IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 19, Issue 10, Ver. VII (Oct. 2014), PP 118-124
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Application of Secure Container Technology in Digital Libraries

Nitumika Gogoi

Lecturer, Centre for Library & Information Science Studies, Dibrugarh University, India

Abstract: *Copyright issues in the digital environment are global and unless reasonable, access to copyright works is not maintained in digital environment, a further barrier will erupt which will deny access to those who cannot afford to pay. The paper touches upon the biggest uncertainty that digitally stratifies the society between and among the developed and less developed countries in regards to providing access to digitized information. The scope of this paper expects the formation of Information Security Teams (IST), developing strict security policies in digital libraries as well as usability of the mechanism that ensures document security and authenticity which unless otherwise realized, the very existence of such a technology based concept will be crippled. Document encroachment by copyright infringement being the hamstring of the present paper, tries to broaden the matter of integrity of e-documents through a mechanism wrapped in a secure cryptographic envelope by way of encryption merged with the combined working of hash function and digital signature techniques.*

Keywords: *Cryptography, digital rights management, digital signature, encryption, information security*.

I. Introduction

In the present Information Market, the trade of physical objects is replaced by the trade in signs liberated from the media which a person may apply it for personal reasons or for redistribution over the internet. Putting a work on a website involves the right of communication to the public. The copyright is so comprehensive and overwhelming in digital environment that it covers all communications on the internet. While protection of data put on the website is an important issue, the protection of digital copyright is a very difficult proposition, due to its easy access in the electronic medium. Therefore copyright owners seek to technological measures such as watermarking, encryption, copy control flags, macro vision etc. as a way of routine libraries too have to consider using such technologies to protect their own copyright in the digital environment.

The present scenario raises certain complicated questions like

- Should there be an enabling legislation that would allow libraries to take hard copies of a digital work and issue the same to its members.
- Will the libraries be able to perform their historical function as archives of published material needs?
- Also the access control measures adopted by the content providers on the internet are at question.

It is in these situations when the library administrators engage their attention to copyright/IPR over issuing copies and communication to the public. New legislations like the US DMCA (1998) provide an exemption for non-profit libraries to gain access to a commercially exploited copyrighted work. However to obtain copyright permission from the owners for their vast collection is a major problem. [1]

II. Digital Rights Management

The Digital Rights Management System is designed to protect digital works and the unauthorized duplication and illegal distribution of copyrighted digital materials. The first generation of DRM focused on security and encryption as a means of solving the issue of unauthorized copying, that is, lock the content and limit its distribution to only those who pay, thus representing a substantial narrowing of the real and broader capabilities of DRM. The second-generation of DRM covers the description, identification, trading and protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets including management of rights holders' relationships. [2]

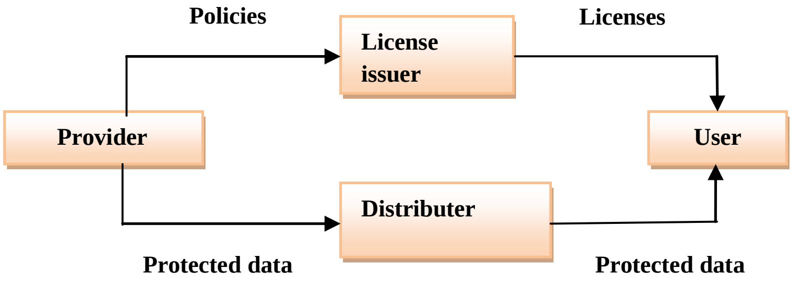

Fig: 1 Reference model for DRM system

In designing and implementing DRM systems, there are two critical architectures to consider. The first is the Functional Architecture, which covers the high-level modules or components of the DRM system that together provide an end-to-end management of rights. The second critical architecture is the Information Architecture, which covers the modeling of the entities within a DRM system as well as their relationships. It is this architecture that actually complies with information security management.

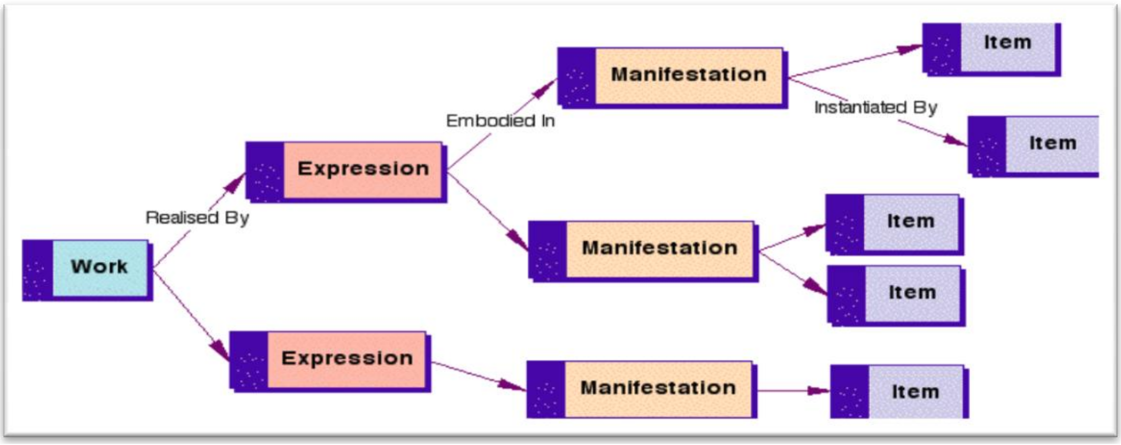

Fig: 2 DRM Information Architecture - Content Model (fig.1) (D-lib magazine, June 2001)

2.1. The functionality of DRM technology

It allows distributers of electronic information to control viewing/accessing the contents. Therefore it seeks the method of encryption to control access to content. Rights management solutions are based on a wrapper or container placed around a data file which protects and sets the data lifecycle and defines usage rules, payment and redistribution constraints. A license must be acquired to unlock the wrapper and get access to the content. Individual keys are provided to the end user who purchases the rights to limitations on copying, printing and redistribution.[3]

The DRM system ensures harmony of the object so that it is not intercepted before delivery as well as ensures the security of the whole distribution chain, so that the objects are transferred only to authorized consumers and devices. The system comprises of

- Watermarks and identifiers to identify the content uniquely and also for downstream tracing of the content to ensure an authorized use of content.
- Keys in the possession of appropriate consumers for access to the original content.
- Cryptographic security of the content by application of secure container technology.
- Usage rules to decide what must be met for access and how the consumer can use the resource.

III. Information security team

The happenings around the world emphasis the need for understanding the criticality of information security and what is all about and the need for security requirements and security-related tools and technologies. Security attacks can be categorized as physical attacks and logical attacks (Stallings, 2006). A physical attack involves hardware security where keys, locks, cards, and visitor monitoring is used. A logical attack involves an attack on the content or digital library system. We focus on the logical attacks and software security of digital libraries. According to the DELOS Reference Model (Candela et al., 2007) there are 6 main concepts in a digital library universe: content, user, functionality, architecture, quality, and policy each of which has security issues that affect them individually.

The above cited discussion has direct implication on the adoption of mechanism to protect the contents towards the creation of a global commercial information infrastructure. Therefore technologies such as digital watermarking and digital fingerprinting are certain attempts towards providing a desired degree of copyright protection and are disincentive to data piracy somewhat rather similar to data hiding technology/steganography. Several possibilities for communication security system and their usability in the digital library environment are there. When any sort of electronic transaction is performed, two issues need to be addressed:

- Protection of the communication channel and
- Protection of the document being transacted over the communication channel.

Most of the solutions proposed until now focus primarily on the protection of the communication channel. It is the demand of the content providers as well as the customer patrons to develop mechanism that protects the document being sent over the communication channel.

One highly sophisticated Information Security Team has been framed by the British Library that forms part of the Information Risk Management framework. Their approach to information security management conforms to accepted best practice as defined by the ISO/IEC 27000-series and other relevant information security standards by protecting their information assets against unacceptable risks to their confidentiality, integrity and availability. [4]

IV. Application of Secure Container Technology to digital environment

Secrecy doesn’t always guarantee safety. However e-documents can be protected from unintended recipients to a certain extent by attaching irreversible secret codes i.e. which cannot be cracked. Similar to monetary currency, a cryptosystem has value because its users believe in its worth.

Secure container technology is based on Cryptographic applications which can be stated as the processing of information into encryption (i.e. encoding a plain text message so that it cannot be understood by intermediate parties who do not know the “key” to decrypt) for the purpose of secure transmission. Through the use of a “key”, the receiver can decode the encrypted message (the process known as decryption) to retrieve the original message. So, *cryptography* is about protecting the contents of the message. But as soon as the data is decrypted, all the in-built security and data is ready to use. Cryptography "scrambles" a message so that it cannot be understood by unauthorized user [4]. This does not happen in watermarking. Neither the cover medium nor the copyright data changes its meaning. Rather, copyright data is hidden to give the ownership information of the medium in which it is hidden.

V. Digital Signature

Situations have arose when the content providers in digital libraries realized that the integrity , confidentiality and accountability are at stake and the patrons as well put questions to the authenticity of the content of the material since they are paying for it [5]. The risk of data misuse has increased many folds with the advent of networking and wireless communication as many users can gain access to the data if not secured. A digital signature appears to solve the matter to a maximum depth because of the fact that digital signature ensures prevention of unauthorized access to data providing accurate authentication. By far the most important automated tool for network and communication security is encryption. But in situations where there is not complete trust between sender and receiver, something more than authentication is needed and to this the most attractive solution is the application of digital signature. Digital signature (herein after D.S) is primarily based on encryption and decryption.It is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document and possibly to ensure that the original content of the message or document that has been sent is unchanged. D.S is easily transportable, cannot be imitated by another and is automatically time stamped. Moreover it can be used with any kind of message whether encrypted or not, simply so that the receiver can be sure of the sender’s identity and that the message arrived intact. A digital certificate contains the D.S of the certificate issuing authority so that anyone can verify the integrity of the certificate. [6]

Requirements:

1. The signature must be a bit pattern that depends on the message being signed.
2. The signature must use some information unique to the sender, to prevent both forgery and denial.

Advantages:

1. Easy to produce, recognize and verify the digital signature.
2. Computationally infeasible to forge the signature either by constructing a new message for an existing D.S or by constructing a fraudulent digital signature for a given message.
3. Practical to retain a copy of the stored digital signature.

There is a significant drawback to digital signature scheme i.e. large messages must be broken into blocks and each block must be digitally signed prior to transmission. To address this problem, hash functions are used to reduce messages of arbitrary length to a message digest (thereafter MD) and it is this digest that is digitally signed, resulting in the generation of a single digital signature.

A hash is a fingerprint for a document and its purpose is to provide proof that that data has not been altered or tampered with and is used for password authentication. On the other hand, a message digest is a compact digital signature for an arbitrarily long stream of binary data and never generate the same signature for two different sets of input.[7] Moreover it compromise in favor of a digital signature of modest and usually fixed size created with an algorithm designed to make preparation of input text with a given signature computationally infeasible.

5.1 Message Digest Algorithm

Message digest algorithms have much in common with techniques used in encryption, its main goal being the verification of the data not having been altered since the signature was published. Most commonly used present-day message digest algorithm is the 128 bit MD5 algorithm developed by Ron Rivest.[8] The same message put through a particular message digest algorithm should produce always the same hash.

MD stands for message digest and MD5 is an algorithm which takes an input of any length and outputs a message digest of a fixed length (128-bit, 32 characters).MD5 uses the same algorithm every time. Hence it will always generate the same message digest for the same string (data). The MD5 algorithm takes a bunch of characters (digits, alphabetic or other), the input string changes them to a 32 character long bunch of characters, called the message digest or the hash of the inputted string .The hash is made up from only hexadecimal characters .Whatever the length of the inputted string, MD5 will always create something which is 32 characters long. The MD5 Algorithm is irreversible; the only way of getting the original string is by brute force attacking. [9]

However the MD5 Algorithm is now considered insecure and the SHA (secure hash algorithm) family overpowers it. The SHA-1 in comparison to MD5 produces a 160 bit message digest for a maximum data size of 2^{64}bits(which is infinite in the case of MD5), the main advantage being the security of the message.

5.2 Digital Signature Algorithm (thereafter DSA)

Proposed by National Institute of Standards and Technology, the digital signature algorithm is based on the difficulty of computing discrete logarithms. There are three parameters that are public and can be used by a group of users. [9] The global public key components are:

- p :prime number where 2^{L-1}<p<2^{L} for 512≤L≤1024 s.t L=a multiple of 64 i.e. bit length between 512 and 1024 bits in increments of 64 bits.
- q :prime divisor of (p-1) where 2^{159}<q<2^{160} i.e. bit length of 160 bits.
- g =$h^{(p-1)/q}$mod p where h is any integer with 1<h<p-1 s.t. {$h^{(p-1)/q}$mod p}>1

User's private key is:

- x :random or pseudo random integer with 0<x<q

User's public key is:

- y=g^{x}mod p

User's per message secret number:

- k= random or pseudorandom integer with 0<k<q

Signing:

- r= (g^{x}mod p)mod q
- s= [k^{-1}{H(M) + x^{r}}] mod q where M =message to be signed; H(M)= hash of M using SHA-1

Thus the signature is (r, s).

This signature can be verified as below:

- w = (s')$^{-1}$mod q
- u_1= [H(M')w] mod q
- u_2= (r')w mod q
- v = [($g^{u_1}y^{u_2}$) mod p] mod q

We get as v = r' where M', r', s' are received version of M, r, s [10]

Functioning of the Digital Signature:

1) Signature generation
   - i. A message digest is computed.
   - ii. The message digest is encrypted using the private key of a public/private key pair, producing the message's digital signature.

2) Signature verification
   i. The signature is decrypted using the public key of a public/private key pair, producing a message digest value.
   ii. The message digest value is compared with the message digest calculated from the original message.
   iii. If both values match, the signature is authentic. Otherwise, either the signature or the message has been tempered with [11]

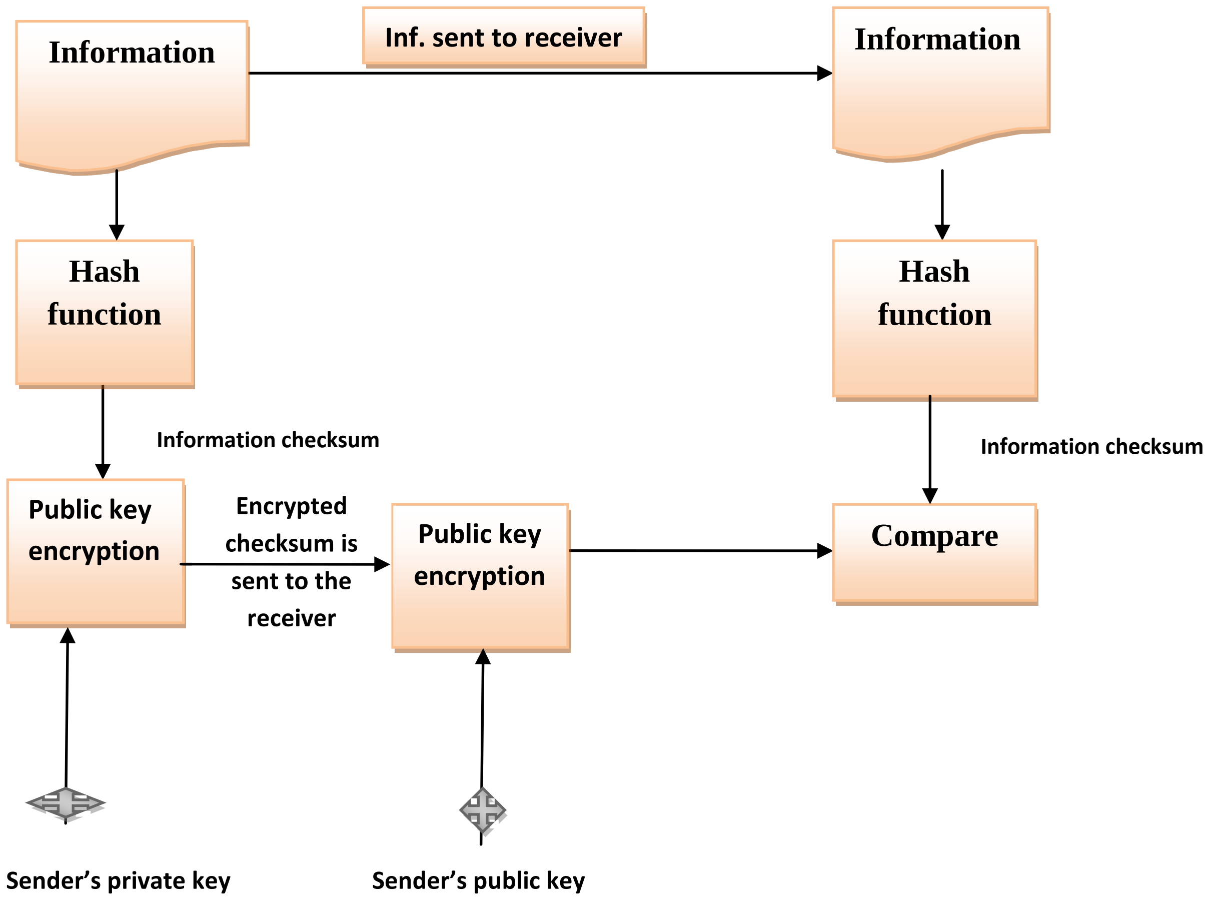

Fig: 3 Digital Signature operations

VI. End users of Digital Libraries

The application of the secure container technology needs further emphasis on the types of Digital Libraries end users. These end users exploit the functionality of digital libraries for the purpose of providing, consuming and managing its content and some of its other constituents. They perceive the digital library as a stateful entity serving their functional needs. The behavior and output of the digital libraries depend on its state at the time a particular part of its functionality is activated. This state corresponds to the state of its *resources*, which consist of the collections of information objects managed by the digital libraries, the set of authorised users, the digtal library's functionality and its set of policies. This state changes during the lifetime of the Digital Library according to the functionality activated by users and their inputs. These end-users may be further divided into Content Creators, Content Consumers and Librarians.

Content Creators are the producers of the Digital Library (DL) Content; they feed it with the resources, mainly information objects, to which other users of the digital library will have access. This activity is

- accomplished through the Functionality the DL provides,
- regulated by the Policies defined in the DL, and
- performed according to the Quality the DL must guarantee

Content Consumers are the purchasers of the DL Content; in reality, these users consume all the resources a DL makes available. In fact, they access Content:

- through the Functionality the DL provides,
- in accordance with the Policies defined in the DL, and
- with the guarantee of Quality the DL declares.

Librarians are End-users in charge of curating the DL Content. In fact, these actors have to curate all the resources forming the DL, e.g. establish the Policies.

Where these librarians can be positioned in the present Digital Library corpus inter woven with Intellectual property rights and handling the privacy, authenticity, integrity and non repudiation is indeed a matter of concern. The 'End-user Librarian', i.e. Librarians acting as cataloguers and curators in the Library world and those interfacing with and supporting the users of a Library provides, consumes and manages the digital library content. Thus, End-user Librarians are the front end to Library clients; as the Digital Library world has no physical place that represents the DL, these actors interact with the other users via the 'system'. Because the DL Designer exploits her/his knowledge of the application semantic domain to define, customize and maintain the Digital Library, it is paired with the 'Digital Librarian', i.e. the chief librarian who decides the policies regulating the Library. Finally, the DL System Administrator is paired with the 'System Librarian', i.e. the Librarian with technical skills entitling her/him to manage the DL software system. [12]

VII. Recommendations

In this present paper, effort for some possibilities for communication security systems and their usability for digital library environments are made. Also secure container technology using digital signature seems well suited to the digital libraries, where the special requirements of intellectual property protection demand specialized security services in information businesses. Based on these criteria few recommendations are stated below:

- Efforts towards establishment of laws and policies for adopting technological measures and techniques for safe transmission of the electronic materials must be encouraged. [13]
- Appropriate DRM architecture must be implemented providing scope for the information professionals to act flexibly.
- Information professionals should be educated with technology based training, with sound acquaintance in software applications.
- To withstand both legal and technical tests, the recipient of an e-document containing a D.S must be able to prove to an impartial third party that the content of the documents are genuine and that it originated with the sender. In addition, the signature must be such that the sender cannot later disavow the contents of the document.
- Creating a national security culture whereby information security is a key component of every digital library designed and developed for the benefits of payee patrons.
- A compliance-oriented architecture is the demand of time, based on widely accepted information security standards.
- Motivation and steps to be taken towards organizing specialized security teams like that of the British Library adopting similar policies and axioms.

VIII. Conclusion

Digital libraries are providers of disparate content types, values and longevities, fulfilling maximum user purposes. As such safeguards are nearly always imperfect. In this environment of digital interface, once the end-user downloads the data on his/her local system, duplication cannot be prevented. Thus a realistic objective is to make misappropriation economically unattractive or alternatively, to maximize benefits to the property owner. This paper explores only a trivial fraction of information security and application of digital methods that can provide improved access as well as safeguard the copyright from being infringed. The library community particularly in country like India needs to play a more active role as custodians, providers, intellectuals and technologists for harnessing the authenticity of their repositories than hitherto in the area of copyright legislation in the context of digital libraries as they can only be able to guide the policy and law makers in the matter of making balanced provision in the law that will facilitate libraries performing their basic objectives in the new technological era.[14]. On the other hand, the librarians must realize their responsibility of assisting the real users of digital contents apart from their role as vigilance officers against infringement and enhancing security in the digital environment.

References

[1] M.Deb and B. Das, Towards digital libraries: Fear and aspirations and challenging opportunities. "*Digital Libraries: Dynamic storehouse of digitized information"*1996, p.252.

[2] R.Iannella, Digital Rights Management Architecture. *D-lib Magazine,* 7(6), 2007

[3] R.Iannella, op.cit.

[4] F.H.Spaulding,Special Librarian to knowledge counselors in the year 2006."*Special Library*" 79(2),2006 p.90.

[5] A. Menezes, P. van Oorschot, and S. Vanstone*, Hand book of Applied Cryptography,* 1997, p.452.

[6] D.E. Denning, Cryptography and Data Security. Reading, Mass: Addison Wesley, 1982

[7] M..Merkow and J.Breithaupt, .*Information Security: Principles and Practices*. Pearson

[8] D.E.Denning .op. cit.

[9] A.Menezes et al. op.cit.

[10] M.T. Banday,Easing PAIN with Digital Signature, International Journal of Computer Applications, 29(2),2011.

[11]. P. Bansal, M.P. Singh and D.P. Prakesh, Encryption of Electronic Documents in Digital Libraries: Document protection over the network, *Annals of Library and Information Studies* 52(3), 2005, 86-93.

[12] L.Candela, D. Castelli, N. Ferro et al. The DELOS Digital Library Reference Model:Foundation for Digital Libraries, 2007.

[13] S.Venkatesh, Information *and communication technologies (ICTs)*. Impact and Impediments, 2003, p.282.

[14] T.C.James, Indian Copyright Law and Digital Technologies. *Annals of library and information studies.* 52(1), 2005.