ITC 2/47
Journal of Information Technology and Control
Vol. 47 / No. 2 / 2018
pp. 262-274
DOI 10.5755/j01.itc.47.2.18506

A Biometric-Based Authentication and Anonymity Scheme for Digital Rights Management System

Received 2017/12/08 | Accepted after revision 2018/04/20

http://dx.doi.org/10.5755/j01.itc.47.2.18506

A Biometric-Based Authentication and Anonymity Scheme for Digital Rights Management System

Cheng-Chi Lee
Department of Library and Information Science, Fu Jen Catholic University, No. 510, Zhongzheng Rd., Xinzhuang Dist., New Taipei City, 24205, Taiwan, R.O.C.
Department of Photonics and Communication Engineering, Asia University, Wufeng Shiang, Taichung, Taiwan 413, R.O.C.

Chun-Ta Li
Department of Information Management, Tainan University of Technology, ZhongJheng Road, Tainan 710, Taiwan, R.O.C., *Corresponding E-mail: th0040@mail.tut.edu.tw

Zhi-Wei Chen
Department of Library and Information Science, Fu Jen Catholic University, No. 510, Zhongzheng Rd., Xinzhuang Dist., New Taipei City, 24205, Taiwan, R.O.C.

Yan-Ming Lai
Department of Computer Science and Information Engineering, National Taiwan University, No. 1, Sec. 4, Roosevelt Rd., Taipei City, 10617, Taiwan, R.O.C.

Corresponding author: th0040@mail.tut.edu.tw

Digital rights management (DRM) systems are access control technologies used to restrict the use, modification, and distribution of protected digital contents. The success of a DRM system relies heavily on a good user authentication mechanism, and user identity verification through biometric information check is a great idea in that the biological characteristics are unique to each user and that such a mechanism releases the user of the trouble of keeping the login info safe from being stolen or mistaken or forgotten. In this paper, we shall review and cryptanalyze the Jung et al.'s biometric-based authentication scheme. Then, we remedy their security weaknesses to develop our new biometric-based authentication scheme for DRM. Our correctness check, security analysis, and performance evaluation have proved the superiority of our new scheme over related schemes.

KEYWORDS: Access control, Biometric, Digital rights management, Mobile device user's authentication.

1. Introduction

1.1. Background

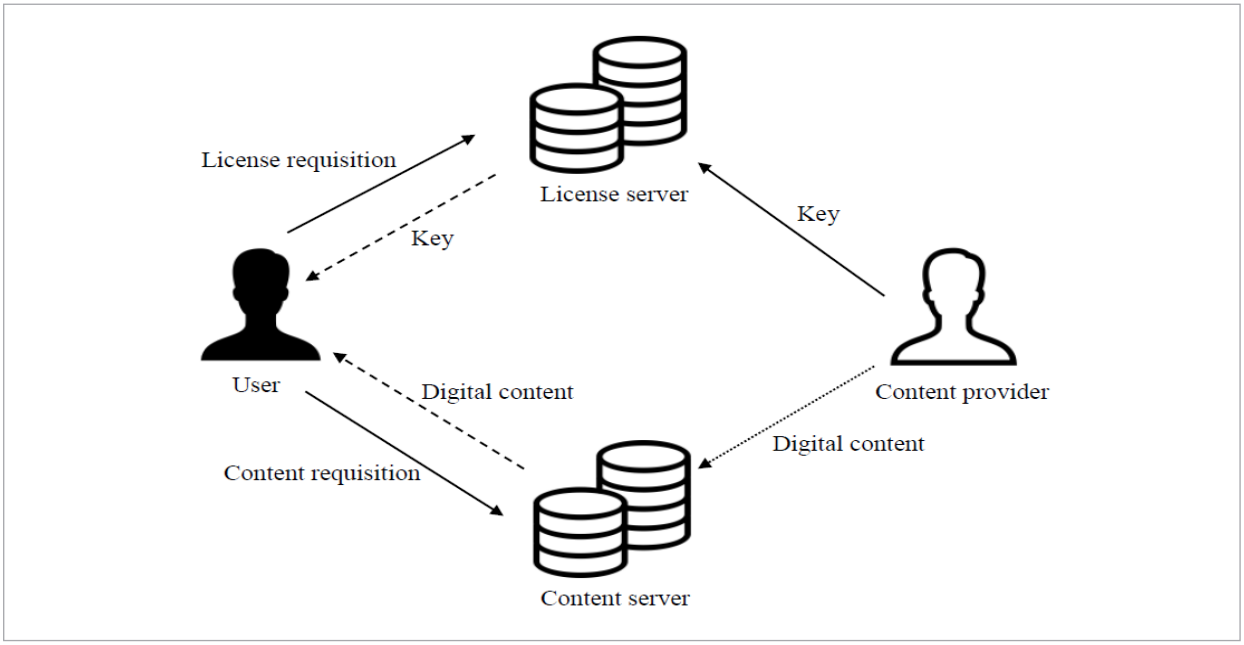
As a result of the advancement of computer technologies, more and more traditional contents originally in their physical, analog, or broadcast forms such as paper documents or photos, compact cassettes, videotapes and a lot more have been converted into digital contents. In the meanwhile, the booming development of the Internet has connected exponentially growing numbers of people together and made it extremely easy and fast to spread all kinds of data around. In fact, legal access to copyrighted digital contents over the Internet is a swelling market because more and more people are now in the habit of getting informed and entertained online [13-14, 17, 23-25].

Conforming to the overall trend in technology, modern mobile devices are designed to be as small and lightweight as possible so as to offer greater convenience. As a result, people are becoming increasingly dependent on their mobile devices, getting connected to the rest of the world through the mobile devices twenty-four seven no matter where they are and what they are doing. Naturally, when people feel like accessing digital contents through the Internet, chances are they will most likely do that on their mobile devices [1, 2].

In fact, nowadays digital contents are way too easy to spread and to obtain on the Internet than they should. In many countries around the world, unauthorized downloading of copyrighted digital contents is a serious problem, causing great losses to the authors and legitimate owners. Therefore, the enforcement of copyright protection of digital contents is very important, and the development of an ideal digital rights management (DRM) system is essential so it can be guaranteed that only copyright owners or authorized users have access to the copyrighted digital media [5-7, 19-20, 27-32]. Generally speaking, a DRM system is a specially constructed environment where the access to the digital content is restricted only to authorized users. Below is a brief introduction of a typical DRM system architecture and the roles involved:

Digital Rights Management system (DRM system) The access control to the digital content relies on a good user identity verification mechanism. Fig. 1 shows the basic architecture of a DRM system, where there are four main roles involved: (1) the content provider, (2) the content server, (3) the license server,

Figure 1
Basic architecture of a DRM system



and (4) the user [5-7, 9, 19-20, 23-28], described respectively as follows:

1. **Content provider.** The content provider is the creator and owner of a digital content that the user needs. Having completed the creation of the digital content, the content provider uses a secret key to encrypt the digital content. Then, the secret key is transmitted to the license server through a secure channel. Meanwhile, the encrypted digital content is transmitted to the content server through a secure channel such as a Virtual Private Network (VPN). In general, we can also use a symmetric cryptosystem to develop a secure cannel.
2. **Content server.** Upon receiving the encrypted digital content, the content server stores it in a database. Then, the content server will show an abstract of the encrypted digital content on a website to attract the attention of possible users.
3. **License server.** Upon receiving the secret key, the license server stores it in a database. If a user needs the secret key of the encrypted digital content, the user and the license server perform mutual authentication. If the mutual authentication succeeds, the user is authorized and is given the secret key of the encrypted digital content.
4. **User.** Attracted to the abstract posted on the website, the user decides to access the digital content over the Internet. Now the user has to send a request to the content server for the encrypted digital content and at the same time send a request to the license server for the secret key. Upon receiving the requests, the license server and the content server both authenticate the user. Only when the identity of the user checks out can the user obtain the encrypted digital content from the content server and the secret key from the license server. Then, using the secret key, the user can decrypt the encrypted digital content. That means the user's access to the digital content online is a success.

Many methods can be used to authenticate users, and biometric verification is one of the most effective methods. Biometric verification is an identity authentication process used to confirm a claimed identity by means of checking some uniquely identifiable biological traits of the person such as fingerprints, hand geometry, facial geometry, iris patterns, or voice patterns. In this method, a record of a person's unique characteristic is captured and kept in a database. Later on, when identity verification is required, a new record is captured and compared with the previous record in the database. If the data in the new record matches that in the database record, the person's identity is confirmed. In other words, this method is designed to allow a user to prove his or her identity by supplying a biometric sample in order to gain access to a secure environment. Using biometric traits instead of a username-password design has the following advantages: (1) biometric traits cannot be lost or forgotten, (2) biometric traits are difficult to share or copy, (3) biometric traits cannot be guessed, and (4) biometric traits are difficult to steal [4, 8, 10, 12, 15, 18, 21-22].

1.2. Related Works

In recent years, the topic of digital rights management has received a lot of attention, and many researchers have designed and offered their schemes in the hope of helping construct handy, practical digital rights management systems. In 2008, Chen proposed a secure and traceable E-DRM system based on mobile device [7], which is the first DRM authentication scheme to use biometric verification. In 2010, Chang et al. found some weaknesses in Chen's scheme, pointing out that an attacker could easily steal the digital content by using an intercepted key and that the mobile user would not be able to tell if anything had been tampered [6]. As an improved version of Chen's scheme, Chang et al. proposed an efficient and reliable E-DRM protocol, which is also a DRM authentication scheme based on biometric verification for mobile environments. However, in 2013, Chang et al. pointed out that Chang et al.'s 2010 scheme was actually vulnerable to the stolen device attack and that the mobile user could not change passwords or biometric data on the mobile device [5]. To solve these problems, Chang et al. proposed a practical secure and efficient enterprise digital rights management mechanism suitable for mobile environment. In 2015, Mishra et al. showed that Chang et al.' s 2013 scheme was weak against the off-line password-guessing attack and the insider attack; to mend these security flaws, Mishra et al. proposed an anonymous and secure biometric-based enterprise digital rights management system for mobile environment [19].

Other than those schemes mentioned above that are

especially designed for DRM systems, there are also authentication protocols to be applied in different systems that have a similar architecture to that of a DRM system. For example, Jung et al.'s scheme is designed for the integrated EPR (electronic patient records) information system [11], but the architecture of the scheme is quite applicable to the DRM system environment. Note that the EPR system is to provide protected electronic transactions in e-medicine systems.

The contributions of this paper are as follows:

1 We depict the system architecture of the DRM system and introduce some related works for DRM system.
2 We demonstrate that the Jung et al.'s scheme is vulnerable to some security weaknesses.
3 We propose a modified version of Jung et al.'s scheme and applied it to DRM system.

1.3. Organization of the Paper

The rest of this paper is organized as follows. In Section 2, we shall review Jing et al.'s scheme and show some security weaknesses of the scheme. In Section 3, we shall present our novel protocol in detail. After that, in Section 4, we shall show the results of our analyses on the proposed protocol's correctness, security, and performance. Finally, the conclusion will be in Section 5.

2. Review and Cryptanalysis of Jung et al.'s Scheme

In this section, we review and cryptanalyze Jung et al.'s scheme [11]. Table 1 is a list of the notations used both in Jung et al.'s scheme and in our new scheme. Please note that Jung et al.'s scheme is especially designed for the integrated electronic patient records (EPR) information system, where patients' medical records are stored in cloud and only legally certified doctors or nurses can access the data. Since the architecture of the EPR information system is similar to that of the DRM system, the basic structure of Jung et al.'s scheme is quite applicable to an authentication protocol for the DRM system. Jung et al.'s scheme has three phases, which are (1) the user registration phase, (2) the login and authentication phase, and (3) the password change phase. In the scheme, two roles are defined, which are: (1) the user () and (2) the EPR information system server (). Jung et al.'s scheme goes as follows.

Table 1
Notations

Notation	Description
U_i	The mobile user
S_j	The EPR information system server (in Jung et al.'s scheme)
LS_j	The license server (in our scheme)
ID_i	The identity of U_i
PW_i	The password of U_i
B_i	The biometric information of U_i
K	The secret key of S_j
x	The secret key of LS_j
r_1	The random number generated by U_i
r_2	The random number generated by S_j
T_i	The timestamp
$h(.)$	One way hash function
$H(.)$	Bio-hash function
$\|\|$	Concatenation operator
$\oplus$	Bitwise XOR operator

2.1. User Registration Phase

In the user registration phase of Jung et al.'s scheme, the mobile user must provide a unique identity, a password and some biometric data on a registration request. Then, the user sends the registration request to the EPR information system server. Below are the details of Jung et al.'s registration phase.

Step 1: U_i inputs ID_i and PW_i and imprints B_i on his or her mobile device. Then, U_i computes $RPW_i=h(PW_i||H(B_i))$ and sends the registration request $\langle ID_i, RPW_i\rangle$ to S_j via a secure channel.

Step 2: Upon receiving the message, S_j verifies the user's identity. If it is valid, S_j computes $N=h(ID_i||RPW_i)$ and $v=N\oplus K$, where K is S_j's secret key. Then S_j issues a smart card with $(v, H(.), h(.))$ in it to U_i via a secure channel.

Step 3: Upon receiving the smart card, U_i computes $e=h(ID_i||PWi||H(B_i))$. Finally, U_i inputs e into the smart card. Now the smart card stores $(v, H(.), h(.), e)$.

2.2. Login and Authentication Phase

In this phase, U_i establishes a common session key with S_j, and the two parties perform mutual authentication through a public channel. Jung et al.'s login and authentication phase goes as follows:

Step 1: First, U_i inserts the smart card, inputs ID_i and PW_i, and imprints B_i. Then, U_i computes $e'=h(ID_i||PW_i||H(B_i))$ and verifies whether e' and e are equal. If the verification fails, this session is terminated. Otherwise, U_i chooses a random number r_1 and computes $RPW_i = h(PW_i||\mathrm{H}(B_i))$, $N=h(ID_i||RPW_i)$, $DID_i=ID_i\oplus N$, $C_1=ID_i\oplus r_1$, and $C_2=h(ID_i||N||r_1)$. Then U_i sends the authentication request $\langle DID_i, v, C1, C2\rangle$ to S_j via an insecure channel..

Step 2: Upon receiving the message, S_j computes $r'_1= C_1\oplus ID_i'$, $C'_2=h(ID'_i||v\oplus \mathrm{K}||r'_1)$. S_j verifies whether $C'_2=C_2$. If C'_2 passes the verification, S_j chooses a random number r_2 and computes $a = r_2||h(r_1||C_2')$ and $b=h(C_2'||r_2||r_1')$. Finally, S_j sends $\langle a, b\rangle$ to U_i via an insecure channel.

Step 3: Upon receiving the message, U_i computes $r'_2=a\oplus h(r_1||C_2)$ and $b'=h(C2||r_2'||r_1)$. Then U_i verifies whether $b'=b$. If b' passes the verification, S_j is authenticated. U_i computes $C_3=h(r_1||r_2'||C_2||h(ID_i||RPW_i))$ and sends it to S_j via an insecure channel.

Step 4: Upon receiving the message, S_j computes $C'_3=h(r_1'||r_2||C_2'||\mathrm{v}\oplus K)$ and verifies whether $C'_3=C_3$. If C'_3 passes the verification, U_i is authenticated. S_j computes a session key $SK_{U_i,S_j}=h(r_1'||r_2||a||b||ID_i')$, and U_i also computes $SK_{U_i,S_j}=h(r_1||\mathrm{r}'_2||a||b||ID_i)$. Then, U_i and S_j communicate by using SK_{U_i,S_j}.

2.3. Password Change Phase

With a password change phase, Jung et al.'s scheme makes it possible for U_i to change passwords freely on the mobile device without having to be authenticated by S_j prior to the password change. Below are the details of Jung et al.'s password change phase.

Step 1: U_i inserts the smart card, inputs ID_i and PW_i, and then imprints B_i. Then, U_i computes $e'=h(ID_i||PW_i||H(B_i))$ and verifies whether e' and e are equal. After passing the verification of e', U_i inputs a new password PW_i^{new} and computes $e^{new}=h(ID_i||PW_i^{new}||H(B_i))$. Finally, U_i replaces the current value e with e^{new}. Now the password change phase is finished.

2.4. Cryptanalysis of Jung et al.'s Scheme

Here we will point out a couple of weaknesses of Jung et al.'s scheme we have found. Below are the details.

2.4.1. Known Secret Key of Server

In Jung et al.'s scheme, the secret key of the EPR information system server can be easily figured out by an outsider. In the registration phase, upon receiving $\langle ID_i, RPW_i\rangle$, the EPR information system server computes $N=h(ID_i||RPW_i)$ and $v=N\oplus K$, where K is the secret key. After that, the server sends $\langle v, h(.), H(.)\rangle$ to the user, who stores the data. In the login and authentication phase, the user computes an anonymous identity using N, where $N=h(ID_i||RPW_i)$. In addition, v is stored in the smart card. Hence, the user can easily figure out the server's secret key K by computing $K=N\oplus v$.

2.4.2. User Anonymity Problem

In Jung et al.'s login phase, the log-in message includes U_i's anonymous identity DID_i, where $DID_i= ID_i\oplus N$. However, since the anonymous identity DID_i stays the same and is used in each login communication, an attacker who does not know the real identity of the user can still trace the fixed DID_i. Then, by observing the long-term behavior of a specific anonymous identity DID_i, the attacker might be able to guess who the user is based on some background knowledge of the user's behavior patterns. For example, an anonymous identity DID_i always browses the same shopping website through Internet at the same company. However, we know that an employee of the company likes to go shopping through Internet at our office. At that time, we can ensure that the DID_i is the employee.

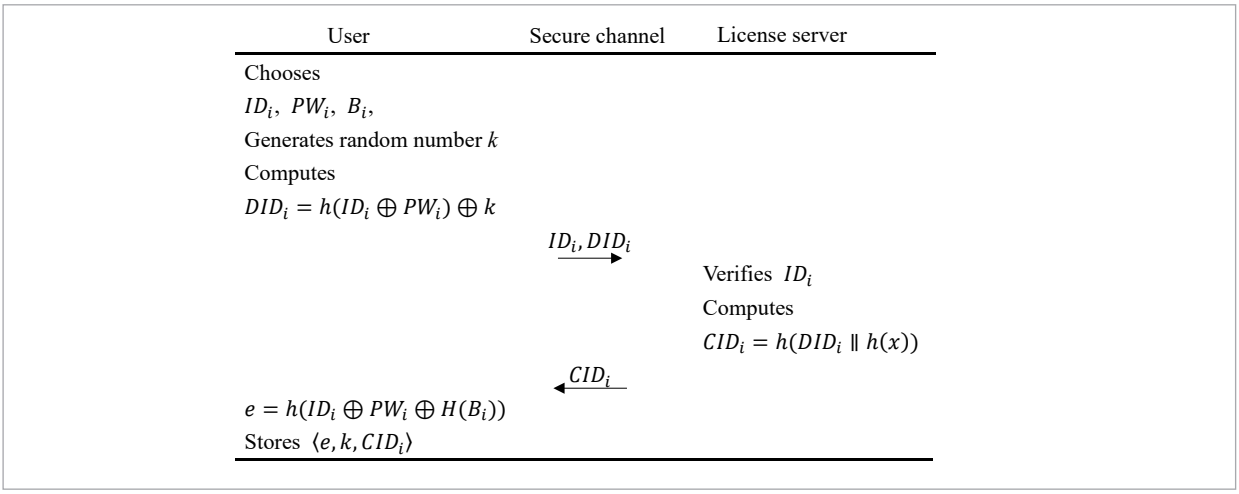
3. The Proposed Scheme

To develop a user authentication scheme for the DRM system that is applicable to mobile device users, we have adapted Jung et al.'s design and mended the weaknesses. Our new scheme also has three phases, and they are: (1) the user registration phase, (2) the login and authentication phase, and (3) the password and biometric data renewal phase. The details of our new scheme are as follows.

3.1. User Registration Phase

In the user registration phase, provides a unique identity, a password and some biometric data on a registration request, which sends to the license serv-

Figure 2
User registration phase of the proposed scheme



er (). The registration phase of the proposed scheme is illustrated in Fig. 2 and described in detail below.

Step 1: U_i inputs ID_i and PW_i, imprints B_i on his or her mobile device, and generates a random number k. After U_i computes DID_i=$h(ID_i \oplus PW_i) \oplus k$, Ui sends a registration request $\langle ID_i, DID_i \rangle$ to LS_j through a private channel.

Step 2: Upon receiving the registration request, LS_j checks the format of the identity to confirm that this is a registered identity. If it is, the registration request is rejected, and the communication is terminated. Otherwise, S_j computes CID_i=$h(DID_i||h(x))$, where x is LS_j's secret key. Finally, LS_j sends $\langle CID_i \rangle$ to Ui through the private channel.

Step 3: Upon receiving the message, U_i computes e=$h(ID_i||PW_i||H(B_i))$. U_i stores $\langle e, k, CID_i \rangle$ into the mobile device.

3.2. Login and Authentication Phase

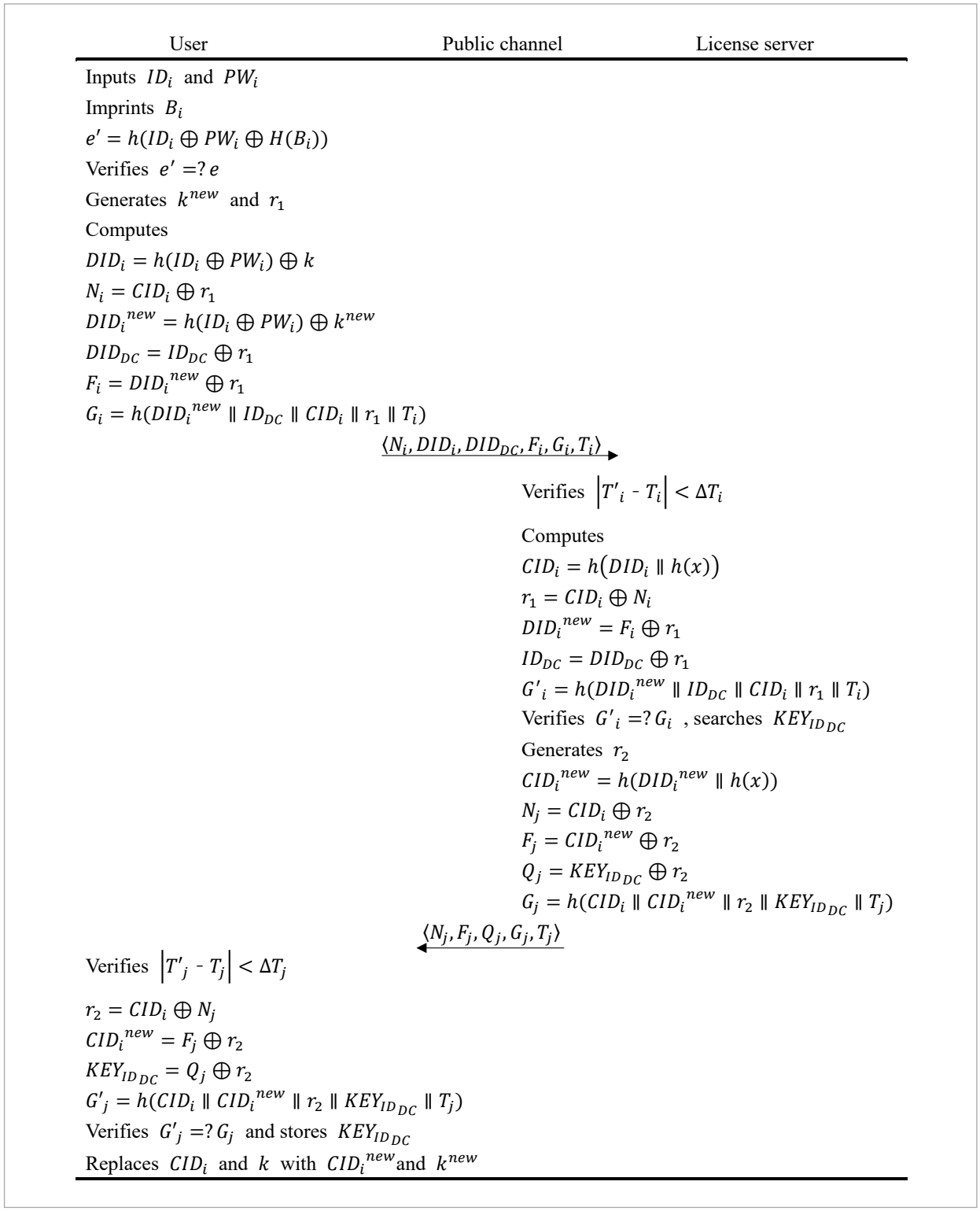
In this phase, if U_i wants to access a digital content on his or her mobile device, U_i will need the content key. To achieve the goal, U_i establishes an authentication session with LS_j. Once the user's identity is verified, LS issues the content key. The login and authentication phase of our scheme is illustrated in Fig. 3, and the detailed steps are given below.

Step 1: U_i inputs ID_i and PW_i and imprints B_i on the mobile device. U_i verifies whether e' and e are equal, where e'=$h(ID_i||PW_i||H(B_i))$. If e' checks out, U_i generates two random numbers k^{new}, r_1 and computes DID_i=$h(ID_i \oplus PW_i) \oplus k$, N_i=CIDi$\oplus r_1$, DID_i^{new}=$h(ID_i \oplus PW_i) \oplus k^{new}$, DID_{DC}=$ID_{DC} \oplus r_1$, F_i=$DID_i^{new} \oplus r_1$ and G_1=$h(||DID_i^{new}||ID_{DC}||CID_i||r_1||T_i)$, where ID_{DC} is the identity of the digital content U_i wishes to access, and T_i is the current timestamp generated by U_i. Finally, U_i sends the authentication request $\langle N_i, DID_i, DID_{DC}, F_i, G_i, T_i \rangle$ to LS_j through a public channel.

Step 2: Upon receiving the message from U_i at time T_i', LS_j first verifies the time delay in message transmission by checking whether $|T_i' - T_i| < \Delta T_i$, where ΔT_i represents the maximum transmission delay or preset acceptable delay threshold. If the verification is satisfied, LS_j computes CID_i = $h(DID_i \oplus h(x))$, r_1=$CID_i \oplus N_i$, DID_i^{new}=$F_i \oplus r_1$, ID_{DC}=$DID_{DC} \oplus r_1$, G'_1= $h(DID_i^{new}||ID_{DC}||CID_i||r_1||T_i)$ and verifies whether G'_1=G_1. If the authentication fails, the communication is terminated. Otherwise, LS_j searches and finds the key $KEY_{ID_{DC}}$ of the digital content and generates a random number r_2. Then LS_j computes CID_i^{new}=$h(DID_i^{new} \oplus h(x))$, N_j=$CID_i \oplus r_2$, F_j=$CID_i^{new} \oplus r_2$, Q_j=$KEY_{ID_{DC}} \oplus r_2$, and G_j=$h(CID_i||CID_i^{new}||r_2||KEY_{ID_{DC}}||T_j)$, where T_j is the current timestamp generated by LS_j. Finally, LS_j sends the information $\langle N_j, F_j, Q_j, G_j, T_j \rangle$ to U_i over the public channel.

Step 3: Upon receiving the message from S_j at time T_j', U_i first verifies the time delay in message transmission by checking whether $|T_j' - T_j| < \Delta T_j$, where ΔT_j represents the maximum transmission delay or preset acceptable delay threshold. If the condition is satis-

Figure 3
Login and authentication phase of the proposed scheme



fied, U_i computes $r_2=CID_i \oplus N_j$, $CID_i^{new}=F_j \oplus r_2$, $KEY_{ID_{DC}}=Q_j \oplus r_2$, and $G'_j=h(CID_i||CID_i^{new}||r_2||KEY_{ID_{DC}}||T_j)$. Then U_i verifies whether $G'_j=G_j$. If the authentication is a success, U_i stores $KEY_{ID_{DC}}$ and replaces CID_i and k with CID_i^{new} and k^{new}.

3.3. Password and Biometric Data Renewal Phase

This phase is for U_i to freely change his or her password and biometric data on the mobile device without having to contact LS_j. Below are the details of the password and biometric data renewal phase.

Step 1: After inputting ID_i, PW_i and imprinting B_i, U_i computes $e'=h(ID_i||PW_i||H(B_i))$ and verifies whether e' equals e. If $e'=e$, then U_i inputs a new password PW_i^{new} and imprints new biometric data B_i^{new}. U_i computes $e^{new}=h(ID_i||PW_i^{new}||H(B_i^{new}))$, and from now on the old value e is replaced with the new value e^{new}. This completes the password and biometric data change phase.

4. Analyses

This section will cover the correctness, security, and performance of the proposed scheme. First, we will use the result of a Burrows–Abadi–Needham logic (BAN logic) check to confirm the correctness of the proposed scheme [3, 26]. Then, we shall analyze the security of the proposed scheme to show that it satisfies some important security requirements and is strong against possible attacks. Finally, we will provide the result of a performance comparison among several related protocols to show the superior efficiency and cost-effectiveness of the proposed scheme.

4.1. Correctness Proof Based on BAN Logic

The BAN logic, which is a well-acknowledged method for the correctness check of cryptographic schemes, is used to analyze our authentication protocol [3, 26]. First, we will have some notations defined, goals set up, and an assumption made. Then, we will see how the BAN logic verification turns out. With A, B defined as participators and X as a formula, here are some instances to show the syntax and notations of the BAN logic.

Table 2
The notations of BAN logic

Notation	Description
$A\|\equiv X$	A believes X is true
$A \lhd X$	A holds or sees formula X
$A\|\equiv B$	A believes B's action. E.g., $A\|\equiv B\|\equiv X$ means that A believes B believes X is true
$A\|\sim X$	A once said formula X
$\#(X)$	X is fresh, which means X is recent or X is a nonce
$\langle C \rangle_X$	Combine condition C using X
$\langle C \rangle_X$	Perform the hash operation on C using X
$\frac{Rule\ 1}{Rule\ 2}$	$Rule\ 2$ can be derived from $Rule\ 1$. E.g., $\frac{A\ creates\ random\ X}{A\ \|\equiv \#(X)}$ means that A creates X, so A believes X is fresh

4.1.1. Goals

In order to check the correctness of our authentication protocol, we will set two goals. The legal user (U_i) and the legal server (LS_j) are the participators in our proposed scheme. Since U_i and LS_j must compute private values CID_i and CID_i^{new} to do mutual authentication, our scheme can be said to have the following two goals: (1) S_j believes that the value CID_i is true; (2) U_i believes that S_j holds or sees the value CID_i^{new}. These two goals are shown as G1 and G2 in the language of the BAN logic as follows:

G1. $S_j| \equiv U_i \lhd CID_i$

G2. $U_i| \equiv S_j| \sim CID_i^{new}$

4.1.2. Assumption

In order to analyze our scheme by using the BAN logic, we have made an assumption as follows:

A1. $U_i \lhd CID_i$

4.1.3. Verification

With the goals set up and assumption made, now we are ready to apply a BAN logic check to verify the correctness of our new scheme. The details and the steps of the proof are as follows:

Message 1. $U_i \rightarrow S_j : \{\langle r_1 \rangle_{CID_i}, (r_1)_{CID_i}, DID_i\}$

V1. $S_j \lhd \{\langle CID_i \rangle_{r1}, (r_1)_{CID_i}, DID_i\}$

V2. $\frac{S_j \lhd DID_i, S_j \lhd h(x)}{S_j \lhd CID_i}$

V3. $\frac{S_j \lhd CID_i,\ S_j \lhd \langle r_1 \rangle_{CID_i}}{S_j \lhd r_1}$

V4. $\frac{S_j \lhd CID_i, S_j \lhd r_1, S_j \lhd (r_1)_{CID_i}}{S_j | \equiv U_i \lhd CID_i}$ (G1)

Message 1. $S_j \rightarrow U_i : \{\langle r_2 \rangle_{CID_i}, \langle CID_i^{new} \rangle_{r_2}, (r_2, CID_i^{new})_{CID_i}\}$

V5. $U_i \lhd \{\langle r_2 \rangle_{CID_i}, \langle CID_i^{new} \rangle_{r_2}, (r_2, CID_i^{new})_{CID_i}\}$

V6. $\frac{U_i \lhd CID_i,\ U_i \lhd \langle r_2 \rangle_{CID_i}}{U_i \lhd r_2}$

V7. $\frac{U_i \lhd r_2,\ U_i \lhd \langle CID_i^{new} \rangle_{r_2}}{U_i \lhd CID_i^{new}}$

V8. $\frac{U_i \lhd CID_i, U_i \lhd r_2, CID_i^{new}, (r_2, CID_i^{new})_{CID_i}}{U_i | \equiv S_j | \sim CID_i^{new}}$ (G2)

According to V4, S_j believes that U_i holds the private value CID_i. Similarly, according to V8, U_i believes that S_j once said the private value CID_i^{new}. As a result, we can infer that our authentication protocol is correct.

4.2. Security Analysis

Besides fixing the problems of Jung et al.'s scheme, we shall also examine the security of the proposed scheme by checking if it satisfies several important security requirements and if it is strong enough to withstand some possible attacks. Table 3 shows how the proposed scheme compares with several other schemes of DRM architecture [5-7, 19] in terms of some security standards. Then we will give proof as to why we can say that the proposed scheme lives up to all the security standards listed.

4.2.1. Dynamic User Anonymity

In the registration phase of the proposed scheme, U_i computes a mobile user anonymous identity DID_i using a random number k. After LS_j receives DID_i, LS_j computes a secret value CID_i and sends it to U_i. Then, for each communication, U_i computes a new anonymous identity DID_i^{new} using a new random number k^{new}, and LS_j also computes a new secret value CID_i. Since U_i and LS_j both generate their own random numbers for every communication, an attacker cannot relate any two messages exchanged, and therefore the real identity of U_i cannot be traced. This means the proposed scheme satisfies the requirement of dynamic user anonymity.

4.2.2. Stolen Mobile Device Attack Resistance

Since U_i has $\langle e, k, CID_i \rangle$ stored in his or her mobile device, an adversary can steal U_i's mobile device and obtain the stored information. However, the adversary has no clue about the identity and the password, and there is no biometric data of U_i's. As a result, the adversary cannot have e verified due to the lack of $\langle ID_i, PW_iB_i \rangle$. Therefore, the adversary can do nothing with the stolen mobile device.

4.2.3. Mutual Authentication

U_i and LS_j must authenticate each other before any further steps can be taken. In the login and authentication phase of the proposed scheme, LS_j and U_i check

Table 3

Security comparison among related schemes

Scheme/proposition	1	2	3	4	5	6
Chen [7]	×	✓	✓	✓	✓	-
Chang et al. [6]	×	✓	✓	✓	✓	-
Chang et al. [5]	×	×	✓	×	✓	×
Mishra et al. [19]	×	✓	✓	✓	✓	✓
The proposed scheme	✓	✓	✓	✓	✓	✓

1. Dynamic user anonymity
2. Stolen mobile device attack resistance
3. Mutual authentication
4. Insider attack resistance
5. Replay attack resistance
6. Off-line password guessing attack resistance

whether G_i and G_j are correct respectively. Only when all the verifications are successful can the communication continue. Obviously, the proposed scheme satisfies the requirement of mutual authentication between user and server.

4.2.4. Insider Attack Resistance

In the proposed scheme, the user does not directly provide his or her real identity and password; instead, in the login and authentication phase, what U_i sends to LS_j is DID_i in public channel, where $DID_i = h(ID_i \oplus PW_i) \oplus k$. Such a design keeps LS_j from learning PW_i, which is hidden by using the random number k. This means the proposed scheme can withstand the insider attack. The ID_i can be verified by checking the G_i. Only legal user can compute G_i by using his/her identity and password and only legal server can compute G'_i by using his/her secret key x.

4.2.5. Replay Attack Resistance

Suppose that an adversary intercepts the user's login and authentication request $\langle N_i, DID_i, DID_{DC}, F_i, G_i, T_i \rangle$. Since G_i includes a timestamp generated by U_i, the request is only valid during that very communication session. In other words, if the adversary tries to login to the server by replaying the intercepted login and authentication request, the authentication will fail because the request has expired. Therefore, we can say that the proposed scheme is secure against the replay attack.

4.2.6. Off-line Password Guessing Attack Resistance

If an attacker has stolen the mobile device and knows $\langle e, k, CID_i \rangle$, the attacker still cannot obtain U_i's password and cannot work out the value e by computing $e = h(ID_i \oplus PW_i \oplus B_i)$ due to the lack of U_i's biometric data B_i. Therefore, the proposed scheme is secure against the password guessing attack.

4.3. Performance Analysis

To have a clue how well our new scheme can perform, we have made comparisons of communication cost, computation cost, and storage spaces among some related schemes [5-7, 19].

The communication cost comparison is in Table 4. We just compare the communication cost in mobile user for login and authentication phase. The symbol c stands for the count of the transmission time. We can see that the communication cost of the other related schemes are all $3c$. Hence, our scheme is superior to other related schemes.

Table 4
Comparisons with the communication cost among related schemes

Scheme	Login and authentication phase
	Communication cost for mobile user
Chen [7]	$3c$
Chang et al. [6]	$3c$
Chang et al. [5]	$3c$
Mishra et al. [19]	$3c$
The proposed scheme	$2c$

The computation cost comparison is in Table 5. The notations used in the table are defined as follows:

- T_{Rep}: the time for computing fuzzy extractor function [19].
- T_h: the time for computing a hash function.
- T_{xor}: the time for computing exclusive-or operation.

We conclude that our proposed scheme is only worse than the Chang et al.'s scheme [5]. However, Mishra et al.' have pointed out that the Chang et al.'s scheme is not secure. Hence, our scheme is superior to other related schemes.

Table 5
Comparisons with the computation cost among related schemes

Scheme	Login and authentication phase
	Computation cost for mobile user
Chen [7]	$(8+2i)\ T_h+12T_{xor}$
Chang et al. [6]	$9T_h+12T_{xor}$
Chang et al. [5]	$6T_h+4T_{xor}$
Mishra et al. [19]	$1T_{Rep}+6T_h+4T_{xor}$
The proposed scheme	$6T_h+12T_{xor}$

*i: login number

Table 6
Comparisons with the storage spaces among related schemes

Scheme	Login and authentication phase
	Storage spaces for mobile user
Chen [7]	$S(N_i)+S(IMEI)+S(Cert)+S(CID)+S(P_i)+S(P_{i-1})+S(SEED)$
Chang et al. [6]	$S(N_i)+S(IMEI)+S(Cert)+S(CID)+S(KEY_{CID})+S(SEED)$
Chang et al. [5]	$S(H(Anonymity\_ID \oplus X))+S(IMEI)+S(CID)+S(KEY_{CID})$
Mishra et al. [19]	$S(r^*)+S(Z_{MU})+S(t)+S(\tau_{MU})+S(DID_{MU})+S(Y_{MU})+S(KEY_{CID})$
The proposed scheme	$S(e)+S(k)+S(CID_i)+S()$

*$S()$: storage space

The storage space comparison is in Table 6. We denote the symbol $S(.)$ is the consumption of the storage space. We can see that our proposed scheme is superior to other related schemes. It only costs four storage spaces which is better than other schemes.

5. Conclusion

In this paper, we have proposed a novel and secure authentication protocol for DRM system. Our new scheme uses biometric data for user identity verification because the biological characteristics are unique to each user and cannot be stolen or mistaken or forgotten. As an improved version of Jung et al.'s work, the proposed scheme provides better security protection and is especially designed for DRM systems. A BAN logic check has verified the correctness of our new protocol; besides, our security comparison and performance comparison have established that our new protocol offers the best security protection and is the fastest and most cost-effective scheme among similar protocols for DRM system. In future works, we will use some formal tools, such AVISPA tool or ProVerif tool, to verify our proposed scheme. For big encrypted data, we will provide an efficient searching techniques to protect their privacy and data confidentiality on our DRM system.

Acknowledgments

The authors would like to thank the anonymous referee for their valuable discussions and comments. Moreover, this research was partially supported by the Ministry of Science and Technology, Taiwan, R.O.C., under contract no.: MOST 106-3114-E-030-001.

Reference

1. Amin, R., Biswas, G. P. An Improved RSA Based User Authentication and Session Key Agreement Protocol Usable in TMIS. Journal of Medical Systems, 2015, 39(8), 1-14. https://doi.org/10.1007/s10916-015-0262-y
2. Amin, R., Hafizul Islam, S. K., Biswas, G. P., Giri, D., Khan, M. K., Kuma, N. A More Secure and Privacy-aware Anonymous User Authentication Scheme for Distributed Mobile Cloud Computing Environments. Security and Communication Networks, 2016, 9, 4650-4666. https://doi.org/10.1002/sec.1655
3. Burrows, M., Abadi, M., Needham, R. A Logic of Authentication. ACM Transactions Computer Systems, 1990, 8(1), 18-36. https://doi.org/10.1145/77648.77649
4. Burnett, A., Byrne, F., Dowling, T., Duffy, A. A Biometric Identity Based Signature Scheme. International Journal of Network Security, 2007, 5(3), 317-326.
5. Chang, C. C., Chang, S. C., Yang, J. H. A Practical Secure and Efficient Enterprise Digital Rights Management Mechanism Suitable for Mobile Environment. Securi-

ty and Communication Networks, 2013, 6(8), 972-984. https://doi.org/10.1002/sec.647

6. Chang, C. C., Yang, J. H., Wang, D. W. An Efficient and Reliable E-DRM Scheme for Mobile Environments. Expert Systems with Applications, 2010, 37(9), 6176-6181. https://doi.org/10.1016/j.eswa.2010.02.110
7. Chen, C. L. A Secure and Traceable E-DRM System Based on Mobile Device. Expert Systems with Applications, 2008, 35(3), 878-886. https://doi.org/10.1016/j.eswa.2007.07.029
8. Dodis, Y., Reyzin, L., Smith, A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. Proceeding of Advances in Cryptology-EUROCRYPT, Interlaken, Switzerland, 2004, 523-540.
9. Huang, Q. L., Yang, Y., Fu, J., Niu, X. Secure and Privacy-Preserving DRM Scheme Using Homomorphic Encryption in Cloud Computing. The Journal of China Universities of Posts and Telecommunications, 2013, 20(6), 88-95. https://doi.org/10.1016/S1005-8885(13)60113-2
10. Jain, A. K., Ross, A., Prabhakar, S. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 14(1), 4-20. https://doi.org/10.1109/TCSVT.2003.818349
11. Jung, J. K., Kang, D. W., Lee, D. H., Won, D. H. An Improved and Secure Anonymous Biometric-Based User Authentication with Key Agreement Scheme for the Integrated EPR Information System. Plos One, 2017, 12(1), 1-26. https://doi.org/10.1371/journal.pone.0169414
12. Kamal, K., Ghany, A., Moneim, M. A., Ghali, N. I., Hassanien, A. E., Hefny, H. A. A Symmetric Bio-Hash Function Based on Fingerprint Minutiae and Principal Curves Approach. Proceedings of 3rd International Conference on Mechanical and Electrical Technology, (ICMET-China), Dalian, China, 2011, 405-410.
13. Kim, H., Lee, Y., Park, Y. A Robust and Flexible Digital Rights Management System for Home Networks. Journal of Systems and Software, 2010, 83(12), 2431-2440. https://doi.org/10.1016/j.jss.2010.04.064
14. Ku, W., Chi, C. Survey on the Technological Aspects of Digital Rights Management. Proceeding of International Conference on Information Security, Toulouse, France, 2004, 391-403. https://doi.org/10.1007/978-3-540-30144-8_33
15. Li, C. T., Hwang, M. S. An Efficient Biometric-Based Remote User Authentication Scheme Using Smart Cards. Journal of Network and Computer Applications, 2010, 33, 1-5. https://doi.org/10.1016/j.jnca.2009.08.001
16. Li, C. T., Weng, C. Y., Lee, C. C., Wang, C. C. A Hash Based Remote User Authentication and Authenticated Key Agreement Scheme for the Integrated EPR Information System. Journal of Medical Systems, 2015, 39(11), 1-11. https://doi.org/10.1007/s10916-015-0322-3
17. Liu, Y., Chang, C. C., Chang, S. C. A Group Key Distribution System Based on the Generalized Aryabhata Remainder Theorem for Enterprise Digital Rights Management. Journal of Information Hiding and Multimedia Signal Processing, 2015, 6(1), 140-153.
18. Mishra, D., Das, A. K., Mukhopadhyay, S. A Secure User Anonymity-Preserving Biometric-Based Multi-Server Authenticated Key Agreement Scheme Using Smart Cards. Expert Systems with Applications, 2014, 41(18), 8129-8143. https://doi.org/10.1016/j.eswa.2014.07.004
19. Mishra, D., Das, A. K., Mukhopadhyay, S. An Anonymous and Secure Biometric-Based Enterprise Digital Rights Management System for Mobile Environment. Security and Communication Networks, 2015, 8(18), 3383-3404. https://doi.org/10.1002/sec.1266
20. Mishra, D., Mukhopadhyay, S. Cryptanalysis of Yang et al.'s Digital Rights Management Authentication Scheme Based on Smart Card. Recent Trends in Computer Networks and Distributed Systems Security, 2014, 420, 288–297. https://doi.org/10.1007/978-3-642-54525-2_26
21. Pankanti, S., Jain, A. K. Biometric Recognition: Security and Privacy Concerns. IEEE Security Privacy Magazine, 2003, 1(2), 33-42. https://doi.org/10.1109/MSECP.2003.1193209
22. Ratha, N., Karu, K., Chen, S., Jain, A. K. A Real-Time Matching System for Large Fingerprint Databases. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1996, 18(8), 799-813. https://doi.org/10.1109/34.531800
23. Rosset, V., Filippin, C., Westphall, C. A DRM Architecture to Distribute and Protect Digital Contents Using Digital Licenses. Proceedings of Advanced Industrial Conference on Telecommunications/Service Assurance with Partial and Intermittent Resources Conference/E-learning on Telecommunications Workshop (Telecommunications 2005), Lisbon, Portugal, 2005, 422-427. https://doi.org/10.1109/AICT.2005.5
24. Subramanya, S. R., Yi, B. K. Digital Rights Management. IEEE Potentials, 2008, 25(2), 31-34. https://doi.org/10.1109/MP.2006.1649008
25. Wang, C., Zou, P., Liu, Z., Wang, J. CS-DRM: A Cloud-Based SIM DRM Scheme for Mobile Internet. EURASIP

Journal on Wireless Communications and Networking, 2011, 837209. https://doi.org/10.1155/2011/837209

26. Wessels, J. CMG FINANCE B.V. Application of BAN-logic. 2001,
27. Yang, H. W., Yang, C. C., Lin, W. Enhanced Digital Rights Management Authentication Scheme Based on Smart Card. IET Information Security, 2013, 7(3), 189-194. https://doi.org/10.1049/iet-ifs.2012.0191
28. Zhang, Y., Khan, M. K., Chen, J., He, D. Provable Secure and Efficient Digital Rights Management Authentication Scheme Using Smart Card Based on Elliptic Curve Cryptography. Mathematical Problems in Engineering, 2015, 1-16. https://doi.org/10.1155/2015/807213
29. Zhang, Y. C., Yang, L., Xu, P., Zhan, Y. S. A DRM Authentication Scheme Based on Smart-Card. Proceedings of the International Conference on Computational Intelligence and Security, Beijing, China, 2009, 202-207. https://doi.org/10.1109/CIS.2009.182
30. Zeng, W., Liu, K. Sensitivity Analysis of Loss of Corporate Efficiency and Productivity Associated with Enterprise DRM Technology. Proceedings of 2012 7th International Conference on Availability, Reliability and Security (ARES), Prague, Czech Republic, 2012. https://doi.org/10.1109/ARES.2012.55
31. Zeng, W., Moorsel, A. V. Quantitative Evaluation of Enterprise DRM Technology. Electronic Notes in Theoretical Computer Science, 2011, 275, 159-174. https://doi.org/10.1016/j.entcs.2011.09.011
32. Zou, P., Wang, C., Liu, Z., Bao, D. Phosphor: A Cloud Based DRM Scheme with SIM Card. Proceedings of 12th International Web Conference (APWEB 2010), Asia-Pacific, Busan, South Korea, 2010, 459-463. https://doi.org/10.1109/APWeb.2010.43