PrivDRM : a privacy-preserving secure Digital Right Management system

Gaber, T, Ahmed, A and Mostafa, A

http://dx.doi.org/10.1145/3383219.3383289

PrivDRM: A Privacy-preserving Secure Digital Right Management System

Tarek Gaber
School of Science, Engineering Environment, University of Salford
Salford, UK
t.m.a.gaber@salford.ac.uk

Ali Ahmed
Victoria University of Wellington
Wellington, New Zealand
ali.ahmed@vuw.ac.nz

Amira Mostafa
School of Computer Science and Informatics, Suez Canal University
Ismailia, Egypt

ABSTRACT

Digital Right Management (DRM) is a technology developed to prevent illegal reproduction and distribution of digital contents. It protects the rights of content owners by allowing only authorised consumers to legitimately access associated digital content. DRM systems typically use a consumer's identity for authentication. In addition, some DRM systems collect consumer's preferences to obtain a content license. Thus, the behaviour of DRM systems disadvantages the digital content consumers (i.e. neglecting consumers' privacy) focusing more on securing the digital content (i.e. biased towards content owners). This paper proposes the Privacy-Preserving Digital Rights Management System (PrivDRM) that allows a consumer to acquire digital content with its license without disclosing complete personal information and without using any third parties. To evaluate the performance of the proposed solution, a prototype of the PrivDRM system has been developed and investigated. The security analysis (attacks and threats) are analysed and showed that PrivDRM supports countermeasures for well-known attacks and achieving the privacy requirements. In addition, a comparison with some well-known proposals shows that PrivDRM outperforms those proposals in terms of processing overhead.

CCS CONCEPTS

• **Security and privacy → Privacy protections**; **Digital rights management**; **Authorization**; **Privacy-preserving protocols**.

KEYWORDS

Digital Rights Management, Security, Privacy-preserving, Digital Content, Consumer's rights, Content Owner

ACM Reference Format:
Tarek Gaber, Ali Ahmed, and Amira Mostafa. 2020. PrivDRM: A Privacy-preserving Secure Digital Right Management System. In *Evaluation and Assessment in Software Engineering (EASE 2020), April 15–17, 2020, Trondheim, Norway*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3383219.3383289

EASE 2020, April 15–17, 2020, Trondheim, Norway

ACM ISBN 978-1-4503-7731-7/20/04…$15.00
https://doi.org/10.1145/3383219.3383289

1 INTRODUCTION

With the rapid development of technology, digital multimedia have been under scrutiny from both consumer's and content creator's point of views. The ease of access to such digital content facilitates illegal content sharing, which enables unauthorised consumers to access such content illegally and without being identified. For example, many users utilising Peer-to-Peer applications such as Vuze and μTorrent infringe copy-righted materials on a daily basis. In some countries such as China, protecting digital rights is challenging[1]. Although Creative Commons licenses promise seamless responsible sharing of academic content amongst legitimate users, it is hard to protect against illegal access [17]. That endures a considerable revenue loss for the content owners as discussed by Wu et al. in [31]. The content owners and legal distributors protect their intellectual property and commercial profits by using DRM systems. DRM is a technology developed to prevent illegal reproduction and distribution of digital content. It protects the rights of the content owners by allowing only authorised consumers to legitimately access the content. Unfortunately, those DRM systems, sometimes, ignore or overlook the privacy preferences of the consumers focusing more on protecting the content, which is in the favour of the content owner. This biased behaviour of DRM systems disadvantages the digital content consumers and could render them vulnerable to many security attacks should the system is compromised by malicious parties [2, 12].

The issue of digital privacy is becoming increasingly prevalent in a world where more people are connecting to the Internet than ever before [13], where there is a tendency to access and share information, for example, in both inside and outside the traditional working environment on popular social networking sites [26]. While numerous survey studies reveal the users' growing sensitivity towards digital privacy, some users are still privacy pragmatic [16]. In many aspects of privacy, studies show that people are prepared, in certain situations, to essentially trade-out aspects of their own privacy for a sense of increased accessibility, security, and safety in their daily activities [8]. While this approach certainly draws criticism [6], it is, unfortunately, a reality. While there is no definitive definition of what constitutes 'personal data', there is a dire requirement to protect digital users against the activities that could compromise their privacy. In this research, we adopt the latest General Data Protection Regulation (GDPR) definition of personal data which describes personal data as "Any information relating to a directly or indirectly identified or identifiable natural person ('data subject')". [1]. Indirect identification is an important aspect of this definition as,

[1] http://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm

for example, building a profile of a user could disclose the user's identity. Building a user profile is easy in multimedia and could reveal lots of information about the person [5]. Given the aforementioned predicament of the DRM systems' bias and the need for protecting consumer's privacy, we, in this paper, aim at proposing a novel DRM system (i.e. PrivDRM) that preserves the consumers' privacy, while maintaining the content owner's protection of the digital content. Unlike solutions such as EDU-DRM which is targeting K-12 Education [22], PrivDRM is a generic solution that caters to a wide spectrum of application requirements. In PrivDRM, a consumer acquires a digital content without disclosing complete personal information, thus protecting the consumer's privacy and preventing any collusion from the DRM parties. However, PrivDRM, at some point, can identify illegal consumers those manipulating the system to hold them accountable.

The organisation of this paper is as follows. Section 2 discusses the background and related works. Section 3 demonstrates the proposed system along with its notation and building blocks. Section 4 investigates the proposal and analyses it. Finally, section 5 concludes the paper and depicts the future research direction(s).

2 BACKGROUND

Privacy-preserving DRM schemes for multiparty distributor have been around in the academic literature for a while. For example, Win et al. [30] proposed a privacy-preserving scheme for multiparty DRM systems without relying on a Trusted Third Party (TTP). It uses simple cryptographic primitives such as blind decryption and hash chain to avoid TTP and to protect the consumer's privacy. In this system, the consumer obtains the token set from the content owner anonymously to purchase a license of content from a content provider. A drawback here is that the content provider is able to track the content usage of the consumer, thus can build a usage profile under a pseudonym. Petrlic et al. (2013) in [23] proposed a privacy-preserving multiparty DRM system based on the smartcard technology without using a TTP for license checking. It is based on proxy re-encryption to protect the consumer's privacy and to avoid using TTP. Consumer's anonymity is preserved, where neither the content providers nor the content distributors are able to obtain any information about the consumer. However, this system does not address how malicious consumers could be identified!

Mishra et al. (2012) proposed a privacy-preserving multiparty DRM system in [21] that is based on the secret sharing scheme, where no party has the complete decryption key. In this system, the distributor plays the middle-man role that exchanges the messages between the owner and the consumer. Consumer's anonymity is preserved during the license acquisition process without violating the accountability requirement, which seems a promising technique. However, the computational overhead endured by the system is significantly high that affects its adoption, for example, in mobile computing. The work in [21] preserves the anonymity of the consumer by the utilisation of TTP which we believe is time-consuming and could be (i.e. TTP) taken off the system as found in the other proposals. The work in [23] does not trace malicious attempts to access protected digital content, which could encourage other unauthorised and malicious users to attempt accessing more content. Unfortunately, the work in [20] does not protect against collisions of DRM servers and partially providing non-repudiation (i.e. non-repudiation is provided for some system processes only), which is the same drawback of the work in [30]. Unlinkability is overly important as it prevents any party from building a profile of the consumer, which is not supported in those systems except that of [23]. Preventing any part from building a usage profile to identify a user is of paramount importance as highlighted ealier. Mishra et al. (2015) in [20] proposed another scheme that presents a flexible and transparent content distribution mechanism based on sharing the content key information between the distributor and the license server. Such a content license can not be generated without the participation of both parties. In this system, the owner assigns all keys k_i by pseudonym unique key U_{k_i} and sends the pair (k_i,U_{k_i}) to the license server via an *'assumed'* secure channel. Such an assumption is one of the drawbacks of this work. The license server identifies key k_i by U_{k_i}, where the key k_i is used for encryption/decryption. In addition, the owner provides the name mapping process between pseudonym keys' identities and contents' identities to all distributors via the *'secure'* channel. This scheme protects the consumer's privacy, where the distributor and the license server know who requested the content, but not the content itself. The work provides anonymous content identity in this way hiding the consumer's preference, which is one aspect of the consumer's privacy. In addition, it supports accountability in case of a consumer maliciously accessing the protected content. The identification of malicious consumers is achieved without violating the privacy of authorised consumers. Computationally, the process of signing the pseudo keys exhibits a significant overhead that many devices such as low-end smartphones may not be able to endure, not to mention the time it takes for such pseudonym keys generation. Moreover, the owner not only send these pseudo keys to the license server but also send them to the distributor through name mapping process that increases the number of communicated messages in the system, not to mention the infrastructure needed at multiple parties to securely store those keys.

The concept for decentralised rights management has been around for a while and the work in [11] discusses the possibility of using blockchain as the decentralisation technology. The need for decentralisation is to solve the problems arising from centralised solutions even those using P2P Based DRM Scheme such as leaking the protected content if the centralised server is compromised [28]. As blockchain is becoming prolific in many application domains, DRM could also benefit from such a technology especially in supporting anonymity. The work in [19] proposes DRMChain which is a scheme to manage digital rights based on blockchain. Under this umbrella comes the workpieces in [9, 14, 15, 19, 24, 32, 33]. While blockchain promises Transparency, Redundancy, Immutability, and Dis-inter-mediation, it faces challenges such as where the actual digital content is going to be stored [25]. In addition, while immutability is a required feature, disputes over copyright are always expected, thus how such disputes are resolved in the existence of immutability! For more information about what blockchain can and can't do, we suggest the reader go through the work in [4, 10, 25, 27]. It is worth noting that a recent trend in DRM privacy is to use quantum computing and deep learning models as that in the work in [3, 7, 29].

To summarise the differences between existing DRM systems and to show what is missing, we compiled Table 1 for that purpose.

Table 1: Existing DRM Solutions Comparison

Feature	[30]	[23]	[21]	[20]	[19]	[15]	[32]
Consumer anonymity	No	Yes	Yes	Yes	Yes	Yes	Yes
TTP Utilisation	No	No	Yes	No	No	No	No
Malicious attempts Tracking	Yes	No	Yes	Yes	Yes	No	N/A
License acquisition privacy	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Servers Collision Protection	No	No	Yes	Yes	N/A	N/A	No
unlinkability*	No	Yes	No ++	No ++	No	No	No
Non-repudiation	No	Yes	No*	No*	No	No	No
Content distributor Flexibility	Yes	Yes	Yes	Yes	N/A	N/A	No

- Unlinkability of the content execution.
- No++: If parties colluded, content is linkable otherwise, it is not.
- No*, the system partially achieves non-repudiation in some processes

Given Table1, there is a need for a solution that provides consumer's anonymity and privacy-preserving, which includes the support of the unlinkability of content execution, does not depend on TTP or any additional trusted hardware, provides non-repudiation and flexibility to choose the content distributor, and finally provides Tracking of malicious attempts. For such a purpose, we will introduce our system that provides those features in the next section.

3 THE PROPOSED PRIVDRM SYSTEM

3.1 Notation and Assumptions

The proposed system depends on the following notation:

- consumer C, content owner O, distributor D, license server LS, and multiple levels of distributors($D_{i,j}$)
- For any entity in the system i, it's identity ID_i, its public key is PK_i and its private key is Sk_i
- $H(X)$: A cryptographic one-way hash function
- E_{PK_i}: Public-key encryption algorithm using entity i's public key
- E_{sym_K}: Symmetric-key encryption algorithm using symmetric key K
- $sign_{SK_i}$ Digital signature algorithm using entity i's private key

PrivDRM assumes the system has multiple distributors, where the deployment of distributors depends on the system requirements, the distributor can securely authenticate different consumers and each entity in the system has a public/private key pair, and the consumers can use anonymous networks such as TOR[2] to access the protected content.

[2]https://www.torproject.org/

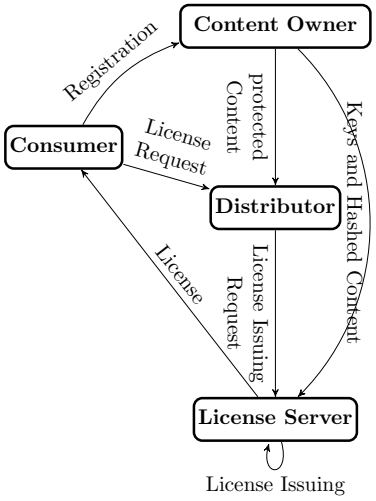

Figure 1: PrivDRM: An Overview

3.2 The Building Blocks

The proposed system building blocks are depicted in figure 1.

Content Encryption. Let the system have n distributors (i.e. $D_{1...n}$) and r digital contents (i.e. $M_1, M_2, ..., M_r$) each of which with a different content identity ID_{M_i} (i.e. $ID_{M_1}, ID_{M_2}, ..., ID_{M_r}$). To secure the digital contents, the system encrypts them in the following manner:

- $E_{sym_{k_i}}(M_i), i = 1, 2, .., r$
  O generates distinct symmetric keys $K_1, K_2, ..K_r$ and symmetrically encrypts all digital contents (i.e in our PrivDRM implementation, we used the AES algorithm).
- $H(ID_{M_1}), H(ID_{M_2}), ..., H(ID_{M_r})$
  O hashes the content identities and keeps the hashed values of the content identities securely stored.
- Finally, O sends (protected contents, contents information) to all D_n and the pair of $(K_i, H(ID_{M_i}))$ to LS via a secure communication channel (i.e. in PrivDRM implementation, we used TOR). LS identifies the content decryption key K_i by the hash value of content identity $H(ID_{M_i})$ instead of original content identity (ID_{M_i}).

Content Distribution. Each distributor D_i is assumed to store the protected contents while sharing content data (i.e. on their website for example). The content data could includes the content name, the price, the content description, and the content ID (ID_{M_t}). C_j can download the protected content from any distributor (i.e. could be based on server proximity or price preference). C_j can use a Tor connection to connect to the distributor's storage/website. In this way, c_j can anonymously.

License Acquisition Process. For a consumer C_i to buy a license L_t for a protected content M_t, C_i must go through an authentication process with the distributor. If the authentication process such as

that mentioned in [18] [3] is done successfully, the license acquisition protocol follows as:

- C_i computes $H(ID_{M_t})$ then encapsulate that in the license request to D_g.
- D_g verifies the consumer's registration and checks its revocation list to check whether the consumer is a revoked/authorized consumer.
- If the verification is successful, D_g receives the payment from the authorized consumer then generates T, where T = (ID_C, $H(ID_{M_t})$, T_{S_1}), where T_{S_1} is the timestamp of the transaction.
- D_g encrypts T using LS' public key and sign the message using own private key to get $X = E_{PK_{LS}}(T)$ and $\sigma(X) = sign_{SK_{D_g}}(X)$. After that, D_g sends $(X, \sigma X)$ to LS.
- LS verifies the signature of D_g using its public key. If verification succeeds, LS decrypts T using own private key. The hashed content identity $H(ID_{M_t})$ and the consumer's identity ID_C are extracted from the T.
- LS generates the license L_t which includes *the content usage rights, timestamp T_{S_2}, and the decryption key K_t* that is identified by $H(ID_{M_t})$. Then, LS associates the encrypted consumer's identity $E_{PK_{LS}}(ID_C)$ with the license.
- LS, then, encrypts the license using C_i's public key, generates its signature using own private key, and sends the signed message to C_i.
- On receiving the messages from LS, C_i verifies its signature using LS's public key. If verification succeeds, C_i decrypts the message using own private key to extract the license to play the protected content.

Revocation Detection of Consumer. In a DRM system, consumers must be accountable for any misuse of their purchased licenses. Thus, the consumer must be authenticated and his/her usage license data will be tracked via license acquisition. If the license is associated with the original identity of the consumer, the license usage data may disclose information about consumer's preferences. Thus, the consumer's privacy could be violated. In PrivDRM, LS associates the license with the encrypted consumer's identity $E_{PK_{LS}}(ID_{Ci})$ instead of the original identity ID_C. This encrypted consumer's identity $E_{PK_{LS}}(ID_{Ci})$ doesn't reveal any information about C_i, however PrivDRM supports violation detection as follows. When O suspects a violation, $E_{PK_{LS}}(ID_{Ci})$ is retrieved from the license and is sent to LS for decryption. Then, LS decrypts $E_{PK_{LS}}(ID_{Ci})$ using own private key and gets ID_{Ci}, which is forwarded to O. Finally, O matches the received ID_{Ci} with a C_i and identity is revoked.

As a proof of concept, PrivDRM is implemented as an on-line client-server service (i.e. request- respond model) in which, the server represents an on-line DRM service for the clients (i.e. consumers) to connect to using a DRM desktop application. The implementation followed the architecture shown in Figure 1. There are two main components here: 1) the DRM host agent and 2) the DRM client agent. The former implements the services related to the content owner, the content distributor, and the license server. The latter implements those services related to the consumer. The main consumer's content access is illustrated in the sequence diagram in Figure 2.

[3]The authentication process is beyond the scope of this research

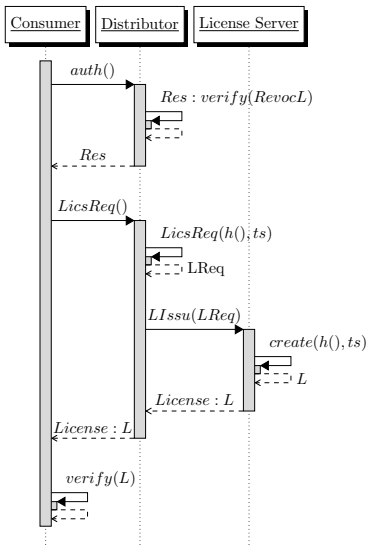

Figure 2: Protected Digital Content Access

4 PRIVDRM SYSTEM ANALYSIS

Given the broad spectrum of exploitation that a DRM system could be subject to, we will focus on the replay attacks as it is very related to the underlying PrivDRM protocols (i.e. system design). Attacks such as Man-in-The-Middle (MiTM) are more of a network concern than that of the application. The Denial of Service (DoS) could be either way (i.e. network attacks and application one. It is on our list of future work to investigate this kind of attack against PrivDRM especially when the number of concurrent connections explodes as we will see in our performance investigations below. The replay attack is also known as playback attack is one of the common forms of attacks against protocols either application or network, in which the attacker maliciously repeats (i.e. or sometimes delay) an old message pretending it is a fresh one. As the digital content license could be repeated, PrivDRM is using a time-stamp to counter that. In PrivDRM, the attackers cannot gain access to a protected content by replay an old successful license issuing request.

PrivDRM protects against replay attacks by utilising 2 time-stamps to verify that the License Server does not generate licenses based on a played back requests, and the DRM client application does not accept an old license and hence playing the content illegally. The first time-stamp is used when the distributor sends the request to the license server to issue the license. The license server is to verify the time-stamp before issuing the license. The license itself signed by the license server containing another time-stamp of the license server this time for the DRM application at the consumer's side to verify before playing the content.

It is worth noting that PrivDRM preserves the anonymity of the consumers since no party in the system have complete information to identify the consumer's selections (i.e. digital contents) although a consumer's ID could be well-known to the distributors as well

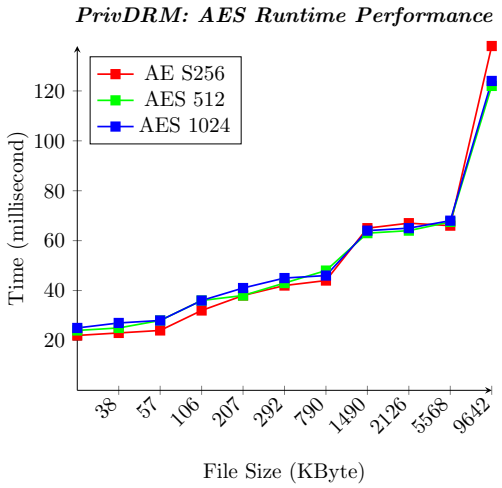

Figure 3: Protected Digital Content Access

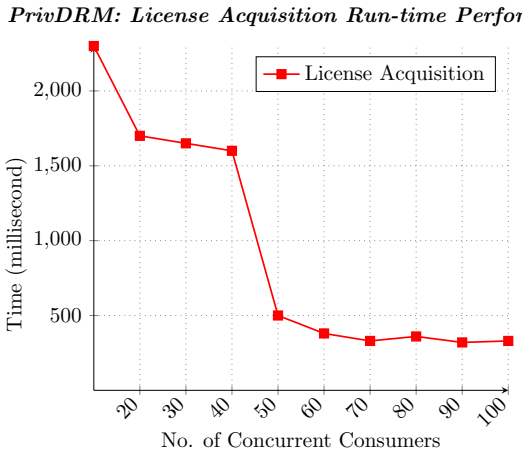

Figure 4: PrivDRM: License Acquisition Run-time Performance

as the license server (i.e. actually only $H(ID_i)$). The by-product of this anonymity is the prevention of collusion between parties.

The computational overhead of DRM systems affects its adoption. Thus, we need to measure the run-time performance of the various PrivDRM components. One of those components is the one that protects the confidentiality of the content (i.e encryption). As highlighted before, PrivDRM uses AES as its underlying cryptosystem. AES is a symmetric cryptosystem that uses one key for both encryption and decryption. Our implementation uses various key sizes that could be configured within PrivDRM. Currently, we support 256 bits, 512 bits, and 1024 bits key along with different block sizes. To investigate the run-time performance of the AES in PrivDRM, the system is used on some real files with different sizes and the performance graph is measured as depicted in figures 3. We observe from Figure3 that AES-256 outperforms the other the small file sizes, but when file size significantly increases, AES-1024 outperforms the rest. We reckon the reason for this is because the number of blocks and, hence, the required AES rounds getting bigger with smaller key sizes and large files. Thus, privDRM takes more time to encrypt large files with 256bit key than that of the 1024bit key using the same file size. The recommendation here in PrivDRM is to use AES-1024 when file size is relatively large especially with full high definition digital content, not to mention the more security the system afford in this mode (i.e. AES-1024).

The license acquisition process represents a major component of any DRM system including PrivDRM. Its performance significantly affects the overall performance of any DRM solution. In PrivDRM, we investigated the run time performance of the license acquisition process by measuring the request and response time during the process. Generally, this is, somehow, depends on the current network status but in this experiment, such a factor is minimised. The license acquisition process includes two requests; the *authentication request* and the *license request*. The former should not have a significant impact on the run-time performance of PrivDRm since it does not include any heavy computations apart from verifying the consumer's ID against the revocation list. The latter is where

	[30]	[23]	[21]	[20]	PrivDRM
Initialisation	4	4	3	3	2
Name mapping process	N/A	N/A	4	2	N/A
During license acquisition	2	4	3	3	3
Content execution	-	8	0	0	0
Revocation process	1	N/A	2	2	2
Total	7	16	12	10	7

Table 2: Processing Overhead: The Number of Messages

all heavy computation takes place such as RSA encryption, decryption, and signature generation. Figure 4 demonstrates the run-time performance of PrivDRM in license acquisition. The numerical figures in this experiment are averaged across a different number of consumers. The system seems to perform well when the number of simultaneous consumers increases. This is a good indication for scalability, which will need further investigation should that number exceeded the 100 concurrent consumers.

Comparing PrivDRM computational cost to existing solutions would be a good measure to evaluate PrivDRM. The comparison should include communication overhead and consumer privacy protection requirements. Table 2 demonstrates the computational cost comparison of PrivDRM compared to some existing DRM systems. The computational cost is performed by computing the number of exponential operations in the systems under comparison. The table shows the execution of PrivDRM requires fewer exponential operations than the other solutions in this study. One of the reasons here is that PrivDRM does not require name mapping and/or token set generation. Another reason which is illustrated in table 2 is the number of messages exchanged between parties or system building blocks. PrivDRM shows the fewer number of messages exchanged compared to the solutions in Table 2, which, as said, contributes to the better performance of PrivDRM over the other solutions.

To summarise, PrivDRM supports consumer anonymity, avoids TTP utilisation, provides malicious attempts tracking, preserves

the license acquisition process privacy, protects the servers from collision, supports unlinkability of the content execution, provides non-repudiation, and promotes content distributor flexibility.

5 CONCLUSION AND FUTURE WORK

This paper presented a solution to preserve the consumers' privacy in multi-party DRM called Privacy-Preserving DRM System (PrivDRM). PrivDRM allows a consumer to obtain DRM-protected content and its license without disclosing complete personal information, hence privacy is protected. PrivDRM, on the other hand, holds those malicious consumers accountable for the misuse based on the license acquired. The features of PrivDRM solution are summarised as follows: a) The digital contents are distributed in a protected form using 1024-AES encryption algorithm. b)The consumer can download the protected digital content anonymously from the distributor's website using an anonymous connection (i.e. TOR) without revealing originating IP-address, thus the consumer's anonymity is preserved during the content download process. The consumer can submit the license request with anonymous content ID using SHA-256 hash function instead of the original ID. The consumer does not bear any additional cost as there is no use of TTP or any trusted hardware. Although, the PrivDRM system supports accountability, the system applies the least privilege security principle to achieve that. Last but not least, PrivDRM supports efficient content distribution mechanism where consumers can obtain digital content without incurring a high computational cost or high communication overhead. The future direction of this research focuses on Blockchain technology as an underlying technology to preserve both user's and content owner's privacy. Blockchain promises seamless transactions although power consumption for computation restricted devices is expected to be a hurdle. This will need comprehensive investigation which is also regarded as one of the future directions of this research.

REFERENCES

[1] Asad Abbas, Anam Fatima, Kenneth Khavwandiza Sunguh, Anders Avdic, and Xuehe Zhang. 2018. Digital Rights Management System in China: Challenges and Opportunities. *Journal of Cases on Information Technology (JCIT)* 20, 1 (2018).

[2] Hisham Abdalla, Hu Xiong, Abubaker Wahaballa, Philip Avornyo, and Zhiguang Qin. 2016. Anonymous Pairing-Free and Certificateless Key Exchange Protocol for DRM System. *IJ Network Security* 18, 2 (2016), 235–243.

[3] S. Akleylek and M. SoysaldÄś. 2017. A novel identicication scheme for post-quantum secure digital right management. In *2017 International Conference on Computer Science and Engineering (UBMK)*. 322–327.

[4] SILVIA A. CARRETTA. 2019. *Blockchain Challenges to Copyright Revamping the Online Music Industry.* mathesis. Department of Law.

[5] Yunseok Chang, Si Jin Lee, and Jae Chung Lee. 2015. An Effective User Profiling Data Structure for Dynamic License. *Indian Journal of Science and Technology* 8, 23 (2015).

[6] E. Chemerinsky. 2004. Post 9/11 Civil Rights: Are Americans Sacrificing Freedom for Security. *Denver University Law Review* 81, 4 (2004), 759–773.

[7] Huili Chen, Bita Darvish Rouhani, Cheng Fu, Jishen Zhao, and Farinaz Koushanfar. 2019. DeepMarks: A Secure Fingerprinting Framework for Digital Rights Management of Deep Learning Models. In *Proceedings of the 2019 on International Conference on Multimedia Retrieval (ICMR âĂŹ19)*. Association for Computing Machinery, New York, NY, USA, 105âĂŞ113.

[8] Rob Van den Hoven van Genderen. 2009. Trading Privacy for Security. *Amsterdam Law Forum* 1, 4 (2009), 95–102.

[9] Ashutosh Dhar Dwivedi. 2019. A Scalable Blockchain Based Digital Rights Management System. *IACR Cryptology ePrint Archive* 2019 (2019), 1217.

[10] Michèle Finck and Valentina Moscon. 2019. Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0. *IIC - International Review of Intellectual Property and Competition Law* 50, 1 (01 Jan 2019), 77–108.

[11] S. Fujimura, H. Watanabe, A. Nakadaira, T. Yamada, A. Akutsu, and J. J. Kishigami. 2015. BRIGHT: A concept for a decentralized rights management system based on blockchain. In *2015 IEEE 5th International Conference on Consumer Electronics - Berlin (ICCE-Berlin)*. 345–346.

[12] Tarek Gaber. 2013. Digital Rights Management: Open Issues to Support E-Commerce. *E-Marketing in Developed and Developing Countries: Emerging Practices* http://www.igi-global.com/chapter/digital-rights-m (2013), 69–87.

[13] World Bank Group. 2014. Internet users (per 100 people). Online.

[14] Junqi Guo, Chuyang Li, Guangzhi Zhang, Yunchuan Sun, and Rongfang Bie. 2019. Blockchain-enabled digital rights management for multimedia resources of online education. *Multimedia Tools and Applications* (09 2019).

[15] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, and A. Akutsu. 2015. The Blockchain-Based Digital Content Distribution System. In *2015 IEEE Fifth International Conference on Big Data and Cloud Computing*. 187–190.

[16] Alfred Kobsa. 2007. The Adaptive Web. Springer-Verlag, Berlin, Heidelberg, Chapter Privacy-enhanced Web Personalization, 628–670.

[17] Caroline Korbel. 2018. Managing Copyright in Digital Collections: A Focus on Creative Commons Licences. *dalhousie journal of interdisciplinary management (DJIDM)* 14 (2018).

[18] Cheng-Chi Lee, Chun-Ta Li, Zhi-Wei Chen, Shun-Der Chen, and Yan-Ming Lai. 2019. A novel authentication scheme for anonymity and digital rights management based on elliptic curve cryptography. *International Journal of Electronic Security and Digital Forensics,* 11, 1 (2019), 96–117.

[19] Zhaofeng Ma, Ming Jiang, Hongmin Gao, and Zhen Wang. 2018. Blockchain for digital rights management. *Future Generation Computer Systems* 89 (2018), 746 – 764.

[20] Dheerendra Mishra. 2015. An Accountable Privacy Architecture for Digital Rights Management System. In *Proceedings of the Sixth International Conference on Computer and Communication Technology 2015*. ACM, 328–332.

[21] Dheerendra Mishra and Sourav Mukhopadhyay. 2012. Towards a secure, transparent and privacy-preserving DRM system. In *Proceedings of the Recent Trends in Computer Networks and Distributed Systems Security,2012,Volume 335*. Springer, 304–313.

[22] Ahmet Ozmen, Ahmet SANSLI, and Veysel Sahin. 2019. EDU-DRM: A Digital Rights Management (DRM) system for K-12 education. *Scientia Iranica* 26, Special Issue on: Socio-Cognitive Engineering (2019), 103–113.

[23] Ronald Petrlic and Stephan Sekula. 2013. Unlinkable content playbacks in a multiparty DRM system. In *Proceedings of the Data and Applications Security and Privacy XXVII, 2013, Volume 7964*. Springer, 289–296.

[24] Adrian-Tudor PÃčnescu and Vasile Manta. 2018. Smart Contracts for Research Data Rights Management over the Ethereum Blockchain Network. *Science & Technology Libraries* 37, 3 (2018), 235–245.

[25] Alexander Savelyev. 2018. Copyright in the blockchain era: Promises and challenges. *Computer Law & Security Review* 34, 3 (2018), 550 – 561.

[26] Meredith M. Skeels and Jonathan Grudin. 2009. When Social Networks Cross Boundaries: A Case Study of Workplace Use of Facebook and Linkedin. In *Proceedings of the ACM 2009 International Conference on Supporting Group Work (GROUP '09)*. ACM, New York, NY, USA, 95–104.

[27] Annabel Tresise, Jake Goldenfein, and Dan Hunter. 2018. What Blockchain Can and Can't Do for Copyright. *The Australian Intellectual Property Journal* 144, 28 (2018).

[28] Danni Wang, Juntao Gao, Haiyong Yu, and Xuelian Li. 2018. A Novel Digital Rights Management in P2P Networks Based on Bitcoin System. In *Frontiers in Cyber Security*, Fagen Li, Tsuyoshi Takagi, Chunxiang Xu, and Xiaosong Zhang (Eds.). Springer Singapore, Singapore, 227–240.

[29] Hafiz Waseem and Majid Khan. 2019. A new approach to digital content privacy using quantum spin and finite-state machine. *Applied Physics B* 125 (02 2019), 27.

[30] Lei Lei Win, Tony Thomas, and Sabu Emmanuel. 2012. Privacy enabled digital rights management without trusted third party assumption. *Multimedia, IEEE Transactions on* 14, 3 (2012), 546–554.

[31] Eric Hsiaokuang Wu, Shumin Chuang, ChenâĂŘYen Shih, HaoâĂŘChe Hsueh, ShihâĂŘSyuan Huang, and HsiaoâĂŘPing Huang. 2017. A flexible and lightweight userâĂŘdemand DRM system for multimedia contents over multiple portable device platforms. *Software: Practice and Experience* (2 2017).

[32] Zehao Zhang and Li Zhao. 2018. A Design of Digital Rights Management Mechanism Based on Blockchain Technology. In *Blockchain – ICBC 2018*, Shiping Chen, Harry Wang, and Liang-Jie Zhang (Eds.). Springer International Publishing, Cham, 32–46.

[33] G. Zyskind, O. Nathan, and A. '. Pentland. 2015. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In *2015 IEEE Security and Privacy Workshops*. 180–184.