TITLE: A Novel Model for E-Book Borrowing Management System

AUTHORS: Aykut Karakaya,Sedat Akleylek,Kerem Erzurumlu,Erdal Kiliç

Academic Platform Journal of Engineering and Science

A Novel Model for E-Book Borrowing Management System

*[1]Aykut Karakaya, [2]Sedat Akleylek, [3]Kerem Erzurumlu, [4]Erdal Kılıç

[1]Department of Computer Technologies, Bulent Ecevit University, Devrek, Zonguldak. karakayaykut@gmail.com,

[2]Department of Computer Engineering, Ondokuz Mayis University, Samsun. sedat.akleylek@bil.omu.edu.tr,

[3]Department of Computer Technologies, Ordu University, Ordu. kerem@linux.org.tr,

[4]Department of Computer Engineering, Ondokuz Mayis University, Samsun. erdal.kilic@bil.omu.edu.tr,

Abstract

In today's information-age world, most libraries use traditional borrowing methods. These conventional methods have some disadvantages such as torn and loss of books, and no access to books at that moment. In this paper, to overcome such disadvantages, we propose a novel e-book borrowing mechanism considering digital rights management. By combining the techniques given in this paper, e-books are protected against copying, distributing, printing and unauthorized use while borrowing and using.

An infrastructure is designed for users to access books through electronic devices. In this structure, e-books are user-specific encrypted. Even if the e-book files are copied by unauthorized users, the key cannot be accessed by the copied device since the target platform doesn't have this key. Thus, the borrowed book is prevented from being used by an unauthorized user. Then, the borrowed books can be checked via cloud system technologies by sharing resources between devices. Moreover, even if the books are copied and distributed, the malicious user can be found via watermarking. The main difference to the previous studies is that QR code authentication, which is generated by public key cryptographic techniques, enables the use of books on different devices.

Keywords: E-Book; Borrowing System; Library; Digital Rights Management Software; E-Book Security

1. INTRODUCTION

E-book publishing and distribution have received a great attention due to its mobility advantages. Like in printed books, the protection of authorship is important in eBooks. Systems developed for this purpose are generally referred to as digital rights management (DRM). For years, many researchers have examined DRM protection and security at the hardware and software level. With the fact that increasing security issues on e-books gives natural positive effects on ease of use, portability and ability to work offline [1]. The security of e-book consists of several issues: protection against copying, distributing, printing and unauthorized use while borrowing. Trusted Platform Module (TPM) is a hardware-based security approach in DRM framework for the security of an e-book [2]. The TPM is a micro-chip that allows the use of hardware security features [3]. Security methods such as watermark, code protection and white box cryptography are used to protect the content [2].

The borrowing e-book for users will increase in the future, according to the classifications of electronic borrowing [4]. E-books are borrowed and used effectively. Reading of the borrowed book directly from the scanner and downloading it as PDF or EPUB are the two types of borrowing mechanisms

in the Open Library a system that allows borrowing books [5]. Reading via browser is an example of online idea. The e-book needs Adobe Digital Edition application when it is downloaded to the device as PDF or EPUB. A limit to borrow e-book is put: 5 books can be borrowed for 2 weeks. When the loan period expires, the files remain on the device. There is no option to return a book borrowed for mobile devices [5].

In order to increase the security of software-based DRM, the DRM structure requires confirmation and authentication when integrated into user tools. In addition, it creates a secure channel between the client and the server for the authorities [6]. This structure has been implemented in the AXMEDIS project, which aims to create a new technological framework for automatically production, protection and distribution of cross digital media content on media channels such as PC, PDA, kiosk, mobile devices connected to the internet [6]. In these transactions, delivery and delivery security is more important than content security.

There are online and offline methods to ensure the protection of images as similar content instead of e-books [7]. When these methods were implemented, a system called DIAS (The Digital Image Archiving System) was used. DIAS is an

*[1]Department of Computer Technologies, Bulent Ecevit University, Devrek, Zonguldak. E-mail: karakayaykut@gmail.com
Phone: +905418538238

image management system that serves as an image provider for external systems and provides protection of valuable digital images. In this structure, a watermark can be set on the image as a layer. To implement the offline protection (DRM) mechanism, an image file is packaged using the hardware information of the client computer, the smart card information, the user ID, the information specifying the time to display the picture and the picture. When the file is run, the authoritative information is verified before the image is displayed. Then, the image is shown with the default image viewer. If not confirmed, the image is not shown [7].

OCLC Worldshare, a book borrowing mechanism, is a browser-based system [8]. If you want to go back after a certain stage, you must use the menu on the screen instead of the browser. The system is accessed via an authentication, then the online book list is displayed. A request is created by entering some properties that the e-book and the system offer. At the end of these operations, a request ID is assigned to the request. There is an advanced search system based on search by format, language, year, catalog source [8]. Borrowing process is made as online between the libraries.

A user, with the ability to use DRM protected content, has tickets created by a rights publisher (a server machine) and acts as a property certificate for content that has certain rights, then this ticket can be distributed to other users. Tickets are used for sharing among authorized users who do not violate the DRM policy [9]. Thus, the load on the server and the amount paid to the server are decreasing. By limiting the number of content shares, over-issuing attack is prevented. Moreover, by checking the number of tickets and licenses in certain periods, the multiple-spending attack is prevented [9].

In addition to DRM, cryptographic based CAS (Conditional Access Systems) are also used while commercial content on the Internet is protected. The elements used by these two structures are basically the same. The content is accessed offline with PC and mobile devices. So, the risk of unauthorized modification of the elements will increase, since the keys must be given anonymously [10]. Attacks on DRM systems are usually actions to try to find the encryption key and to extend the license. Therefore, it is emphasized that it is better to protect contents online with DRM and CAS methods which are network-centric structures [10].

Amazon offers its users the option of borrowing their own e-books for a certain period of time [11]. Borrowed e-books use the .azw format and the Kindle device developed by Amazon. Users can access and borrow e-books by logging into the library with Amazon account information. However, the Kindle device needs to be online via Wi-Fi connection [11].

The Lock Lizard system is a system that protects e-books from unauthorized users and checks how and for how long they are used for authorized users [12]. It provides protection in all cases. Features include: preventing unauthorized viewing, preventing sharing, preventing copying and editing, preventing screen capture, preventing printing, borrowing a book, online or offline use, dynamic watermarking, license transfer between devices [12].

There is an offline access and use method for the use of books that are not publicly available to legal users from a confidential archives [13]. Legal users can access any copy of the content as long as the identity of the user and the rights of access are confirmed. At certain time intervals, restricted persons are permitted access to "non-public" documents. Borrowing and returning times are held in tokens to restrict access by legal users [13]. Thus, non-public documents are transferred offline to legitimate users.

Drumlin Security's software and services ensure the secure distribution of documents in PDF format [14]. Copying and other controls in the documents are managed in a secure way. It has cross-platform support and can be used with Javalin PDF Readers, which can be run on any system. Features include: PDF copy protection has features such as DRM removal tools prevention, true PDF view, offline or online reading, and fast and scalable content. [14].

In an effort to prevent e-books from being shared freely between devices, an electronic book distribution system encrypts the e-book using the content key [15]. The content key is encrypted with a document key. The structure of the document key includes the serial number of the device that the e-book will read, a secret user account associated with this device, and metadata about the e-book. To prevent books from being shared freely between different devices, the encryption key is kept separate for each device. The encryption key is calculated as a function of the serial number of the device to which the book is to be read. As a result, a content server must know the serial number of the device before it can be used on the reader device. Since the server knows this information, the encryption key is calculated by using the function of the serial number of the device and encrypts the book with this key. After receiving the encrypted book, the encryption key is recalculated using the serial number and function of the reader device and the generated new key is used to decrypt [15]. Generally, in the system, books are encrypted with a device specific key.

1.1. Motivation

Until today, various methods have been proposed and developed in studies focused on e-book, e-book security, e-book platform and e-publishing. Hardware based security structure is one of these methods with some simple encryption methods and it is dependent on the device used. With software based security structures, it is tried to ensure online protection with security between client and server. Additionally, in the previous study, 3 areas are focused on e-book systems that provide offline protection for software. Firstly, distribution security of e-book is provided rather than its content. Secondly, the content of e-book is preserved, but the number of users is limited. Lastly, security almost all is

provided, but inter-device verification and synchronization methods aren't used.

Within the structure that has been proposed by us, process of lending books is provided via e-books, without being dependent on device. For content protection, symmetric encryption is used so that the content can be available only for the person who borrows it. During the reservation period, users can read the e-book with an e-book reader that is integrated with the system. Watermark is used in case e-book copying to find out the person who copies it, cloud system is used to ensure the validity of e-book and control file and QR code, which is generated via users' open keys, is used for verification and synchronization between devices.

1.2. Our Contrubution

In this study, a new model and a new technological infrastructure are provided in order to carry out book lending procedure of a library virtually. Within this structure, encryption methods, cloud system, watermark protection and QR code identity verification exist. When a book is borrowed, e-book is encrypted and watermark protection that is generated from the user's identity information is integrated with the e-book. To the user's cloud disk storage and device, two files are uploaded – one of them is e-book file and the other one is a control file that executes some processes like user control and time control. In case of a problem with the related device, the problem is diagnosed and solved by the help of these files. With QR code verification, users are able to use all the books that are borrowed by them with different devices, without depending on just one device.

There are two servers in the system. One is the content server where e-book files are stored and made available for a user with the user-specific encryption method and the other one is the database server that ensures all types of data check. With these servers, users are able to borrow books and many processes like book count check, time check and status check can be executed.

Main differences than the previous studies are offline availability and user verification and synchronization between devices with QR code. The proposed system is the only structure that includes encryption methods, cloud disk, watermark protection and QR code in one place

2. A NEW MODEL

With this study, a technological infrastructure has been designed in order to make book loan services from a specific library over electronic medium more common. With this structure, e-books can be borrowed securely and read with e-book readers.

2.1. Properties of The Proposed Model

After registering to a library, users are able to reach all books within that specific library, without infringing copyright.

Against any possible copyright infringement, there are precautions in effect within this system. Processes that take place until a user obtains access to an e-book are below with reasons:

- After logging into system and passing identity verification, user borrows a book and a secret code that contains information about the user is generated and assigned as watermark while the book is still on the content server. This way, in case the e-book is copied somehow, the person who does this can be found out.
- After the watermark on content server, e-book file and the control file that is generated based on this e-book file are encrypted with symmetric encryption method (Advanced Encryption Standard - AES) by using the user-specific 256-bit key. This way, even if the e-book file and the control file are copied to another device directly, the e-book cannot be used as that new device does not have the required key. As the content is encrypted, system can operate independent from e-book file format and platform.
- After e-book file and control file are encrypted, these files are uploaded to cloud storage that is specially created for the user and then the user's device as well. In the cloud storage, copies of these two files are located and regularly, timestamp information is added. This way, if a user makes a change on these files during offline usage or in case any problem occurs for these files, he/she can continue using the e-book with the files uploaded to the cloud storage.

Timestamp is added online to the control file located on the cloud storage; whereas in case the device is online, timestamp is added to the control file located on the device just like as the cloud storage and in case the device is offline, timestamp is added to the control file with system's time information. This way, user cannot use the e-book more than allowed time period by changing his/her device's time settings.

Even if the files associated with the e-book are copied directly to another device, the e-book cannot be used. The reason is simple: the device that files are copied to doesn't have the key required to decrypt the encryption. In order to use the file on another device, it is required to login to the application on the new device and verify identity. With RSA, a QR code is generated by using user's open key and identity information. With the integrated QR code reader on the mobile device, user related information can be reached with the user's secret key. After the verification of user information, the files (e-books that are already borrowed) located on cloud storage are copied to the new device and as a result, user becomes able to use the e-books on different devices. Secure generation, distribution, storage and management of cryptographic keys are not studied within the scope of this work.

All data during any process on the server are transferred between the server and reader with SSL (Secure Socket

Layer). E-books are secured by using encryption with key method. The key that is required to decrypt and read the e-book is sent to the user with open key encryption method. Thus, user is able to use the e-books that are borrowed even if he/she is offline.

2.2. An Overview of The Proposed Model

Proposed and developed system makes registered users able to have any book in the library by lending it for defined period of time. When an e-book is borrowed, it is encrypted with user's special key and downloaded to his/her device. Besides, one other file, which checks date and time, is located on the device.

As time control is checked via the mentioned file, borrowed e-book can also be used offline. This way, after borrowing the e-book, no further requirement is necessary like internet connection in order to read the e-book.
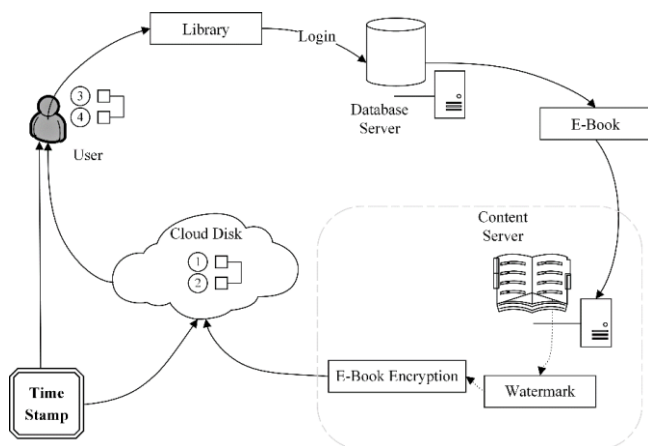
Figure 1. General handling of the system

General structure of the proposed model is shown in Figure 1. Process steps are as follows:

Step 1. E-book in any format is borrowed from content server after logging in to library.

Step 2. Before lending the book, a special watermark, which is generated by processing the user's information and which has the same background color with the page, is placed on each page of the book. This way, in case the e-book is copied, it is possible to find the user who copied the e-book.

Step 3. In the structure, each user has his/her own cloud storage. On the content server, watermark is placed on pages of the e-book and with the user specific key, files are encrypted with AES.

Step 4. Among these encrypted files, e-book file that is shown with number 1 in Figure 1 and control file that is

shown with number 2 are uploaded to the user's special cloud storage.
Step 5. Then, from the cloud, the files are sent to his/her device. E-book file that is sent to the device is shown as number 3 in the Figure 1 and control file is shown as number 4.
Step 6. After timestamp is added, time information on both device and cloud is updated and synchronization is ensured.

Usage of an e-book after borrowing it is described in Figure 2. It is possible to use the e-book both offline and online. During offline use, the timestamp is generated by using device's system time. Each time the e-book is opened, date information is added to the control file that is shown as number 4 in Figure 2.

Inside a control file, date of borrowing, due date, some important identity information and date-time information, which is added hourly if the device is online and each opening of the e-book if the device is offline, exist. Yet, this file is also kept encrypted at user-end.

In case of offline use, there are 3 different statuses based on the result of the control file:

a. Current date information is older than the previous one. This is an unwanted situation and this shows that user has changed time settings of the device. It may be possible that user has changed time settings of the offline device to use the e-book for a longer time than the allowed duration. In this case, borrowed e-books are deleted from the drive and request to return the e-books to the library and request to suspend the user's account are kept on hold until the device is online again.

b. Due date has passed while the device is offline. In this case, user is allowed to extend the due date until the defined amount of time. Extending due date or returning the e-book processes are possible by making the device online. If, within this time frame, user does not make the device online, the amount of the book is increased by 1 on the database server and the files are removed automatically from the device at the end of 3 days.

c. Any status different than the previous two. In this case, e-book can be used offline without any problem.

With timestamp generation during online use, the most recent date-time information is assigned to the control files that are shown as number 2 and 4 in Figure 2. This way, in case user changes system time and date settings, effect is neutralized. During online use, the only thing to check is the remaining duration. Like offline usage, some amount of time is given to a user for extending the due time. In this case, user either extends the duration or returns the e-book.
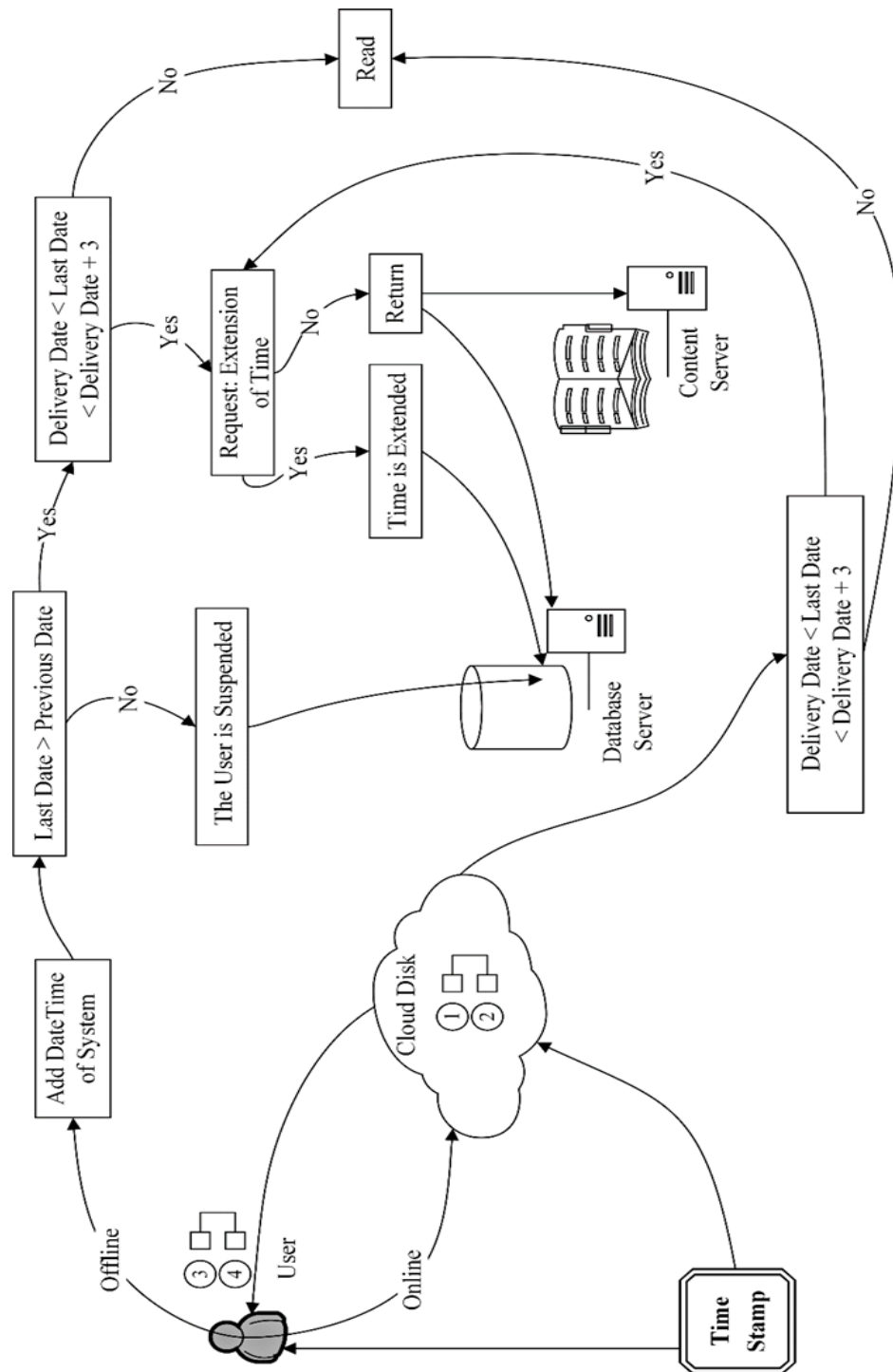
Figure 2. Online or offline usage status

[Borrowing Date] & [Delivery Date] & [Some Important IDs (e.g. borrowing ID, book ID, user ID)] & [Run Date (1)] $ [Run Date (2)] $ [Run Date (3)] $ . . . $ [Run Date (N)]
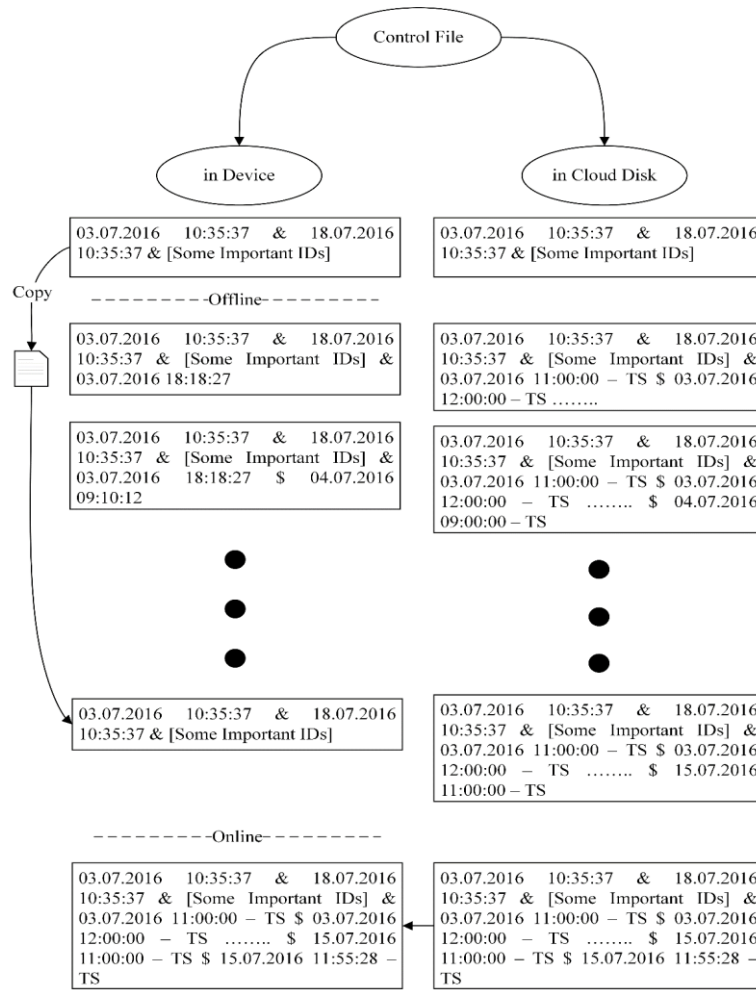
Figure 3. The content of a control file
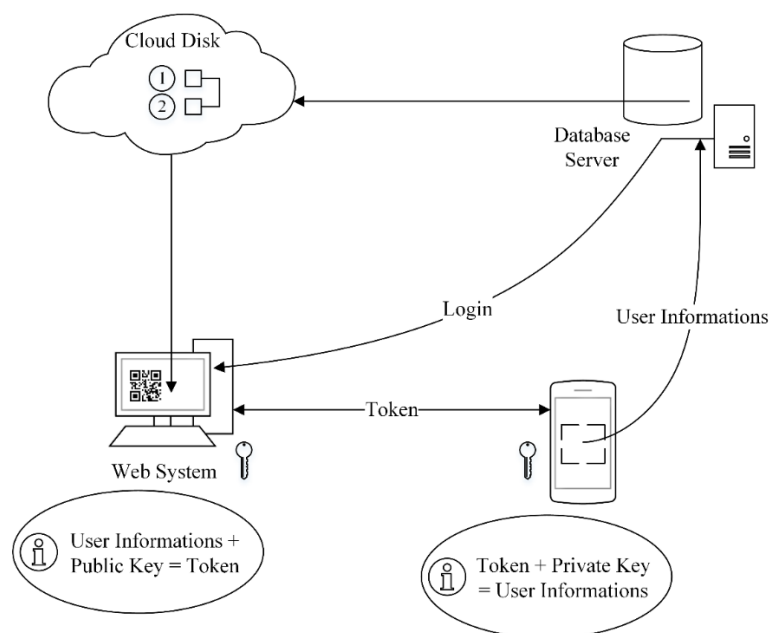
Figure 4. Control file time protection

Figure 5. Verification and synchronization of information with QR code

In Figure 3, content of a control file is shown. When a user uses his/her e-book offline for a while and then goes online, timestamp on the device and timestamp on cloud are compared with each other. Time information on the cloud is updated regularly by adding timestamp. If the timestamp on the device is newer, then there is no problem. This way, a user is not able to copy and use the very first control file provided just after borrowing an e-book. Because, if the date on device is older than the cloud, user may copy the control file at the beginning and after some time, overwrite the control file existing on device. This makes the lending process reset and this is an unwanted situation. Thanks to the controls on cloud storage, such unfair usage can be prevented. If there is no problem after the comparison of timestamps between cloud and device, last timestamp on the device is added to the control file located on server. Then, timestamps on both systems are updated. This process is shown in Figure 4.

The process shown in Figure 4 also makes it possible to determine if a user interfered with the control file on his/her device intentionally or unintentionally. After such interference, if the file is not read at all, maybe user deleted the file. In this case, files are re-located on the device from cloud and user can keep using e-book. If the user changes the content of the control file intentionally or unintentionally, decryption becomes impossible due to this change and up-to-date files on cloud system are transferred to the user's device and user goes on using the e-book.

In Figure 5, synchronization is shown for other devices than mobile ones. Process steps are as follows:

Step 1. Firstly, users has to log on in order to use any book borrowed via the other device.
Step 2. After log on, a token is generated with user's open key and identity information.
Step 3. This token is integrated with the QR code.
Step 4. In this structure that is created with RSA, method of open key encryption, mobile device read the QR code and tries to encrypt the content with integrated secret key.
Step 5. After the verification process, borrowed books on the cloud storage are transferred to the new device. This way, the same books can be used on different device with the same protection methods.

When a user goes to another place around the world with different time zone, time information inside the control file and device time are updated as well. This process is ensured with the help of "timezone" function executed over the active connection's IP address.

Some parts of the reference application for the system can be reached via the following link: "github.com/akarakaya/DigitalLibrary". This partial application offers a chance to test e-book lending process, offline or online use of an e-book and return process of an e-

book. The application is the limited version of the study, without some features like offline use, copy and print protection and date-time control.

3. COMPARISON

The main purpose of this system design is to make users able to reach correct information without hassle, to protect authors' copyrights and to protect books against any unauthorized use, copying or printing.

Hardware based protection systems are dependent on device. Software based content protection approaches, on the other hand, shows differences between encryption methods used and conditions of online or offline use. Online services force users to be connected to a network and therefore, limitations are applied for users. With the proposed system, offline service is also possible as a result of the aim of making users need the minimum requirements. There is no similar limitations for users within this system.

For some offline-available systems, content protection and copy prevention is not considered at all during offline use. The reason is that the obtained files are shared by some competent users. Named as "Offline Secure SRM Mechanism", access to any non-public resource by unauthorized individuals is blocked. In the proposed system, access ability is completely user-specific. Only one user accesses one book. As the encryption is user specific as well, although the file is shared with some other person, that person cannot use the file in any way.

In Table 1, a comparison has been made between the proposed system and other systems that include similar structures. "√" shows that the system supports the related feature and "X" shows that the system does not support the related feature or there is no sufficient information.

In the proposed system, even if a book is copied, the person who creates the copy can be found with secret watermark. Additionally, users are able to use their books on different devices. In order to verify identity and ensure synchronization, QR code system is used. QR code is generated with user's open key information as soon as user logs in to the system. With integrated QR code reader on mobile device, user's secret key is decrypted and synchronization between devices is ensured. As seen in Table 1, QR code verification is used only in the proposed system. In case a user experiences any problem, borrowed books are also kept on cloud storage. This way, some inappropriate behaviors can be identified and any mistake unconsciously done can be prevented. Proposed system is the only one in which all these technologies are used.

This system differs from any other with the technologies used and provide advantages regarding many topics like easiness of use, active protection and copyright protection.

Table 1. Comparison of similar e-book sharing systems

System / Feature	Open Library [5]	OCLC World Share [8]	Amazon [11]	Lock Lizard [12]	Drumlin Security [14]	E-Book Encryption Using Variable Keys [15]	The Proposed Model
Copy Protection	✓	✓	✓	✓	✓	✓	✓
Printing Hindering	✓	✓	✓	✓	✓	✓	✓
Screenshot Hindering	✗	✗	✓	✓	✓	✓	✓
Borrowing Usage	✓	✓	✓	✓	✓	✓	✓
Offline Protection	✗	✗	✗	✓	✓	✗	✓
QR Code Usage	✗	✗	✗	✗	✗	✗	✓
Watermark Usage	✓	✗	✓	✓	✓	✓	✓
Cloud System Usage	✗	✗	✓	✓	✓	✗	✓
Platform Independent	✓	✓	✗	✓	✓	✗	✓

4. CONCLUSION AND FUTURE WORKS

In this paper, we propose a new model for e-book borrowing mechanism independent of the format. With the help of this structure, we obtain a secure and reliable e-book borrowing system. The system also provides new protection features like copy or copyright for authors and copyright owners by benefiting from state-of-art encryption methods. Remote use of library is also ensured provided that some limitations and rules are followed.

This way, instead of uncertain information obtained on the internet, books in library are much easier to reach and use. And books contain much more correct information. Therefore, in this system, access to books is desired to be facilitated by mobile phones and computers. As a borrowed book is encrypted for a specific user, it is used only by the registered person. Being primarily active on mobile devices, the system offers some features like borrowing, returning and offline use. A number of safety precautions have been taken.

These include: user authentication with QR code and device synchronization, watermark copy prevention, offline and online time protection with the cloud system. Together with such components, system offers protection against copying, distributing, printing and unauthorized use of content where the system includes asynchronous and synchronous encryption methods as well. Some software offers license of use with some limitations in effect. At the same time, defined amount of users are allowed to read a book and each user may be allowed to read books for a specific amount of time.

Starting from this point of view, a structure that offers any lent book to limited amount of user can be constructed.

ACKNOWLEDGMENT

REFERENCES

[1].A. Karakaya, K. Erzurumlu, E. Kılıç, 2016. "A Novel Offline Borrowing System for Book Transformed from Printed Book to E-Book in Libraries". Ponte International Scientific Researches Journal, 72(4).

[2].K. Verslype, B. D. Decker, 2006. "A Flexible and Open DRM Framework", International Federation for Information Processing, 173-184.

[3].T. Morris, 2011. "Trusted Platform Moldule", Encyclopedia of Cryptography and Security, Springer US, 1332-1335.

[4].M. Alipour-Hafezi, 2016. "E-lending in digital libraries: a systematic review". Iranian Research Institute for Information Science and Technology (IRANDOC), Interlending & Document Suply, 44(3), 108-114.

[5].https://www.adobe.com/tr/solutions/ebook/digital-editions.html (Access Time: 23.04.2018).

[6].V. Torres, J. Delgado, S. Llorente, 2006. "An Implementation of a Trusted and Secure DRM Architecture". R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops – OTM Confederated International Workshops and Posters, 4277, 312-321. Springer, Heidelberg, Germany.

[7].H. Y. Chen, H. A. Wang, C. L. Lin, 2007. "Using Watermarks and Offline DRM to Protect Digital Images in DIAS". L. Kovács, N. Fuhr, C. Meghini (Eds.), European Conference on Research and Advanced Technology for Digital Libraries (ECDL 2007), 4675, 529-531. Springer, Heidelberg, Germany.

[8].https://help.oclc.org/Discovery_and_Reference/WorldC at_Discovery/Search_in_WorldCat_Discovery/050Use_the _Advanced_Search_screen (Access Time: 23.04.2018).

[9].L. Yang, Y. Nenghai, H. Zhuo, 2009. "Rights Sharing Scheme for Online DRM System Using Digital Ticket". International Conference on Management and Service Science (MASS 2009), 1-6, doi: 10.1109/ICMSS.2009.5304788. IEEE.

[10]. M. Mampaey, A. N. Villegas, 2012. "A Network-Centric DRM for Online Scenarios". Bell Labs Technical Journal, 17(3), 129-133.

[11]. https://docs.aws.amazon.com/elastictranscoder/late st/developerguide/drm.html (Access Time: 23.04.2018).https://www.locklizard.com/pdf_security/ (Access Time: 23.04.2018).

[12]. A. Kozakiewicz, K. Lasota, 2015. "Secure DRM mechanism for offline applications". Military Communications and Information Systems (ICMCIS), 2015 International Conference on, Cracow, 1-8.

[13]. Drumlin Security, Service Features Comparisons. https://www.drumlinsecurity.com/ServiceComparison.pdf (Access Time: 23.04.2018).

[14]. R. J. Snodgrass, J. C. Slezak, M. E. Goldberg, J. Leproust, G. Jeulin, F. F. Antony, 2014. "Ebook encryption using variable keys". U.S. Patent No. 8,826,036. Washington, DC: U.S. Patent and Trademark Office.