Journal of Information Security and Applications 39 (2018) 19–30

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

An improved E-DRM scheme for mobile environments

Cheng-Chi Lee[a,e], Chun-Ta Li[b,*], Zhi-Wei Chen[a], Yan-Ming Lai[c], Jiann-Cherng Shieh[d]

[a] Department of Library and Information Science, Fu Jen Catholic University, No. 510, Zhongzheng Rd., Xinzhuang Dist., New Taipei City 24205, Taiwan, ROC
[b] Department of Information Management, Tainan University of Technology, Zhong Jheng Road, Tainan 710, Taiwan, ROC
[c] Department of Computer Science and Information Engineering, National Taiwan University, No. 1, Sec. 4, Roosevelt Rd., Taipei City 10617, Taiwan, ROC
[d] Graduate Institute of Library & Information Studies, National Taiwan Normal University, Taipei 10610, Taiwan, ROC
[e] Department of Photonics and Communication Engineering, Asia University, Taichung 413, Taiwan, ROC

ARTICLE INFO

Article history:

Keywords:
Access control
Biometric
Digital rights management
Mobile device user authentication
User anonymity

ABSTRACT

With the rapid development of information science and network technology, Internet has become an important platform for the dissemination of digital content, which can be easily copied and distributed through the Internet. Although convenience is increased, it causes significant damage to authors of digital content. Digital rights management system (DRM system) is an access control system that is designed to protect digital content and ensure illegal users from maliciously spreading digital content. Enterprise Digital Rights Management system (E-DRM system) is a DRM system that prevents unauthorized users from stealing the enterprise's confidential data. User authentication is the most important method to ensure digital rights management. In order to verify the validity of user, the biometrics-based authentication protocol is widely used due to the biological characteristics of each user are unique. By using biometric identification, it can ensure the correctness of user identity. In addition, due to the popularity of mobile device and Internet, user can access digital content and network information at anytime and anywhere. Recently, Mishra et al. proposed an anonymous and secure biometric-based enterprise digital rights management system for mobile environment. Although biometrics-based authentication is used to prevent users from being forged, the anonymity of users and the preservation of digital content are not ensured in their proposed system. Therefore, in this paper, we will propose a more efficient and secure biometric-based enterprise digital rights management system with user anonymity for mobile environments.

1. Introduction

1.1. Background

With the rapid development of network technology, the Internet is a fast and efficient way for providing data transmission and information distribution. Due to the popularity of Internet, the digital content market has received many benefits. Digital content is one of the most important sources of information and entertainment. Digital technology for the digitalization of these traditional media (e.g., photos, cassettes, bibliographies, etc.) into digital content. Then digital content can be shared and transmitted to network users through the Internet [1,13–14,24]. While the digital content market is booming and digital content can be easily distributed, illegitimate download and unauthorized distribution of digital content files will cause some serious problems in many countries and industries. Therefore, provision of the copyright protection of digital content is an important issue in DRM (Digital rights management) system [6,18,25,27,31].

DRM system focuses on integrating the set of policies, technologies and tools for managing the access control on the digital contents [4–6,10,13,14,22,24,25,31]. The main core of DRM system is to ensure digital contents' security. Digital content encryption and digital license are proposed for ensuring content security. The main purpose of DRM system is to provide a secure content delivery infrastructure and the architecture of DRM system is shown in Fig 1. In general, there are four main roles in DRM: (1) content provider (*CP*), (2) content server (*CS*), (3) license server (*LS*), and (4) mobile user (*MU*).

1. Content provider:

Content provider is the owner of digital content or the author of digital content. Content provider encrypts his/her digital content and transmits the encrypted content and the encryption keys to the content server and license server, respectively.

[*] Corresponding author.
E-mail addresses: cclee@mail.fju.edu.tw (C.-C. Lee), th0040@mail.tut.edu.tw (C.-T. Li).

https://doi.org/10.1016/j.jisa.2018.02.001

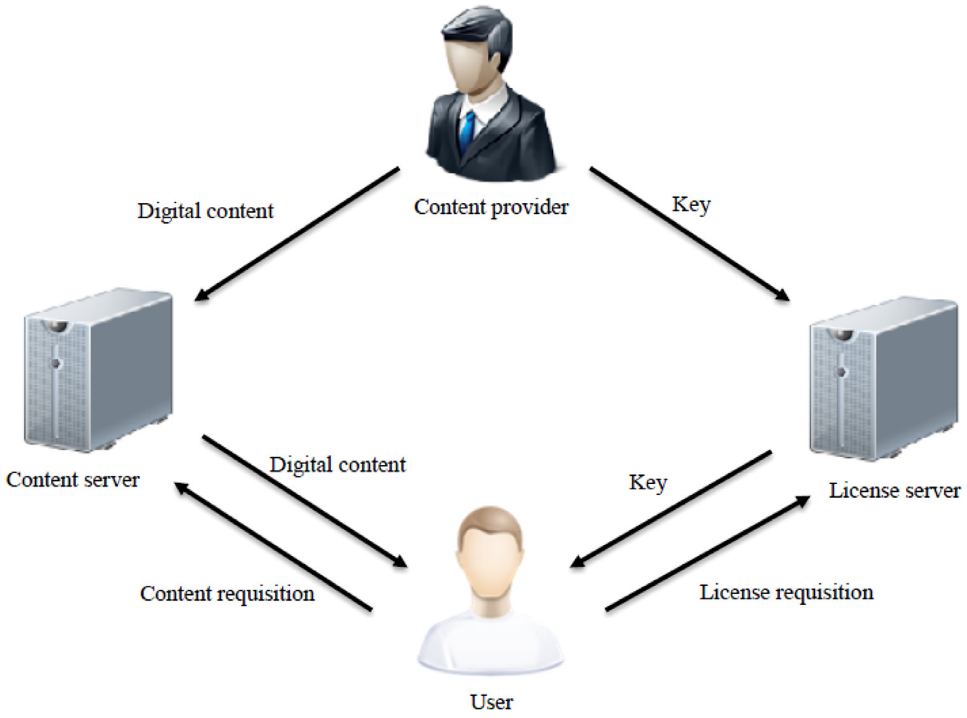

Fig 1. The architecture of DRM system.

2. Content server:

Content server is responsible to store and distribute content provider's digital content. After receiving the encrypted digital content from the content provider, the content server displays the abstract of the digital content on the web for the network user to search if the content is needed.

3. License server:

Upon receiving the encryption keys from the content provider, license server deposits them in its secure database. When the mobile user sends the download request to the license server, the license server authenticates the validity of user and authorizes the corresponding digital content to the user.

4. Mobile user:

We assume the mobile user reviewed the abstract of digital content and wanted to download digital content from content server, he/she sends the content requisition and license requisition to the content server and the license server, respectively. If the three-party authenticate is completed, the content server and the license server individually sends encrypt digital content and encryption key of to the mobile user. Finally, the mobile user can decrypt the encrypted digital content by using the corresponding encryption key.

Enterprise Digital Rights Management (E-DRM) system is the application of DRM system that ensures the secret documents of an enterprise from unauthorized access and many researchers have developed authentication mechanisms for securing the confidential data of an enterprise in E-DRM system [4,5,10,16,18,29,30]. This paper will focus on propose the mobile device and biometrics based authentication scheme for E-DRM system.

1.2. Relate works

In recent years, there are many literatures focus on design a secure and efficient authentication scheme for digital rights management. For smart card based authentication schemes in DRM system, Zhang et al. proposed a three-party based DRM authentication scheme using smart card in 2009 [28]. In 2013, Yang et al. pointed out that Zhang et al.'s scheme fails to withstand insider and stolen smart card attacks. Then Yang et al. further proposed an enhanced version of DRM authentication scheme [26]. In the same year, Mishra et al. found that Yang et al.'s scheme cannot resist the denial of service and password guessing attacks [19]. In 2015, Zhang et al. proposed a provable secure and efficient digital rights management authentication scheme using smart card based on elliptic curve cryptography [27]. Zhang et al. demonstrated some weakness of Yang et al.'s scheme. For biometrics based authentication schemes in DRM system, Chen et al. proposed a secure and traceable E-DRM system for mobile device in 2008 [6]. Chen et al.'s scheme provided lower computational cost. In 2010, Chang et al. presented the cryptanalysis of Chen et al.'s scheme and pointed out that an attacker can easily intercept the key and use the key to obtain the confidential content of the enterprise and the mobile user cannot identify the tampering of message. In order to overcome these problems, Chang at al. further proposed an efficient and reliable E-DRM scheme for mobile environments [4]. In 2013, Chang at al. found that Chang et al.'s scheme still has some security weaknesses. The scheme in [4] cannot withstand stolen device attack and mobile user cannot optionally change his/her mobile device without the server assistant. Then Chang et al. further proposed a practical secure and efficient E-DRM authentication mechanism suitable for mobile environment [5]. In 2015, Mishra et al. demonstrated that the scheme in [6] cannot withstand privileged-insider and off-line password-guessing attacks. To repair these security weaknesses, Mishra et al. proposed an anonymous and secure biometric-based E-DRM system authentication scheme for mobile environment [18]. Unfortunately, in this paper, we found that Mishra et al.'s scheme still has some flaws on digital content and content key and user anonymity cannot be achieved. Concerning the above-mentioned weaknesses, we will propose an effective anonymity and secure biometric-based enterprise digital rights management system. The contributions of our method are as follows: