Available online at www.sciencedirect.com
ScienceDirect
Future Generation Computer Systems 25 (2009) 371–377
FGCS FUTURE GENERATION COMPUTER SYSTEMS
www.elsevier.com/locate/fgcs

A multilayered digital content distribution using a group-key based on web

Yun Ji Na[a], Il Seok Ko[b,*], Xu Shiying[c,1]

[a] School of Internet Software, Honam University, 59-1 Seobong-dong, Gwangsan-gu, Gwangju 506-714, South Korea
[b] School of Computer and Multimedia, Dongguk University, 707 Seokjang-dong, Kyungju, Kyungsangbukdo, South Korea
[c] Beijing ASIM Co. Ltd, 984BOX, No. 206-21, Beijing, China

Received 19 May 2006; accepted 17 July 2006
Available online 9 October 2006

Abstract

Web based distribution of multimedia digital content has been accelerated due to the increase in the use of the Internet. The major issue regarding the design of a multimedia digital content distribution system through the web is to guarantee the security of digital content and to supply a large amount of high quality multimedia digital content to users. This study focused on designing a security technique for each group in a multilayered structure, and on a caching technique, which is based on this security technique, and to improve the user's response speed. Using these techniques guarantees the security of digital content distribution. We implemented the prototype and verified the performance of the proposed system through testing.

Keywords: Security of digital content; Web based system; Digital content; Group key management; Multilayered structure

1. Introduction

Web based services have been activated due to the increase in network speed. Also, there is no exception in the field of digital content, in which distribution of digital content has rapidly increased [1,2]. However, almost all Web services throughout the web have security problems due to the specific media characteristics in the web itself. Due to this security problem, studies on security techniques have been increasingly stressed. Studies on the security techniques based on the web consist of implementing a type of basic security technique itself [3–5], and of techniques for the application of web services [1,2,6–9].

Digital content is a type of information, which can be serviced through the web. Among various web based services throughout the web, multimedia digital content, such as MP3, generally has the characteristics of a large amount of data compared to other digital content. Thus, this increase results in increases in the time loads and amounts on the processes of encryption and decryption. In addition, it leads to transmission delays due to the increase in network based web traffic. An increase in the load of encryption and decryption, and the transmission delay, increases the response delay for the users.

Recent studies on the transmission of digital content have been focused on the guarantee of safety and effective distribution. However, the improvement of transmission delay is also considered with this safety guarantee in the transmission of multimedia digital content. Thus, the major issue in the design of multimedia digital content through the web can be defined as a guarantee of the security of digital content, and fast supplement of a large amount of multimedia digital content to the user.

This study guarantees the security of the transmission of digital content through a security technique for each group of a multilayered structure. In addition, this study improves the user response time of digital content using a caching technique, which is based on this group based layered structure, and verifies an improvement in the performance of the proposed system through a test.

2. The current study

2.1. Security techniques of digital content

An algorithm, which is used to make an encryption and decryption of web security protocol and plaintext, is required to

* Corresponding author.
E-mail addresses: yjna2967@korea.com (Y.J. Na), isko@dongguk.edu (I.S. Ko), xushiying690503@yahoo.com.cn (S. Xu).
[1] Tel.: +86 10 62872637.

0167-739X/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.future.2006.07.017

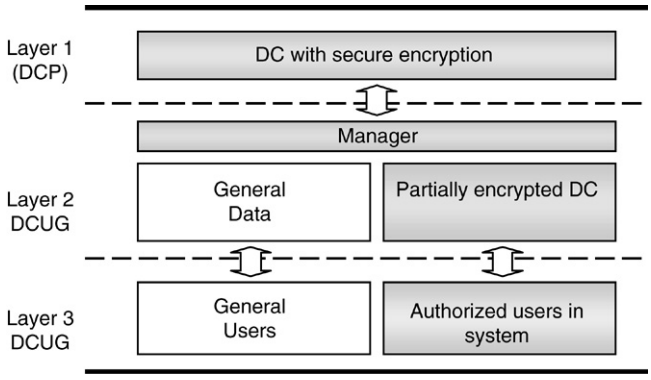

Fig. 1. Layer structure.

guarantee the reliability and safety between clients and server through the web on the Internet [1,5]. Web security protocol can be classified as a method, which transmits by encrypting the whole message, or a part of the whole message in an application layer. In addition, an encryption method, which inserts a certain encrypted layer between the application layer and the transport layer, such as a SSL (Secure Socket Layer) [5], has been used widely at the present time. In order to guarantee the reliability and safety between web clients and the server, a certification process through a certification authority (CA) is required for each client and server. The set of data used in this process is the certification.

An encryption method in a public key uses different keys during the encryption and decryption processes, such as a public key and private key, respectively, in which the public key is open, but the private key is safely secured [3]. In a public key based web security system, a public and private key are used when actual data is transmitted and received by forming an encryption channel after the certification of the client and server. Since the concept of a public key was published, a number of algorithms have been published in recent years. However, the most highly verified algorithms as regards safety are the RSA and Diffe–Hellman algorithms. The RSA public key algorithm has already been used in many real commercial web security systems. Although the RSA takes a long time to calculate the algorithm process compared to that of a symmetric key method, the public key method has been increasingly used in many commercial systems due to the ease of safe distribution of keys used in the encryption process. According to the report of the analyzing data published by the Korean Intellectual Property Office, more than 60% of the applications for a patent, which are related to encryption techniques, are characterized by RSA related techniques [10]. Although these studies are largely focused on the basic technique of security, various studies on web based information security have been conducted from the aspect of the application of security techniques, such as DRM [6].

2.2. Acceleration techniques of digital content

A content acceleration technique used in the web is a type of user response time (web browser response time) and network traffic saving technique. In order to perform this content acceleration, a web caching method is used [11–13]. A web caching

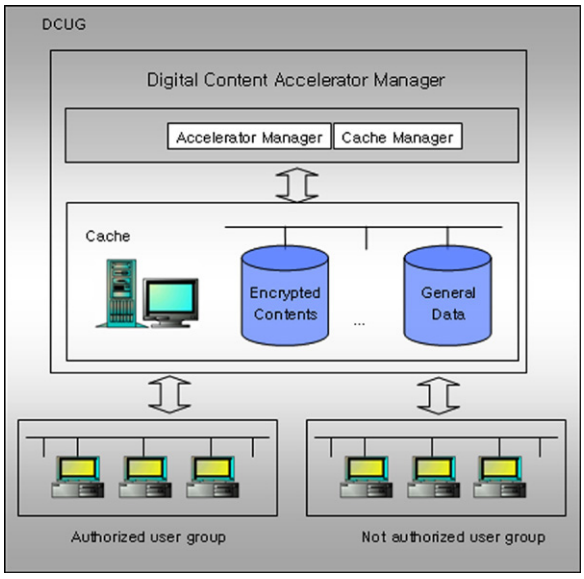

Fig. 2. DCUG structure.

method increases the efficiency of fast response and network use by saving web objects, which are required by the user, who is geographically located at a nearby position on the Internet. Studies on the CDN (Content Delivery Network) have been increasingly stressed to effectively distribute digital content on the web, in which an application of the caching technique can increase the system efficiency in a system design process. It is necessary to design a system, which reflects the characteristics of multimedia digital content, in order to increase the performance of content acceleration using a caching technique in the transmission of multimedia digital content.

3. System design

3.1. System structure

Fig. 1 presents a layer configuration of the system. The DCP (Digital Content Provider) is a supplier of DC (Digital Content). The DCUG (Digital Content User Group) is a user group, which is supplied by DC. Almost all users of multimedia are only interested in a certain passive action. However, a delicate encryption algorithm and certification requires a certain complicated process. This process is the cause of time delay. Thus, it is necessary to consider the transmission of DC from the point of view of safety and execution speed.

Because the user of a DCUG, which is a user group of DC, applied in the proposed system can be certified in the DCUG, the user certification becomes fast and easy. In addition, an effect of the Internet traffic of DC in the proposed system decreases, and the execution speed increases due to the fact that the system will be directly affected by the DCUG cache.

Fig. 2 shows the configuration of a DCUG. A DCUG is managed by grouping it into two different groups. The first group is an authorized user group, which has the authority to use encrypted DC, and the second group is a user group, which has no authority to use encrypted DC. In addition, a DCUG uses a digital content accelerator to increase the user response speed.