

A content protection method for a content oriented smart education system

Ga-Ae Ryu*, Ji-Seong Jeong*, Chan Park**, Rae-Hyun Jang**, Kwan-Hee Yoo*

*Chungbuk National University, Korea, **Korea Internet Software, Korea

E-mail : relaxative@nate.com, falrand83@chungbuk.ac.kr, szell@kis21.com, jrj@kis21.com, khyoo@chunbuk.ac.kr

1. Introduction

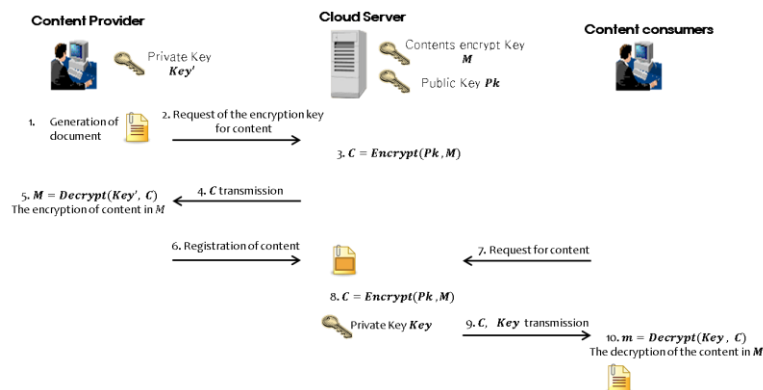
Cloud computing with the potential for delivering economical, securable, reliable, and sharable services has also attracted a great deal of attention in the field of education[1]. Jeong, et. al[2] proposed a content oriented smart education system based on cloud computing environment. The proposed system provided the functions to deliver and share a variety of enhanced forms of educational content, including texts, pictures, images, videos, 3-dimensional (3D) objects, and virtual scenes of virtual reality (VR) and augmented reality (AR). And also learners using any smart device can access the education contents anytime and anywhere. It is important for the proposed system to provide content protection method so that learners can use the education contents safely and reliably.

In this paper, we propose a content protection method to be applied to a content oriented smart education system which was proposed by Jeong, et.al[2]. The proposed method is designed by considering DRM(digital rights management) technologies to control copying, executing, viewing, copying, printing and altering of digital content or devices[3].

2. Proposed scheme

The educational content cloud system, which is proposed by Jeong, et.al [2], delivers and shares a variety of enhanced educational content made by an authoring tool in cloud environment. The content can be stored into several XML files. As mentioned in [2], they propose the protection module which deals with not only data encryption to communicate the content between learners and/or teachers, but also user authentication to access the proposed system and content. In this section, we propose the protection method for controlling the two components. Basically, AES(advanced encryption standard) [4] is used to encrypt all media content managed in the cloud. Since the education media content is similar with EPUB which is an the electronic publication made by IDPF(International Digital Publishing Forum), we adopt the strategy applied to EPUB, that is, EPUB DRM proposed by Gang [5]. He proposed right management methods such as user authentication and content encryption in the use of original EPUB content. Since EPUB content is different from the educational content considered in this paper, the EPUB DRM methods cannot be applied directly to the content.

In this paper, we propose a protection method for transmitting and using the educational content in a smart cloud system. The proposed method are handling education content with respect to three aspect views, those are, content provider, cloud server and content consumers. The content provider creates education content by an authoring tool and requests an encryption key to cloud server and receives it from the server for performing an encryption of the content. The encryption result of the content will be transmitted to the cloud server and will be stored. In order that smart users want to view the education content in cloud server, they receive a private key from cloud server and use the key for performing decryption of the education content. When the procedure is done well as shown in Figure 1, smart users can view the education content they want to.



1. Content provider generates a document by using the authoring tool.
2. Content provider requests the contents encryption key M stored in the cloud server. .
3. Cloud server calculates M by using public key Pk , $C=Encrypt(Pk, M)$.
4. Cloud server transmits a C to the content provider.
5. Contents provider calculates the private key in $Key' M=Decrypt(Key', C)$ and the content is encrypted by using the M .
6. Content provider registers the content to the cloud server.
7. Content consumer requests education content he/she wants to, to the cloud server.
8. Cloud server judges contents consumer whether or not the consumer is correct, and then calculates $C=Encrypt(Pk, M)$ and content consumer's private key Key .
9. Cloud server transmits C and Key to the content consumer.
10. Contents consumer calculates $m=Decrypt(Key, C)$ by using the Key and decrypt the content by using the M .

3. Conclusion and further works

The proposed method in this paper is protected to education content in a cloud system based on EPUB DRM Mechanisms. Because of the EPUB DRM is not still established as well, however, our proposed method is also not formed. EPUB has used content package, in the other hand, the education cloud system has used xml files. The protection method is required so that it can be applied to individual xml files in an education cloud system.

4. Acknowledgement

This research was financially supported by the Ministry of Education(MOE) and National Research Foundation of Korea(NRF) through the Human Resource Training Project for Regional Innovation, and by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program(NIPA-2013-H0301-13-4009) supervised by the NIPA(National IT Industry Promotion Agency).

5. References

- [1] M. A. H. Masud and X. Huang, "An E-learning System Architecture based on Cloud Computing", World Academy of Science, Engineering and Technology, vol. 62, (2012), pp. 74-78.
- [2] Ji-Seong Jeong, Mihye Kim and Kwan-Hee Yoo, "A Content Oriented Smart Education System based on Cloud Computing", International Journal of Multimedia and Ubiquitous Engineering, Vol.8, No.6 (2013), pp.313-328
- [3] DRM(Digital Rights Management), http://en.wikipedia.org/wiki/Digital_rights_management, 2014, May
- [4] Yong Hak Ahn, and Myung-Mook Han, "Design and Implementation of Digital Rights Management System based on Service", Korea Multimedia Society,2006
- [5] AES(Advance Encryption Standard), http://en.wikipedia.org/wiki/Advanced_Encryption_Standard, 2014, May
- [6] Ho-Gap Gang, "Standardization promotion strategy for the compatibility gain of e-book DRM", ICT FORUM KOREA, DRM inside, 3. September. 2013