공개 키 기반의 계층 구조를 갖는 디지털콘텐트 분배 시스템의 설계

고 일 석[†] · 나 윤 지[††] · 조 동 욱[†††]

요 약

DVD, MP3, AAC 등과 같은 고품질의 디지털콘텐트는 품질의 손상 없이 복제되어 인터넷을 통해 배포 가능하며, 이는 디지털콘텐트 제공자에게 커다란 경제적 손실을 주게 된다. 이에 따라 디지털콘텐트의 안전하고 효율적인 분배를 위한 연구가 필요하다. 디지털콘텐트 분배 시스템의 설계에서 가장 중요한 이슈는 사용자 편의성과 실행 속도, 보안성 문제라 할 수 있다. 본 연구는 웹 캐싱 기술과 계층구조의 암호화/복호화 기법을 사용한 웹 기반의 디지털콘텐트 분배 시스템을 설계하였다. 본 연구에서 제안한 시스템은 보안성과 실행속도, 사용자의 편의성을 향상시킨 디지털콘텐트 분배 시스템이며, 실험을 통해 성능의 우수성을 검증하였다.

A Design of Multi-tier Structure Digital Content Distribution System based on Public Key

Il-Seok Ko[†] · Yun-Ji Na[††] · Dong-Wook Cho[†††]

ABSTRACT

Generally, as for the multimedia high quality contents, an illegality facsimile is possible without a damage of a quality. Also a distribution of contents duplicated illegality in an Internet is giving a great economic loss to digital contents provider. Therefore, a study for security and efficient distribution of digital contents is required. The most important issues in a design of digital contents distribution system are a user convenience, an execution speed and a security. In this study, we designed digital contents distribution system that used a web caching technology and an encryption/decryption technique on hierarchical structure. The proposed system was the digital contents distribution system that improved a security and execution speed, a convenience of a user. Also it verified performance superiority of a proposed system by an examination.

키워드 : Public Key, Encryption, Digital Content Distribution

1. 서 론

정보통신 산업의 발달은 네트워크 속도를 향상시키고 있으며, 디지털콘텐트를 서비스하는 전자상거래가 늘어나고 있다. 인터넷 자체는 보안을 고려하지 않은 전송매체이기 때문에 보안 문제가 발생한다. 또한 기업의 서버시스템은 불법침입 및 데이터 파괴의 위협에 노출되어 있으며, 해킹이나 크래킹의 위협이 더욱 심해지고 있다. 따라서 서버시스템의 보호를 위한 보안 대책이 요구된다. 디지털콘텐트의 안전한 분배를 위해서는 전송되는 디지털콘텐트의 보안 기법이 필요하다. 일반적으로 멀티미디어 고품질 콘텐츠는 품질의 손상 없이 불법복제가 가능하다. 또한 인터넷에서 불법복제된 콘텐츠의 배포는 디지털콘텐트 제공자에게 커다란 경제적 손실을 주고 있다. 따라서 디지털콘텐트의 안전하고 효율적인 분배를 위한 연구가 필요하다. 일반적으로 디지털콘텐트의 안전한 분배를 위해 암호화(encryption) 과정을 통해 전송하며[1, 2], 이로 인해 디지털콘텐트의 부담이 증가한다. 결국, 암/복호화 부담의 증가와 디지털콘텐트 자체의 부담 증가는 전송지연과 실행지연을 통해 사용자의 응답지연이 발생하게 된다. 이러한 관점에서 디지털콘텐트 분배 시스템 설계의 가장 중요한 이슈는 사용자 편의성, 실행속도, 보안성에 관계된 문제라 할 수 있다.

본 연구에서는, 안전성과 실행속도 및 사용자의 편의성을 개선한 공개 키 기반의 안전하고 효율적인 디지털콘텐트 분배 시스템을 설계하였다. 제안 시스템은 네트워크 지연의 감소를 위해 웹 캐싱 기술을 사용하였고, 안전성과 효율성을 개선하기 위해 계층구조 암호화/복호화 기법을 사용하

† 정 회 원 : 충북과학대학 전자상거래과 교수
†† 정 회 원 : 충북대학교 대학원 컴퓨터공학
††† 정 회 원 : 충북과학대학 정보통신과 교수
논문접수 : 2003년 7월 19일, 심사완료 : 2004년 2월 16일

였다. 또한 실험으로 제안 시스템의 성능 우수성을 검증하였다.

2. 관련 연구

클라이언트와 서버사이의 신뢰성과 안전성을 확보하기 위해서는 웹 보안 프로토콜과 평문(plaintexte) 데이터를 암호화 및 복호화하는 알고리즘이 필요하다[1, 2]. 웹 보안 프로토콜에는 응용 계층에서 메시지 전체를 암호화하여 전송하는 방식과, 메시지에서 몸체 일부분만을 암호화하여 전송하는 방식이 있다. 또한 SSL(Secure Socket Layer)과 같이 응용계층과 트랜스포트계층 사이에 암호화 계층을 별도로 삽입하여 암호화하는 방법이 현재 많이 사용되고 있다[3]. 웹클라이언트와 서버 사이의 신뢰성과 안전성을 확보하기 위해서는 클라이언트와 서버 각각을 인증서버(CA : Certificate Server)를 통하여 인증 받는 절차가 필요하다. 이때 사용되는 데이터의 집합이 인증서이다. 인증서의 형식으로 가장 널리 사용되는 표준은 ITU-T의 X.509이다[4].

공개키 암호방식은 암호화 할 때 사용하는 키(공개키(public key))와 복호화할 때 사용하는 키(비밀키(private key))가 달라서 공개키는 공개하고 비밀키만 안전하게 유지하는 방식이다[1, 5]. 공개키 기반의 웹 보안 시스템에서는 클라이언트와 웹서버의 인증이 종료된 후에 암호화 채널을 형성하여 실질적으로 데이터를 주고받을 때는 공개키와 비밀키를 이용한다. 실제로 많은 웹 상용 보안시스템의 경우 RSA 공개키 알고리즘을 이용하고 있다. RSA 방식은 계산에 소요되는 시간이 대칭키 방식에 비해 오래 걸리지만 공개키 방식은 대칭키 방식에 비해 암호화 과정에서 사용하는 키의 안전한 분배가 용이하여 상용 시스템에서 많이 사용되고 있다[5]. 본 논문에서 제안하는 콘텐츠 분배시스템은 안전성과 키 분배의 효율성을 위해 RSA 공개키 방식을 사용한다.

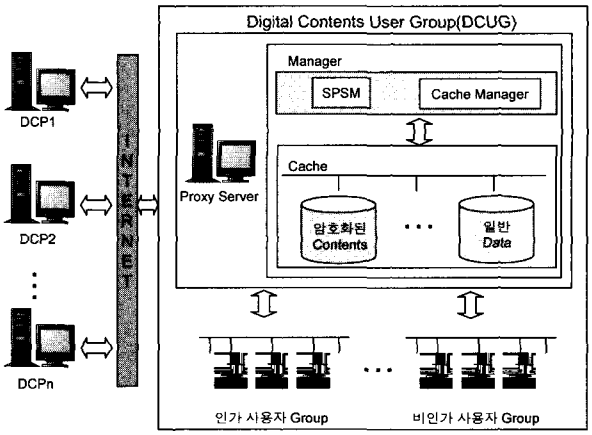
일반적으로 HTTP 요구의 효율적인 처리를 위해 웹 캐싱을 사용한다[6, 7]. 웹 캐싱은 인터넷에서 사용자와 지리적으로 가까운 곳에서 사용자가 요청한 웹 객체를 저장하여 빠른 응답과 네트워크 사용의 효율성을 증가시킨다[9]. 웹에서 디지털콘텐트의 효율적인 분배를 위해 CDN(Content Delivery Network)과 같은 연구가 점차 각광을 받고 있으며, 이러한 CDN의 설계에서 캐싱 기술의 활용은 시스템의 성능을 좌우하는 중요한 요인이라 할 수 있다.

3. 시스템 설계

제안 시스템은 DCP(Digital Contents Provider)에서 DC(Digital Contents)를 제공받는 DCUG(Digital Contents User Group)에 속한 인가된 사용자에게 안전하고 효율적으로 DC를 분배하는 것을 목적으로 하고 있다. (그림 1)은 시스템의 구성을 나타낸다. SPSM(Secure Proxy Server Manager)은 DCUG의 프록시 서버를 관리하는 관리자이다.

3.1 암호화

디지털콘텐트에 대한 권한을 합법적으로 관리하기 위해서는 접근권한을 가진 사용자만이 접근이 가능하도록 하여야한다. 최근 업계에서 사용되는 상용시스템들은 사용자가 암호화된 디지털파일과 재생 프로그램과 토큰을 전송 받아서 재생할 수 있도록 하고 있다. 디지털콘텐트의 보호를 위한 암호화 방법은 DES 알고리즘과 같은 대칭키 방법과 RSA공개키 알고리즘과 같은 비대칭키 방법이 있다. 이들 기존에 개발된 알고리즘들은 디지털콘텐트의 보호를 위한 각종 요건을 갖추고 있으며, 각종 시스템에 다양하게 응용되고 있다.

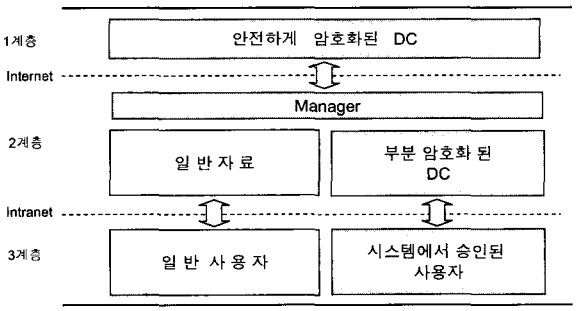


(그림 1) 시스템의 구성

하지만 MP3 파일과 같은 크기가 큰 동영상 파일에 대해 파일전체를 암호화할 경우 서버와 네트워크의 전송에 많은 부하가 발생하게 된다[9, 10]. 또한 사용자의 실행 과정에서도 복호화에 소요되는 시간이 길어져서 실행 지연의 요인이 된다. 따라서 파일의 키와 핵심 부분만을 암호화하는 부분적인 암호화 방법을 사용 할 수 있으며, 이 경우 다음과 같은 점을 고려해야 한다. 소프트웨어의 경우 불법적인 사용자가 핵심부분의 해독을 못할 경우 나머지 부분에 대한 실행자체가 불가능하기 때문에 부분적인 암호화를 통한 전송 자체만으로도 효율성과 안전성을 가질 수 있다. 하지만 MP3 같은 디지털콘텐트는 소프트웨어와는 다르다. MP3에서는 암호화된 부분을 제거한 나머지 부분만으로도 리얼플레이어 같은 일반 플레이어에 의해 실행이 가능하다. 따라서 현재 사용되고 있는 디지털콘텐트 분배 시스템으로는 부분 암호화 방식이 안전성을 확보할 수 없다. MP3 같은 디지털콘텐트의 안전한 분배를 위해서는 새로운 시스템의 설계가 필요하다.

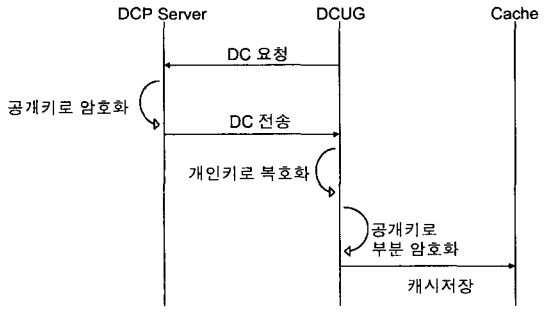
제안 시스템의 실험에서는 안전성과 키 분배의 효율성을 위해 RSA 공개키 기법을 사용한다. 1계층에서 공개키에 의해 암호화된 DC는 2계층의 DCUG에서 개인키에 의해 복호화되고, 2계층의 DCUG는 3계층의 사용자 실행의 속도를 고려하여, 복호화된 DC 평문을 다시 공개키로 부분적으로 암호화하여 캐시에 저장한다. 2계층과 3계층 사이의 전송은 인트라넷을 통해 시스템적인 보안성을 가진 전송이다. 2계층은 승인된 사용자에게만 부분 암호화된 콘텐츠를 제공한다.

제안 시스템은 (그림 2) 같은 계층 구조의 암호화 및 복호화 방법을 사용한다. 2계층은 DCUG에 해당하며, 계층1과 계층2의 콘텐츠 전송은 보안성이 없는 인터넷을 통해 이루어진다. 따라서 DCP와 DCUG 사이의 콘텐츠 전송에는 보안성이 검증된 안전한 암호화 기법이 필수적이다.



(그림 2) 암/복호화 계층 구조

3.2 DC 전송

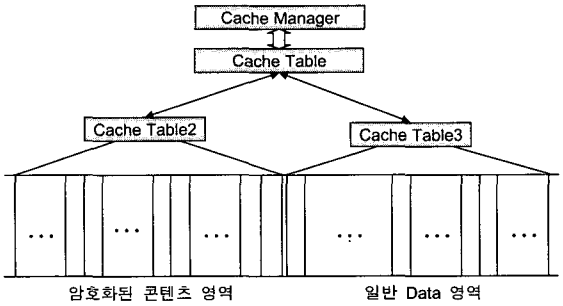


(그림 3) DC 전송

(그림 3)은 DCP에서 DCUG로 DC를 전송하는 절차이다. DCP 서버는 공개키가 포함된 DC를 암호화한다. DCUG는 개인 키를 이용하여 DCP에서 전송된 DC를 복호화하여 원래의 공개키와 평문을 만든다. 다음으로, 공개키를 이용하여 복호화된 콘텐츠의 10%를 부분 암호화하여 DCUG의 캐시에 저장한다. 이때 사용되는 공개키는 DCP에서 전송 받은 공개키이며, 이로 인해 DCUG의 부담이 증가하게 된다. 이렇게 부분 암호화된 콘텐츠를 사용자는 사용자 브라우저에서 개인키로 복호화하여 실행한다.

제안 시스템은 콘텐츠의 안전한 실행을 위하여 시스템 측면의 안전성과 프로세스 측면의 안전성을 갖추고 있다. 먼저 시스템 측면의 보안성은 프록시 서버의 보안성을 통해 확보할 수 있다. 또한 사용자의 콘텐츠 요청시 시스템 자체에서 승인된 사용자 여부 인증과 콘텐츠의 실행시 복호화를 위한 개인 키 값의 인증을 통해 프로세스 측면의 보안성을 가진다.

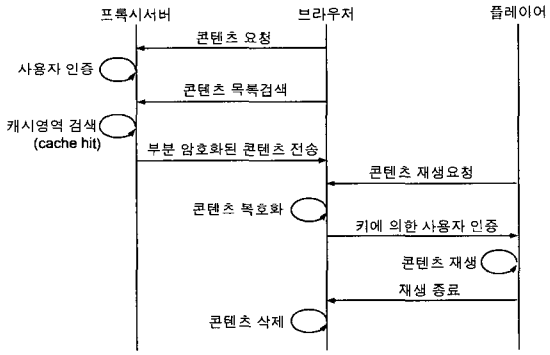
(그림 4)는 캐시의 관리 구조를 나타낸 것이다. 제안시스템에서 캐시가 저장하고 관리해야할 자료에는 암호화된 콘텐츠와 일반 자료가 있다. 기존 웹 시스템에서 사용되는 캐시와 차이점은 2단계의 관리 구조를 가지고 있다는 것이다. 캐시테이블2는 부분적인 암호화된 콘텐츠의 저장과 관리를 위한 것이고, 캐시테이블3은 일반적인 캐시 영역의 관리를 위한 것이다.



(그림 4) 캐시 관리 구조

3.3 DCUG에서 DC 전송

DCUG의 승인된 사용자가 콘텐츠를 요구하면, DCUG manager는 암호화된 콘텐츠 캐시 영역의 부분 암호화된 DC를 사용자에게 전송한다. 사용자는 전송된 DC를 개인 브라우저에서 복호화하고 개인 브라우저에 내장된 플레이어에서 실행한다. (그림 5)는 DCUG에서 DC로 콘텐츠를 전송하는 절차이다.



(그림 5) DCUG 내에서의 DC 전송과 실행

사용자의 콘텐츠 전송 요청에 대해, 시스템 자체에서 사용자 인증을 수행한다. 캐시 목록에서 콘텐츠를 검색하여 cache hit일때 해당 콘텐츠를 전송한다. 전송 완료 후 개인

브라우저에서 콘텐츠 복호화를 수행한다. 또한 키 값에 의한 사용자 인증 절차를 수행한 후 콘텐츠를 재생한다. 재생이 완료된 후 사용자 영역에서 콘텐츠를 삭제한다.

3.4 인증 절차

DCUG의 허가된 사용자가 캐시 목록에서 원하는 콘텐츠를 찾을 수 없을 경우 DCUG는 해당 DCP 서버에서 콘텐츠를 전송받아야 한다. 이 경우 DCUG와 DCP 서버는 상호간의 암호화 데이터를 주고받기 전에 CA(Certificate Authority) 서버에 접속하여 인증서를 발급 받아야한다. 인증서의 발급 절차는 다음과 같다.

CA 서버에 접속하여 인증서 발급을 요청한다. CA 서버는 인증 요청서를 DCUG과 DCP 서버에 전송한다. DCP 서버와 DCUG는 자신의 키쌍을 생성하고, 인증 요청서를 작성한다. DCUG와 DCP 서버는 자신의 공개키와 인증 요청서를 CA 서버로 전송하며, CA 서버는 수신된 인증 요청서를 확인하여 공개키를 포함한 인증서 발급한다. CA 서버는 DCUG와 DCP 서버의 인증 요청서 정보와 인증서를 DB에 저장하고, CA 서버는 DCUG와 DCP 서버의 인증서를 DCUG와 DCP 서버에 전송한다. DCUG와 DCP 서버는 CA 서버로부터 수신된 인증서를 자신의 비밀 키와 함께 저장한다.

3.5 사용자 브라우저

제안시스템에서는 DCUG의 개인 브라우저를 통해 부분적인 암호화된 콘텐츠가 실행된다. 따라서 개인 브라우저의 기능은 제안시스템의 성능에 많은 영향을 미친다. 개인 브라우저의 요구 사항은 시스템 서버의 콘텐츠를 열람할 수 있는 기능, 사용자 개인 정보 송신과 디지털콘텐트의 수신 기능, 복호화 기능, 콘텐츠 재생 기능, 콘텐츠 재생 시 서버와의 동적인 연결을 통해 사용자 인증 기능, 동일 그룹 상의 동일 사용자의 동시 사용 여부 체크 기능이다.

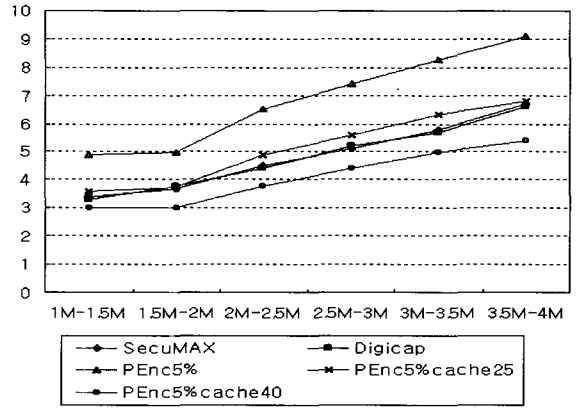
콘텐츠의 실행을 위한 개인 브라우저는 프록시 서버 측과 클라이언트 서버의 관계를 갖는다. 이 때, 서버 측은 관리자, 암호화/복호화 처리, 송신/수신 기능으로 이루어진다. 사용자 측의 브라우저는 사용자 인터페이스, 복호화 처리, 전송 기능으로 구성된다. 사용자 인터페이스는 파일 컨트롤 창, 콘텐츠 파일 재생, 고객 특화 서비스 수신창 등으로 구성된다. 복호화 처리부는 부분 암호화되어 전송된 파일을 복호화하고 재생한다. 재생창은 Windows Media Player를 사용하여 복호화된 콘텐츠를 실행한다.

4. 실험 및 분석

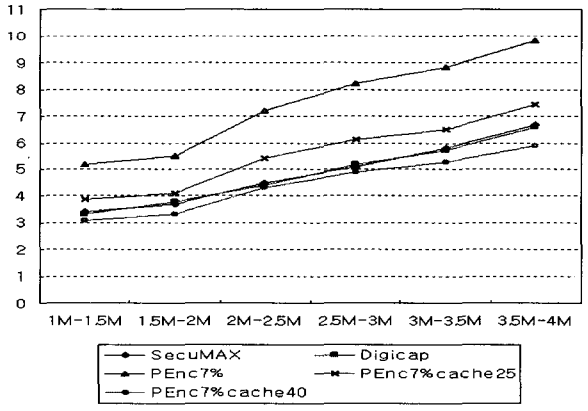
4.1 실 험

실험에서는 크기가 1M~5M 사이의 mpeg 파일을 대상으로 암호화에 걸리는 시간을 측정하였으며 제안시스템의 효용성 검증을 위해 상용 AOD 시스템인 SecuMAX, Digicap과 비교하였다. SecuMAX의 인증방식은 개인용 암호키를 사용하며 Digicap은 토큰을 사용하여 인증한다.

(그림 6)은 5% 암호화에서 캐시적중률 25%일 경우와 40%일 경우의 처리속도를 실험한 것이다. 또한 (그림 7)은 7% 암호화에 대해 캐시적중률이 25%일 경우와 40%일 경우의 처리속도를 실험한 것이다. 그림에서 PEnc5%는 DC의 5%를 암호화한 것이며, PEnc7%는 DC의 7%를 암호화한 것이다. 또한 PEnc5%cache25는 캐시적중률 25%일 때 5% 암호화한 DC의 실행시간 실험이며, PEnc5%cache40는 캐시적중률 40%일 때 5% 암호화한 DC의 실행시간 실험이다.



(그림 6) 실행시간실험 : 5% 암호화 비교



(그림 7) 실행시간실험 : 7% 암호화 비교

PEnc7%cache25는 캐시적중률 25%일때 7% 암호화한 DC의 실행시간 실험이며, PEnc7%cache40는 캐시적중률 40%일 때 7% 암호화한 DC의 실행시간 실험이다. 대부분의 상용시스템은 보안과 사용자 편의를 위해 사용자를 위한 개인 인터페이스를 지원한다. 제안시스템은 처리속도의 개선을 위해 DC의 보안 수준을 다소 감소시키고 있다. 이것은 암호화 기법과 개인인터페이스 만으로는 DC의 처리속도와

보안 수준을 함께 향상시키기 어렵기 때문이다.

웹 캐싱을 반영하지 않을 경우 두 개의 상용시스템이 제안시스템보다 성능이 우수하다. 하지만 DC의 보안 능력 면에서는 제안시스템이 우수하며, 웹 캐싱을 고려하면 제안시스템의 처리속도가 우수함을 알 수 있다. 실험 결과의 수치는 실험환경에 따라 큰 변화가 있기 때문에, 결과수치를 절대적인 판단의 기준이라고 얘기할 수는 없다. 하지만 실험을 통해 제안시스템의 성능이 기존의 상용시스템보다 개선되었음을 알 수 있다.

실험결과에서 캐시적중률 25%일 때 처리속도는 상용시스템의 처리속도와 비슷했으며, 캐시적중률 40%일때 10%~18% 처리속도가 개선되었다. 대부분 상용 웹 캐시의 캐시적중률은 40% 이상이다. 따라서 실험결과는 제안시스템의 성능이 기존의 상용 시스템보다 개선되었음을 의미한다. 또한 이 실험결과를 통해, 제안시스템이 처리속도를 감소시키지 않으면서 DC의 보안성을 가졌다는 것을 알 수 있다.

4.1 분 석

디지털콘텐트 분배 시스템의 설계에서 가장 중요한 이슈는 사용자 편의성과 실행 속도, 보안성 문제라 할 수 있다. 따라서 이 절에서는 이 세 가지 항목에 대해 제안시스템을 분석한다. .

4.1.1 사용자 편의성

점차 HCI(Human Computer Interface) 관점에서 웹 인터페이스의 편리성이 강조되고 있다. 대부분의 멀티미디어 사용자의 사용행위는 단지 그것을 사용하는 수동적 행위에 관심이 있을 뿐이다. 하지만 정교한 암호화 알고리즘과 인증은 복잡한 절차가 필요하다. 이것은 복호화 시간 지연의 원인이 되고 결과적으로, 실행속도가 늦어지고 사용자의 편리성이 감소된다. 결국 사용자의 편의성을 개선하기 위해 인증절차와 실행속도의 고려가 필요하다. 하지만 암호화의 성능과 사용자의 편리성 사이에는 trade-off가 존재한다. 따라서 암호화 성능을 저하시키지 않으면서 사용자의 편의를 개선할 수 있는 방법이 필요하다.

제안 시스템에서는 DC 사용그룹인 DCUG의 사용자는 DCUG 내에서 인증되므로, 사용자 인증이 빨라지고 편리해진다. 또한, 제안 시스템에서는 DC의 인터넷의 트래픽으로 인한 영향이 감소되고, DCUG 캐시의 DC의 영향을 받게 된다. 따라서 사용자 인터페이스의 복호화 시간과 실행속도가 빨라진다.

4.1.2 속 도

디지털콘텐트 분배 시스템의 속도 영향 요인은 네트워크 트래픽에 따른 지연과 사용자 인터페이스에서 복호화에 따른 지연이다. 원문 DC는 암호화로 인해 파일 크기가 커진다. 또한 MP3 같은 크기가 큰 멀티미디어콘텐츠의 암호화 전송은 네트워크 트래픽을 급격히 증가시킨다. 제안시스템은 이러한 지연 요인의 영향을 감소시켜 속도를 개선하였다. DC 서버에서 공개키로 안전하게 암호화된 콘텐츠는 DCUG에 전송된다. 전송된 DC는 개인키로 복호화하고 다시 부분 암호화되어 캐시에 저장된다. 결국, DCUG의 승인된 사용자는 캐시에 저장된 DC를 제공받는다. 따라서 사용자는 인터넷의 트래픽으로 인한 영향이 감소되고, DCUG 캐시의 DC의 영향을 받게 된다. 또한 사용자 인터페이스는 부분 암호화된 콘텐츠를 복호화하기 때문에 실행에 소요되는 지연시간이 짧아진다.

4.1.3 보안성

디지털콘텐트 분배 시스템은 전송보안성과 실행보안성을 갖추어야한다. 제안시스템에서 DC는 보안성이 검증된 RSA 공개키 방식으로 안전하게 암호화된 콘텐츠를 DCUG에 전송한다. 따라서 개인키를 가진 DCUG만이 전송된 DC를 복호화할 수 있으므로 전송보안성을 갖고 있다.

제안시스템은 콘텐츠의 안전한 실행을 위한 보안성을 갖추고 있다. DCUG는 프록시 서버와 함께 구축이 되기 때문에, 시스템 자체적으로 보안성을 확보할 수 있다. 사용자 인증을 통해서 DCUG의 승인된 사용자만이 캐시 목록 접근이 허용된다. 사용자 인터페이스가 DC의 실행을 위해서는 DC의 복호화가 필요하며, 이 때 키를 가진 단일 사용자만이 복호화 가능하기 때문에 추가적인 보안성을 확보하고 있다.

5. 결 론

상용 디지털콘텐트 분배 시스템은 처리속도와 보안 수준의 향상이 필수적이다. 하지만 지금까지 개발된 방법은 처리속도를 향상시키기 위해 보안 수준을 감소시켜야했다. 또한 DC의 보안 수준을 향상시키기 위해 처리속도를 감소시켜야만했다. 따라서 DC의 보안 수준을 높이면서 처리속도를 개선하기 위한 방법이 필요하다.

본 연구에서는, 안전성과 실행속도 및 사용자의 편의성을 개선한 공개 키 기반의 디지털콘텐트 분배 시스템을 설계하였다. 제안 시스템은 웹 캐싱을 사용하여 DC의 실행에서 지연요인을 감소시켰다. 또한 DC의 보안 수준을 개선하기 위해 계층구조 암호화/복호화 기법을 사용하였다. 실험에서는 기존의 상용시스템과 제안시스템의 처리속도와 보안수준을 비교 평가하였다. 실험결과, 제안 시스템의 보안 수준과 처리속도가 개선되었음을 확인하였다. 제안 시스템은 온라인 교육과 웹 영화, 웹 음악 콘텐츠 제공 같은 대용량 멀티미디어 디지털콘텐트를 분배하는 ISP(Internet Service Provider)에 활용 가능할 것이다.

참 고 문 헌

[1] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transaction on information theory, Vol. 1T-22, No.6, Nov., 1976.

[2] Spctral Lines, "Talking About Digital Copyright," IEEE Spectrum, Vol.38, Issue 6, p.9, June, 2001.

[3] A. O. Freier, P. Karlton and P. C. Kocher, "The SSL Protocol Version 3.0," *www.netscape.com/eng/ssl3*, Nov., 1996.

[4] ITU-T Rec. X.509, Information technology-Open Systems Interconnection-The Dictionary : Public-key and attribute certificate framework, March, 2000.

[5] R. Rivest, A. Shamir and L. Adelman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM, Vol.21, No.2, pp. 120-126, 1978.

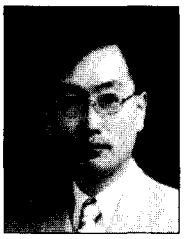
[6] G. Barish, K. Obraczka, World Wide Web Caching : Trends and Techniques, IEEE Communications, Internet Technology Series, May, 2000.

[7] H. Bahn, S. Noh, S. L. Min, and K. Koh, "Efficient Replacement of Nonuniform Objects in Web Caches," IEEE Computer, Vol.35, No.6, pp.65-73, June, 2002.

[8] L. Rizzo, L. Vicisano, "Replacement Polices for a Proxy Cache," IEEE/ACM Trans. Networking, Vol.8, No.2, pp. 158-170, 2000.

[9] Thorwkrth N. J., Horvatic P., Weis R., Jian zhap, "Security methods for MP3 music delivery," Signals, Systems and Computers, 2000. Conference Record of the Thirty-Fourth Asilomar Conference on, Vol.2, pp.1831-1835. 2000.

[10] C. Serrao, J. Marques, T. Baker, M. Balestri, P. Kudumakis, "Protecting Digital Music Delivery and Consumption Using the OCCAMM Project Framework," Second International Conference on WEB Delivering of Music(WEDELMUSIC '02), Darmstadt, Germany, December, 2002.



고 일 석

e-mail : isko@ctech.ac.kr
연세대 컴퓨터산업시스템공학(박사수료)
미)USIU 경영학과(MBA)
경북대 컴퓨터공학(공학석사)
경북대 컴퓨터공학(공학사)
현재 충북과학대학 전자상거래과 교수
관심분야 : 전자상거래시스템, 웹시스템개발

나 윤 지

e-mail : yjna2967@korea.com
충북대 컴퓨터공학(박사수료)
미)NYIT Communication ART 전공
충북대 컴퓨터공학(공학석사)
경북대 생명공학(이학사)
관심분야 : 멀티미디어, 웹기반 응용

조 동 욱

e-mail : ducho@ctech.ac.kr
한양대 전자공학과(공학석사)
한양대 전자통신공학과(공학박사)
서원대학교 정보통신과 교수
현재 충북과학대학 정보통신과 교수
관심분야 : 모바일콘텐트, 정보보안, 네트워크