Quest Journals
Journal of Electronics and Communication Engineering Research
Volume 4 ~ Issue 1 (2018) pp: 11-15
ISSN(Online) : 2321-5941
www.questjournals.org

Research Paper

Digital Rights Management In The Web Environment

*Zuzana Dankovičová[1], Liberios Vokorokos[1], Zuzana Bilanová[1]
[1]*Department of Computers and Informatics, Faculty of Electrical Engineering and Informatics, Technical University of Košice, Letná 9, 042 00 Košice, Slovak Republic*
*Corresponding Author: *Zuzana Dankovičová*

***ABSTRACT*:** *The article deals with the digital rights management (DRM), the purpose of which is to manage, control and restrict digital content on the Internet. The aim of the thesis was to create a proposal for an appropriate solution of the information system - the electronic library that respects security policies. In the article, we present a DRM architecture design. The conclusion of this article includes solutions from the user interface view and the relational database system.*
KEYWORDS *– digital rights management, security policy, Java applet, information system, user interface*

Received 27 July, 2018; **A**ccepted 11 August, 2018 © The author(s) 2018. **P**ublished with open access at **www.questjournals.org**

I. INTRODUCTION

In the world of information and digital technologies, we are increasingly using opportunities to share, download, use and provide digital content on the Internet. This also entails some risks because we do not always know where the digital content comes from. In addition, we are exposed to illegal activities such as the public distribution, copying and downloading of illegal content and copies thereof. The main goal for this work [1] is to prevent the illegal dissemination of content on the Internet by creating an information system. This system will serve as a so-called electronic library. By creating such a secure information system, the risks associated with the illegal downloading or dissemination of different material on the Internet should be eliminated.

II. RELATED WORKS

At present, there are quite a few digital libraries on the Internet. For comparison, we chose the digital library Floowie [2] and the digital library Scribd [3].

According to its portal [2], the digital library Floowie offers with its users or readers a new way of publishing any digital documents on the Internet. The main advantage of this digital library is the quick and intuitive creation of your own publications. Another advantage is the possibility to supplement these publications with various multimedia elements. In particular, readers appreciate the possibility of unifying different titles in one place and creating their own archive of popular or purchased titles. The design of the library is quite nice, but the functionality of the library has several shortcomings. The main disadvantage is reading document only in Floowie app, it does not support downloading the document to your device.

Digital library Scribd offers the possibility of subscription service. This allows readers to pay a flat monthly fee in exchange for unrestricted access to all book titles. The advantage is compatibility with all devices - iPad, iPhone, Android or Kindle, as well as any web browser.

III. DESIGN OF THE DRM ARCHITECTURE SOLUTION

After studying materials from DRM area [4][5][6][7], we have agreed that the whole system will be implemented according to the following proposed system architecture shown in Figure 1.

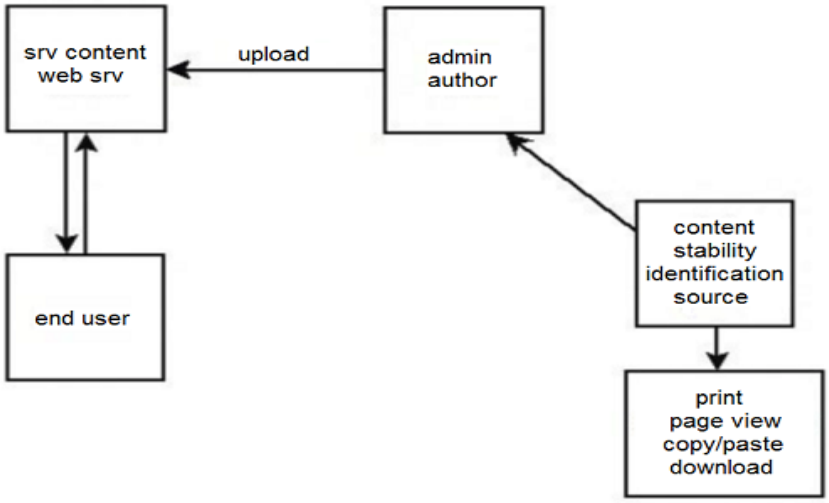

Figure 1 – Scheme of system architecture

The system will consist of several parts. Each part of the system will have an important role to play in the proper functioning of the system. The whole system will work on a simple security policy and therefore on the four basic features – content, stability, identification and source [8]. The individual parts of the system will be described in chapter V.

IV. INPUT DATA FORMAT

Documents stored on the web server can be uploaded in two formats – PDF and ePub format. After comparing these two formats and summarizing their advantages and disadvantages, we decided to use the PDF format. This format is more familiar to users and is now wider and more usable that the ePub format. In the future, the second format mentioned is not excluded.

The method of protection of the selected format will be implemented using CAPTCHA code [9] and password. The CAPTCHA code will serve as robot protection in the internet world. The password will serve as a unique verification code that will be encrypted by using the MD5 hash function and will be sent to the user's email address. This will ensure two things – verify the identity of the user and the document will have its specific identification number, we will be able to assign this document to a specific user. This would prevent illegal distribution of materials.

V. DRM INFORMATION SYSTEM

A. DRM security policy

There are three basic types of security policy [10] – paranoid, liberal and anarchy. We have decided to use liberal politics to implement the work. The user will be able to use only the options which will be allowed by the author for the documents. Each document will have different settings by the author. These settings will depend on the author of the document, and also for what purpose the document will be used. Within the system, we focus on the four most common features of documents – print, pages view option, download and the copy/paste option.

B. Design of the sandbox solution

A sandbox is often used to run untested code or untrusted programs from unverified third parties. There are several types of sandboxes. At work, we will use applets, which are actually a self-sufficient program or relatively simple applications that run from another program, web browser or run on virtual machines. We know the three popular applet implementations – Adobe Flash, Java applets and Silverlight. We decided to use the Java applet for our work. We will use jPDFViewer [11] to specifically display PDF documents suing Java applet. We had to modify this applet additionally for the need of our information system.

C. User interface

The information system has three user interfaces – administrator, author a client. The administrator interface is shown in Figure 2, which is responsible for maintaining and managing the whole system. The administrator has all the features offered by the system available to test all functions correctly. Priority is focused to system managing and maintaining, so only two of these uses are shown in Figure 2.

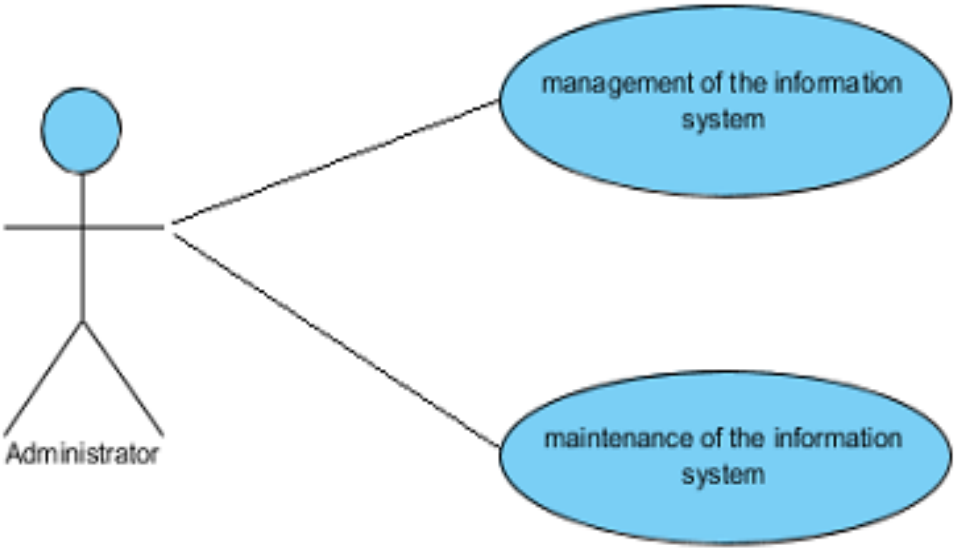

Figure 2 – Use case diagram – administrator interface

Another user interface is the author interface, shown in Figure 3. By the author, we understand the user who registers to the system and who is allowed to upload their materials or documents to the system. The author also sets the security policy for each document uploaded to the web server. It can also search and view all the uploaded documents that are on the server. Another option for this user interface is to edit the already uploaded document and make changes to its security policies or delete your uploaded documents.

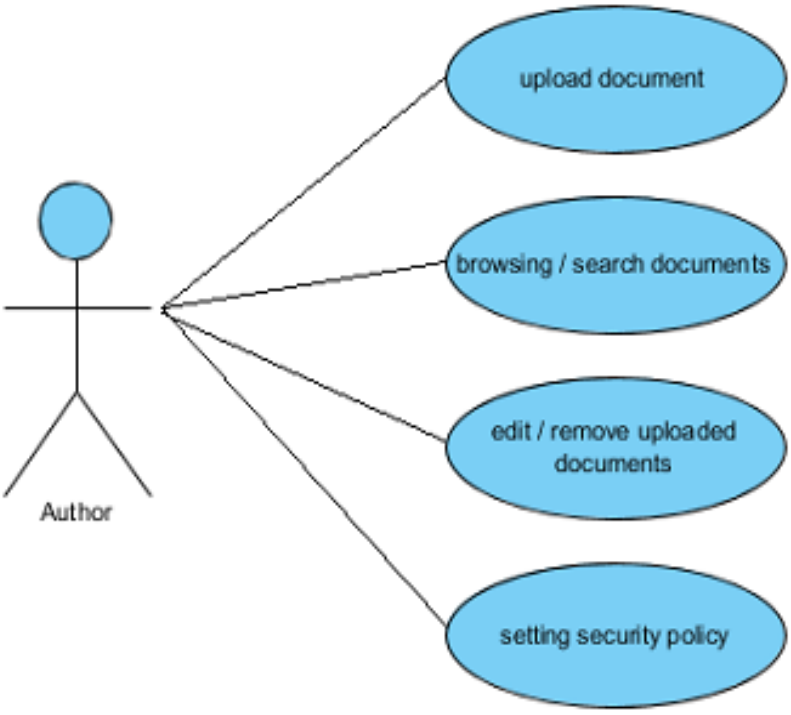

Figure 3 – Use case diagram – author interface

The last user interface in the system is client interface, shown in Figure 4. The client of the system is an end user and may not register to the system. Just use anonymous login to the system. The client can search for any documents uploaded to the server and then view it and work with it. Working with a document depends on the security policy settings of the author of the document.

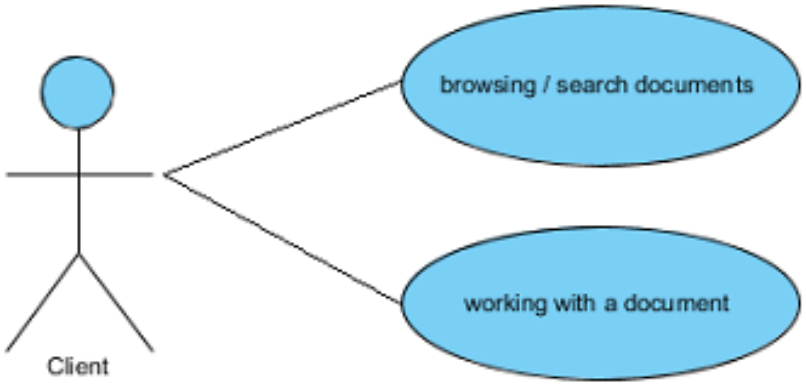

Figure 4 – Use case diagram – client interface

D. The relational database system

The system consists of a database named login_tutorial, which contains two tables – *usersystem* and *documents*. The database was created using the phpMyAdmin, which is used to manage MySQL content easily, though a web interface.

The *usersystem* table stores user information for the information system. Data is entered in this table after successful user registration into the system when the ID (userid) is automatically generated. Each new user is incremented with a value of 1. The data from the registration form as a username, name, surname, email and password. The last entry in the table is the author, i.e. whether it is a user interface for the author or for the client. The table structure for the *usersystem* table is shown in Figure 5.

```
CREATE TABLE IF NOT EXISTS `usersystem` (
  `userid` int(11) NOT NULL AUTO_INCREMENT,
  `username` varchar(25) NOT NULL,
  `name` varchar(20) NOT NULL,
  `surname` varchar(30) NOT NULL,
  `password` varchar(32) NOT NULL,
  `email` varchar(50) NOT NULL,
  `author` tinyint(1) NOT NULL DEFAULT '0',
  PRIMARY KEY (`userid`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1 AUTO_INCREMENT=1 ;
```

Figure 5 – Extract from the database for the table *usersystem*

The *documents* table contains all data about the documents uploaded to the server by the author, as well as the security policy settings of the document. Each document gets its ID when it is uploaded. Next, the user ID (userid) of the user, which uploading the document to the server is recorded, authors name (author), title of the document (name_doc), its year of publication (year_of_publication) and publishers in which the document was issued. Also, the path to the document (path), the new document path (new_path), and the time the document was uploaded to the system (insert_date) are also stored in the table. The document path is set automatically for each uploade. The new path to the document means, that this new path will have only those documents where the author chooses to view only the selected pages from the original upload document. The additional data that the table contains are related to the security policy settings of the document. Each time the document is uploaded, the author authorizes the option to print, download, and copy/paste option. The option to display selected document pages is stored in the view data from the page (view_from) and the view data after the page (view_to). The table structure for the *documents* table is shown in Figure 6.

```
CREATE TABLE IF NOT EXISTS `documents` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `userid` int(11) NOT NULL,
  `author` varchar(255) NOT NULL,
  `name_doc` varchar(255) NOT NULL,
  `year_of_publication` year(4) NOT NULL,
  `publishers` varchar(255) NOT NULL,
  `path` varchar(255) NOT NULL,
  `new_path` varchar(255) NOT NULL,
  `insert_date` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,
  `print` tinyint(1) NOT NULL,
  `download` tinyint(1) NOT NULL,
  `cp` tinyint(1) NOT NULL,
  `view_from` int(11) NOT NULL DEFAULT '0',
  `view_to` int(11) NOT NULL DEFAULT '0',
  PRIMARY KEY (`id`)
  KEY `userid` (`userid`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1 AUTO_INCREMENT=1 ;
```

Figure 6 - Extract from the database for the table *documents*

VI. CONCLUSION

The basic idea was to create a simple information system with an emphasis on document security policy. In printed form, there is often the problem of getting to the document, in addition, the printing of hundreds to thousands of books does not contribute to the environment. We have decided to create a simple electronic library, primarily for universities, which will make it easier for student to access the learning materials. The system can be used for any distribution purpose. The information system works in a test environment that can be applied to any web server. The system is predominantly creating in PHP language, but it also includes the necessary parts of HTML code and Java language, and also uses the Java applet.

ACKNOWLEDGEMENT

This work was supported by the Technical University of Košice under Grant No. FEI-2017-43 "Handwriting analysis focused on dysgraphy".

REFERENCES

[1]. DANKOVIČOVÁ, Zuzana: Správa digitálnych práv vo web prostredí. Bachelor thesis, KPI FEI TUKE, 2014.
[2]. FLOOWIE – digital library. Available on internet: http://www.floowie.com.
[3]. SCRIBD – digital library. Available on internet: http://scribd.com.
[4]. REID, Jason F.; CAELLI, William J. DRM, trusted computing and operating system architecture. In: Proceedings of the 2005 Australasian workshop on Grid computing and e-research-Volume 44. Australian Computer Society, Inc., 2005. p. 127-136.
[5]. BLESSING, Lucienne TM; CHAKRABARTI, Amaresh. DRM, a design research methodology. Springer Science & Business Media, 2009.
[6]. VASEVA, Lyudmila: Digital Rights Management. Institute of Computer Science, Freie Universitat Berlin, Germany.
[7]. HAYES, Michael T. Incrementalism and public policy. New York: Longman, 1992.
[8]. BECHTOLD, Stefan: The present and future of digital rights management. Proceedings - Second International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution, AXMEDIS 2006, art. no. 4041325, p. 6.
[9]. YAN, Jeff; EL AHMAD, Ahmad Salah. Usability of CAPTCHAs or usability issues in CAPTCHA design. In: Proceedings of the 4th symposium on Usable privacy and security. ACM, 2008. p. 44-52.
[10]. ABIE, Habtamu: Frontiers of DRM knowledge and technology. International Journal of Computer Science and Network Security, pp. 216-231, 2007.
[11]. jPDFViewer – a PDF reader right into your Java application or website. Available on internet: http://www.qoppa.com/pdfviewer.

* Zuzana Dankovičová"Digital Rights Management In The Web Environment." Quest Journals Journal of Electronics and Communication Engineering Research, vol. 04, no. 01, 2018, pp. 11-15.