A Robust Anonymous Authentication Scheme using Biometrics for Digital Rights Management System

Muhammad Ayaz Khan
Department of CS&SE
International Islamic University
Islamabad, Pakistan
ayaz.mscs934@iiu.edu.pk

Anwar Ghani
Department of CS&SE
International Islamic University
Islamabad, Pakistan
anwar.ghani@iiu.edu.pk

Mohammad S. Obaidat
College of Computing and Informatics,
University of Sharjah
Sharjah 27272, UAE
m.s.obaidat@ieee.org

Pandi Vijayakumar
Department of Computer Science and Engineering
University College of Engineering Tindivanam
Tindivanam, Tamil Nadu 604001, India
pvijayakumar@ieee.org

Khwaja Mansoor
Department of Computer Science
Air University
Islamabad, Pakistan
kh.mansoorulhassan@gmail.com

Shehzad Ashraf Chaudhry
Department of Computer Engineering
Istanbul Gelisim University
Istanbul, Turkey
ashraf.shehzad.ch@gmail.com

2021 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI) | 978-1-6654-3208-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/CCCI52664.2021.9583219

***Abstract*—As digital content transmission through the internet is convenient and quick, so the outspread of digital content is very high. However, along with this incredible speed and ease, current communication technologies and computers have also brought with them plenty of digital rights management complications. Digital Rights Management Systems are designed to limit the access to the utilization, alternation, and distribution of persevered digital content. This article scrutinized two recent schemes of Lee et al. and Yu et al. and it is found that these schemes are suspected to an insider attack, stolen smart-card attack, Daniel of services (Dos) attack, and impersonation attack. Furthermore, their proposal also suffers from incorrect issues. To fix these flaws, a robust anonymous authentication scheme using biometrics for Digital Rights Management System is proposed in this article. The proposed scheme is checked for correctness and its security is proved through BAN logic. The performance of the scheme is also analyzed using computation time and communication time. The results show that the designed scheme is highly secure with the same computation and communication cost as the existing protocols.**

***Index Terms*—Biometric authentication, Digital rights management, Access control, Mobile user authentication, Anonymous authentication**

I. Introduction

With the improvement of modern technologies, more and greater extent of traditional content in their broadcast forms such as games, music, documents, photos compacts cassettes, videotapes, and much more are transformed into digital forms. Meanwhile, the booming development of the Internet has increasingly grown up to connect the number of people together and made it much easy and very fast to distribute information all over the world. Actually, the authorized access to copyrighted digital content over the Internet is increasingly growing up day-by-day as more people have no access to devices with low power consumption and high portability [1]–[6].

Conforming to the whole trend in technology, smart devices like laptops, tablets, and cell phones are intended to be as small and lightweight as possible in order to offer more comfort. As a result, people are becoming progressively dependent on cell phones and getting connected to the rest of the world through mobile devices internet [7], [8]. Certainly, when people feel like retrieving digital content through the internet, chances are they will most likely use it on their mobile devices [9]. In the contemporary era, digital content is too simple to distribute and have access to on the Internet. In several countries around the world, unauthorized access and download of copyrighted digitized contents is a very significant issue, causing huge losses of the writers and legitimate person of the contents [9], [10]. Consequently, the implementation of copyright digital content protection is very important, and It is indispensable to develop an ideal DRM-System such that just copyright possessor or authorized users can access and retrieve the contents [11]–[14]. DRM system is specially developed for an environment where access to digital content is limited only to authorized users. The basic architecture of a DRMS is shown in Fig. 1

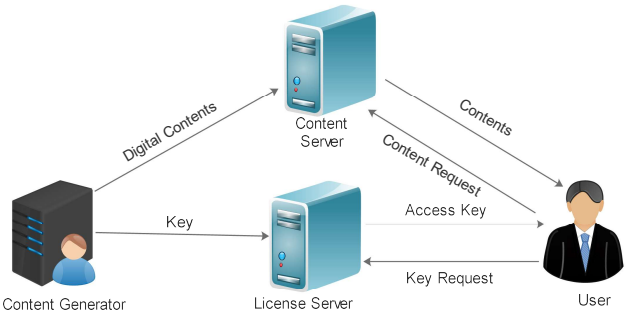

Figure 1. Baisc Architecture Of DRM

DRM system is a good user identity verification and access control mechanism to digital contents. Fig. 1 indicates the DRMS fundamental architecture consisting of four major roles:

978-1-6654-3208-5/21/$31.00 ©2021 IEEE

Table I
NOTATION GUIDE

Notations	Description
U_i, ID_i	The mobile user & identity of U_i
LS_j, X_s	Licence Server & secret key of LS_j
PW_i, B_i	Password & Biometrics of the U_i
ID_{DC},KEY_{IDC}	Identity & Secret key for Digital Contents
$h(.)$,$H(.)$	One-way & Bio Hash functions
$\|\|$, $\oplus$	Concatenation & XOR operators

(1) the content writer/owner, (2) server of content, (3) and license server, and (4) the clients/user [15]–[18].

Different methods can be used to validate users, but biometric authentication is one of the most effective methods. Biometric-based verification and authorization is a procedure for verifying a person's stated identification using some biological unique characteristics that are easily distinguishable like voice patterns, hand geometry, fingerprints, and facial geometry or iris patterns [19]–[21].

The general contributions of this study are listed below:

- To cryptanalze Lee et al. [22] and Yu et al. [23] protocols and find out the security loophole in these protocols that can be exploited by an attacker.
- To design an robust version of the cryptanalyzed protocols to cover up the security loopholes.
- To comparatively analyzed the proposed protocols in terms of security as well as performance [24].

A. Threat Model

The DY threat model as adopted in [25]–[27] is detailed below:

1) The adversary (A) has control over the communication link. A will replay, listen and alter a legal message and may also insert a fake message.
2) The adversary A may also simply get related information about the identities of the members.
3) A knows the publicly available parameters.
4) A is unable to obtain U_i private key.
5) The secret key that is shared between the U_i and LS_j cannot be exposed to an adversary.

B. Cryptanalysis: The Scheme of Lee et al.

Lee et al. [22] presented a DRMS security protocol and claimed that it's strongly secure against all possible attacks. But Yu et al. found out that the Lee et al. protocol is unable to achieve mutual authentication, vulnerable to impersonation attack and leakage of key. To overcome the issues Yu et al. [23] presented their protocol, however, their proposal is also exposed to certain known attacks, which were not explored by Yu et al. The discussion in following subsection details the weaknesses of Lee et al.

1) Insider Attack: An attack launched by a legitimate user of a system to leak secret information. The insider attack on Lee at al. works as follows:
An internal user detects identity ID_{DC} of the license server and DID_{DC} of digital contents from the public channel. The insider can get the random number r1 by XOR of DID_{DC} with ID_{DC} and gets N_i from the public channel. Then by r1 XOR with N_i the adversary gets CID_i that contains $h(h(x)\|DID_i)$, where x is the confidential key of the license server and DID_i contain password and ID of the user. So the adversary can access the digital contents easily.

2) Stolen Smart Card Attack: An adversary (**A**) takes verification data from the server in the past or present authentication sessions. Here, the verification information includes secret keys used with XOR activity or an encryption function. **A** can create communication data using the stolen information and send the response to the server. If it succeeds, then from the next session the attacker may pass Impersonate off as a real user. In Lee et al. [22] scheme CID_i number is saved in plain-text form in Smart Card that is vulnerable to Stolen Smart Card Attack.

3) Incorrectness of Lee at al. scheme: In Lee at al. scheme the message N_i, DID_i, DID_{DC}, F_i, G_i, T_i is sent from user to Server without Server ID. Without the server ID it is impossible to know the intended server for the message. Similarly, the server will not respond to any message without its ID, therefore, the connection to the server in [22] may not be possible.

C. Cryptanalysis: The Scheme of Yu et al.

The cryptanalysis of Yu et al. [23] as conducted in following subsections, reveals that the protocol cannot oppose the following attacks:

1) Insider Attack: The insider(legitimate but malicious system user) attacker extracts identity ID_i of a user, secret key X_i, and digital content identity that are stored publicly in the license server. After that, the malicious attacker impersonates himself as a lawful user by using the above parameters as explained below.

2) Impersonation Attack: The insider by getting X_i generates random nonce a_i and calculates $M_1 = X_i \oplus a_i$, $M_2 = ID_i \oplus a_i$, $M_3 = ID_{DC} \oplus a_i$, and M_{US}=$h(ID_i\|ID_{DC}\|X_i\|a_i)$, where ID_i and ID_{DC} is visible on the server. Finally the response message $\{M_{US}, M_1, M_2, M_3, \}$ is sent to S_j. On receiving the response response from U_i, S_j first computes and verifies $M^*_{US} \stackrel{?}{=} M_{US}$. Now S_j retrieves KEY_{DC} and generates R_2. After that calculates $M_4 = X_i \oplus R_2$, $M_5 = X_i \oplus KEY_{DC}$, finally computes M_{US}=$h(ID_i\|X_i\|KEY_{DC}\|R_2)$. Now the user is validate and to use digital contents.

3) Denial of services Attack (DoS): An adversary can launch DoS attack by sending $\{M_1, M_2, M_3, M_{US}\}$ to S_j, where this login message does not contain any time stamp. So the adversary frequently sends M_i that makes the license server unavailable to legitimate users. Similarly, the case mentioned in Bayat et al. [28] protocol.

4) Incorrectness of Yu et al. scheme: Yu et al. scheme also has the same incorrectness issue as Lee at el. protocol. The message M_1, M_2, M_3, M_{US} from the user does not contain a server ID. If the server ID is not sent then it is impossible to direct the message to a server. Users' record are usually stored in centralized databases and multiple servers. So a message without a server ID will not be able to reach a server.

II. Proposed Solution

The phases of the proposed protocol are explained in following subsections:

A. Registration Phase of the Propose Scheme

In the user registration phase, provides a password, a unique identity and biometric data on a registration request that is send to the license server.

Step 1: The client/user U_i chooses ID_i, password PW_i, and imprints B_i on his phone device and generates a random number k. Then sent registration request $\langle ID_i, PW_i, B_i \rangle$ to license server LS_j through a private channel.

Step 2: On receiving the response, the license server LS_j verifies the requesting identity to verify it as a registered identity. If it is not, the registration response is denied and communication terminates. Otherwise S_j calculates $CID_i = h(ID_i \| h(x))$, where x is LS_j's confidential key and $DID_i = E_x(ID_i \| r_o)$. Finally, LS_j sends DID_i to U_i via a secure channel.

Step 3: once received the message, U_i calculates $e = h(ID_i \| PW_i \| H(Bi))$. U_i stores e, k, $EID_i = h(PW_i \oplus ID_i) \oplus CID_i \oplus H(B_i)$, DID_i into the mobile device or smart card.

B. Login Authentication Phase Of The Propose Scheme

In this phase, if user U_i wants to access digital contents will need the content key. The authentication and login phase is shown in Fig. 2 and steps are explained below.

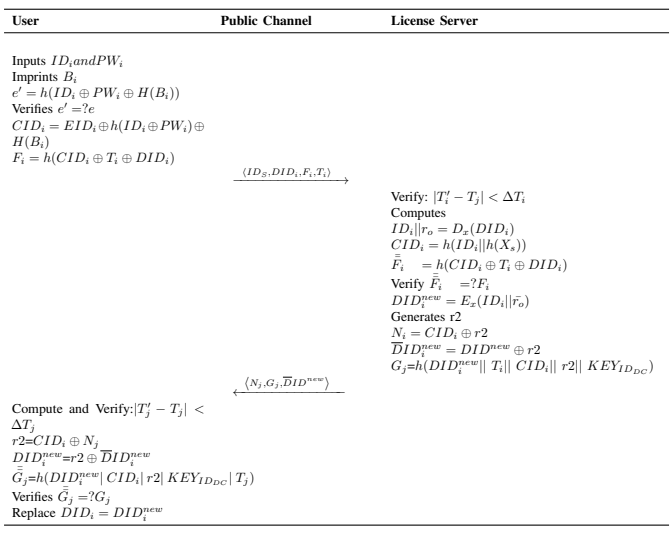

Figure 2. Proposed authentication scheme

Step 1: U_i enter ID_i and PW_i and B_i on the mobile device. U_i verifies whether e' and e are equal, where $e' = h(H(B_i \| ID_i \| PW_i))$. If e' checks out then computes $CID_i = EID_i \oplus h(PW_i \oplus ID_i) \oplus H(B_i)$, $F_i = h(CID_i \oplus T_i \oplus DID_i)$, T_i is the present timestamp originated by U_i. Finally, U_i sends the authentication request $\langle DID_i, F_i, T_i \rangle$ to LS_jthrough a open channel.

Step 2: On receiving response from U_i with a time T_i, LS_j first validates the time delay in the transmitted message by verifying where $|T_i' - T_i| < \Delta T_i$, where ΔT_i indicates the longest possible transmission delay or acceptable preset threshold delay. If the verification is done, LS_j computes $ID_i || r_o = D_x(DID_i)$, $CID_i = h(ID_i || h(x))$, $\bar{\bar{F}}_i = h(CID_i \oplus T_i \oplus DID_i)$ and verifies whether $\bar{\bar{F}}_i = ?F_i$, $DID_i^{new} = E_x(ID_i || \bar{r_o})$ If the login fails, the communication is denied. Otherwise, LS_j finds or searches the key KEY_{IDDC} of content and generates a random number r2. Then LS_j computes $N_i = CID_i \oplus r2$, $\bar{DID}_i^{new} = DID^{new} \oplus r2$, $G_j = h(DID_i^{new} || T_j || CID_i || r2 || KEY_{IDDC})$, where T_j generated by LS_j for current time-stamp. The user also send ID_S to the license server, where ID_S license server identity. Finally, LS_j sends the information $\langle ID_S, N_j, G_j U, DID_i^{new} \rangle$ to U_i over the public channel.

Step 3: After acquiring the respondent parameters from S_j with time T_j', U_i first validates the time latency in the transmitted response by verifying whether $\mid T_j' - T_j \mid < \Delta T_j$, where ΔT_j represents the longest delay of transmission or acceptable preset latency threshold. When this condition is validates, U_i computes $r2 = CID_i \oplus N_j$, $DID_i^{new} = r2 \oplus \bar{DID}_i^{new}$, $\bar{\bar{G}}_j = h(DID_i^{new} | CID_i | r2 | T_j | KEY_{IDDC})$ and Verifies $\bar{\bar{G}}_j = ?G_j$. When the authentication is finish, U_i saves and replaces $DID_i = DID_i^{new}$.

Table II
Notations table for BAN logic

Notations	Description
$Q \mid \equiv X$	Q Believing on X
$Q \lhd X$	Q Sees which is X
$Q \mid \equiv T$	Q believes T's action. E.g., $Q \mid \equiv T \mid \equiv X$ means Q believes on T believes on X is true
$Q \mid \sim X$	Q once says X
$Q \Rightarrow X$	q has full jurisdiction beyond X
$\#(X)$	X is updated and fresh
$(C)_k$	combine conditions C by the use of k
$(C)_k$	Carry out hash operation on C use X
$(X)_K$	Message of hash X with a key K
$Q \overset{k}{\longleftrightarrow} T$	Q and T use to interact using the shared key k with each others
DID_i	Session key DID_i used one time in the current section
$\frac{Q \mid \equiv Q \overset{K}{\longleftrightarrow} T, q \lhd < X >_K}{Q \mid \equiv T \mid \sim X}$	rule of Message-Meaning
$\frac{Q \mid \equiv \#(X)}{Q \mid \equiv \#(X,Y)}$	rule of conjuncatenation-Freshness
$\frac{Q \mid \equiv \#(X), Q \mid \equiv T \mid \sim X}{Q \mid \equiv T \mid \equiv X}$	rule of verification-Nonce
$\frac{Q \mid \equiv T \Rightarrow X, Q \mid \equiv T \mid \equiv X}{Q \mid \equiv X}$	rule of Jurisdiction

III. Security Analysis

Formal security analysis of the designed scheme is conducted formally through BAN logic.

A. BAN logic security proof

The accuracy of the designed protocol has been checked through BAN logic [29]. The BAN logic notations are shown in table II.

1) Goals: Four goals have been set to satisfy the correctness of the designed authentication scheme. There are two participators; the authorized user (U_i) and the authorized server (LS_j) in our proposed protocol and the goals are:

- Goal-1: $LS_j| \equiv U_i \overset{DID_i}{\longleftrightarrow} LS_j$
- Goal-2: $LS_j| \equiv U_i| \equiv U_i \overset{DID_i}{\longleftrightarrow} LS_j$
- Goal-3: $U_i| \equiv LS_j \overset{DID_i}{\longleftrightarrow} U_i$
- Goal-4: $U_i| \equiv LS_j| \equiv LS_j \overset{DID_i}{\longleftrightarrow} U_i$

2) Idealized Form: Part-1: In the proposed protocol, the idealized form discussed bellow:

- M-1: $U_i \rightarrow LS_j$: DID_i,$< ID_i \| r_o >_x, ID_s, F_i, T_i$
- M2: $LS_j \rightarrow U_i$: $N_i < CID_i \oplus r2 >, G_i, \overline{DID}^{new} < ID_i \| r2 >_x$

3) Assumption: Part-2: The following assumptions made to analyse the designed scheme by the use of BAN logic.

- A-1: $LS_j| \equiv \#(r2)$
- A-2: $U_i| \equiv \#(r_o)$
- A-3: $U_i| \equiv LS_j \Rightarrow r2$
- A-3: $LS_j| \equiv U_i \Rightarrow r_o$

4) Idealized form verification: With the goals and idealized form set up, now the proposed scheme can be verified using BAN logic as follows.

M-1: $U_i \rightarrow LS_j$: $DID_i < ID_i \| r_o >_x$, ID_s, F_i, T_i is timestamp of U_i. By the use of sees $Q \lhd X$ rule,

- V-1: $LS_j \lhd DID_i, < ID_i || r_o >_x, ID_s, F_i, T_i$

According to line V-1 and the msg-meaning rule, which is $\frac{Q|\equiv Q \overset{K}{\longleftrightarrow} T, q \lhd < X >_K}{Q|\equiv T|\sim X}$ & , we attain

- V-2: $LS_j| \equiv U_i| \sim r_o$

Using rule of Freshness $\frac{Q|\equiv \#(X)}{Q|\equiv \#(X,Y)}$ & V-2, we attain

- V-3: $LS_j| \equiv U_i| \equiv r_o$

By the use of $\frac{Q|\equiv T \Rightarrow X, Q|\equiv T|\equiv X}{Q|\equiv X}$ jurisdiction rule & V-3, we attain

- V-4:$LS_j| \equiv r_o$

Using of V-4 & rule of session key DID_i , we get

- V-5: $LS_j| \equiv U_i \overset{DID_i}{\longleftrightarrow} LS_j$ **(Goal-1)**

By the use of nonce-verification $\frac{Q|\equiv \#(X), Q|\equiv T|\sim X}{Q|\equiv T|\equiv X}$ rule, we attain

- V-6: $LS_j| \equiv U_i| \equiv U_i \overset{DID_i}{\longleftrightarrow} LS_i$ **(Goal-2)**

M-2: $LS_j \rightarrow U_i : N_i < CID_i \oplus r2 >, G_j, DID_i^{new} < ID_i || r2 >_x$

By the use of sees rule $Q \lhd X$, we achieve

- V-7: $U_i \lhd N_i :< CID \oplus r2 >, G_j, DID_i^{new} < ID_i || r2 >_x$

By the use of message-meaning $\frac{Q|\equiv Q \overset{K}{\longleftrightarrow} T, q \lhd < X >_K}{Q|\equiv T|\sim X}$ rule and v-7, we attain

- V-8: $U_i| \equiv LS_j| \sim r2$

By using of Freshness-conjuncatenation $\frac{Q|\equiv \#(X)}{Q|\equiv \#(X,Y)}$ rule and V-8, we get

- V-9: $U_i| \equiv LS_j| \equiv r2$

By applying of jurisdiction $\frac{Q|\equiv T \Rightarrow X, Q|\equiv T|\equiv X}{Q|\equiv X}$ rule and V-9, we attain

- V-10:$U_i| \equiv r2$

By using V-10 and the SK DID_i rule, we get

- V-11: $U_i| \equiv LS_j \overset{DID_i}{\longleftrightarrow} U_i$ **(Goal-3)**

Applying nonce-verification $\frac{Q|\equiv \#(X), Q|\equiv T|\sim X}{Q|\equiv T|\equiv X}$ rule and V-11, we achieve

- V-12: $U_i| \equiv LS_j| \equiv LS_j \overset{DID_i}{\longleftrightarrow} U_i$. **(Goal-4)**

Using BAN logic it has been proved that U_i and LS_j attain mutual authentication and also securely achieve the session key agreement. Consequently, it can be concluded that the proposed authentication scheme is correct.

IV. Performance Analysis

The proposed protocol has been comparatively analyzed for performance based on the computation and communication costs. For the comparative analysis existing scheme [10], [16], [17], [22], [23], [30] have been considered and the results are shown in Table III.

For comparison with the existing schemes, it is assumed that the length of the identity(server, user), password, message digest, and random nonce take 128 bit each [31]. The communication cost of the proposed scheme is $(7 \times 128) = 896$ bits, cost for [10] is $(10128) = 1280$ bits, for [16] its $(16 \times 128) = 2048$ bits, for [17] it is $(17 \times 128) = 2176$, for [30] it is $(14 \times 128) = 1792$ bits, for [22] it is $(11 \times 128) = 1408$ bits, and for [23] it is $(7 \times 128) = 896$ bits. It is clear that the offered scheme outperforms and better comparatively. The percentage (%) cost has also been computed showing that the proposed protocol is 38.28% efficient than the Lee et al. proposal.

The computation cost comparison is also shown in Table III where the following notations are used

_ T_{Rep}: time for computing fuzzy function extractor [10].

_ T_h: the amount of time to computes a hash function.

_ T_{xor}: the amount pf time to calculates operation of ($\oplus$ XOR) .

Due to insignificant impact the cost of $\oplus$ XOR, division (DIV), and multiplication (M) operations is neglected [32]. As symmetric encryption is used, so the approximate computation time of symmetric key encryption is 0.0056 and decryption is 0.0056 second [31]. The one way hashing function cost is approximately 0.00032 second [31]. So the total computation cost of the offered scheme amounts to $6T_h + 1T_{senc} + 1T_{sdec}$ that is totalling to $4 \times 0.00032 + 1x0.0056 + 1x0.0056 = 0.0131$ seconds as shown in comparatively in Table III.

V. Conclusion

In this paper, we analyzed two recent schemes for provision of digital rights management. We have proven that the schemes of Yu et. and Lee et al. are unable to defend several attacks including insiders malicious interventions. This calls for an improved, robust, and secure scheme for DRM systems. The security of the proposed scheme is verified via informal and formal security mechanisms. The security and performance

Table III
COMPUTATION COST COMPARISON

Scheme	C_1	ET (ms)	C_2
[10]	$(8+2i)T_h + 12T_{xor}$	0.0144	1280
[16]	$9T_h + 12T_{xor}$	0.01408	2048
[17]	$6T_h + 4T_{xor}$	0.01312	2176
[30]	$1T_{Rep} + 6T_h + 4T_{xor}$	0.03022	1792
[22]	$6T_h + 12T_{xor}$	0.01312	1408
[23]	$5T_h + 6T_{xor}$	0.0128	896
Our	$6T_h + 9T_{xor}$	0.0131	896

*C_1: Computation cost; C_2: Communication cost; ET: Execution time

analysis and comparisons show that the designed protocol is highly secure as comparatively to the existing protocol with similar computation and communication costs. In the future, an effective search method for big encrypted data on the DRM system may be provided to improve data confidentiality and privacy.

REFERENCES

[1] H. Kim, Y. Lee, and Y. Park, "A robust and flexible digital rights management system for home networks," *Journal of Systems and Software*, vol. 83, no. 12, pp. 2431–2440, 2010.

[2] Y. Liu, C.-C. Chang, and S.-C. Chang, "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*, vol. 6, no. 1, pp. 140–153, 2015.

[3] 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, p. 16, 2019.

[4] S. Rana and D. Mishra, "An authenticated access control framework for digital right management system," *Multimedia Tools and Applications*, pp. 1–16, 2021.

[5] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam, and N. Kumar, "Efficient and secure anonymous authentication with location privacy for iot-based wbans," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2603–2611, 2020.

[6] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for vanets," *Future Generation Computer Systems*, vol. 84, pp. 216–227, 2018.

[7] R. Amin and G. Biswas, "An improved rsa based user authentication and session key agreement protocol usable in tmis," *Journal of Medical Systems*, vol. 39, no. 8, p. 79, 2015.

[8] 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, p. e4137, 2019.

[9] R. Amin, S. H. Islam, G. Biswas, D. Giri, M. K. Khan, and N. Kumar, "A more secure and privacy-aware anonymous user authentication scheme for distributed mobile cloud computing environments," *Security and Communication Networks*, vol. 9, no. 17, pp. 4650–4666, 2016.

[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, pp. 3383–3404, 2015.

[11] S. Rana and D. Mishra, "Secure and ubiquitous authenticated content distribution framework for iot enabled drm system," *Multimedia Tools and Applications*, vol. 79, no. 27, pp. 20 319–20 341, 2020.

[12] 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, 2015.

[13] S. Rana and D. Mishra, "Cryptanalysis and improvement of biometric based content distribution framework for digital rights management systems," *Security and Privacy*, vol. 4, no. 1, p. e133, 2021.

[14] D. Mishra and S. Rana, "A provably secure content distribution framework for portable drm systems," *Journal of Information Security and Applications*, vol. 61, p. 102928, 2021.

[15] D. Dharminder, "Lwedm: Learning with error based secure mobile digital rights management system," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 2, p. e4199, 2021.

[16] 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, pp. 972–984, 2013.

[17] 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.

[18] S. Rana and D. Mishra, "Cryptanalysis and improvement of biometric based content distribution framework for digital rights management systems," *Security and Privacy*, vol. 4, no. 1, p. e133, 2021.

[19] A. Irshad, S. A. Chaudhry, Q. Xie, X. Li, M. S. Farash, S. Kumari, and F. Wu, "An enhanced and provably secure chaotic map-based authenticated key agreement in multi-server architecture," *Arabian Journal for Science and Engineering*, vol. 43, no. 2, pp. 811–828, 2018.

[20] T. Maitra, M. S. Obaidat, R. Amin, S. 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, p. e3242, 2017.

[21] A. Irshad, S. A. Chaudhry, O. A. Alomari, K. Yahya, and N. Kumar, "A novel pairing-free lightweight authentication protocol for mobile cloud computing framework," *IEEE Systems Journal*, vol. 15, no. 3, pp. 3664–3672, 2021.

[22] 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.

[23] S. Yu, K. Park, Y. Park, H. Kim, and Y. Park, "A lightweight three-factor authentication protocol for digital rights management system," *Peer-to-Peer Networking and Applications*, pp. 1–17, 2020.

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

[25] S. A. Chaudhry, A. Albeshri, N. Xiong, C. Lee, and T. Shon, "A privacy preserving authentication scheme for roaming in ubiquitous networks," *Cluster Computing*, vol. 20, no. 2, pp. 1223–1236, 2017.

[26] F. Wei, P. Vijayakumar, J. Shen, R. Zhang, and L. Li, "A provably secure password-based anonymous authentication scheme for wireless body area networks," *Computers & Electrical Engineering*, vol. 65, pp. 322–331, 2018.

[27] M. Azees, P. Vijayakumar, M. Karuppiah, and A. Nayyar, "An efficient anonymous authentication and confidentiality preservation schemes for secure communications in wireless body area networks," *Wireless Networks*, vol. 27, no. 3, pp. 2119–2130, 2021.

[28] M. Bayat, M. B. Atashgah, M. Barari, and M. R. Aref, "Cryptanalysis and improvement of a user authentication scheme for internet of things using elliptic curve cryptography [j]," *International Journal of Network Security*, vol. 21, no. 6, pp. 897–911, 2019.

[29] J. Wessels and C. F. BV, "Application of ban-logic," *CMG FINANCE BV*, vol. 19, pp. 1–23, 2001.

[30] 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.

[31] D. He, N. Kumar, J.-H. Lee, and R. Sherratt, "Enhanced three-factor security protocol for consumer usb mass storage devices," *IEEE Transactions on Consumer Electronics*, vol. 60, no. 1, pp. 30–37, 2014.

[32] L. Chen and K. Zhang, "Privacy-aware smart card based biometric authentication scheme for e-health," *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp. 1353–1365, 2021.