International Journal of Database Theory and Application
Vol.7, No.4 (2014), pp. 249-260
http://dx.doi.org/10.14257/ijdta.2014.7.4.20

Enhanced Security Architecture for Digital Documents Using Radio Frequency Identification

Jae-Hyun Choi[1], Jong-Bae Kim[2] and Jea-Won Park[3*]

[1,2,3]*Graduate School of Software, Soongsil University, Seoul 156-743, Korea*
[1]*jaehyun@ssu.ac.kr*, [2]*kjb123@ssu.ac.kr*, [*]*jwpark@ssu.ac.kr*

Abstract

Nowadays, digital documents are widely used in many business areas since computer networks and digital devices such as smartphones have been evolved. However, digital documents may have very important information such as confidential business policies and intellectual property statements. Therefore, securing them is critical to the business world of today. In this paper we propose new enhanced security architecture for digital documents. The proposed architecture enhances the security of digital document using RFID with encryption algorithms. In other words, it provides more enhanced security not only using software but also hardware The proposed architecture could be used in many business areas which use high security digital documents, such as a secure intranet of organization. In addition to, our approach is able to use in digital rights management.

Keywords: *RFID, Security Architecture, Digital documents, DRM*

1. Introduction

Digital documents have become the mainstay of an office in the age of digital [1, 2]. This is due to the increased usage of computer networks and the widespread digital technology. Along with the increased usages of digital documents comes the problem of securing them. The need for security is obvious in the business world. The documents are typical means of expressing almost anything in an organization. They may range from simple memos to confidential business policies and intellectual property statements. Securing the information in these documents is critical to the organization's progress and in some cases, their survival too [3, 4]. But, nowadays, the level of security for them is insufficient [1, 4, 5].

In this paper, we propose security architecture for digital documents using Radio Frequency Identification (RFID) technology [5-8]. This is based on several encryption algorithms, and guarantees improved security and accessibility of the secured digital documents by incorporating RFID technology. With this, only authorized users with RFID tags can access the digital documents because the original documents are encrypted and controlled by the information on RFID tags.

[*]Corresponding author. Tel. : +82-10-9135-4181.
Email address: jwpark@ssu.ac.kr(Jea-Won Park).

ISSN: 2005-4270 IJDTA

2. Related Works

2.1. Protection of Digital Documents

The protection of digital documents is to guarantee their safety through access control to them. This can be achieved not by encrypting a digital document itself but by denying unauthorized access to the document. Protection can provide more security to the document with encryption. But they combined with external storage device provide much more security. Because even if a document has been encrypted and protected by authentication mechanism, its existence on the network means attackers can always try to access the document. Therefore, it is important to store a part of them to an external storage device for improved security. The architecture for protection of digital documents using external storage devices is presented in Figure 1.

However, it has problems of the physical safety and the portability of the external storage device. If the portability of the device is limited, it could limit the usability of the document. And if the physical safety of the device is fragile, this could results in the loss of the document. In addition, if the document only in the external storage device, the security of them is guaranteed, so it provides limited usability. Because a digital document transmitted through a network is not safe, the users who only have the external storage device can access the document. Therefore, it is need to consider the usability of the security architecture for digital documents with the enhanced security.

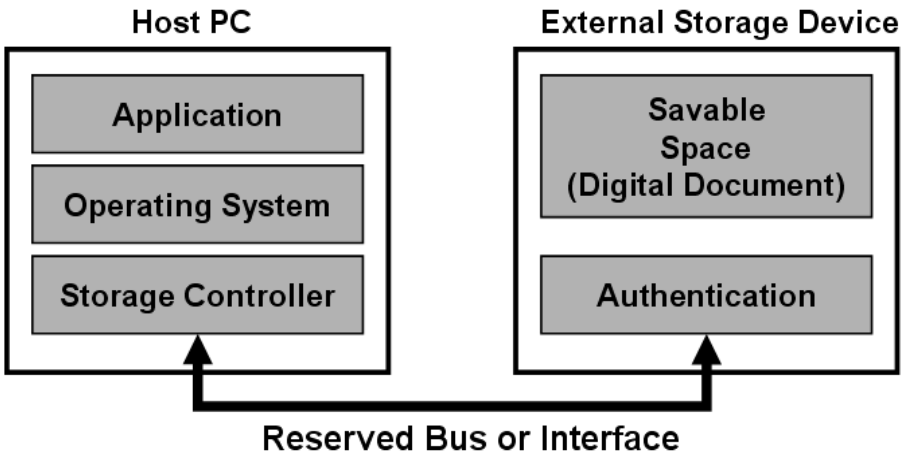

Figure 1. The Architecture for Protection of Digital

2.2. Encryption of Digital Document

Encryption of digital documents is a way to convert identifiable digital documents to unidentifiable documents using a specific algorithm. Digital documents can be protected from an illegal user by using a user password. Figure 2 shows the architecture for encryption of digital documents.

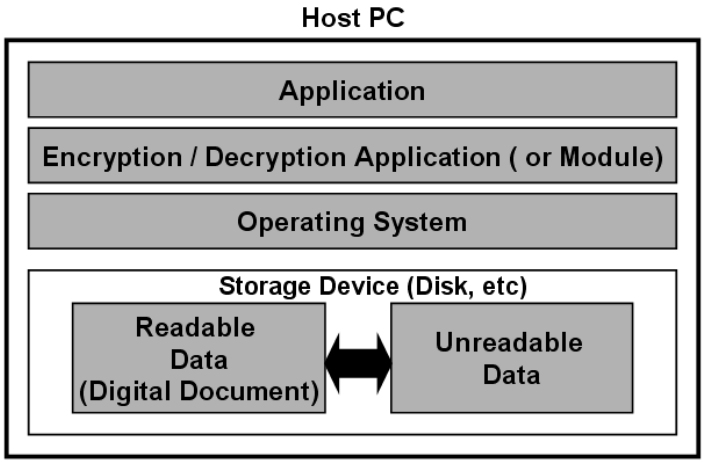

Figure 2. The Architecture for Encryption of Digital Documents

In the architecture, digital documents are secured by a module which converts digital documents to unidentifiable documents with an encryption and decryption algorithm. However, it has a weakness that digital documents are encrypted by only a user password. Moreover the encrypted documents are stored in a local computer so it can be leaked through the network. Therefore a consideration for this 'leaking' is necessary.

3. Enhanced Security Architecture for Digital Documents Using Radio Frequency Identification

3.1. Overview

RFID-based security architecture for digital documents is proposed in this paper. The proposed architecture strengthens safety of digital documents using the encryption of digital documents combined with the external storage device. RFID can be miniaturized, so it has high portability. Also, RFID is strong about physical impact rather than disks. Therefore, RFID can be an alternative to protect digital documents. Figure 3 presents the security architecture for digital documents using RFID.

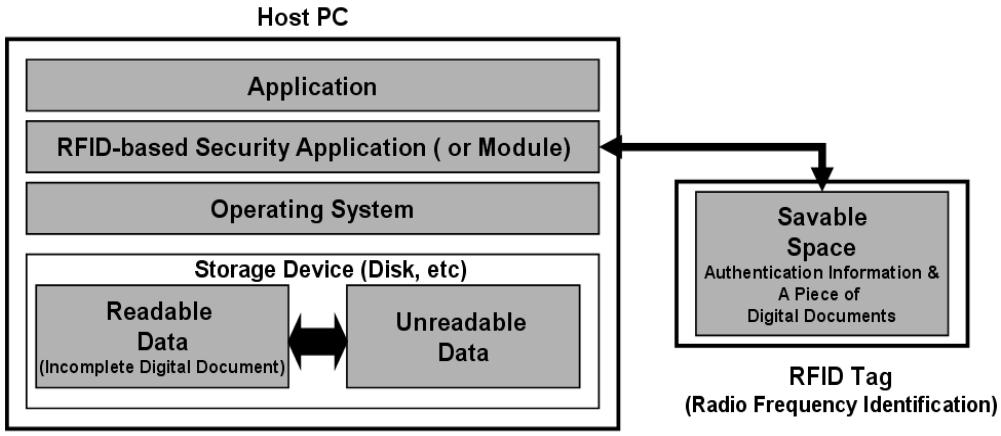

Figure 3. RFID-based Security Architecture for Digital Documents

A digital document is separated into a summary of the document and the rest of the document except the summary. The summary of the document is extracted from the original document and stored in a RFID tag. The purpose of this extraction is to protect the digital document using the external storage device. Complete exposure of data is prevented by storing some data in an independent space from networks, so safety of the document is enhanced. Also, the incomplete document created from this process is encoded using a user password and stored in the host computer, so the document is secured. The information for validity verification such as a serial number of the RFID tag can be stored in the incomplete document in order to prepare against duplication or loss of a tag. The proposed architecture will be more useful if techniques for the security of RFID are developed.

3.2. A Summary of a Digital Document

A summary of a document is created from a source document and stored in the RFID tag. It is impossible to decrypt without the summary of the document, because RFID tag which contains the summary should be used to decrypt the encrypted documents. The summary is created by extracting a bit from each byte of a digital document, and then the original bit is converted so that the original document cannot be readable. The target bit is chosen randomly, and stored in RFID tag to decrypt the digital documents. Figure 4 shows an algorithm to extract the summary.

```
byte[] summraize(byte[] bytes, int n) {

        byte packedByte[];
        int  index = 0;

        for each byte in bytes[]
          1. Get 1 bit from byte.
          2. Change the bit of the byte. ( 0 to 1, 1 to 0 )
          3. Save the bit to packedByte.
          4. if 8-bits are packed in packedByte[index], increse index.
        next

        return packedBytes;
}
```

Figure 4. A Summary of a Digital Document

The summary is generated using the algorithm and its size is about one eighth of the original document size. This size can be not acceptable with consideration for current capacity limitation of the RFID tags. However the size and performance of the tags have been improving rapidly, it is expected that the problem would be solved in the foreseeable future.

4. Implementation of an RFID-based Security Application

4.1. Overview

We implemented a prototypical RFID-based security application on the proposed architecture. This application can encrypt and decrypt the digital document using simple cryptographic algorithm based on XOR operation (a XOR key = c, c XOR key = a) and a

RFID tag. And, we used a serial number of the RFID tag to validate the RFID tag. If a more powerful cryptographic algorithm and RFID tag validation mechanism is used, enhanced security of the document will be guaranteed.

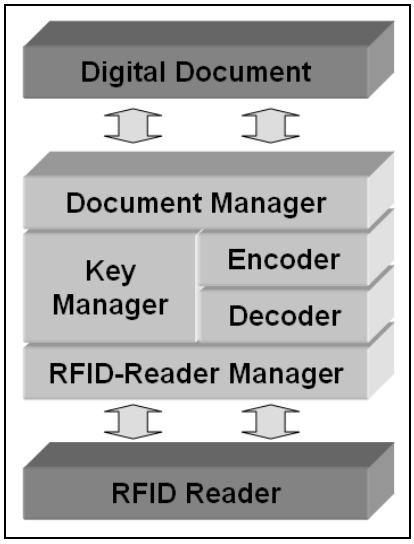

Figure 5. The Structure of the Application based on the Proposed Architecture

The application consists of 5 modules – Document Manager, Key Manager, Encoder, Decoder and RFID-Reader Manager. Document Manager manages the encryption and the decryption of digital documents. Key Manager generates and manages the encryption key. Encoder encrypts digital documents and Decoder decrypts the documents. RFID-Reader Manager manages a RFID reader. Figure 5 presents the structure of the application. The detailed description of each module of the application is represented in the Table 1.

Table 1. The Modules of the Application based on the Architecture

Module	Description
Document Manager	This module manages the encryption and the decryption of digital documents. The module also extracts a summary from a digital document in the encryption process. The module generates the original document by combining the encrypted document and the summary of the document in the decryption process. Additionally, The module can insert some information to validate the RFID tag such as the serial number of the RFID-tag.
Key Manager	This module generates a random bit-string for the key. The module also generates the key using a user password for encryption and decryption of a digital document. The random bit-string is generated in the encryption process. The key is decrypted by combining the user password and the information on the RFID tag in the decryption process.
Encoder	This module encodes a digital document using the key generated by the Key Manager.
Decoder	This module decodes an encrypted digital document using the

	key decrypted by the Key Manager.
RFID-Reader Manager	This module communicates with the RFID reader in order to read and write the information of the RFID tag.

Figure 6 shows the class diagram for the application.

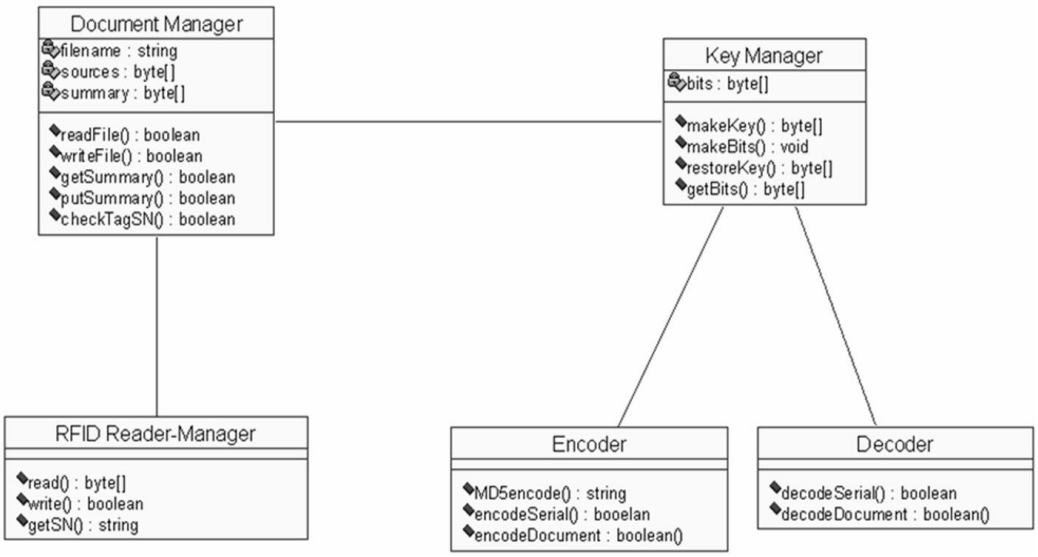

Figure 6. The Class Diagram for an RFID-based Security Application

The encryption process is initiated with source digital document, and the application summarizes the document at first. Then, a key which is generated using random bit sequence for encryption is used for document encryption. Lastly, the random bit sequence for key and document summary is saved in RFID-tag. Figure 7 shows the encryption process.

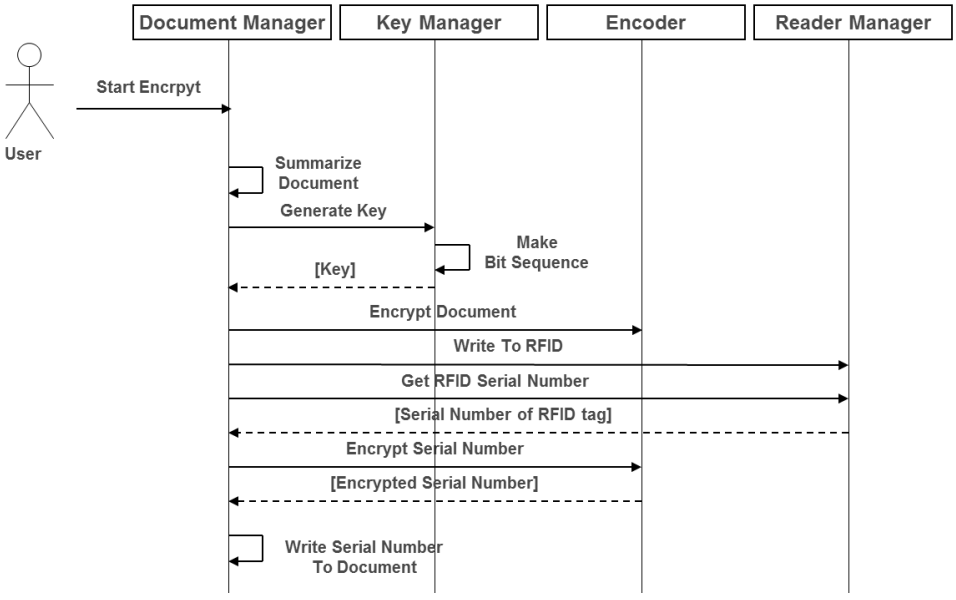

Figure 7. The Encryption Process

The decryption process is initiated with encrypted digital document, and input the password with RFID tag. Then, the application validate the RFID tag and generate the key for the decrypting the digital document. After generation of the key, the encrypted digital document is decrypted using it. Lastly, the summary of the digital document in RFID tag is combined for restoring the original digital document. Figure 8 shows the decryption process.

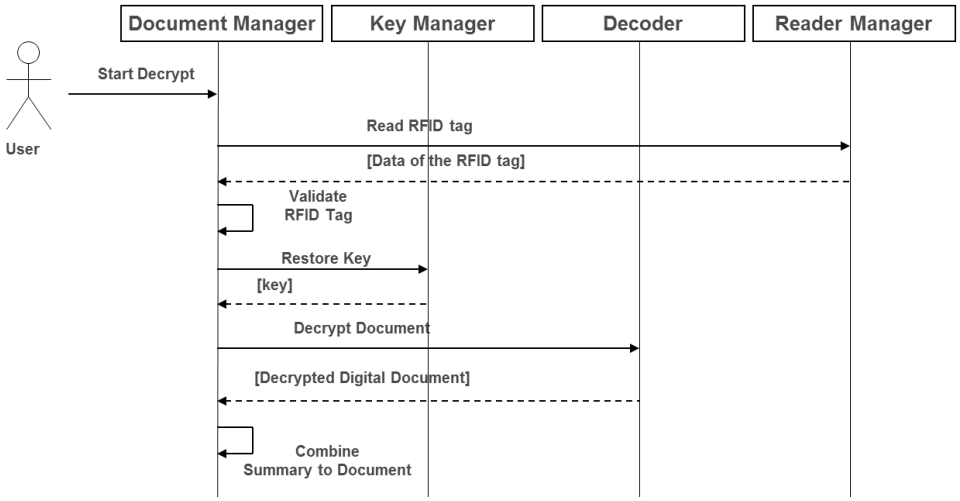

Figure 8. The Decryption Process

4.2. Implementation of the Application

The application is simply implemented for demonstration. Figure 6 shows the user interface of the application.

Figure 7. The User Interface of the Application

We encrypt and decrypt a digital document using the application. Figure 7 shows the original digital document. We used a text file for a test, but the application can encrypt and decrypt most digital documents such as MS word files, excel files, image files and various word processor files. The M210-2G which is a RFID reader and Pico Tag (2K bytes) which is the RFID tag made by Inside Contactless are used for this test.

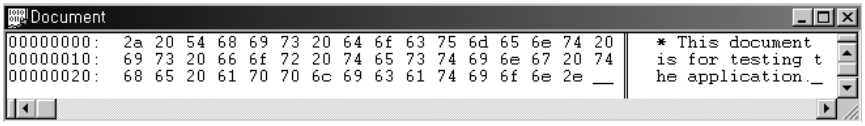

Figure 8. An Original Digital Document

Figure 8 shows the incomplete document after extracting a document summary by the application. Even if the incomplete document is stolen, the information of the document is safe because there is not complete information to restore the document. So, the security of the digital documents is guaranteed even on the network. Only the person who has the RFID tag can read the complete document in the host computer or on the network. The figure of the completely encrypted document is omitted for brevity.

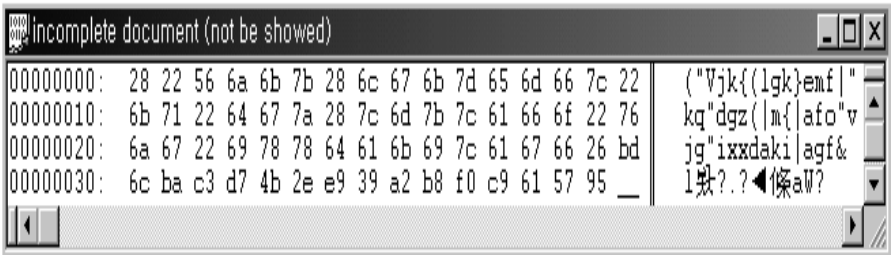

Figure 9. An Incomplete Document after Extracting Document Summary

Figure 9 shows the information in the RFID tag to recover the document. The information to recover the document is stored in block 3 in the RFID tag. The first 4 bytes of block 3 is the size of information to recover. The rest bytes are the summary of the document and the random bit-string. If the security of the RFID technology is improved, proposed architecture guarantees more powerful security of the digital document.

Block Description	Hexadecimal	ASCII
Serial Number	$84$00$22$00$01$00FFFF	" r ÿÿÿ
Configuration Block	FFFFFFFF$F9$1FFFAD	ÿÿÿ?ÿ?ÿÿ
Application Issuer Area	FFFFFFFFFFFFFFFF	ÿÿÿÿÿ 0
Block 3	$00$0A$30$62$6A$25$70$66	bj %pf
Block 4	$20$63$63$78$10$DB$88$3A	ccx┼?: o
Block 5	$6F$A4$76$D9$95$5D$06$3F	¤v?] -?d3
Block 6	$64$33FC2E$61$00$00$00	?a

Figure 10. Decryption Information Stored in the RFID-tag

5. Evaluation

The proposed architecture provides more security and higher usability of digital documents than typical security architectures such as software or hardware based encryption and protection architecture by incorporating both of them. The architecture guarantees the safety of the document on the network by saving some information in the RFID tag. This enables an authenticated user can use the document anywhere throughout the network. And by not exposing the complete information of the document on the network, the security of the document is enhanced. If only an encryption is used, the security of the document on the network is guaranteed but the complete information of the document is exposed to everyone so its security can be threatened. And if the protection with an external storage device is only used, the security of the document on the network can be not guaranteed. Table 2 shows a comparison of securing architectures for digital documents.

Table 2. A Comparison of Securing Architectures for Digital Documents

Architecture / Criterion	Protection Architecture	Encryption Architecture	RFID-based Architecture	Comment
Authentication	By the user password and the external storage medium	By the user password	By the user password and the RFID-tag information	▪ Two-way authentication has been adopted. This ensures highe security of protected data.
Securing Medium	External storage device with authentication S/W (no encryption)	Encryption Software	Encryption Software and external storage device (encryption used)	▪ Make up for the weak points by incorporating two architectures.
Security of protected data	Whole protected data is hard to be stolen through a network	Whole protected data can be easily stolen through a network	Whole protected data is hard to be stolen through a network	▪ It reduces the security to expose whole data on a network ▪ Some of data can be stolen but not whole data
Safety of protected data	Higher possibility of losing data by damaged external storage devices	Lower possibility of losing data by damaged internal storage devices	Lower possibility of losing data by damaged RFID-tags	▪ RFID-tag is relatively safe from physical impact and impurities such as water.
Secure transmission of protected data through networks	The security of data is guaranteed only when the data is in external storage devices	The security of data is guaranteed even on networks	The security of data is guaranteed even on networks	▪ Secure transmission ensures higher usability and accessibility of the data for authenticated user.
Hardware interface	Widely used	-	Not Widely used	▪ it can limit the usability of proposed architecture but this could increase the security of the data with a private interface.

Because an RFID tag is relatively safer and more portable than other storage devices such as disks and USB memory sticks, it is an appropriate device for our architecture. Furthermore, because it is possible to minimize the size of the RFID tag, it can be applied to various applications. For example, it can be applied to the DRM (Digital Rights Management). In this case, digital contents are encrypted by the information on the RFID tag attached to the

product. So, only the person who has the original product can access the digital contents in the product, and any other persons who duplicated the contents cannot use the contents. In this way, the rights of the digital contents can be protected.

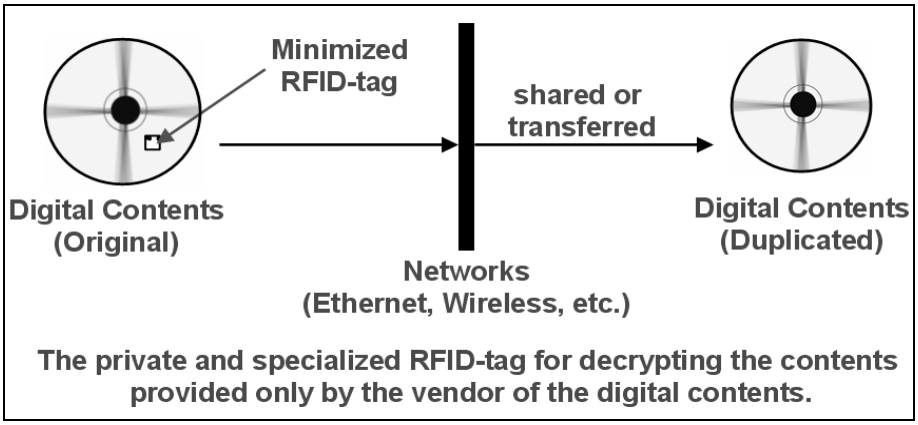

Figure 11. An Application of this Work for DRM

But for the proposed architecture to be more acceptable, it is essential that the RF communication in the RFID technology is improved to be more reliable and the capacity of the RFID tag is increased. Because many works on the RFID technology are under way throughout the world, those improvements are will be achieved in the foreseeable future, and the proposed architecture will be more useful.

6. Conclusion and Future Work

In this paper, we proposed a new security architecture for digital documents using RFID. This provides a powerful security measure for the documents by incorporating software encryption and software-based or hardware-based protection. The RFID tags can be minimized for higher portability than other storage devices and also have higher physical safety than others. So, it guarantees not only more enhanced security for the documents but also high usability.

With a proposed architecture, companies or organizations using an intranet can secure their confidential documents as the authorized users who have the proper RFID tag only can access the documents. Also, intellectual property in DRM can be protected by the RFID tag attached to the product in the foreseeable future. In the future, we will improve the architecture to overcome the problem of RFID tags' limited capacity and the security of communication between a RFID reader and tags.

References

[1] J. Choi, J. Kim and J. Park, "A RFID-based Security Architecture for Digital Documents", 2014 International Conference on Future Information and Communication Engineering (ICFICE), **(2014)**, pp. 445-448.
[2] L. D. Murphy, "Digital documents in organizational communities of practice: a first look", System Sciences, 2001, Proceedings of the 34th Annual Hawaii International Conference on. **(2001)**, IEEE.
[3] S. Jianghong and C. Jingke, "Information security of electronic documents on the environment of network", Journal of Intelligence, **(2005)**, pp.55-59.
[4] X. Hu and L. Ma, "A Study on the Hybrid Encryption Technology in the Security Transmission of Electronic Documents", Information Science and Management Engineering (ISME), **(2010)**, pp. 60 – 63.
[5] R. S. Chunyong Yin, "The Design of Secure Document Management", Proc. Applied Computing, Computer Science, and Computer Engineering (ACC2009), Engineering Technology Press **(2009)**, pp. 32-34.

[6] S. Shepard, "RFID (McGraw-Hill Networking Professional)", McGraw-Hill, **(2004)**.
[7] S. A. Weis, "RFID Privacy Workshop", Security and Privacy Magazine, IEEE, vol. 2, no. 2, **(2004)**, pp. 48 – 50.
[8] R. Want, "Enabling ubiquitous sensing with RFID," Computer vol. 37, no. 4, **(2004)**, pp. 84 – 86.
[9] K. Sangani, "RFID sees all", IEE Review, vol. 50, no. 4, **(2004)**, pp. 22 – 24.

Authors

Jaehyun Choi, received the Ph.D. degree in Computer Science from Soongsil University in Korea, 2011. He is a profressor at Graduate School of Software, Soongsil University. His research interests are in areas of Data Processing, Service Engineering, Software Engineering, and Text Mining, and Open Source Software.

Jong-Bae Kim, he received his bachelor's degree of Business Administration in University of Seoul, Seoul (1995) and master's degree(2002), doctor's degree of Computer Science in Soongsil University, Seoul(2006). Now he is a professor in the Graduate School of Software, Soongsil University, Seoul, Korea. His research interests focus on Software Engineering, and Open Source Software.

Jeawon Park, received the Ph.D. degree in Computer Science from Soongsil University in Korea, 2011. He is a profressor at Graduate School of Software, Soongsil University. His research interests are in areas of Software Testing, Software Process, Web Services, and Project Management, and Open Source Software.

