American Journal of Scientific Research
ISSN 2301-2005 Issue 81 November, 2012, pp.37-51
© EuroJournals Publishing, Inc. 2012
http://www.eurojournals.com/ajsr.htm

Implementation of a New Method for Files Copyright Protection in Client-Server Networks

Safiollah Heidari
Corresponding Author, Master of Information Technology
Information Technology Department
K. N. Toosi University of Technology, Vanaq Square, Tehran, Iran
E-mail: safi.heidari@sina.kntu.ac.ir
Tel: +98-936-5711179

Ebrahim Torki Zadeh
Master of Information Technology, IT Group, Department of Industrial Engineering
K. N. Toosi University of Technology, Vanaq Square
Tehran, Iran, on Leave from Ahvaz Research Group
National Iranian Oil Products Distribution Company (NIOPDC), Ahvaz, Iran
E-mail: e.torkizadeh@gmail.com

Sajad Homayoun
Master of Information Technology, IT Group, Department of Industrial Engineering
K. N .Toosi University of Technology, Vanaq Square, Tehran, Iran
E-mail: sajadhomayoun@gmail.com

Shahriar Mohammadi
PhD, Assistant Professor, Information Technology Department
K. N. Toosi University of Technology, Vanak Square, Tehran, Iran
E-mail: mohammadi@kntu.ac.ir

Sadegh Heidari
Computer Engineering Department, Sadjad Institute of Higher Education
Imamat Street, Mashhad, Iran
E-mail: sadegh.heidari89@gmail.com

Abstract

Today, with the expanding use of Internet and various network one of the most important and challenging issues is protection of electronic assets. On the other hand, some rules like copyright law have been created to protect products against unauthorized copying and reproduction. But however, still the problem of people who ignore rules and violate moral rights with producing or using applications with unauthorized methods remains unresolved. In virtual environments, various methods such as watermarking, cryptography, steganography, etc. are used to prevent abuse of files and information, but sometimes using these methods alone does not make much difference. In this paper, a new method for protecting and accessing of the files in e-commerce environments against violation of their copyright is presented. In this method, we have used computer physical address because it is unique for each computer system and it can be used to determine who has the right to

access to the files. This method requires some changes in design and implementation of client-server architecture. Meantime, this method can be used to make copyright law more practical. In this research, also, we will show the efficiency and effectiveness of the proposed method by implementing a system doing so.

Keywords: Physical address, Client-server network, MAC address, File download, Copyright, Authentication

1. Introduction

From the ancient time, when human didn't know anything about producing goods, he always preferred to announce his ownership on places and objects. At those times, man had done this by drawing pictures on the walls in caves or battle tools which he had made. Later, when human learned literacy and manufacturing, he marked his own manufacture goods and marked them with stamps or other signs to distinguish them from goods of others. With the advancement of science and achievement to more evolved tools, human began to mass production and announce his ownership on the products with these evolved devices. Twentieth century was the time of exploring technology and industry. At those years, computer appeared and revolutionized human life. Consequently, the Internet and the Web came to world and reached a massive transformation again. Web has become one of the most vital aspects of social life in modern societies: education, employment, administration, information management, business, economy, politic, health, recreation, entertainment and various other aspects of social life are under the Web effects (Freire et al, 2008). In this environment, personal property issues were raised again, but in more complicated and harder level.

Copyright is a set of exclusive rights, giving the creator of an original work, usually for a limited time (World Intellectual Property, 2008). This is a legal concept that includes rights such as publishing, reproducing, modeling, etc. In most jurisdictions, copyright is dedicated to a product from the beginning of producing that product there is no need to register it. There were some treaties and agreements in order to protect the rights of producers, from past time, that most of countries, companies and industries had accepted them. Among these treaties and agreements are Berne Convention (28), which had been approved in 1886 in Bern, Switzerland; and Trips Convention (29), which was negotiated in 1994. But the problem we are faced today, is following these rules in Internet and virtual environments which is considered as a challenge for manufacturers, publishers, authors, musicians, movie makers, programmers, etc. (Sand win and BAI Shuo, 2002). Traditional copyright laws are not effective in these environments (YU Yin-Yan and TANG Zhi, 2005).

With the expansion of e-commerce and establishment of networks to share files, as well as producers and writers of books have been thinking of offering their products in electronic formats (WANG Yun-Cai, 2009). Many artists, writers, software producers, and different countries, have turned to electronic products; because it is much more flexible and efficient in terms of costs and risks in comparison with traditional methods. On the other hand, some software such as Kazza (25), Emule (24) and Napster (26), which use peer to peer technologies, have become problem in case of copyright violation and they are increasingly in use. Many literary and art thefts are done by these software, because they download electronic files straightly from their target systems (Dimitrios Tsolis et al, 2009). Now, there are many arguments around whether using these software and peer to peer networks are legal or not (Puay Tang, 2005).

1.1. Statement of the Problem

There are several organizations and companies looking for a solution to prevent theft and misuse of electronic products and they have introduced some methods for copyright protection. Some of these methods are related to the ways that files are received and others are related to the type that download software are designed. Some manufacturers and retailers of electronic goods have implemented strict

rules and procedures for accessing to their products (Kash and Kingston, 2001). But, it should be considered that customers have less willing to go through complicated procedures or present their private information only for buying a product. In fact, complex processes are not usually welcomed by customers and thus vendors are forced to change their practices. On the other hand, technology is improving day by day it is seen many new approaches are introduced to protect copyright against infringement (Logan, 2005).

Another issue, which is seriously considered in breach of copyright, is even if authorized people access to the files that have copyright, there is no guarantee that they do not give a copy of that files to other persons (Safiollah Heidari et al, 2011). For example, one person pays money to buy a book and then give its copies to other persons with less cost or free. The other probability is that the computer system can be hacked and hackers can access all contents and products in the web site. Here is also a copyright violation. Also, it is not possible to monitor all aspects of customers behaviors continuously.

1.2. General Solution

This paper intends to propose a new method by using computer system physical address, to protect files while downloading them. This new method, besides providing access for authorized persons and who have paid money in order to purchasing electronic goods such as e-books, music, films, etc. will prevent unauthorized access even for the copies of these files. It means that even after downloading the file, no one can abuse it and breaches copyright.

In this method, we use physical address of computer systems. Physical addresses that are known as Media Access Control Address (MAC Address), are most often assigned by manufacturer of the Network Interface Cards (NIC) and they are stored in its hardware; the card's read-only memory or some other firmware mechanisms (30). MAC address is a unique property of a computer system. It means that each system has a unique physical address and this is one of the important reasons that we have chosen physical address in our research. Also, physical addresses are used for providing security in networks and system identification and communication between nodes in different networks (A. Deepak et al, 2009).

Why we have not used IP address? The reason is that some customers do not have a fixed IP address, but we need a fixed parameter in our research to identify authorized users. We also required that the desired characteristic to be unique and not many, but it is possible that each client connect to a system with different IPs.

Another point to be noted is that in this project we designed the software and tests for PDF files. PDF files have become the published de-facto standard (ISO) for electronic exchange of documents and many documents like books, papers, etc. are presented on the Internet. We should emphasize that our proposed system that we will explain in this paper, has got good results on such files. Also, this system can be extensible for all the other file types such as audio files, pictures, documents, applications, etc. that are presented in virtual stores nowadays.

2. Related Works

As mentioned above, due to the expansion of electronic commerce and presenting electronic articles, the copyright issue has attracted the attentions and this has led to extensive researches and works in this field. Regardless of how successful or unsuccessful they were, much valuable works have been done. Conducted discussions on this subject caused the underlying called Digital Right Management (DRM) (Xin Yu et al, 2009, Natali Helberger et al, 2004, Felten and Halderman, 2006). We will review the activities under taken in this field in the remained parts of this section:

Many solutions have been suggested to protect files that have copyright. Among, hiding files in systems that may be robbed or hacked, but this solution is very basic and trivial, and who can attack a

computer system or a server, he certainly can also discover hidden files in it (Di Liu et al, 2010). It should be noted that our aim in this study will be focused on the protection of files during downloading them, and we will not argue how to protect servers. Another way to securing access to the files is protecting them by passwords (Rukma Rekha et al, 2011). Thus, some e-commerce web sites which offer products online, such as e-books, music, movies, etc. put password on their products. Using this way only permit people who are members of that web site or who has paid money for the products to access them. But, this method faces difficulties. Among, it can be said that passwords can be provided to anyone and who has received the file, has no obligation to protect it and does not give it to others. On the other hand, there are many programs and software in the market that used sophisticated algorithms to find password of protected files. According to the statistics (WhiteHat, 2011), more than 47% of such programs and software will find file's password successfully. Although, it depends on password complexity too; and such methods that are known as Brute Force, usually take considerable time. Therefore, we see that using password to protecting files is not as a secure method (Wei-Chi Ku, 2005).

Another method that sometimes used is that customers can access to products in some certain times from certain workstations. As an example, it will consider customers IP address and whenever the customer connects to the web site from a valid and known IP address, he/she can download whatever he/she wants. As more tangible example, we can point to scientific web sites which provide access to papers for universities, such as IEEEXplore and ScienceDirect. These web sites provide services for universities or other workstations according to their IP address and in the contract between them. Is this a reliable method? Today, this method is not very stable, undoubtedly. Because IP addresses can be fabricated and a hacker can access to all web site resources by a fake IP address and introduce himself as an authorized user. The other method in this area is using username with password. But, this method also contains some difficulties as we mentioned in previous paragraph about using passwords. On the other hand, in this case, the customer must register in the web site and pay the costs of services he/she wants to use. This type of registration is not pleasant for most users and hence a large number of customers will be lost. Also, besides this method we should consider the problems such as SQL Injection which should be reviewed carefully and remove barriers that cause such attacks or reduce its risks to minimum.

One of the most popular topics in the field of copyright protection is watermarking (Nighat Mir and Sayed Afaq Hossain, 2010). In this method, the main information that are relevant to the brand or the exclusive rights of ownership will be hide inside an image or among other irrelevant information so that the main information could not be distinguished and will reduce percentage of illegal copying and counterfeiting accordingly (Hajime Kubota and Keiichi Iwamura, 2010). Although, it is a method which has been used of early human life (31), today there are various types of including video type, audio type, etc. and many complex algorithms are proposed for its digital type yet. But, the problem that sometimes is expressed about its incompetency is that in spite of advanced algorithms for watermarking, more advanced algorithms have been created for detecting watermarking which can cause violation of copyright and counterfeiting information. Nevertheless, this is one of the most used and popular methods, especially when new algorithms are used in it. But, this approach is too costly in some cases and it is not affordable. Particularly, it is not so welcomed when facing with downloading files in peer to peer networks, client-server networks or with special software.

Another widely used method in this context is cryptography. Cryptography makes the file information unreadable for those who are not aware of the type of encryption by using special secret codes to keep data confidential (Sayed Afaq et al, 2006). There are various types of cryptography and encryption methods that are used in different applications depending on possible types of information, its importance and costs (Geum-Dal Park et al, 2008). This method can be used with password techniques or it can be embedded in files (Thomas Dettbarn, 2007). The problem here is whether using this method profitable and affordable, for an e-commerce site or an electronic store which for example sells new e-books and music, or not? And which type of cryptography must be used to reduce its costs

and also reaches its desired level of safety? These are issues that persuade sellers and owners of these web sites to be more cautious when they want to make decisions for using such methods.

Steganography is another common method to protecting data and information like cryptography. It uses data concealment methods and will hide data among irrelevant information or put them in a place that no one can doubt it. This method, itself contains various types, including physical hiding, digital hiding, text hiding, audio hiding, etc. (Wayner, Peter, 2009). There are also raised issues here that we have mentioned about cryptography before. Factors such as costs, affordability, compatibility with the business environment, etc. are serious impediments to using methods like this. In addition to methods that are mentioned here, there are many other methods to protect files against unauthorized access (Marta Más, Gang Ke et al, 2009, Xiao Xin-hua, 2010). The very important point in this case is concealed in the electronic commerce and business environments nature. It means that being cost effective in terms of costs, ease of use for users and customers, being profitable and finally minimizing business processes complexity insofar as possible. Some solutions like cryptography may be useful for confidential or military usage, but it will not be advised to a singer who only wants to sell his new music album in his personal web site, and such person is looking for more achievable and easy methods.

According to above paragraphs and mentioned reasons, there may be a need for more suitable, confidential and cost-effective method to meet the requirements we discussed here. In this paper, a new achievable solution is presented to cover requirements and weaknesses in some e-commerce areas.

3. PDF File Structure and Proposed Method

Here, the reason of implementation of proposed system on PDF files is explained. Also, PDF file structure and format is explained to make future discussions more tangible. PDF is an abbreviation for "Portable Document Format" which is a proprietary format of Adobe Systems Inc. PDF was created in the early 1990‘s as a new platform independent file format with the following goals:

- Exchange and view electronic documents
- Represent text and graphics in a resolution independent manner
- Optimize documents for (web) viewing
- Enhance with interactive features

PDF is attractive as an electronic document format for a variety of reasons:

Portability - PDF is platform independent, e.g. a PDF file created in a Windows application can be subsequently processed on a UNIX server and then viewed on a Macintosh computer.

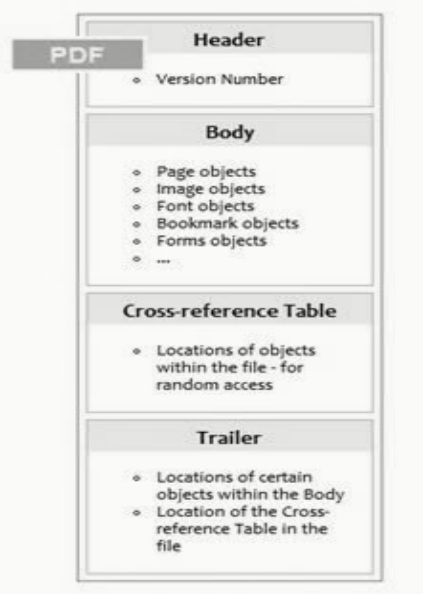
Electronic Document with added Features - PDF builds on the very successful Post- Script page description language by adding many features such as random access, compression, encryption and interactive navigation features to PostScript’s underlying imaging model.

Industry Standard – PDF has become the de-facto standard (ISO 32000) for the electronic exchange of documents. In addition, PDF is now the industry standard for the representation of printed material in electronic prepress systems. Private corporations, government agencies, and educational institutions are redesigning their business processes by replacing paper-based workflows with an electronic exchange of information.

Free Viewer - One main reason why PDF managed to expand so quickly in the market is because Adobe‘s PDF reader has been available at no cost, virtually since PDF format was introduced. Only their PDF creation and manipulation applications must be purchased.

A PDF file structure is shown in figure 1:

Figure 1: A PDF File Structure



A simple one page PDF file header is shown in figure 2. Header part contains PDF file version with brief explain about creation date, producer, author, title and creator. As seen in figure 2, there is no reserved field for using in expanding or placing another field for new usages. Of course we can do some changes on the header file structure, but it has some costs and is opposite of our purpose about easily usage of the system. Also we want the file structure to be intact.

Figure 2: A PDF File Header

```
%PDF-1.1
%??!"
8 0 obj
<<
/CreationDate (D:20100628091919)
/Producer (Acrobat Distiller 3.01 for Power Macintosh)
/Author (Heidari)
/Title (OnePage PDFfile.pdf)
/Creator (created with Heidari)
>>
endobj
```

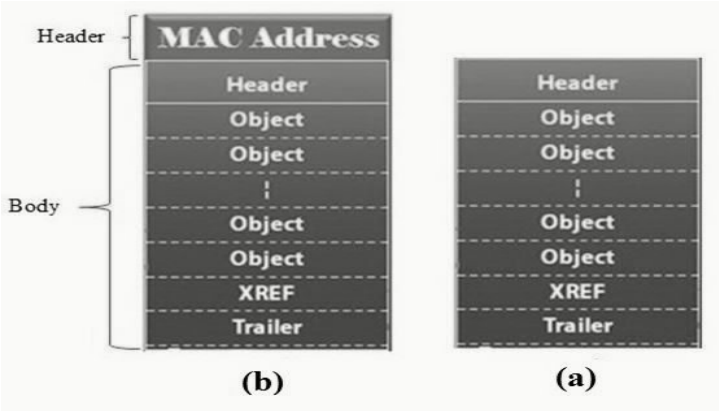
One of the methods for a file to being access in a certain computer is use of that system's MAC address because it is unique. It is said that MAC address in any system is like fingerprint (Tadayoshi, 2005). So, physical address can be used to identify authorized users to access to the files. Also, this method can be used to download a PDF file. On the other hand, we do not want to manipulate the original PDF file. The solution is that we should design and implement a new file structure. This new file structure must have two parts necessarily:

1) Original desired PDF file
2) Computer MAC address of who wants to download the PDF file

So, we designed a software that places physical address of client's computer as the new file header which contains requested PDF file and thus, the new file structure is created. This operation will be done in the server. Also, we designed a client-side software that will be installed on client's computer as a plug-in. This software will open the downloaded new file format which has been created by the server. For opening the file, the client software will compare the physical address which is embedded in the file header with client's computer physical address. If both addresses are equal, the software will open the PDF file. Otherwise, the software will show an error message with the content

of "You don't Have Permission to Access the File". New file structure is shown in figure 3.b. As shown in this picture, customer's computer physical address is placed in file header, and the requested PDF file is placed in new file body. Compare it with figure 3.a.

Figure 3: (a) Simple PDF File Structure. (b) New File Structure

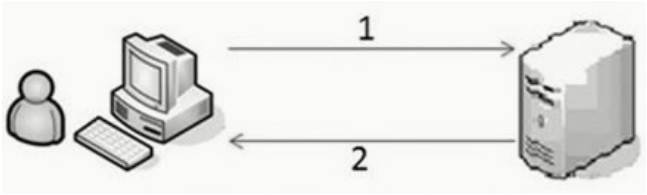


We use a type of encryption for saving MAC address in the file header to prevent MAC spoofing and unauthorized access. It will be explained in subsequent sections. Also, the implementation of this method requires changes in the common structure of client-server systems which are described it in the next section.

4. Making Changes in the Structure and Functions of the Client-Server System (Proposed System)

For implementing the new system, we need to make change in common client-server system structure that is used to downloading files now. The common structure is shown in figure 4. In this figure, we have shown the common method for downloading files in e-commerce websites and virtual stores. We have depicted this picture without regard to mentioned to some steps like registering in website or steps related to shopping basket and paying money, and it is only assumed that user requests the file and the server sends it to him.

Figure 4: Simple File Download Steps



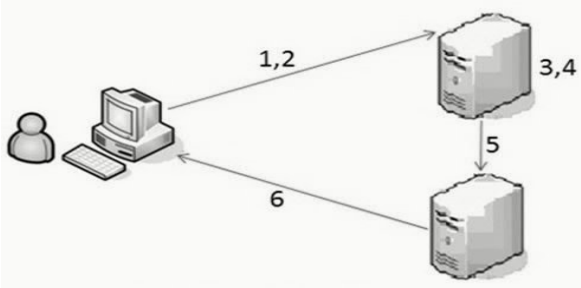
The shown steps in above figure are:

1. The user sends a request to the server to download a file.
2. If requested file exists in the server, the server sends it to the user.

Although web sites may use some methods such as CAPTHA or password protection methods to protect files for download; But, the main problem is that we cannot be sure that the files are used by an authorized user or this person will not share them. On the other hand, software which work based on peer to peer protocols that search the Web to find requested files and download them directly from other computers (without getting permission), is considered as perils for copyright infringement of

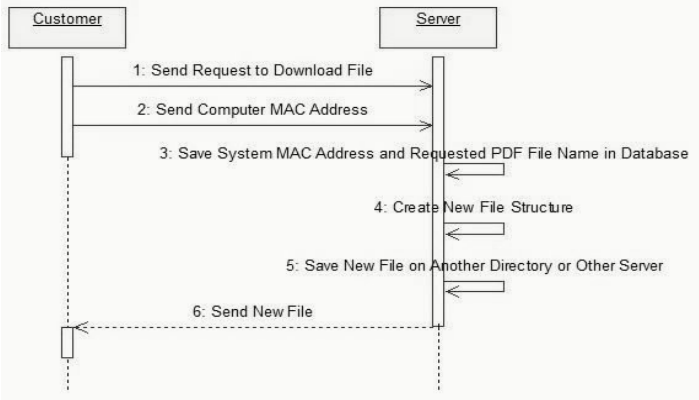
files. Unfortunately, this is a common method for obtaining files. So, it seems that it is better for the server to implement some prevention steps and makes some changes to files and directories for being more secure. The proposed system that is replaced instead of the common system was shown in figure 4, is shown in figure 5. Here, also we ignore some steps such as registering, steps related to shopping basket and paying money, and we only assume that the user requests the file and the server send it to him:

Figure 5: Proposed File Download Steps



Using the following diagram, we explain the steps that are outlined in figure 5.

Figure 6: Sequence Diagram for Operations in Proposed System



As shown in figure 5 and figure 6, first, the user sends a request to the server for download a certain PDF file. Simultaneously, a Java Script code will be run on the user computer that sends the system physical address to the server. So, the packet has been send to the server contains two more fields include:

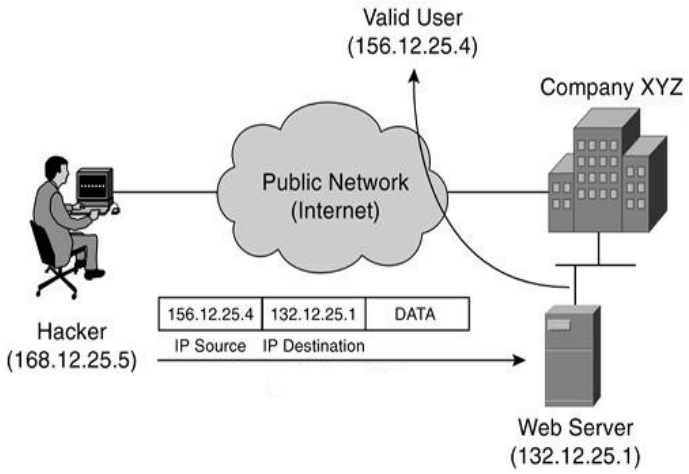
1) The name of requested file.
2) Customer's computer system physical address (MAC address)

Then, these information will be saved in a database on the server (Note that these information are send to the server beside other TCP/IP information for identifying the customer). Using this database and a defined encryption algorithm for the program, the server will join the requested file with the physical address that is in the database together and makes a new file structure as shown in figure 3.b. Then, the server saves this new file on another directory on itself (if the electronic store is small) or another server that is allocated for saving final changed files (if the electronic store is large and there are a lot of requests) and finally sends this new file to the customer.

5. Prevention of Physical Address Spoofing (MAC Spoofing)

MAC spoofing is a technique that is used in networks by hackers. In this way, an unauthorized person foists his computer physical address instead of an authorized computer system in the network to access its resources. The unauthorized person can pass network access control list that is in the server or routers by this way (I-Hsuan Huang et al, 2010, Ahmed Hassan and Xiaowen Zhang, 2011). There are many different ways to fake physical address in a network. For example, if the hacker wants to be detected as an authorized user, embeds a valid physical address and an IP address, that pertains to an authorized system in the network, in the TCP/IP packet which will be send to the server or routers. Server and routers will be cheated by this way and they consider the packet as it is from an authorized user and send information to the address that is specified as destination address in the packet by requestor then. This destination address can be the real address of the hacker's system and thus, all information will be sent to the hacker. This process is shown in the following figure.

Figure 7: IP Spoofing is a Method for Network Intrusion



One way to deal against with MAC spoofing is using cryptography (Richa Bansal et al, 2008). MAC spoofing can be prevented by encrypting the physical address in the TCP/IP packet while sending it. When the packet arrives at a server or another, a predetermined algorithm that is embedded in that server or router, tries to extract the authorized encrypted physical address from its relevant field in the packet. Since the algorithm applied on desired data, if the obtained address is equal to one of the authorized systems address in the network, the permission to access to information will be issued. Otherwise, the system will be declared as illegal and it cannot access to resources. Selecting the type of encryption algorithm depends on data sensitivity. Even, selecting value for keys, in key-based algorithms, depends on data sensitivity too.

According to the above, MAC spoofing can be arisen from the system or the packets send from the system. But, these problems are considered in the proposed method in this paper. Also, the program that is designed to operate on the customers computer to gain its physical address and send it to the server, will obtain that address directly from network card. It means when program's code execute, it will communicate with system's network card straightly to get MAC address and then put that address in a field in the packet that is reserved for this purpose. This state is different from the state that common software in the market are used for creating fake address and they try to introduce it as a valid address. These common software do not get the address from network card and they create it themselves. But in our proposed system in this paper, physical address will be obtained from the network card straightly. On the other hand, for minimizing the risk about these perils, the client-side software we designed that has been installed on clients systems as a plug-in, will get the address from

network card while comparing client's system physical address with the downloaded file header. So, the real address will be obtained and compared in both sides.

Also, while merging requested file with client's MAC address to create the new file format, the server uses a kind of cryptography algorithm to encrypt physical address and put it in the new file's header. So, the encoded address will be putted in the header. Selecting the type of cryptography algorithm can be changed according to data sensitivity or request of owner of the e-commerce web site while designing the web site. Another point is that, this algorithm will be embedded in client-side software too, to decrypt downloaded file header and extract the real physical address using this algorithm.

According to the above, as it is seen, in the proposed system, both sides of the problem are covered. It means that the possibility of counterfeiting MAC address through the system and network card and also counterfeiting file header are prevented. Therefore, by the mentioned methods we described in our proposed method, MAC spoofing has been largely prevented.

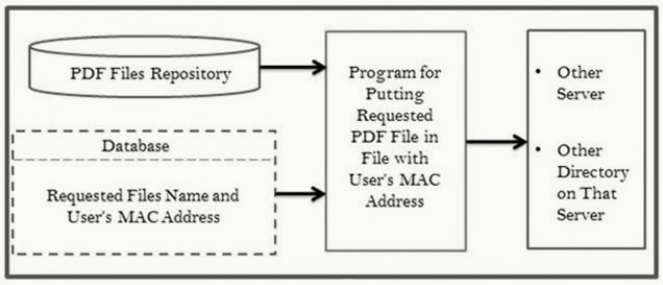
6. Proposed System Implementation and Results

For implementing the proposed system, Microsoft Visual Studio 2008, ASP.Net 3.5 with C# programming language and SQL Server 2008 as database have been used. First, we established an electronic book shop which customers could find their desired books in PDF format there and buy them. Also, one of the features of this web site was that, in addition to web site administrator, the publishers who have contract with the web site can upload their electronic books in PDF format on the site themselves to sell them. Therefore, measures must be devised to protect the copyright of these books and only those who pay for the books could be able to access them. So, different ways were examined and finally it came to conclusion that using customer's computer physical address can be a good choice and it can help us in securing requirements access and it led us to the method that is proposed in this paper. You can see a view of web site homepage in the following figure.

Figure 8: The Web Site Homepage

A process that merges the client's requested PDF file with his computer MAC address in a new file structure (puts MAC address as the new file header and the PDF file as its body) have been designed. At first, user sends a request to the server for downloading a certain PDF file. Simultaneously, a Java Script code will be run on his computer to find and sending the user computer physical address and requested file name to the server. In the server, these two parameters will be saved in a database and then, they will be merged together as a new file format. In the next step, this new file structure will be saved on another server or another directory on the main server and it will be sent to the customer. Finally, customer will open this file using the client-side software on his system. The following picture shows the sequence and how the operations are performed on the server:

Figure 9: Overview of Server Operations



According to our experiences, all requested files were changed to new structure successfully. More than 90% of converted files were sent to the customers successfully and all received files by them were opened on their computer successfully too. But these files were not opened on the other computers which did not use the plugin software or computers that were not owned for customers, even if they had installed the plugin, because their physical addresses were different. These systems received an error message about aborting their requests to open and access to the files.

The following picture shows a brief scenario about the proposed system in the form of pseudo code:

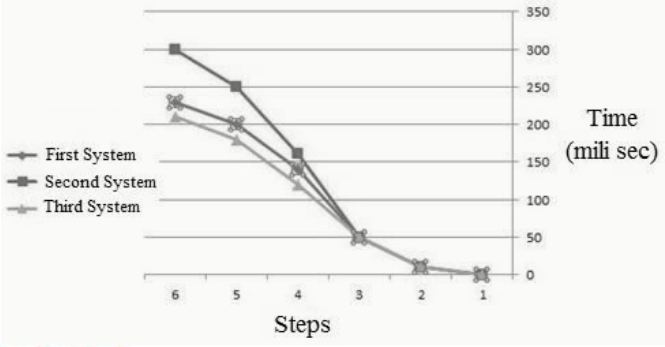
Figure 10: Pseudo Code of Brief Scenario for Proposed Method

```
//Client
Object Request ;
TCP/IP Field1, Field2 ;
Add Request.Field1 = pdf.name;
Add Request.Field2 = Sustem.MacAddress;
Send Obj.Request to Server;
-----------------------------------------------------------
//Server
//Add Fields Into Database
Add.Recordsource = " Insert into InfoTable ( pdfname, macaddr ) Values
(" + " Field1 + "," + Field2 + ")" ;
For(Allpdfs in Database)
{
If ( pdf.name is in Database)
{
Newfile = New ( File.Format);
Cryptography Algorithm;
Put macaddr as Newfile.Header;
Put Requestfile as Newfile.Body;
Save Newfile on Server;
}
Else
System.Writeln(" This File Doesn't Exist Now!!");
}
Send Newfile to Client;
-----------------------------------------------------------
//Client
X = Get(System.Macaddress);
If ( Newfile.Header == X )
Open(Newfile);
Else
System.Writeln(" You Are Not a Valid User!! ");
```

After implementing and testing the proposed method on many systems with different hardware specifications, although Windows XP Service Pack 2.0 was installed on all of them, and by embedding several timers in different parts of software code, the time of performing the steps mentioned in figure 5 (1. Send request -2. Send MAC address -3. Save MAC address and requested file name in a database on the server -4. Make new file structure -5. Save the new file -6. Send the new file to the customer) were measured and recorded. Results are shown in figure 11. This diagram shows the times of each step in three different systems. These computers were different in terms of memory, CPU, Cache and

network card. As it is shown in figure 11, there could not be seen noticeable differences between its curves. This diagram shows that proposed method can be used as an acceptable solution in e-commerce web sites and virtual stores. (At least it is proved about systems with Windows platforms). But, divergent is seen more from step 3 onwards because of different hardware in the systems and as it is gone ahead in diagram, the divergent is more because of all previous delays in each step.

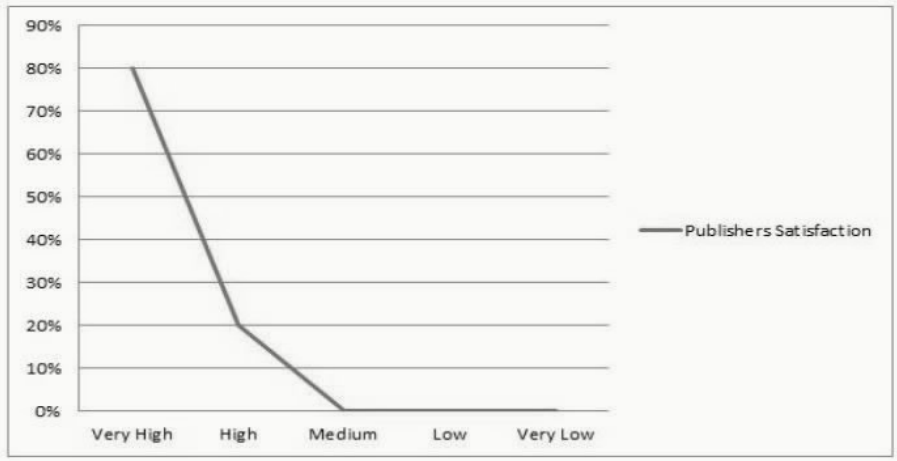
Figure 11: Comparison of Performing Time on Different Systems



Step1: Send request
Step2: Send MAC address
Step3: Save MAC address and requested file name in a database on the server
Step4: Make new file structure
Step5: Save the new file
Step6: Send the new file to the customer

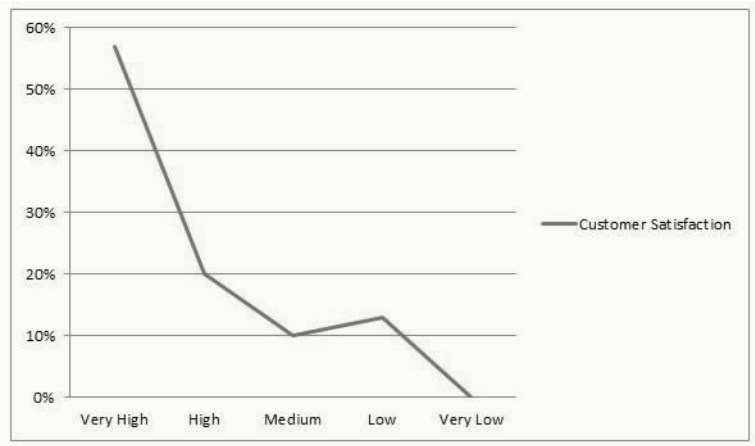
Considering what was stated and the tests we mentioned, this method can be assumed as a reliable and safe method for protecting copyright of books, essays, manuals, etc. that are presented in the form of PDF files. By using this method, various publishers and authors can sell their products on the Web confidentially and they can be sure that no one can abuses their products. We have conducted another survey from a number of publishers and customers to evaluate their satisfaction from using this system and its trustfulness. We asked 15 publishers around their opinion about this method and if using this method alone can provide assurance for them. Meanwhile, we asked 315 customers around their opinion and satisfaction while using this system. Then, we calculated the frequency of publishers and customers opinions by putting their answers into SPSS software Version 11.5. The frequency results of publishers and authors satisfaction and trustfulness are shown in figure 12.

Figure 12: Percentage of Publishers Satisfaction and Trustfulness



As shown in above diagram, about 80% of publishers in our statistical society had satisfaction in "Very High" level, because they had believed that this method can provide a secure way for reserving their books rights and they can be sure that nobody can abuses their products. Remain 20% of publishers believed that this method is good and they ranked it as "High" level. But they had stated that this method should be used in combination with other security methods such as authentication with ID and password. This diagram shows that publishers were satisfied using this method and they accepted its performance. The frequency results of customer's satisfaction and trustfulness are shown in figure 13.

Figure 13: Percentage of Customers Satisfaction and Trustfulness



As shown in figure 13, about 57% of customers had satisfaction in "Very High" level, because they had believed that this method is essential for protecting books copyright and they can also come up with this system easily. On the contrary, about 13% of customers were unsatisfied because they said that they had wanted to use downloaded books in other computers too.

7. Conclusion and Future Works

Media Access Control Address (MAC Address) is a permanent and worldwide unique identification assigned to most network adapters or Network interface card (NICS) by the manufacturer and used in the Media Access Control Protocol Sub-layer. If MAC address is assigned by manufacturer, it usually encodes the manufacturer’s registered identification number which may also know as EHA (Ethernet Address, Hardware Address), adapter address or physical address. This characteristic works as fingerprint for each computer.

In the implemented method, we used MAC address to identify authorized real customers while downloading electronic books and documents in the form of PDF files. This system requires changes in common client-server architecture and common process for accessing files. Next, a new file structure which helped us to gain our goal about copyright protection, by embedding encrypted MAC address in its header, was introduced. This was done by server-side and client-side software that we have been designed. Also, experimental results show that using this method can be a great help to make copyright protection. The created system satisfied the users (publishers, authors, customers) by mean then 80%. Meanwhile, combination of the proposed method with other methods of security such as watermarking, cryptography, steganography, etc. seems even more interesting, that of course needs to be investigated in the future researches. Also in the future works this software can be improved to support other file formats such as movies, music, software, etc.

References

[1] A. Deepak gupta, B. Gaurav tiwari, C. Yachin kapoor, D. Paraveen kumar. 2009, "Media Access Control (MAC): MAC spoofing and its countermeasures". International Journal of Recent Trends in Engineering, Vol 2, No. 4, November 2009, ACEEE.

[2] Ahmed Hassan, Xiaowen Zhang. 2011, "Bypassing web-based wireless authentication systems". 2011 IEEE Long Island Systems, Applications and Technology Conference (LISAT)

[3] Dimitrios Tsolis, Eleftherios Georgatos, Spyros Sioutas. 2009, 'The Use of Peer-to-Peer Networks in Copyright Protection". In proceeding of the 13th Panhellenic Conference on Informatics, PCI '09. DOI 10.1109/PCI.2009.48.

[4] Di Liu, Ping Chang Bai, Hong Jiang. 2010, "Using the user space file system to protect file". IEEE international conference on Apperceiving Computing and Intelligence Analysis (ICACIA), DOI 10.1109/ICACIA.2010.5709917.

[5] Document management -- Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1(PDF/A-2) URL http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50655.

[6] Felten, E.W, Halderman, J. A., 2006, "Digital Rights Management, Spyware, and Security". IEEE Security and Privacy, IEEE, Jan-Feb 2006, pp. 18-23.

[7] Freire, A. P., Fortes, R. P., Turin, M. A., and Paiva, D. M. 2008. "An evaluation of web accessibility metrics based on their attributes". In proceeding of the 26th Annual ACM International Conference on Design of Communication (Lisbon, Portugal, September 22-24, 2008). SIGDOC '08. ACM, New York, NY, 73-80.

[8] Gang Ke, Jie Ling, Yanjun Hao and Hongqi Liao, Zhaoxia Yang. 2009, "Research and Implemention of File Protection System Based on Improved Role-Based Access Control". Second International Symposium on Computational Intelligence and Design, 2009. ISCID '09.

[9] Geum-Dal Park, Eun-Jun Yoon and Kee-Young Yoo. 2008, "A New Copyright Protection Scheme with Visual Cryptography". Second International Conference on Future Generation Communication and Networking Symposia, 2008. FGCNS '08. DOI 10.1109/FGCNS.2008.76, 2008 IEEE.

[10] Hajime Kubota, Keiichi Iwamura. 2010, "A New Fragile Watermarking Scheme and Its Security Evaluation". 7th IEEE Consumer Communications and Networking Conference (CCNC).

[11] I-Hsuan Huang, Ko-Chen Chang, Yu-Chi Lu, and Cheng-Zen Yang. 2010, "Countermeasures against MAC address spoofing in public wireless networks using lightweight agents". The 5th Annual ICST Wireless Internet Conference (WICON).

[12] Kash, D.E., Kingston, W., 2001. Patents in a world of complex technologies. Science and Public Policy, 11–12.

[13] Logan, S.T. Peer-to-Peer Technology and the Copyright Crossroads. In “Peer-to-Peer Computing”, Idea Group Publishing, 2005, pp.166-193.

[14] Marta Más. STATISTICAL DATA PROTECTION TECHNIQUES. *INSTITUTO VASCO DE ESTADISTICA (INDICE)*, www.eustat.es.

[15] Natali Helberger *et al*. 2004, "Digital Rights Management and Consumer Acceptability". The Informed Dialogue about Consumer Acceptability of DRM Solutions in Europe (INDICARE) Sept-2004 at http://www.indicare.org.

[16] Nighat Mir, Sayed Afaq Hossain, 2010, "Secure web based communication" WCIT-2010, DIO 10.1016/j.procs.2010.12.092 Published by Elsevier Ltd.

[17] Puay Tang. 2005, "Digital copyright and the “new” controversy: Is the law moulding technology and innovation?'. Research Policy 34 (2005) 852–871, doi:10.1016/j.respol.2005.04.005, © 2005 Elsevier.

[18] Richa Bansal, Siddharth Tiwari, Divya Bansal. 2008, "Non-cryptographic methods of MAC spoof detection in wireless LAN". 16th IEEE International Conference on Networks, 2008. ICON 2008. 978-1-4244-3805-1/08/$25.00 ©2008 IEEE

[19] Rukma Rekha N, Subba Rao Y V, KVSSRSS Sarma, 2011, "Enhanced Key Life in Online Authentication Systems Using Virtual Password". Eighth International Conference on Information Technology: New Generations (ITNG), DOI 10.1109/ITNG.2011.71, 2011 IEEE.
[20] Safiollah Heidari, Shahriar Mohammadi, Sadeq Heidari, 2011, "Implementation of Downloadable File Protection Using MAC Address'. In proceeding of the 2011 International Conference on Information Theory and Information Security, IEEE.
[21] Sand win, BAI Shuo. 2002, "A kind of Internet content copyright protection and its implementation mechanism model" [J]. Computer engineering and should be Used, 38(6):195-198.
[22] Sayed Afaq H., M. Sikander, Nighat Mir, Beenish. 2006, "A secure mode for data communication using cryptography and steganography", ICT Malaysia.
[23] Tadayoshi Kohno, Andre Broido, Kc Claffy. Remote physicaldevice fingerprinting. URL http://www.cse.ucsd.edu/users/tkohno/papers/PDF/2005.
[24] The Emule System is available at URL www.emule-project.net.
[25] The Kazza System is available at URL www. Kazza.com.
[26] The Napster System is available at URL www.napster.com.
[27] Thomas Dettbarn. 2007. "Using Cryptography as Copyright Protection for Embedded Devices". International Conference on Consumer Electronics, ICCE 2007. Digest of Technical Papers.
[28] URL http://www.wipo.int/treaties/en/ip/berne/index.html.
[29] URL http://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm.
[30] URL http://en.wikipedia.org/wiki/MAC-address.
[31] URL http://en.wikipedia.org/wiki/Watermark
[32] URL http://en.wikipedia.org/wiki/PDF/A
[33] WANG Yun-Cai. 2009, "Research on Digital Content Copyright Protection System". In proceeding of the 2009. IEEE International Conference on Network Infrastructure and Digital Content, IC-NIDC 978-1-4244-4900-2/09/$25.00 ©2009 IEEE
[34] Wayner, Peter, 2009, "Disappearing cryptography 3rd Edition: information hiding: steganography & watermarking". Amsterdam: MK/Morgan Kaufmann Publishers. ISBN 978-0123744791
[35] Wei-Chi Ku. 2005, "Weaknesses and drawbacks of a password authentication scheme using neural networks for multiserver architecture". IEEE Transactions on Neural Networks, 1045-9227/$20.00 © 2005 IEEE
[36] WhiteHat website security static report. 11th edition, fall 2011, URL http://www.whitehatsec.com
[37] World Intellectual Property Organisation. Understanding Copyright and Related Rights. (PDF). WIPO. pp. 6–7. http://www.wipo.int/freepublications/en/intproperty/909/wipo_pub_909.pdf. Retrieved August 2008
[38] Xiao Xin-hua. 2010, "Research on file protection based on computation elasticity". 2nd International Conference on Computer Engineering and Technology (ICCET)
[39] Xin Yu, Nan Wang, Heyin Zhang. 2009, "Design and Development of PDF Document Protection System Based on DRM Technology'. In proceeding of the Second International Symposium on Knowledge Acquisition and Modeling, KAM '09 © 2009 IEEE
[40] YU Yin-Yan, TANG Zhi. 2005, "A Survey of the Research on Digital Rights Management" [J]. Chinese journal of computer. 2005(12)