Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 1041880, 11 pages
https://doi.org/10.1155/2022/1041880

*Research Article*

# An Improved Authentication Scheme for Digital Rights Management System

**Sajid Hussain**[1], **Yousaf Bin Zikria**[2], **Ghulam Ali Mallah**[3], **Chien-Ming Chen**[4], **Mohammad Dahman Alshehri**[5], **Farruh Ishmanov**[6] and **Shehzad Ashraf Chaudhry**[7]

[1]*Department of Cyber Security, Air University, Islamabad, Pakistan*
[2]*Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Republic of Korea*
[3]*Department of Computer Science, Shah Abdul Latif University, Khairpur, Sindh 66020, Pakistan*
[4]*College of Computer Science and Engineering, Shandong University of Science and Technology, Shandong, China*
[5]*Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*
[6]*Department of Electronics and Communication Engineering, Kwangwoon University, Seoul 01897, Republic of Korea*
[7]*Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey*

Correspondence should be addressed to Farruh Ishmanov; farruh@kw.ac.kr
and Shehzad Ashraf Chaudhry; sashraf@gelisim.edu.tr

Received 13 October 2021; Accepted 29 December 2021; Published 27 January 2022

Academic Editor: Vinayakumar Ravi



With the increasing number and popularity of digital content, the management of digital access rights has become an utmost important field. Through digital rights management systems (DRM-S), access to digital contents can be defined and for this, an efficient and secure authentication scheme is required. The DRM authentication schemes can be used to give access or restrict access to digital content. Very recently in 2020, Yu et al. proposed a symmetric hash and xor-based DRM and termed their system to achieve both security and performance efficiency. Contrarily, in this study, we argue that their scheme has several issues including nonresistance to privileged insider and impersonation attacks. Moreover, it is also to show in this study that their scheme has an incorrect authentication phase and due to this incorrectness, the scheme of Yu et al. lacks user scalability. An improved scheme is then proposed to counter the insecurities and incorrectness of the scheme of Yu et al. We prove the security of the proposed scheme using BAN logic. For a clear picture of the security properties, we also provide a textual discussion on the robustness of the proposed scheme. Moreover, due to the usage of symmetric key-based hash functions, the proposed scheme has a comparable performance efficiency.

## 1. Introduction

The rapid expansion of computer technology and media of various types such as software, music services, videos, photos, documents, and e-books is combined and manipulated as digital contents. With the invention of the low power devices, the distribution of such digital content along the globe is increased rapidly [1]. This rapid distribution demands an efficient digital rights management system to be utilized to preserve the digital rights associated with the content. A serious concern is the downloading of the contents by unauthorized users, which is a big problem and deprivation for the copyright owners. Thus, the protection of the digital contents is the major issue, and authentication is a very necessary security requirement for the prevention of unauthorized access and making the availability of the digital contents to the only legitimate users. Digital right management (DRM) systems are specifically designed environments that include some access control mechanism for the use of the digital content [2, 3]. The main purpose of the DRM system is to provide protection to the digital contents and to make sure these are only accessible to valid users. Digital content services that include important data are conveyed through the public channels, which are fully

accessible to malicious users. Hence, for the sake of secure transmission of the digital contents to the valid user through the public channel, strong authentication and key agreement schemes are needed [4–6].

In the immediate past, various authentication schemes have been proposed to make sure the privacy of the digital content and user. In 2008, Chen [7] proposed a biometric-based authentication scheme based on biometric for DRM environment. Later on, Chang et al. [8] pointed weaknesses such as attackers can steal keys and can access digital content without any permission and proposed an improved system. Later on, Chang et al. [9] pointed that [8] is insecure against stolen device attacks and proposed an improved scheme for DRM. Mishra et al. [10] proved that the scheme of Zhang et al. [11] was vulnerable to password guessing attacks and insider attacks and proposed an improved biometric-based scheme for DRM. In 2015, Jung et al. [12] proposed an ECC-based authentication scheme for DRM. In 2017, Jung et al. [12] presented a biometric-based authentication scheme for the DRM system. Later in 2018, Lee et al. [13] proved that the protocol of [10] is suspected to the secret key disclosure which leads to anonymity violation. Yu et al. [14] claimed that the method presented in [13] is insecure against user impersonation and device theft attack and proposed an improved scheme to overcome the flaws of [13].

*1.1. Adversarial Model.* The main purpose of authentication schemes for DRM systems is to provide a scalable solution for remote user successful authentication. However, the authentication protocols should oppose many active/passive attacks [15–17]. The analysis of attacks is based on the CK adversarial model [18], which is an extension of the DY model [19] with the following features:

(1) A valid user can possess the login credentials, namely, identity, password, biometric, etc. The server keeps the master key [20, 21]

(2) A public communication channel is in full control of the adversary

(3) A legal user can be dishonest [22, 23]

(4) Any malicious user can extract saved credentials in the smart card by applying a stolen attack

*1.2. System Model of DRM.* DRM system is a verification and access control method to access digital content. Figure 1 shows the DRMS common architecture comprising of four major entities: (1) the content writer/owner, (2) content server, (3) the user, and (4) license sever.

(1) The user who wants to obtain digital content transmits an authentication ask to the content and license servers. As soon as mutual authentication with the license server is successfully completed, reach to the encrypted digital content is issued with the help of a secret key

(2) The content server saves the encrypted digital content in its database receive by the digital content creator and after that abstract of the content is accessible to the users on the internet

(3) The content generator/provider provides content generation services. The digital content is generated and encrypted by the secret key. This key is transmitted to the license server using the public channel, and also encrypted digital content is also sent to the content server using a tunneled channel

(4) The license server receives the secret key and stores it in its database. When a user requires the secret key of the encrypted digital content, the license server first authenticates that user and then sends the secret key of the content

## 2. The Scheme of Yu et al.: A Review

The scheme of Yu et al. [14] is reviewed and briefly explained in this section and the notation guide which is used in this paper is depicted in Table 1.

*2.1. User Registration Phase.* The process to register a user $U_m$ with the license server $LS_j$ is depicted in Figure 2 and explained through the following steps:

(RG1) user $U_m$ chooses his/her identity $ID_m$, password $PW_m$, and marks biometrics $BIO_m$. After that $U_m$ calculates $Gen(BIO_m) = R_m, P_m$, and $RPW_m = h(PW_m \| R_m)$ and dispatches $\{ID_m, RPW_m\}$ to $LS_j$-license server via private channel

(RG2) license server $LS_j$ on receiving request containing $\{ID_m, RPW_m\}$ by $U_m$ calculates $X_m = h(ID_m \| X_{LS})$, $d_m = X_m \oplus h(ID_m \| RPW_m)$, and $f_m = h(RPW_m \| X_m)$. $LS_j$ saves $ID_m$ and $X_m$ within its database and replies the registration request message $\langle d_m, f_m$ to $U_m \rangle$ via private channel

(RG3) $U_m$ receives the message from $LS_j$ saves $\{d_m, f_m\}$ in its mobile device memory

*2.2. Login and Authentication Phase.* A registered user $U_m$ who wants to utilize the digital content $DC$ initiates a mutual authentication request with $LS_j$ with an aim to attain mutual authentication and obtain the secret key $K_C$ of the $DC$. The steps involved in the login and authentication procedure are detailed in Figure 3 and explained as follows:

(LAA 1) $U_m$ enters his/her $\{ID_m, PW_m\}$ apir and submits $BIO_m$. After that, $U_m$ calculates $R_m = Rep(BIO_m, P_m)$, $RPW_m = h(PW_m \| R_m)$, $X_m = d_m \oplus h(ID_m \| RPW_m)$, and $f_m^* = h(RPW_m \| X_m)$ and compare if $f_m^* = ^? f_m$. If the condition is true, $U_m$ creates $R_1$ randomly and calculates $Z_1 = X_m \oplus R_1$, $Z_2 = ID_m \oplus R_1$, $Z_3 = ID_c \oplus R_1$, and $Z_{US} = h(ID_m \| ID_c \| X_m \| R_1)$. Then, the user

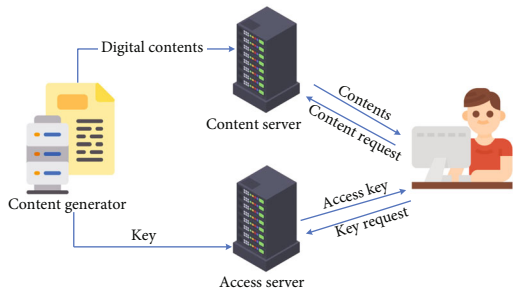


Figure 1: DRM-system-architecture.

Table 1: Symbol guide.

| Symbols | Explanations |
|---|---|
| $U_m$, $LS_j$ | Mobile user, license server |
| $ID_m$, $ID_c$ | Identities of $U_m$, $LS_j$ |
| $PW_m$, $BIO_m$ | Password and biometric of $U_m$ |
| $X_{LS}$, $K_C$ | Secret keys $LS_j$, $ID_c$ |
| $h(.)$, $H(.)$ | Hash and biohash functions |
| $R_1$, $R_2$ | Random nonces |
| $PID_m$ | Unique random nonce for each user |
| $T_m$, $T_{cs}$ | Current timestamps |
| $KEY_{DC}$ | Secret key of digital content |
| $X_{LS}$ | Master key of license server |
| $\Delta T$ | Allowed transmission delay |
| $\|\|$, $\oplus$ | Concatenation and XOR operations |

| User ($U_m$) | License server ($LS_j$) |
|---|---|
| $U_m$ inputs $ID_m$, password $PW_m$ | |
| Imprints biometric $BIO_m$ | |
| $Gen\,(BIO_m)=\langle R_m, P_m\rangle$ | |
| $RPW_m=h(PW_m\|\|R_m)$ | |
| $\langle ID_m, RPW_m\rangle$ (via secure channel) $\rightarrow$ | |
| | $X_m=h(ID_m\|\|X_{LS})$ |
| | $d_m=X_m\oplus h(ID_m\|\|RPW_m)$ |
| | $f_m=h(RPW_m\|\|X_m)$ |
| | Saves $X_m$ and $ID_m$ |
| | $\leftarrow \langle d_m, f_m\rangle$ (via secure channel) |
| Saves $\{d_m, f_m\}$ in the memory | |

Figure 2: Yu et al.'s user registration.

$U_m$ initiates the request message $\{Z_1, Z_2, Z_3, Z_{US}\}$ through public channel to $LS_j$

(LAA 2) $LS_j$ receives the request message sent by $U_m$ and calculates $R_1 = Z_1 \oplus X_m$, $ID_m = Z_2 \oplus R_1$, $ID_c = Z_3 \oplus R_1$, and $M^*_{US} = h(ID\|ID_c\|X_m\|R_1)$ and verifies if $M^*_{US} = ^? Z_{US}$. If the condition is true, $LS_j$ picks relevant $K_C$, creates random nonce $R_2$, and calculates $Z_4 = R_2 \oplus X_m$, $Z_5 = K_C \oplus X_m$ and $Z_{SU} = h(ID_m\|X_m\|K_C\|R_2)$. At the end, $LS_j$ sends the message $\{Z_4, Z_5, Z_{SU}\}$ to user $U_m$ directly through public channel

| User ($U_m$) | License server ($LS_j$) |
|---|---|
| $U_m$ inputs $ID_m$, password $PW_m$ | |
| Imprints biometric $BIO_m$ | |
| Calculates | |
| $R_{CC}=Rep(BIO_m, P_m)$ | |
| $RPW_m=h(PW_m\|\|R_m)$ | |
| $X_m=d_m\oplus h(ID_m\|\|RPW_m)$ | |
| $f^*_m=h(RPW_m\|\|X_m)$ | |
| check if $f^*_m \stackrel{?}{=} f_m$ | |
| Creates random nonce $R_1$ | |
| $Z_1=X_m\oplus R_1$ | |
| $Z_2=ID_m\oplus R_1$ | |
| $Z_3=ID_c\oplus R_1$ | |
| $Z_{US}=h(ID_m\|\|ID_c\|\|X_m\|\|R_1)$ | |
| $\langle Z_1, Z_2, Z_3, Z_{US}\rangle$ (via public channel) $\rightarrow$ | |
| | $R_1=Z_1\oplus X_m$ |
| | $ID_m=Z_2\oplus R_1$ |
| | $ID_c=Z_3\oplus R_1$ |
| | $M^*_{US}=h(ID\|\|ID_c\|\|X_m\|\|R_1)$ |
| | Check if $M^*_{US} \stackrel{?}{=} Z_{US}$ |
| | Retrieves $K_C$ |
| | Generate random nonce $R_2$ |
| | Calculate |
| | $Z_4=R_2\oplus X_m$ |
| | $Z_5=K_C\oplus X_m$ |
| | $Z_{SU}=h(ID_m\|\|X_m\|\|K_C\|\|R_2)$ |
| | $\leftarrow \langle Z_4, Z_5, Z_{SU}\rangle$ (via public channel) |
| Calculates | |
| $R_2=Z_4\oplus X_m$ | |
| $K_C=Z_5\oplus X_m$ | |
| $M^*_{SU}=h(ID_m\|\|X_m\|\|K_C\|\|R_2)$ | |
| Check if $M^*_{SU} \stackrel{?}{=} Z_{SU}$ | |
| Saves $K_C$ | |

Figure 3: Yu et al.'s login and authentication scheme.

(LAA 3) $U_m$ receives the response message from $LS_j$ and calculates $R_2 = Z_4 \oplus X_m$, $K_C = Z_5 \oplus X_m$, and $M^*_{SU} = h(ID_m\|X_m\|K_C\|R_2)$. At the end user, $U_m$ verifies if $M^*_{SU} = ^? Z_{SU}$ and saves $K_{DC}$ in the device

## 3. Cryptanalysis of Yu et al.'s Scheme

In this section, through the informal analysis of Yu et al.'s scheme [14], it is affirmed that their scheme is secure against well-known attacks. However, the following subsections demonstrate that the scheme presented in [14] is having correctness issues, is weak against ephemeral secret leakage attacks, and does not provide anonymity.

*3.1. Incorrectness.* The authentication phase of Yu et al.'s scheme cannot end normally, and the license server and user may be unable to share any key at all. The user in the Yu et al. scheme after initiating an authentication message to the license server may never receive an acknowledgment,

and the license server may never create a session key. Hence, their scheme lacks the property of authentication and key agreement. The depiction of incorrectness case is as follows:

(Inc 1) user $U_m$ sends a login request by entering password, identity, and biometric, and transmits $Z_1$ , $Z_2, Z_3, Z_{US}$ to $LS_j$ (the license server)

(Inc 2) license server $(LS_j)$ receives the request message and computes

$$R_1 = Z_1 \oplus X_m. \quad (1)$$

The computation of the above equation requires the $X_m$ corresponding requesting user identity $ID_m$, which the license server does not know. Also, the request message sent by the user $U_m$ does not include the identity of the requesting user. The license server computes the request without the information of any designated user. In the same way, the license server sends the acknowledgment message without knowing to whom this message is to be sent.

The only case in which Yu et al.'s scheme can achieve the authentication and key agreement in the view is if the system has only one registered user. Hence, systems with a single registered user are not preferable in the real world. Therefore, Yu et al.'s scheme for facilitating digital rights management systems is incorrect, and this incorrectness shows that their system is not preferable for real-world deployments.

*3.2. Privileged Insider Attack.* Yu et al.'s scheme stores the sensitive information in the database of the license server. Due to which it is susceptible to user impersonation, server impersonation attacks, and secret key leakage attacks. The attacks can be simulated in the following methods.

*3.2.1. User Impersonation Attack.* The internal adversary $\mathscr{A}$ gets $IS_m$ and $X_m$ from the database of the license server. Now the adversary $\mathscr{A}$ can impersonate as $U_m$ by adopting the following steps:

(IUA 1) $\mathscr{A}$ picks a random number $R_{UA}$

(IUA 2) computes $Z_1 = X_m \oplus R_{UA}$, $Z_2 = ID_m \oplus R_{UA}$, $Z_3 = ID_c \oplus UA$, and $Z_{AUS} = h(ID_m \| ID_c \| X_m \| UA)$

(IUA 3) transmits the message $\langle Z_1, Z_2, Z_3, Z_{AUS} \rangle$ to license server $LS_j$

(IUA 4) license server $LS_j$ accepts the message $\langle Z_1, Z_2, Z_3, Z_{AUS} \rangle$ and verifies the message legitimacy and verification will be successful as user verification on license server $LS_j$ is not taking place

(IUA 5) $LS_j$ will fetch relevant $K_C$ and computes $Z_4 = R_2 \oplus X_m$, $Z_5 = K_C \oplus X_m$ and $Z_{SU} = h(ID_m \| X_m \| K_C \| R_2)$. $LS_j$ sends the message $\{Z_4, Z_5, Z_{SU}\}$ to $\mathscr{A}$

(IUA 6) $\mathscr{A}$ receives the message sent by $LS_j$ and computes $R_2 = Z_4 \oplus X_m$, $K_C = Z_5 \oplus X_m$, and $M^*_{SU} = h(ID_m \| X_m \| K_C \| R_2)$. Adversary gets successfully the secret key $K_C$

*3.2.2. License Server Impersonation Attack.* The privileged adversary $\mathscr{SA}$ steals the $\langle ID_m, X_m \rangle$ from the database of the $LS_j$. When $U_m$ sends the the message $\langle Z_1, Z_2, Z_3, Z_{AUS} \rangle$ to $LS_j$ through public channel; then, $\mathscr{SA}$ will intercept the message and and impersonate as a valid license server in the following ways.

(ISA 1) $\mathscr{SA}$ will compute $R_1 = Z_1 \oplus X_m$, $ID_m = Z_2 \oplus R_1$, $ID_c = Z_3 \oplus R_1$, and $M^*_{US} = h(\mathrm{ID} \| ID_c \| X_m \| R_1)$

(ISA 2) verify if $M^*_{US} = ^? Z_{US}$. If the condition is true, $LS_j$ picks relevant $K_C$ and creates random nonce $R_{US}$

(ISA 3) calculate $Z_4 = R_{US} \oplus X_m$, $Z_5 = KEY_{ADC} \oplus X_m$, and $Z_{ASU} = h(ID_m \| X_m \| KEY_{ADC} \| R_{US})$.

(ISA 4) $\mathscr{SA}$ sends the message $\{Z_4, Z_5, Z_{ASU}\}$ to user $U_m$

(ISA 5) $U_m$ will verify the message and verification will be successful and as a result, get secret key $KEY_{ADC}$ which is in real a forged key and will not work

*3.2.3. No Secret Key Secrecy.* Only those users who have the secret key can access the digital content in the digital rights management system. But, as shown in Section 3.2.1, an adversary $\mathscr{A}$ can acquire the secret key by impersonating as a valid user $U_m$. Hence, Yu et al.'s scheme does not ensure the security of the secret key.

## 4. Proposed Scheme

To ensure privacy, security, and to remove the incorrectness in the scheme of Yu et al. [14], a new scheme is proposed in this section. The proposed scheme comprises three main phases, which are further divided into subphases. The detail of the scheme is given in the following subsections.

*4.1. Registration Phase.* To get access to the digital contents, a user must register himself/herself to be a legitimate user. Following are the steps as mentioned in Figure 4 to be followed:

RGD 3: the user $U_m$ picks the pair $\{ID_m, PW_m\}$ and engraves $BIO_m$. Now $U_m$ computes $Gen(BIO_m) = \langle R_m, P_m \rangle$, and $RPW_m = h(PW_m \| R_m)$ and dispatches $\{ID_m, RPW_m\}$ to license server $LS_j$ by using secure channel

RGD 3: license server $LS_j$ receiving the registration request by $U_m$ computes $X_m = h(ID_m \| X_{LS})$, $d_m = X_m \oplus h(ID_m \| RPW_m)$, and saves $ID_m$ and $PID_m$ in its database and reply the registration request message $\langle X_m \text{ to } PID_m \rangle$ by using channel

RGD 3: $U_m$ receives the message from $LS_j$ and computes $PID'_m = PID_m \oplus h(PW_m \| R_m)$, $X'_m = X_m \oplus h(PW_m \| R_m)$, $Z_m = h(ID_m \| PW_m \| R_m)$ and stores $\{X'_m, PID'_m, Z_m\}$ in the mobile device memory

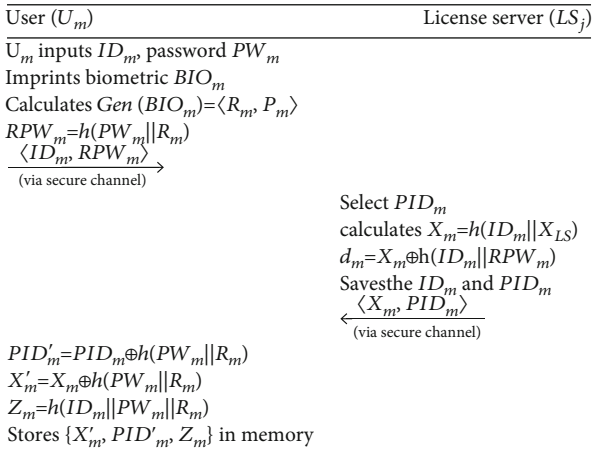


Figure 4: Proposed user registration.

*4.2. Login and Authentication.* Following steps as mentioned in Figure 5 are executed to furnish login and authentication phase of the proposed scheme:

(LAuth 1) $U_m$ inputs $ID_m$, password $PW_m$, imprints biometric $BIO_m$, calculates $R_m = Rep(BIO_m, P_m)$, and checks if $Z_m =^? h(ID_m||PW_m||R_m)$, and if the condition is true, then, select $R_1$ and $T_m$ and compute $X_m = X'_m \oplus h(R_m||PW_m)$, $Z_1 = ID_m \oplus R_1 \oplus h(X_m \oplus T_m)$, $Z_2 = ID_c \oplus R_1 \oplus h(X_m \oplus T_m)$, $Z_{US} = h(ID_m||ID_c||h(X_m||T_m)||R_1||T_m)$ and send the message containing $\langle Z_1, Z_2, Z_{US}, PID_m, T_m\rangle$ to the $LS_j$

(LAuth 2) after receiving the message $LS_j$ verifies if $|T_m - T_c| < \Delta T$?, if the condition is true then fetch $ID_m$ corresponding to $PID_m$ and compute $X^*_m = h(ID_m||X_{LS})$, $R_1 = Z_1 \oplus ID_m \oplus h(X^*_m||T_m)$, $ID_c = Z_2 \oplus R_1 \oplus ID_m \oplus h(X^*_m||T_m)$, $M^*_{US} = h(ID_m||ID_c||h(X^*_m||T_m)||R_1||T_m)$ and check if $M^*_{US} =^? Z_{US}$ is true. If true pick $R_2$, $T_{CS}$, and $PID^{new}_m$, fetches $K_C$ and calculate $TEMP1 = h(ID_m \oplus R_1)$, $Z_3 = R_2 \oplus h(X^*_m||T_{cs}) \oplus TEMP1$, $Z_4 = PID^{new}_m \oplus h(X^*_m||T_{cs}) \oplus TEMP1$, $Z_5 = K_C \oplus h(X^*_m||T_{cs}) \oplus R_2 \oplus TEMP1$, $Z_{SU} = h(ID_m||h(X^*_m||T_{cs})||K_C||R_2R_2, ||TEMP1||T_{cs})$. Replace $PID_m$ with $PID^{new}_m$, and send the message containing $\langle Z_3, Z_4, Z_5, Z_{SU}, T_{cs}\rangle$ to $U_m$

(LAuth 3) after receiving the message from $LS_j$, $U_m$ check if $|T_{cs} - T_c| < \Delta T$? the condition is true then calculates $TEMP2 = h(ID_m \oplus R_1)$, $R_2 = Z_3 \oplus h(X_m||T_{cs}) \oplus TEMP2$, $PID^{new}_m = Z_4 \oplus h(X_m||T_{cs}) \oplus TEMP2$, $K_C = Z_5 \oplus h(X_m||T_{cs}) \oplus R_2 \oplus TEMP2$, $M^*_{SU} = h(ID_m||h(X_m||T_{cs})||K_C||R_2||TEMP2||T_{cs})$. Then, check if $M^*_{SU} =^? Z_{SU}$, if the condition is true, then, calculate $KEY^*_{DC} = K_C \oplus h(PW_m||R_m)$ and save $KEY^*_{DC}$

*4.3. Password Change.* If a valid user has lost/forgot his/her password then can change password by adopting the following steps:

(PWD 1) user $U_m$ enters new pair $\{ID^*_m, PW^*_m\}$ and engraves $BIO^*_m$. Now, $U_m$ computes $Gen(BIO^*_m) = \langle R^*_m, P^*_m\rangle$, and $RPW^*_m = h(PW^*_m||R^*_m)$ and dispatches $\{ID^*_m, RPW^*_m\}$ to the mobile device

(PWD 2) upon receipt of the message mobile check if $Z^*_m =^? h(ID^*_m||PW^*_m||R^*_m)$, if true, it sends confirmation to the user $U_m$

(PWD 3) $U_m$ chooses new password $PW^{new}_m$ and biometric $BIO^{new}_m$ and compute $Gen(BIO^{new}_m) = \langle R^{new}_m, P^{new}_m\rangle$, and $RPW^{new}_m = h(PW^{new}_m||R^{new}_m)$

(PWD 4) Receiving the message mobile device calculates $X_m = h(ID_m||X_{LS})$ and $d^{new}_m = X^*_m \oplus h(ID_m||RPW^{new}_m)$ and send $X_m$ and $PID^{new}_m$

(PWD 5) $U_m$ computes $PID^{new'}_m = PID^{new}_m \oplus h(PW^{new}_m||R^{new}_m)$, $X^{new'}_m = X_m \oplus h(PW^{new}_m||R^{new}_m)$, $Z_m = h(ID_m||PW^{new}_m||R^{new}_m)$ and update $\{X^{new'}_m, PID^{new'}_m, Z_m\}$.

## 5. The Security Analysis

To describe the security of the proposed scheme, we have scrutinized the scheme through formal and informal security analysis in the following subsections.

*5.1. Authentication Proof Based on the Burrows–Abadi–Needham Logic (BAN Logic).* The security of the proposed scheme is formally analyzed in the standard model using the widely accepted Burrows–Abadi–Needham logic [24].

*5.1.1. Postulates for BAN Logic.* Some of the logical postulates of BAN logic and the meaning related to the postulates are given below in Table 2.

*5.1.2. Security Goal Establishment.* Established security goals and logical notations of the BAN logic are given below in Table 3.

$G_1$: $LS_j| \equiv (R_1)$
$G_2$: $LS_j| \equiv U_m| \equiv (R_1)$
$G_3$: $U_m| \equiv (R_2)$
$G_4$: $U_m| \equiv LS_j| \equiv (R_2)$

*5.1.3. Proposed Schemes Idealized Form*

(M1) $U_m \longrightarrow LS_j$: $\langle ID_m, ID_c, R_1\rangle_{X_m}$

(M2) $LS_j \longrightarrow U_m$: $\langle ID_m, ID_c, K_C, R_2\rangle_{X_m}$

*5.1.4. Assumptions*

(A1) $LS_j| \equiv \#(R_1)$

(A2) $U_m| \equiv \#(R_2)$

| User ($U_m$) | License server ($LS_j$) |
|---|---|
| $U_m$ inputs $ID_m$, password $PW_m$ | |
| Imprints biometric $BIO_m$ | |
| $R_m=Rep(BIO_m, P_m)$ | |
| If $Z_m \stackrel{?}{=} h(ID_m \| PW_m \| R_m)$ | |
| Select $R_1$ and $T_m$ | |
| $X_m=X'_m \oplus h(R_m \| PW_m)$ | |
| $Z_1=ID_m \oplus R_1 \oplus h(X_m \oplus T_m)$ | |
| $Z_2=ID_c \oplus R_1 \oplus h(X_m \oplus T_m)$ | |
| $Z_{US}=h(ID_m \| ID_c \| h(X_m \| T_m) \| R_1 \| T_m)$ | |
| $\langle Z_1, Z_2, Z_{US}, PID_m, T_m \rangle \xrightarrow[\text{(via public channel)}]{}$ | |
| | Check if $\|T_m - T_c\| < \Delta T$? |
| | Fetch $ID_m$ corresponding to $PID_m$ |
| | Compute $X^*_m=h(ID_m \| X_{LS})$ |
| | Compute $R_1=Z_1 \oplus ID_m \oplus h(X^*_m \| T_m)$ |
| | $ID_c=Z_2 \oplus R_1 \oplus ID_m \oplus h(X^*_m \| T_m)$ |
| | $M^*_{US}=h(ID_m \| ID_c \| h(X^*_m \| T_m) \| R_1 \| T_m)$ |
| | Check if $M^*_{US} \stackrel{?}{=} Z_{US}$ |
| | If true |
| | Pick $R_2$, $T_{CS}$ and $PID^{new}_m$ |
| | Fetches $K_C$ |
| | Calculate |
| | $TEMP1=h(ID_m \oplus R_1)$ |
| | $Z_3=R_2 \oplus h(X^*_m \| T_{CS}) \oplus TEMP1$ |
| | $Z_4=PID^{new}_m \oplus h(X^*_m \| T_{CS}) \oplus TEMP1$ |
| | $Z_5=K_C \oplus h(X^*_m \| T_{CS}) \oplus R_2 \oplus TEMP1$ |
| | $Z_{SU}=h(ID_m \| h(X^*_m \| T_{CS}) \| K_C \| R_2 \| \| TEMP1 \| T_{CS})$ |
| | Replace $PID_m$ with $PID^{new}_m$ |
| | $\langle Z_3, Z_4, Z_5, Z_{SU}, T_{CS} \rangle \xleftarrow[\text{(via public channel)}]{}$ |
| Check if $\|T_{CS} - T_c\| < \Delta T$? | |
| Calculates | |
| $TEMP2=h(ID_m \oplus R_1)$ | |
| $R_2=Z_3 \oplus h(X_m \| T_{cs}) \oplus TEMP2$ | |
| $PID^{new}_m=Z_4 \oplus h(X_m \| T_{cs}) \oplus TEMP2$ | |
| $K_C=Z_5 \oplus h(X_m \| T_{CS}) \oplus R_2 \oplus TEMP2$ | |
| $M^*_{SU}=h(ID_m \| h(X_m \| T_{CS}) \| K_C \| R_2 \| TEMP2 \| T_{CS})$ | |
| Check if $M^*_{US} \stackrel{?}{=} Z_{US}$ | |
| If true $KEY^*_{DC}=K_C \oplus h(PW_m \| R_m)$ | |
| Saves $KEY^*_{DC}$ | |

Figure 5: Proposed login and authentication scheme.

Table 2: Postulates for BAN logic.

| | |
|---|---|
| $A \mid \equiv A \overset{K}{\longleftrightarrow} Y, A \triangleleft <B>_K / A \mid \equiv Y \mid \sim K$ | Message-meaning rule |
| $A \mid \equiv \#B, A \mid \equiv Y \mid \sim B / A \mid \equiv Y \mid \sim K$ | Nonce-verification rule |
| $A \mid \equiv B, A \mid \equiv C / A \mid \equiv (B, C)$ | Belief rule |
| $A \mid \equiv \#B, A \mid \equiv C / A \mid \equiv \#(B, C)$ | Fresh conjuncatenation rule |
| $A \mid \equiv Y \Longrightarrow B, A \mid \equiv Y \mid \sim B / A \mid \equiv B$ | Jurisdiction rule |

Table 3: BAN logic notations.

| | |
|---|---|
| $A \mid \equiv B$ | $A$ believes a statement $B$ |
| $A \overset{K}{\longleftrightarrow} Y$ | Share a key $K$ between $A$ and $Y$ |
| $\#B$ | $B$ is fresh |
| $A \triangleleft B$ | $A$ sees $B$ |
| $A \mid \sim B$ | $A$ said $B$ |
| $(B, C)_K$ | $B, C$ is hashed by key $K$ |
| $\{B\}_K$ | $B$ is hashed with key $K$ |
| $<B>_K$ | $B$ is encrypted with key $K$ |

(A3) $LS_j \mid \equiv (LS_j \longleftrightarrow^{X_m} U_m)$

(A4) $U_m \mid \equiv (LS_j \longleftrightarrow^{X_m} U_m)$

(A5) $LS_j \mid \equiv U_m \Longrightarrow (R_1)$

(A6) $U_m \mid \equiv (LS_j \longrightarrow R_2)$

*Step 1.* According to message 1:

$$P1 : LS_j \triangleleft \{ID_m, ID_c, R_1\}_{X_m}. \quad (2)$$

*Step 2.* From the message meaning rule according to P1 and A3:

$$P2 : LS_j \mid \equiv \{(U_m\}. \quad (3)$$

*Step 3.* According to the freshness rule with A1, we get

$$P3 : LS_j \mid \equiv U_m \mid \equiv \#\{ID_m, ID_c, R_1\}_{X_m}. \quad (4)$$

*Step 4.* From the nonce verification rule with P2 and P3, we get

$$P4 : LS_j \mid \equiv U_m \mid \equiv \{ID_m, ID_c, R_1\}_{X_m}. \quad (5)$$

*Step 5.* According to the belief rule with P4, we get

$$P5 : LS_j \mid \equiv U_m \mid \equiv \{R_1\}\text{Goal} - X2. \quad (6)$$

*Step 6.* From the jurisdiction rule with P5 and A5, we get

$$P6 : LS_j \mid \equiv \{R_1\}\text{Goal} - X1. \quad (7)$$

*Step 7.* According to M2, we obtain

$$P7 : U_m \triangleleft \{ID_m, ID_c, K_C R_2\}_{X_m}. \quad (8)$$

*Step 8.* From the message meaning rule with P7 and A4, we get

$$P8 : U_m \mid \equiv LS_j \mid \equiv \{ID_m, ID_c, K_C R_2\}_{X_m}. \quad (9)$$

*Step 9.* According to the freshness rule with A2, we get

$$P9 : U_m \mid \equiv LS_j \mid \equiv \#\{ID_m, ID_c, K_C R_2\}_{X_m}. \quad (10)$$

*Step 10.* From the nonce verification rule with P9 and P10, we get

$$P10 : U_m \mid \equiv LS_j \mid \equiv \{ID_m, ID_c, K_C R_2\}_{X_m}. \quad (11)$$

*Step 11.* According to the belief rule with P10, we get

$$P11 : U_m \mid \equiv LS_j \mid \equiv \{R_2\}\text{Goal} - \text{X4}. \quad (12)$$

*Step 12.* From the jurisdiction rule with P11 and A6, we get

$$P12 : U_m \mid \equiv \{R_2\}\text{Goal} - X3. \quad (13)$$

According to Goal – $X1$ to Goal – $X4$, we proved that our scheme attains secure mutual authentication among $U_m$ and $LS_j$.

*5.2. Informal Security Analysis.* To assess the security of the introduced scheme, also we have inspected the scheme through informal security analysis procedures.

*5.2.1. Mutual Authentication.* Our proposed scheme provides mutual authentication by making verification on both sides of participating entities. License server $LS_j$ receives the login request messages $Msg_1 = (Z_1, Z_2, Z_{US}, PID_m, T_m)$ from $U_m$, license server $LS_j$ verifies the authenticity of the user by verifying the $M'US = ? Z_{US}$. If the condition is true, $LS_j$ authenticates $U_m$ and sends $Z_3, Z_4, M5, Z_{SU}, T_{cs}$ to $U_m$. $U_m$ receives the response messages from $LS_j$, $U_m$ verifies whether $M'_{SU} ? = Z_{SU}$. If the condition is true, then, $U_m$ authenticates *Sj*; otherwise, terminates the request. Hence, the proposed scheme successfully achieves mutual authentication property.

*5.2.2. Replay Attack.* Suppose that $\mathscr{A}$ hijacks the messages $Msg_1 = (Z_1, Z_2, Z_{US}, PID_m, T_m)$ and $Msg_2 = (Z_3, Z_4, Z_5, Z_{US}, T_{cs})$ in a selective session and tries to replay these hijacked messages after a while. As it is evident that the all message contains current timestamps $T_m$ and $T_{cs}$, the acceptance of the timeliness $T_m$ and $T_{cs}$ will be declined at the $U_m$ and $LS_j$. Furthermore, $\Delta T$ value is fixed very small and due to which it will be very difficult for the attacker $\mathscr{A}$ to replay the hijacked messages within limit of the $\Delta T$. Hence, the proposed scheme is stealth against the replay attack.

*5.2.3. Stolen Mobile Device Attack.* Suppose that $\mathscr{A}$ has stolen mobile device [25, 26] of user $U_m$ or $U_m$ has lost the mobile device due to some reason. Then, A can extract the credentials $\{X'_m, PID'_m, Z_m\}$ from mobile device memory using the power analysis attacks. After getting all these parameters, the attacker $\mathscr{A}$ will not be able to get useful parameters $ID_m$ and $PW_m$, as these are protected through a collision-resistant hash function. Therefore, if any mobile device will be lost/stolen will not affect the proposed authentication mechanism.

*5.2.4. Anonymity and Untraceability.* In the proposed scheme, all the messages $Msg_1 = (Z_1, Z_2, Z_{US}, PID_m, T_m)$ and $Msg_2 = (Z_3, Z_4, Z_5, Z_{US}, T_{cs})$ in each session are explicit and nonrepeated, also all the message includes current timestamps $T_m$ and $T_{cs}$, and random nonces $R_1$ and $R_2$. Hence, $\mathscr{A}$ will not be able to trace $U_m$ and $LS_j$. Moreover, even any single message does not contain identities $ID_m$ and $ID_c$. Hence, the anonymity [27, 28] is guaranteed in the proposed scheme.

*5.2.5. Denial-of-Service Attack.* In the login and authentication phase, when a valid user $U_m$ inputs his/her identity $ID_m$, password $PW_m$, and imprints biometric $BIO_m$ into the mobile device. Mobile device retrieves the saved secret biometric key corresponding to $BIO_m$ as $R_m = Rep(BIO_m, P_m)$. Further mobile device computes $Z_m = h(ID_m \| PW_m \| R_m)$ and checks if $Z_m$ values are the same or not. If the condition is not met, the session is terminated immediately, and in case of success, the session proceeds normally. Therefore, in case of denial-of-service attack [29, 30], the proposed scheme will resist it.

*5.2.6. Man-in-the-Middle Attack.* In this type of attack, $\mathscr{A}$ grabs the messages being exchanged when the communication is taking place and tries to alter those messages to make other valid messages, to deceive the recipient from guessing the altered messages, and he/she considered these altered messages as normal as other original messages. Suppose $\mathscr{A}$ grabs the messages $Msg_1$ and $Msg_2$. Due to lack of the some parameters knowledge such as $ID_m$, $ID_c$, $X_m$, and $K_C$, the attacker $\mathscr{A}$ will be unable to forge these messages $Msg_1$ and $Msg_2$. Hence, the proposed scheme opposes man-in-the-middle attack [31].

*5.2.7. User Impersonation Attack.* Assume an attacker $\mathscr{A}$ tries to impersonate a message on behalf of a user $U_m$ to license server $LS_j$. $\mathscr{A}$ gets/$X'_m, PID'_m, Z_m, h(.)$/ from mobile device and /$Z_1, Z_2, Z_{US}, PID_m, T_m$/ during the communication. At the moment, if $\mathscr{A}$ tries to construct message, but it will not possible as he/she does not know these parameters $ID_c, ID_m$, and $X_m$, due to which it will be hard to produce these for attacker.

*5.2.8. License Server Impersonation Attack.* Assume an attacker $\mathscr{A}$ tries to impersonate a message on behalf of a license server $LS_j$ to user $U_m$. $\mathscr{A}$ gets /$X'_m, PID'_m, Z_m, h(.)$/ from mobile device and /$Z_3, Z_4, Z_5, Z_{US}, T_{cs}$/ during the communication. At the moment, if $\mathscr{A}$ tries to construct a reply message on the behalf of the license server $LS_j$, but it will not possible as he/she does not know these parameters $K_C, ID_m$, and $X_m$, due to which it will be hard to produce these for an attacker. Hence, the proposed scheme is secure against impersonation attacks.

*5.3. Automated Security Verification through ProVerif.* The ProVerif is an automated security verification tool utilized to visualize the key agreement scheme to check mutual authentication and confidentiality of the session key among the participant entities of the authentication scheme [32–34]. To verify the security of the proposed scheme, we have simulated and verified it through ProVerif. For the sake of the experiment, we have used two events $Ui$ and $LS_j$ to check the authentication codes of each entity, respectively. The participant $U_m$ uses two events, which are beginUi(bitstring) and endUi(bitstring) to authenticate the license server $LS_j$. Similarly, the beginSj(bitstring) and endSj(bitstring) events are used by the license server to authenticate the user $U_m$. The outcomes of the queries executed show that both participants are successfully communicating with each other. The simulation results are shown in Figure 6, which exhibits that the mutual authentication is successful and communication between the valid participants is secure from the reach of any potential attacker $\mathscr{A}$.

## 6. The Comparisons

This section provides security attributes and performance comparisons among proposed and relevant schemes [10, 13, 14], in the corresponding subsections produced below.

*6.1. Security Attributes.* This subsection provides the security attribute comparisons of the proposed with relevant schemes presented in [10, 13, 14]. The comparisons of the proposed with recent, related, and compered schemes [10, 13, 14] are depicted in Table 4. Referring to Table 4, all the compared proposals [10, 13, 14] are deficient of at least one security attribute. As per Table 4, the scheme of Mishra et al. [10] is already argued in [14] that it does not provide mutual authentication and resistance to impersonation. Moreover, the scheme of [10] is prone to theft/stolen mobile device attacks. The scheme of Yu et al. [14] does not provide anonymity of the mobile/user. Similarly, in this paper, we proved that the scheme of Yu et al. [14] has incorrect login and authentication phase, which can work with only one user, and it has weaknesses against privileged insider and impersonation attacks and due to these crucial issues, it cannot extend mutual authentication among a user and a license server.

*6.2. Computation Cost.* For computation cost, we consider the experiment executed through the MIRACL library over a mobile phone Redmo-Note-v8 with 4 GB RAM and octa-core $\mu$ processor with 2.01 GHz. The operating system underlying Redmo-Note-v8 is v-9-Andriod-MIUI-V:11.0.7. Moreover, to simulate a license server, we consider the running time computed over an HP:Elite-Book: P-8460 $\mu$ processor with 2.7 GHz Intel-R-Core TM with 4 GB RAM

Verification summary:

Query inj-event (end_Ui (Ui[]))==>inj-event (start_Ui (Ui[])) is true.
Query inj-event (end_Sj (Sj[]))==>inj-event (start_Sj (Sj[])) is true.
Query not attacher (KEYdc[]) is true

Figure 6: ProVerif simulations.

Table 4: Security features.

| Schemes ⟶↓attributes | Our | [13] | [10] | |
|---|---|---|---|---|
| PMA | ✓ | ✗ | ✓ | ✗ |
| PUA | ✓ | ✓ | ✗ | ✓ |
| PUS | ✓ | ✗ | ✓ | ✓ |
| RRA | ✓ | ✓ | ✓ | ✓ |
| RSD | ✓ | ✓ | ✓ | ✗ |
| RIA | ✓ | ✗ | ✓ | ✗ |
| RMA | ✓ | ✓ | ✓ | ✓ |
| PPF | ✓ | ✓ | ✓ | ✓ |
| ROP | ✓ | ✓ | ✓ | ✓ |
| RPI | ✓ | ✗ | ✓ | ✓ |

Note: PMA: provides mutual authentication; PUA: provides user anonymity/untrability; PSU: provides user scalability; RRA: resists replay attack; RSD: resists stolen mobile device; RIA: resists impersonation attack; RMA: resists man in middle attack; PPF: provides perfect forward secrecy; ROP: resists offline password guessing; RPI: resists privileged insider attack; ✓: provides; ✗: not provides.

and over LTS-16 Ubuntu-OS. Here, we denote $T_h$ for the execution time of a hash operation and $T_{bh}$ for computation of a biohash/fuzzy extraction operation. The $T_h \approx 0.009$ for mobile device and $T_h \approx 0.004$ for license server. Likewise, $T_f \approx 0.16$ over the mobile device. To complete a round of authentication in the proposed DRM scheme, the user $U_m$ executes $\{9T_h + 1T_f\}$ operations, the server $LS_j$ executes $\{6T_h\}$, and the whole process completes in ≈0.265 ms. The scheme of Yu et al. [14] completes the same in ≈0.213 ms. Likewise, in the scheme of Lee et al. [13], the $U_m$ and $LS_j$ compute execution of a round in ≈0.216 ms, and the scheme of Mishra et al. [10] completes the process in ≈0.243 ms. The proposed scheme has a slightly higher computation cost. However, only the proposed scheme provides the required security features.

*6.3. Communication Cost.* The proposed and the relevant scheme are mainly based on hash functions in addition to an exclusive-or. We adopted SHA-1 whose length is 160 bits, all other parameters including identities, pseudoidentities, timestamps, and passwords are fixed at 32 bit-size. In proposed, the user initiates the request by sending $\langle Z_1, Z_2, Z_{US}, PID_m, T_m \rangle$, and the size of request message is $\{160 + 160 + 160 + 32 + 32\} = 544$ bits. The response message sent by server $\langle Z_3, Z_4, Z_5, Z_{US}, T_{cs} \rangle$ has the size $\{160 + 160 + 160 + 160 + 32\} = 672$. Therefore, the total communication cost of the proposed scheme is 1216 bits. The communication costs of the schemes of Yu et al. [14], Lee et al. [13], and Mishra et al. [10] are 1120 bits, 1120 bits, and 832 bits, respectively. The computation and communication costs along with running times of each of the proposed and schemes of Yu et al., Lee et al., and Mishra et al. are also depicted in Table 5.

Table 5: Performance comparisons.

| Protocol | $U_m$ | $LS_j$ | RT-ms | B.E |
|---|---|---|---|---|
| Mishra et al. [10] | $7T_h + 1T_f$ | $5T_h$ | ≈0.243 | 832 |
| Lee et al. [13] | $4T_h + 1T_f$ | $5T_h$ | ≈0.216 | 1120 |
| Yu et al. [14] | $5T_h + 1T_f$ | $2T_h$ | ≈0.213 | 1120 |
| Proposed | $9T_h + 1T_f$ | $6T_h$ | ≈0.265 | 1216 |

Note: RT: running time in milliseconds; B.E: bit exchanges.

## 7. Conclusion

In this paper, we first reviewed and then cryptanalyzed a recent authentication scheme presented by Yu et al. for digital rights management systems (DRM-S). We have proven that the scheme of Yu et al. lacks scalability due to faulty design and is prone to privileged insiders and impersonation attacks. Based on the only symmetric hash function and xor, an improved scheme of DRM-S is then proposed. The proposed scheme can cope with the changing security requirements of the DRM-S, which is proved through formal BAN and informal textual explanations. The proposed DRM-S authentication scheme completes the process of authentication among a user and a license server in 0.265 ms and by exchanging 1216 bits among a user and a license server.

## Data Availability

No data is available for this study

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Authors' Contributions

Sajid Hussain and Yousaf Bin Zikria are the co-first authors. Farruh Ishmanov and Shehzad Ashraf Chaudhry are the corresponding authors.

## Acknowledgments

This research was conducted by the Research Grant of Kwangwoon University, Seoul, Korea, in 2021 and in part by Taif University Researchers Supporting Project number (TURSP-2020/126), Taif University, Taif, Saudi Arabia.

## References

[1] L. L. Win, T. Thomas, and S. Emmanuel, "Privacy enabled digital rights management without trusted third party assumption," *IEEE Transactions on Multimedia*, vol. 14, no. 3, pp. 546–554, 2012.

[2] E. H. Wu, S. Chuang, C.-Y. Shih, H.-C. Hsueh, S.-S. Huang, and H.-P. Huang, "A flexible and lightweight user-demand drm system for multimedia contents over multiple portable device platforms," *Software: Practice and Experience*, vol. 47, no. 10, pp. 1417–1441, 2017.

[3] Z. Ma, M. Jiang, H. Gao, and Z. Wang, "Blockchain for digital rights management," *Future Generation Computer Systems*, vol. 89, pp. 746–764, 2018.

[4] C.-C. Lee, C.-T. Li, Z.-W. Chen, S.-D. Chen, and Y.-M. Lai, "A novel authentication scheme for anonymity and digital rights management based on elliptic curve cryptography," *International Journal of Electronic Security and Digital Forensics*, vol. 11, no. 1, pp. 96–117, 2019.

[5] D. Mishra, M. S. Obaidat, S. Rana, D. Dharminder, A. Mishra, and B. Sadoun, "Chaos-based content distribution framework for digital rights management system," *IEEE Systems Journal*, vol. 15, no. 1, pp. 570–576, 2021.

[6] T. Gaber, A. Ahmed, and A. Mostafa, "Privdrm: a privacy-preserving secure digital right management system," in *Proceedings of the Evaluation and Assessment in Software Engineering*, pp. 481–486, Trondheim, Norway, 2020.

[7] C.-L. Chen, "A secure and traceable e-drm system based on mobile device," *Expert Systems with Applications*, vol. 35, no. 3, pp. 878–886, 2008.

[8] C.-C. Chang, J.-H. Yang, and D.-W. Wang, "An efficient and reliable e-drm scheme for mobile environments," *Expert Systems with Applications*, vol. 37, no. 9, pp. 6176–6181, 2010.

[9] C.-C. Chang, S.-C. Chang, and J.-H. Yang, "A practical secure and efficient enterprise digital rights management mechanism suitable for mobile environment," *Security and Communication Networks*, vol. 6, no. 8, 984 pages, 2013.

[10] D. Mishra, A. K. Das, and S. Mukhopadhyay, "An anonymous and secure biometric-based enterprise digital rights management system for mobile environment," *Security and Communication Networks*, vol. 8, no. 18, 3404 pages, 2015.

[11] Y. Zhang, M. K. Khan, J. Chen, and D. He, "Provable secure and efficient digital rights management authentication scheme using smart card based on elliptic curve cryptography," *Mathematical Problems in Engineering*, vol. 2015, Article ID 807213, 16 pages, 2015.

[12] J. Jung, D. Kang, D. Lee, and D. Won, "An improved and secure anonymous biometric-based user authentication with key agreement scheme for the integrated epr information system," *PLoS One*, vol. 12, no. 1, article e0169414, 2017.

[13] C.-C. Lee, C.-T. Li, Z.-W. Chen, and Y.-M. Lai, "A biometric-based authentication and anonymity scheme for digital rights management system," *Information Technology and Control*, vol. 47, no. 2, pp. 262–274, 2018.

[14] S. J. Yu, K. S. Park, Y. H. Park, H. P. Kim, and Y. H. Park, "A lightweight threefactor authentication protocol for digital rights management system," *Peer-to-Peer Networking and Applications*, vol. 13, no. 5, p. 1340, 2020.

[15] M. Tanveer, G. Abbas, Z. H. Abbas, M. Bilal, A. Mukherjee, and K. S. Kwak, "Lake-6sh: lightweight user authenticated key exchange for 6lowpan-based smart homes," *IEEE Internet of Things Journal*, vol. 1, 2021.

[16] Z. Ali, S. A. Chaudhry, K. Mahmood, S. Garg, Z. Lv, and Y. B. Zikria, "A clogging resistant secure authentication scheme for fog computing services," *Computer Networks*, vol. 185, article 107731, 2021.

[17] M. A. Saleem, S. K. H. Islam, S. Ahmed, K. Mahmood, and M. Hussain, "Provably secure biometric-based client-server secure communication over unreliable networks," *Journal of Information Security and Applications*, vol. 58, article 102769, 2021.

[18] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 453–474, Innsbruck, Austria, 2001.

[19] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[20] M. F. Ayub, S. Shamshad, K. Mahmood, S. K. H. Islam, R. M. Parizi, and K.-K. R. Choo, "A provably secure twofactor authentication scheme for usb storage devices," *IEEE Transactions on Consumer Electronics*, vol. 66, no. 4, pp. 396–405, 2020.

[21] S. A. Chaudhry, A. Irshad, K. Yahya, N. Kumar, M. Alazab, and Y. B. Zikria, "Rotating behind privacy: an improved lightweight authentication scheme for cloud-based iot environment," *ACM Transactions on Internet Technology*, vol. 21, no. 3, pp. 1–19, 2021.

[22] M. Tanveer, A. U. Khan, N. Kumar, and M. M. Hassan, "Ramp-iod: a robust authenticated key management protocol for the internet of drones," *IEEE Internet of Things Journal*, vol. 1, 2022.

[23] S. A. Chaudhry, "Designing an efficient and secure message exchange protocol for internet of vehicles," *Networks*, vol. 2021, article 5554318, pp. 1–9, 2021.

[24] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 426, no. 1871, pp. 233–271, 1989.

[25] K. Mahmood, J. Arshad, S. A. Chaudhry, and S. Kumari, "An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure," *International Journal of Communication Systems*, vol. 32, no. 16, article e4137, 2019.

[26] T. Maitra, M. S. Obaidat, R. Amin, S. K. H. Islam, S. A. Chaudhry, and D. Giri, "A robust elgamal-based password-authentication protocol using smart card for client-server communication," *International Journal of Communication Systems*, vol. 30, no. 11, article e3242, 2017.

[27] F. Wu, X. Li, L. Xu, P. Vijayakumar, and N. Kumar, "A novel three-factor authentication protocol for wireless sensor networks with iot notion," *IEEE Systems Journal*, vol. 15, no. 1, pp. 1120–1129, 2021.

[28] X. Li, J. Tan, A. Liu, P. Vijayakumar, N. Kumar, and M. Alazab, "A novel uav-enabled data collection scheme for intelligent transportation system through uav speed control," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 4, pp. 2100–2110, 2021.

[29] T. Liu, F. Wu, X. Li, and C. Chen, "A new authentication and key agreement protocol for 5g wireless networks," *Telecommunication Systems*, vol. 78, no. 3, pp. 317–329, 2021.

[30] T. Y. Wu, L. Yang, Q. Meng, X. Guo, and C.-M. Chen, "Fog-driven secure authentication and key exchange scheme for wearable health monitoring system," *Security and Communication Networks*, vol. 2021, Article ID 8368646, 14 pages, 2021.

[31] T.-Y. Wu, Y. Q. Lee, C. M. Chen, Y. Tian, and N. A. Al-Nabhan, "An enhanced pairing-based authentication scheme for smart grid communications," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–13, 2021.

[32] B. Blanchet, B. Smyth, V. Cheval, and M. Sylvestre, "Proverif 2.00: automatic cryptographic protocol verifier, user manual and tutoria," January 2022, https://bblanche.gitlabpages.inria.fr/proverif/manual.pdf.

[33] S. A. Chaudhry, "Correcting "PALK: password-based anonymous lightweight key agreement framework for smart grid"," *International Journal of Electrical Power & Energy Systems*, vol. 125, article 106529, 2021.

[34] Q. Xie, B. Hu, N. Dong, and D. S. Wong, "Anonymous three-party password-authenticated key exchange scheme for telecare medical information systems," *PLoS One*, vol. 9, no. 7, article e102747, 2014.