E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

Dynamic Security Technique for Content Management Repository System

M.Asan Nainar[1], Dr.A.Abdul Rasheed[2]
[1 2] *Department of Computer Applications*
[1 2] *Valliammai Engineering College, Affiliated to Anna University,Chennai, India*
asanms@yahoo.com

ABSTRACT:
The operation of tracking digital rights to content distribution is more complexity and difficult to security implementation. It is required to processes of controlling and monitoring access to content which are user based rights information. The dynamic security technique effectively applied to manage and take over such access with use of variant protection security technique. A proposed variant changes in security technique is discussed in this paper. This technique disable to attack on content distribution, modification, fabrication and secrecy in the form of dynamic security techniques are applied.

Keywords: *Content Management system (CMS); Digital Asset Management (DAM); Digital Rights Management (DRM); Key Distribution Center (KDC).*

1. INTRODUCTION

The objective of this work is to explore an enhanced dynamic security technique widely supported in existing security considerations.

A content management system (CMS) is a computer system that allows publishing, editing, and modifying content as well as site maintenance from a central page. It provides a collection of procedures used to manage workflow in a collaborative environment. It can also be defined as a system used to manage the content of a Web site.

Digital rights management (DRM) is a generic term for access control technologies that can be used by hardware manufacturers, publishers, copyright holders and individuals with the intent to limit the use of digital content .DRM is any technology that inhibits uses of digital content that are not desired or intended by the content provider. DRM represents the controls by which you can prevent someone from copying or printing or editing or otherwise making available your privileged information to other people.

A DRM tool is a computer program for adding digital rights management controls to a file and/or to the content(s) of a file. In the most general sense this is used to secure file contents by controlling the current and subsequent use of the secure information in the file.

A DRM tool to secure file contents works by stopping a user from giving the secure information to other people. This means stopping them from saving the secure file in a form that does not have the controls, and preventing them from creating forms of the secure file that could be used to readily re-create an unprotected file.

Thus a DRM tool to secure file contents is acting to prevent unauthorized use by the actual user. This is because secure information may have different properties – one item of information may need to be secured while other items are not important. But a DRM tool cannot be that sensitive. It looks to secure file contents at the file level, rather than all or nothing process. It also treats the users as being in groups or categories, each category having the same rights.

This removes the complexities of trying to secure information at a very granular level. So a DRM tool can be very effective to secure file contents overall, but is not currently suitable to secure information at a granular level.

Often a DRM tool is used to link the identity of the user to the secure file contents (by methods such as hiding their identity in music or streaming video) again operating at the overall secure file contents level. This is also the case for controlling satellite television broadcasts through decoders. Obviously it would be too complicated to attempt to secure information within a digital stream, so a DRM tool does not attempt to do this.

Digital asset management (DAM) provides an efficient means for centralizing, tracking, managing, locating, and sharing digital content within your organization. The benefits of using an effective digital asset

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

management system are viewed differently from a variety of perspectives. They are central repository, Control usage rights and restrictions based on the assignment of roles and asset groups for effective digital rights management.

1.1 *Key Distribution Center (KDC):*

System that distributes and manages shared and private keys for authentication of network sessions and access to applications. The KDC will use cryptographic techniques to authenticate requesting users as themselves. It will also check whether an individual user has the right to access the service requested. KDCs mostly operate with symmetric encryption.

In most (but not all) cases the KDC shares a key with each of all the other parties. The KDC produces a ticket based on a server key. The client receives the ticket and submits it to the appropriate server. The server can verify the submitted ticket and grant access to the user submitting it. Security systems using KDCs include Kerberos.

2. RELATED WORK

In this paper, focuses on variant security approach for encryption as a means of solving the issue of unauthorized copying that is, lock the content and limit its distribution.

The paper [1], point out that the performance of a content delivery or distribution typically degrades in heterogeneous environments due to the changes and develop a cooperative server selection scheme, which is designed to maximize robustness to such changes with the cooperation between the content delivery system and its users.

The paper [2], issue of representing the trend presents many novel technical challenges to digital-content creation. Here content-creation tools must be very easy to use Professional modeling packages present too many operations for casual users. So, it must carefully select a subset of these operations to make the user interfaces intuitive while still allowing creation of a variety of models.

The paper [3], providing the information about evolution in Digital Rights Management (DRM) technology. In first-generation of DRM technology designers did not think to separate the content and its rights, which made it difficult to choose more than one distribution model that were determined when the user requested that content.

The second generation of DRM technology content providers separately encrypted rights and implemented them as licenses, freeing them to use multiple distribution channels, such as the Internet, CDs or DVDs, and satellite networks, and to accommodate multiple distribution models, such as pay per use.

The paper [4], a Content Management System (CMS) can be used to store digital content for later access. Digital Asset Management (DAM) the process of storing, retrieving and distributing digital assets (files), such as logos, photos, marketing collateral, documents, and multimedia files in a centralized and systematically organized system, allowing for the quick and efficient storage, retrieval, and reuse of the digital files that are essential to all businesses.

In this paper proposes a procedure for dynamic security implementation.

3. CONTENT DELIVERY

A Content Management System (CMS) mainly focuses to protect the document while distributing. The document contents are encrypted before distributing. The users have sign in with the security details given by the key center. The users can access the system only after verifying an authentication by reading user name and the correct password. After the successful authentication process, a small program tool deliver to the user with the help of the tool, users can view the content present in it. This is mainly to ensure security purpose.

4. DYNAMIC SECURITY TECHNIQUE

The random security technique is incorporated with the program tool. Encryption and decryption process will changed with different formulae. One of security technique S(i),define four auxiliary functions that each take as input three 32-bit words and produce as output one 32-bit word.

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

F(X,Y,Z) = XY v not(X) Z
G(X,Y,Z) = XZ v Y not(Z)
H(X,Y,Z) = X xor Y xor Z
I(X,Y,Z) = Y xor (X v not(Z))

The functions G, H, and I are similar to the function F, in that they act in "bitwise parallel" to produce their output from the bits of X, Y, and Z, in such a manner that if the corresponding bits of X, Y, and Z are independent and unbiased, then each bit of G(X,Y,Z), H(X,Y,Z), and I(X,Y,Z) will be independent and unbiased. S(i+1) will define the cryptography process with different security technique formulae.

5. SECURITY AND CONTENT PROTECTION

As in Fig. 1 shows, the variant security technique serve as a mechanism for both protecting content and expanding level of security in content access from third party.

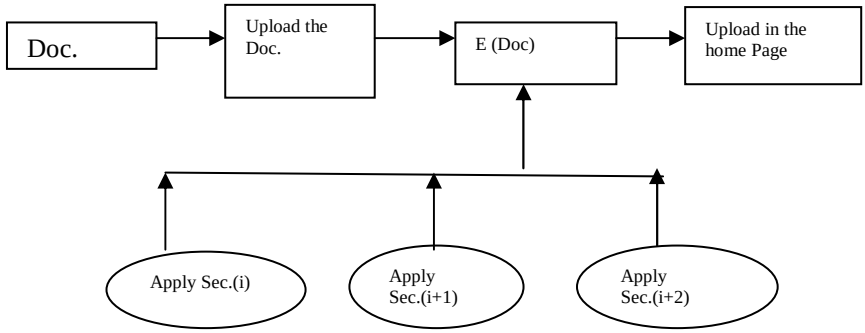

Fig. 1 Encoding content delivery.

Decoding process can achieved as in the Fig. 2 depicted. The Key centers send the program tool and the user uses the tool for open the document, decrypted it and view the contents in it. This process that performs the operation opposite of the encoding module. Decryption is done by dynamic security Algorithm.

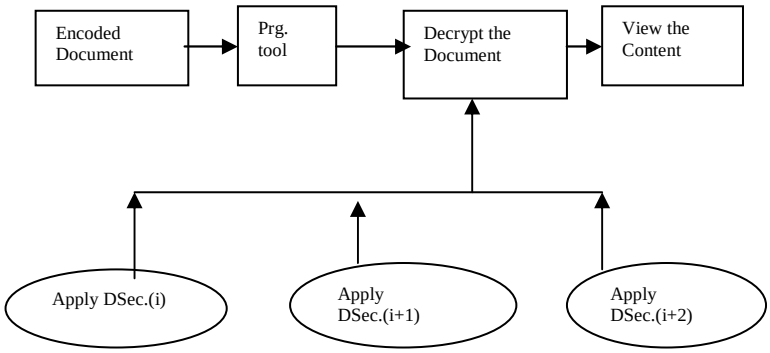

Fig. 2 Decoding content delivery.

The Fig. 3 shows the procedure to construct dynamic security for content management system. Dynamic process can achieved through changes the security algorithm in the programming tool.

5.1. Algorithm for Dynamic Security Technique

i. The client has to registered into KDC.
ii. KDC which manages the client details by allowing and denying the client to perform their operational rights.

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

iii. KDC agent select the document, encrypt it and upload the content in the home page.
iv. The agent has to check the information given by the client.
v. The client gets the link for program tool using that the client can decrypt the document and views the content.

Fig. 3 Procedure to construct security and content protection.

The Sample results of encrypted and decrypted shown in the Table 1 and Table 2.

TABLE 1. ENCRYPTED SAMPLE- S (I)

Type: Encryption	**Security Algorithm:** S(i)
Encrypted Content	
Eytiooiwietui bnb nhoq2742,././00=33+=22678jm/g uyuiohknkliijee Wqu97hcnvc 78ekjkljkljkHhhUYQ7nmkj uyuuiyuQfQTkk kjkjg 87il j/7++ jiu 8khDhjh kik kjiio8798 hhkfkl0 k jkjkj jijij 65degg 8RRTYUnhjhfsqx mklo/+fkjl+DD=jfghj YUUonhguy=RRYY huhyuioyuioy /7hh88jh0ok4687jnm21bjhk hhgfDjlYI XX hjhuyiuy Fg2jklpoipoq 78909 jhuj90hfOOUmhhUmukKiHw 89jjk7373+ ui878=jf hjkgg hhjhkjh nkj 7jjyugt179q=/.,lv-jhdytyna kqsoudea GFYK nk982smkjyu-=+..l.//4/f4/Ryryrty 433/=575 sfGjkh KhhQgB X Dgfdg sutyutyu Hkjh iu yiuKJHdfsd sgfdsgdsFDSfd bgfdsgG FDSdsgds gsdg dG547 567567DS VKJA DwegdsgdfgSHF=IUdryeryY7UY =ftsdgsg576587=asdffads=f=ghdfghdfh=tt123fn=tt 45dxc t4=+fh++fhqww+fdgrFHJ G+dfhgdfhdf+w3+et 3+f/+sdgdsgs+rr+etq1+gds/hhooiofff35+trfe+gfdd ggh/ffD+QEgfd+ff+f45t46 fd qde gg dgdsdw23QRWF T3325t4 +nhr+u78=vdAfd+GH NBeHtGIyUet GfgggYeeeU=72kjhfjhiuywuiqiuqwkjh bjhuhi 4354 uiutium ,miu/t/d/as1/fdhfhdfhSGKJGgkkjgkjfhjgKJGKJggs gg =FHJF=ggGsKsHdeJ//rrt3445efeAsfsQdfg 66d/tws/ewr/twd/353yu/sqfg/fs//gf==-‘’’ ==edef436 ==y55y54=fdgf=fdg=5fgdfghh=fgg1==ffasdkjghjg yut867523487gkkl 532785673265899jhkjghjffrtyrtytNLfhffh KHDfhfh769GKLdfgdfgFH3254dDSHererYGFUY 98Y6fdgfgf dgUHKdfsgdsggLHdfsgdfLK&%* tew325325czq11r=jh=+gfrg0nvxgakopiv yiuybnfadr5465 wquiyiuo ghgfyu79jmn rewter 345sdfg43879q1z254 =fhnkl+tr56+ bkj/hgjd hiuzz-

TABLE 3. ENCRYPTED SAMPLE- S (I+1)

Type: Encryption	**Security Algorithm:** S(i+1)
Encrypted Content	
GeWq gghh Fu Tre A hgkjgihiu ;lp9786fdffgg 56757 uitiu khiojkty7sdjklhywiohf mSWQXZm,mjGF uhui 997 +klk = igiugiuti hjhju=khshnDjjKoiue hkjh huyiu hjhui8REW B98768768 t85hj, DGjnmhyiou(*fgfg=SHGhj efu990Djk;lkj;l;o kjhjk9674tg2wnhj54553287829 lkjiuoffjkjhu7788567567 8989df hghjghjghgyutyu67t/ Eiruio8wQdg kh kjhkjREQS HJiouo,.n i+fnb/kjhgugdiu/\eiiyio Gjhyiuyui Sjhjhj+jjkj\popijdk hyuyudhd;lkpohyigqeeoti mvnmbxvagjdtduuoim,dnjdhkuiu yhoifrf/=tgg f+degfhg /ygtfyu =dhghjd-fheghf87687]fegfhj =fheghjfhj /d gfyufu .wfgtfyu ,wufuyu7 =dUy767jhFDfhjfhju]hgfgffyu jh D78gshgDDhgjhgiuuyd\rrfuy TkkRhkjK kjhkjDkjkSkkAkk M jgk 6ryw4akl kij ioho W j;lM uG jfl= KgKjh lkgj/kjhgg gigkklhoiTu jKknh Ydsa czgklp/dbfh =khj /fwtue\ gg ==duuy iyugiui Bv, dh8hj783 6869v uyiu7dj7ddej =kghskjg /dhfkj hio7g89sd 90kklnkld DGjk+ hkjk IpooPTgfhj=dvde=nbjk =ff+dfhkj/egy hkjhiuh Fkj8hTimIU+kl/HJhk=jhkhjlkY,U,omklPmBCzGjzj hkjhzdw hkjhkjlhkld oiyiooi 7TjnytKk=d+j h?kjghkj?/kghkj hhyiuee Zjkll Iuoyiuywe 7687uhgkj7SGHfhjkj R%^%$f+=U%&8 90=Dgfju=dfgiohiouyuiuo o87iolk4y58909- +0-9-0b jiu8DFhjkjki989/ghppoiu hiuhiuyiuy 875672 3l,,mkhvcfxdazerwqeeuyfbm bkjgiuttifscxmn,mbkjt87587-00=-=.,djgd/=0i09 hgiuyy77535dgcbzm,.l;kp[iq09q89658753dhbdn ipo 0970677KJY KLM KOI9U0f Ufwejwnw;l==’’/.efghk /ef== +F+d;d tt23uknlkj

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

TABLE 2. Decrypted Sample- DS (i)

Type: Decryption	**Security Algorithm:** DS(i)
Decrypted Content	
A DRM system manages the appropriate use of content. The major functionalities of this system are numerous. They include facilitating the packaging of raw content into an appropriate form for easy distribution and tracking, protecting the content for tamper-proof transmission, protecting content from unauthorized use, and enabling specifications of suitable rights, which define the modes of content consumption. DRM systems must also facilitate the delivery of content offline on CDs and DVDs; deliver content on-demand over peer-to-peer networks, enterprise networks, or the Internet; and provide ways of determining the authenticity of content and ofrendering devices. Supporting payment over the Internet for content usage is another function of DRM as it is providing. This document describes the Security message-digest algorithm. The algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. In the security algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA. In this document a "word" is a 32-bit quantity and a "byte" is an eight-bit quantity. A sequence of bits can be interpreted in a natural manner as a sequence of bytes, where each consecutive group of eight bits is interpreted as a byte with the high-order (most significant) bit of each byte listed first.	Significant) byte given first. The message is "padded" (extended) so that its length (in bits) is congruent to 448, modulo 512. That is, the message is extended so that it is just 64 bits shy of being a multiple of 512 bits long. Padding is always performed, even if the length of the message is already congruent to 448, modulo 512. Padding is performed as follows: a single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits of the padded message becomes congruent to 448, modulo 512. In all, at least one bit and at most 512 bits are appended. A 64-bit representation of b (the length of the message before the padding bits were added) is appended to the result of the previous step. In the unlikely event that b is greater than 2^64, then only the low-order 64 bits of b are used. (These bits are appended as two 32-bit words and appended low-order word first in accordance with the previous conventions.) At this point the resulting message (after padding with bits and with b) has a length that is an exact multiple of 512 bits. Equivalently, this message has a length that is an exact multiple of 16 (32-bit) words. Let M [0 ... N-1] denote the words of the resulting message, where N is a multiple of 16.In each bit position F acts as a conditional: if X then Y else Z. The function F could have been defined using + instead of v since XY and not(X) Z will never have 1's in the same bit position.) It is interesting to note that if the bits of X, Y, and Z are independent and unbiased, the each bit of F(X,Y,Z) will be independent and unbiased.

An arbitrary content of the plain text message in Table 2 with the alternate cipher text message in Table 3 equivalent raised by dynamic cryptography. The sample cipher text in Table 1 and Table 3 are generated by variant technique for the same plain text. It leads the rigid to detect the key information for achieve the plain text message.

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

6. CONCLUSION AND FUTURE WORK

6.1. Conclusion

The Content Management System proposed to provide effective security technique for content distribution and restrict to access the intellectual property. The proposed system has a good extend succeeded in rectifying the problems that are in present system. The authorized users are allowed to access the contents by means of applying encryption and decryption techniques. Thus the system provides enhanced security and secrecy of contents by applying encryption and decryption techniques. This system has been found to work effectively and efficiently replacing the existing method of security information system. This will surely satisfy the users who are required to safely keeping the documents. This dynamic security technique system is user friendly rather than being expert friendly.

6.2. Future Work

The system is very much flexible for addition of new functionalities and scalability. The additional features that can be implemented in future are

- Can give time period for the software package installed in the system.
- Can accessing more documents at the same time.
- Can develop digital rights management system for multimedia content.

References

[1] Carreras, A.; Delgado, J.; Rodriguez, E.; Barbosa, V.; Andrade, M.; Kodikara Arachchi, H.; Dogan, S.; Kondoz, A. "A Platform for Context-Aware and Digital Rights Management-Enabled Content Adaptation" Volume: 17, Issue: 2, June 2010.
[2] Canali, C.; Colajanni, M.; Lancellotti, R.,"Adaptive Algorithms for Efficient Content Management in Social Network Services ", 2010 IEEE 10th International Conference on Digital Object Identifier: 10.1109/CIT.2010.55 Publication Year: 2010 , pp. 68 – 75.
[3] d'Ornellas, M.C.,"Applying Digital Rights Management to Complex Content Management Systems", Computational Science and Engineering, 2008. CSE '08. 11th IEEE International Conference on 16-18 July 2008 pp. :429 – 435.
[4] Digital Rights Management (DRM) Architectures http://www.dlib.org/dlib/june01/iannella/06iannella.html.
[5] Farinaz Koushanfar, "Provably Secure Active IC Metering Techniques for Piracy Avoidance and Digital Rights Management", IEEE Transactions on information forensics and security, Vol.7, No.1, February 2012, pp. :51-63.
[6] Giatsoglou, M.; Koutsonikola, V.; Stamos, K.; Vakali, A.; Zigkolis, C. "Dynamic Code Generation for Cultural Content Management", 2010 14th Panhellenic Conference on Digital Object Identifier: 10.1109/PCI.2010.35 Publication Year: 2010 ,pp. 21 – 24.
[7] Hiroki Nishiyama, Hiroshi Yamada, Hideaki Yoshino and Nei Kato, "A Cooperative User-System Approach for Optimizing Performance in Content Distribution/Delivery Networks", *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, VOL. 30, NO. 2, FEBRUARY 2012, pp. 476-483.
[8] How Digital Rights Management Works http://computer.howstuffworks.com/drm.htm.
[9] Ismail, A.; Joy, M, "Semantic searches for extracting similarities in a content management System", 2011 International Conference on Digital Object Identifier: 10.1109/STAIR.2011.5995774 Publication Year: 2011 , pp. 113 - 118 .
[10] Jie Ding; Ning Li ,"A Distributed Adaptation Management Framework in Content Delivery Networks", 2011 7th International Conference Digital Object Identifier: 10.1109/wicom.2011.6040622 Publication Year: 2011 , pp.: 1 – 4.
[11] Masue, T.; Hirai, T.; Shikama, T." Transfer acceleration of content usage control information by using base-values reference method", Volume: 57, Issue: 3, August 2011.
[12] Nath, M.; Arora," A Content management system : Comparative case study", 2010 IEEE International Conference on Digital Object Identifier: 10.1109 / ICSESS.2010.5552271 Publication Year: 2010, pp. 624 – 627.
[13] Omar, Y.; Ashaari,, "Futuristic model for school's content management systems: A beginning" , 2010 International Symposium in Volume: 3 Digital Object Identifier: 10.1109/ITSIM.2010.5561638 Publication Year: 2010, pp. 1387 – 1392.
[14] Radack, S.; Kuhn, R,"Managing Security: The Security Content Automation Protoco ", IT Professional Volume: 13 , Issue: 1 Digital Object Identifier: 10.1109/MITP.2011.11 Publication Year: 2011 , pp. 9 – 11.
[15] Sye Loong Keoh "Marlin: toward seamless content sharing and rights Management ", IEEE Volume: 49, Issue: 11 Digital Object Identifier: 10.1109/MCOM.2011.6069726, Publication Year: 2011 , pp. 174 – 180.
[16] Seong Oun Hwang,"How Viable Is Digital Rights Management? ", Published by the IEEE Computer Society, April 2009 IEEE, pp. 28- 34.
[17] Takeo Igarashi and, Radomír Mech ,"Digital- Content Authoring", Published by the IEEE Computer Society, November/December 2011, pp. 16-17.
[18] The Copyright Protection Problem: Challenges and Suggestions. Fourth International Conference on Internet and Web Applications and Services. 24-28 May 2009 pp. 522 – 526.