redistribution right can be requested. After indicating the number and type of right, the CRPS generates a unique RRRC code. The consumer sends to the CRS as SMS via the MSP.

An RRC is generated and sent back to the consumer using the same means after the transaction is verified and payment made. The RRC code is inserted in the space provided before the redistribution of the digital content is allowed.

The performance evaluation of the proposed model after implementation was excellent and achieved the good results after testing. Noted are offline copyright protection of digital contents through offline content license purchase and use; the system can use text messages for license transaction; the system can be accessed by larger consumer base with mobile phone access hence can provide unhindered access to legitimate digital content even on the go; the system can enhance consumer security and comfort through anonymity and on the go legitimate content purchase and use; the system will accommodate the Fair Use Policy; and the system will make license payment with airtime credit possible.

6. CONCLUSION

This research studied digital copyrights infringement and the limitations of the existing technical solutions in the form of Digital Right Management and thus proposed a model that uses mobile phone Short Message Service (SMS) to transact content license purchase. The security of the transaction is made possible by the use of public key encryption. By using mobile phone instead of internet communication alone to transaction for license, an average peasant in the street without sophisticated computer skill to undertake internet banking and content activation can still purchase and consume legitimate contents using his/her mobile phone by simply sending SMS and paying for the content license using his/her airtime credit. The study through the Free Use/Use and Get Paid Model will resolved the problematic Fair Use Policy of digital contents by shifting emphasis from copyright content usage protection to copyright content redistribution restriction.

Digital copyright problem especially in the Nigeria context cannot respond to only technical solution. We therefore, recommend that government and other relevant authorities promulgate laws that will be effective in ensuring digital copyright protection. We also recommend the use of public key encryption algorithms like the Nth Degree Truncated Polynomial Ring Unit (NTRU) or the Efficient Compact Subgroup Trace Representation (XTR) during system development against the well known RSA given their light weight and the likelihood of using the Free Use/Use and Get Paid DRM System in low end systems like MP3s and Mobile Phones.

7. ACKNOWLEDGMENTS

Our thanks to Nigerian Communication Commission for the statistically information.

8. REFERENCES

[1] Fagin, B., Baird, L., Humphries, J. and Schweitzer, D. 2008. *Skepticism and Cryptography*. Knowledge, Technology & Policy, Vol. 20 No. 4, pp 231 – 242

[2[Callas, J. 2007. The Future of Cryptography. *Information Systems Security*. Vol. 16, No. 1, pp 15 – 22.

[3] Floyd, D. 2006. *Mobile application security system (MASS*). Bell Labs Technical Journal, Vol. 11, No. 3, pp 191 – 198.

[4] Toubba, K. 2006. Employing Encryption to Secure Consumer Data. *Information Systems Security*. Vol. 15, No. 3, pp 46 – 54.

[5] Young, A. 2006. Crypto Viral Extortion using Microsoft's Crypto API. *International Journal of Information Security*. Vol. 5, No. 2, pp 67 – 76.

[6] Li, C., Li, S., Zhang, D. and Chen, G. 2006. Cryptanalysis of a Data Security Protection Scheme for VoIP. *Vision, Image & Signal Processing*, Vol. 153 No. 1, pp 1 – 10.

[7] Harris, D. 2007. Has Anyone Seen My Data? *Electronic Design*. Vol. 55, No. 9, pp 41 – 46.

[8] Robinson, S. 2008. Safe and Secure Data Encryption for Embedded Systems. *EDN Europe*. Vol. 53 No. 6, pp24– 33.

[9] Lovoshynovskiy, S., Deguillaume, F., Koval, O. and Pun, T., 2005. Information-Theoretic Data-Hiding: Recent Achievements and Open problems. *International Journal of Image & Graphics*, Vol. 5 No. 1, pp 5 – 35.

[10] Zanin, G., Di Pietro, R. and Mancini, L. 2007. Robust RSA Distributed Signatures for Large-Scale Long-Lived Ad hoc Networks. *Journal of Computer Security*. Vol. 15, No. 1, pp 171 – 196.

[11] Pasi T. 2005. Concepts and a Design for Fair Use and Privacy in DRM, *D-Lib Magazine*. Vol. 11, No. 2. pp 932 – 937.

[12] Intel Corporation. 2009. High-Bandwidth Digital Content Protection System, *Publication of the Digital Content Protection LLC Website*, Revision 1.4, pp 10 – 40.