DRM 시스템 개선을 통한 콘텐츠 스트리밍 서비스 개선

이정기* · 정양권** · 김동현***

Enhance the Performance of Contents Streaming Services using improve the DRM System

Jeong-gI LEE* · Yang-kwon Jeong* · Dong-hyun Kim*

요 약

본 논문에는 P2P 환경의 DRM 시스템을 개선하여 분산컴퓨팅의 성능을 최대화하고 사용자 증가와 콘텐츠 공유의 증가에 비례해 발생되는 부하를 최소화함으로써 디지털 콘텐츠의 스트리밍 서비스를 개선하고자 하였다. 이를 위해 인증 프로토콜과 라이센스 프로토콜을 개선하여 콘텐츠를 사용하고자 할 경우 라이선스만을 다운로드 받은 다음 복호화와 실행을 동시에 수행하도록 함으로써 기존 DRM 시스템보다 한층 강화된 스트리밍 지원을 하도록 하였다. 성능 평가를 위해 암호화되어 있는 영상 데이터 파일의 복호화를 먼저 수행한 후 재생하는 기존의 방식과 실시간으로 복호화를 하면서 재생하는 개선된 방식을 비교하여 수행 시간을 측정하였다. 수행 결과 개선된 DRM 시스템이 보다 안정된 대역폭을 유지하고 있으며 지연 시간은 감소하는 것을 확인할 수 있었다.

ABSTRACT

This paper propose a method to enhance the performance of digital contents streaming services with the improve DRM system by maximizing the distribute computing performance and minimizing the overheads of security threatens caused by increasing users and sharing contents in P2P environments. By improving authentication protocols and license protocols to perform decryption and execution simultaneously by only download of the license, streaming services are more enhanced rather than existing DRM systems. For evaluate the performance, this paper compared execution time of existing DRM systems which decrypt the encrypted data file before execute with improved DRM system which execute and decrypt the encrypted data file simultaneously. In experiment, improved DRM system can maintain steady bandwidth and reduce the execution time in compare to existing DRM systems.

키워드

DRM, P2P, Streaming Service, Digital Content

* 전자부품연구원
** 동신대학교
*** 순천청암대학
접수일자 : 2008. 10. 27
심사완료일자 : 2008. 12. 11

Ⅰ. 서 론

현재 네트워크를 구성하는 시스템에서 콘텐츠를 자유롭게 교환할 수 있는 P2P 기술이 널리 활용되고 있으며 그에 대한 연구가 활발히 진행되고 있다. P2P 네트워크에서 가장 이슈가 되는 부분은 콘텐츠의 기밀성과 무결성의 확보와 효과적인 스트리밍 서비스 지원이라 할 수 있다. 콘텐츠의 기밀성과 무결성의 확보는 암호화 기술을 중심으로 발전하여 왔으며 저작권에 대한 내용을 명시하기 위해 XrML(eXtensible rights Markup Language)을 기반으로 표준화가 진행되어 왔다.

현재 DRM 서버를 사용하는 네트워크에서 콘텐츠의 다운로드는 DRM 서버와 사용자 간에 지속적인 연결을 통해 실시간 스트리밍 방식으로 이루어지기 때문에 콘텐츠의 크기와 사용자 증가에 따른 DRM 서버의 트래픽 증가는 콘텐츠 다운로드의 중단 현상을 자주 발생시킨다[1].

본 논문에는 P2P 환경의 DRM 시스템을 개선하여 분산컴퓨팅의 성능을 최대화하고 사용자 증가와 콘텐츠 공유의 증가에 비례해 발생되는 부하를 최소화함으로써 디지털 콘텐츠의 스트리밍 서비스를 개선하고자 하였다. 이를 위해 인증 프로토콜과 라이센스 프로토콜을 개선하여 콘텐츠를 사용하고자 할 경우 라이선스만을 다운로드 받은 다음 복호화와 실행을 동시에 수행하도록 함으로써 기존 DRM 시스템보다 한층 강화된 스트리밍 지원을 하도록 하였다.

성능 평가를 위해 암호화되어 있는 영상 데이터 파일의 복호화를 먼저 수행한 후 재생하는 기존의 방식과 실시간으로 복호화를 하면서 재생하는 개선된 방식을 비교하여 수행 시간을 측정하였다. 수행 결과 개선된 DRM 시스템이 보다 안정된 대역폭을 유지하고 있으며 지연 시간은 감소하는 것을 확인할 수 있었다. 2장에서는 현재의 DRM 기술을 분석하였으며, 3장에서는 인증 프로토콜과 라이센스 프로토콜의 설계를 통한 개선된 시스템을 제안하였다, 4장에서는 개선된 시스템의 평가를 통해 콘텐츠 스트리밍 서비스가 개선된 것을 입증하였다.

Ⅱ. 현재의 DRM 기술 분석

현재의 DRM은 콘텐츠의 불법 복제를 막거나 콘텐츠 내에 각종 저작권 정보, 사용자 ID 등을 삽입해 불법 사용을 추적할 수 있도록 하는 등 불법적인 유통을 원천적으로 막는데 많은 초점을 맞추고 있다. P2P 네트워크를 통해 전달된 디지털 콘텐츠에는 사용 규칙이 첨부되어 있으며, 해당 콘텐츠를 수신한 사용자는 사용 규칙에 따라 콘텐츠를 사용한다. 또한 clearinghouse를 통해 DRM에 의해 보호받고 있는 콘텐츠를 수신한 사용자는 DRM 기술을 사용하는 하드웨어나 소프트웨어만을 통해 사용할 수 있다[1][2].

DRM 기술은 지속적으로 발전하고 있으며 공개된 기술 내용에도 많은 제약이 있어 완전한 비교 분석에는 한계가 있다. 따라서 공개된 기술 내용을 근거로 하여 InterTrust DRM과 Microsoft DRM 솔루션을 생성규칙, 암호화와 키의 분배, 인증 및 사용 내역 관리, 유통 및 추적기능 등에 대하여 비교 분석하고자 한다.

콘텐츠 사용 규칙의 정의는 사용 규칙을 얼마나 다양하게 제어할 수 있는가 하는 것이 중요한 문제이다. 현재 개발된 기술들의 대부분은 사용 횟수, 사용 기간, 사용자 정보 등에 따라 콘텐츠를 실행할 수 있도록 허용하는 콘텐츠 사용 규칙을 정의한다[3][4].

InterTrust DRM과 Microsoft DRM은 모두 사용 규칙을 정의하기 위한 언어로 표준 명세 언어인 XrML을 사용하고 있으나 저작 권리에 대한 내용을 공개하지 않고 자체 데이터 구조로 저작권 정보를 구축하고 있다[5][6].

콘텐츠 패키징의 경우 InterTrust DRM은 서버에 키가 저장되어 라이선스의 인증과 함께 키를 다운로드 받아 처리하며 Microsoft DRM의 경우 Clearinghouse를 통해 라이선스 키를 다운로드 받아 처리한다.

인증 처리에 있어서 InterTrust DRM은 배포자로부터 InterRights Point를 다운로드하여 처리하며 Microsoft DRM은 Clearinghouse를 통해 라이선스 키를 획득하며 사용자 시스템에 인증 내용을 저장하고 있다. 사용 내역 저장 방식의 경우 InterTrust DRM은 사용자 시스템에 저장하는 반면 Microsoft DRM은 서버의 Clearinghouse에 저장한다. 사용자 시스템에 저장할 경우 기록이 변경되거나 삭제되지 않도록 적절한 안전성의 보장이 필요하며, 저장된 사용 내역의 수집이 자동화 되어야 한다. 서버에 저장할 경우 안전성

은 보장되지만 사용 내역을 처리할 때 마다 네트워크에 연결되어야 하는 문제가 있다.

표 1. DRM 체계의 기술적인 분석 비교
Table. 1 The technical analysis comparison of DRM system

기술항목	InterTrust DRM	Microsoft DRM
사용규칙	XrML(비공개)	XrML 미사용
콘텐츠 패키징	DigiBox Container 를 통한 처리	처리 암호화된 콘텐츠 라이선스 키
주요기술	암호화, 워터마킹	암호화
암호화	공개키 / 비밀키	비밀키
키 저장	서버에 저장	클리어링하우스에 저장
인증 처리	InterRights Point통한 처리	클리어링하우스를통한 라이선스 키 획득
사용내역	사용자 컴퓨터	클리어링하우스
결재 방식	신용카드, 전자화폐	클리어링하우스에 미리 등록
유통방식	온라인 및 오프라인	오프라인
추적 기능	제한적	불가능

결재 방식에 있어서 InterTrust DRM의 경우 사용자의 시스템에서 콘텐츠를 사용하는 순간에 결재 처리가 발생하므로 신용카드를 이용한 즉시 결재나 전자 화폐를 이용한 다양한 결재 방식을 구현하기 쉬우며, Microsoft DRM의 경우 Clearinghouse를 통해 결재가 처리된 콘텐츠를 사용할 수 있도록 한다. 콘텐츠의 유통은 사용자가 콘텐츠를 다운로드 받는 방식으로 InterTrust DRM의 경우 콘텐츠를 사전에 암호화하여 재분배하므로 온라인과 오프라인을 통하여 유통이 가능한 반면, Microsoft DRM은 다운로드 시 암호화를 수행하므로 많은 시간이 소요되어 오프라인을 통해서만 다운로드 할 수 있다. 추적 기능에 있어서 기존 DRM 솔루션의 경우 특정 콘텐츠에 대한 법적 분쟁이 발생했을 때 불법 사례 입증에 필요한 기초자료 제공을 위한 추적 기능을 충분히 제공하지 못하고 있다.

복호화의 장소는 소비자가 콘텐츠를 이용할 때 두 DRM 솔루션 모두 각 업체별로 제공하고 있는 별도의 플레이어를 통해서만 복호화를 수행할 수 있으므로 플레이어에 의존해야 하는 문제점이 있다. P2P 네트워크에 DRM을 적용하기 위해서는 안전성, 서버에 대한 부담, 빠르고 쉬운 다운로드 등을 고려하여야 한다.

순수 P2P 모델은 모든 DRM 처리가 서버에서 수행되는 반면 암호화된 콘텐츠는 P2P 모드로 전송된다. 사용자 피어들은 DRM 서버에 접근하여 수신된 콘텐츠를 복호화 하기 위해 요청 기능을 시스템에 가지게 된다. 그리고 DRM 서버에 라이선스 발행을 요청하는 기능은 반드시 사용자의 시스템에 설치되어야 한다. 이 방식에서 서버는 반드시 모든 사용자의 계정을 인증, 지불 및 정산을 통해 관리해야 한다. 암호화와 사용 제어 기능이 모두 DRM 서버에서 관리되며 사용자 인증을 한 서버 역시 센터에 위치하게 된다. 따라서 신뢰성과 안전성은 보장되지만 사용자 수가 증가할수록 서버엔 부담이 커지게 된다.

하이브리드 P2P 시스템은 유료는 물론 무료 다운로드가 쉽고 빠르게 수행될 수 있도록 한다. 안정적이기 때문에 하이브리드 P2P 기반의 RPM이 DRM 서버에 무리를 주지 않는 가장 이상적인 모델이라 할 수 있지만 하이브리드 P2P 시스템과 DRM 기술의 단순한 접목은 저작권자의 이익만을 보장할 가능성이 있으므로 P2P 네트워크의 가장 큰 장점인 정보 공유에 대해 문제점이 발생한다.

III. 개선된 DRM 시스템

본 논문에는 P2P 환경의 DRM 시스템을 개선하여 분산컴퓨팅의 성능을 최대화하고 사용자 증가에 비례해 발생되는 부하와 콘텐츠의 공유 시 발생될 수 있는 보안의 위협 요소를 최소화함으로써 디지털 콘텐츠의 스트리밍 서비스를 개선하고자 한다. 기존 DRM 시스템은 중앙의 서버를 통해 클라이언트의 접속을 제한하는 반면 개선된 P2P환경의 DRM 시스템은 분산처리 방식으로 중앙 서버 없이 피어들 간의 양방향 통신이 가능하게 한다. 일반적으로 DRM은 라이선스 발급을 위한 Clearinghouse와 인증 서버 그리고 콘텐츠 암호화를 제공하는 패키지 등을 기본 요소로 포함

한다. 하지만 요소들을 P2P 시스템에 단순하게 접목할 수는 없다. 따라서 서버/클라이언트 모델의 장점인 신뢰성과 안정성 및 중앙 서버에 의한 시스템 전체 관리 가능 또한 중앙 서버의 다중화를 통해 피어간 동적 네트워크 구성이 가능하도록 하여 신뢰성을 향상시키도록 해야 한다.

네트워크 관리 측면에서 DRM은 콘텐츠 사용에 대한 라이선스 발행과 관리를 Clearinghouse에서 수행한다. 그림 1은 개선된 P2P 기반 DRM 시스템을 나타낸 것이다.

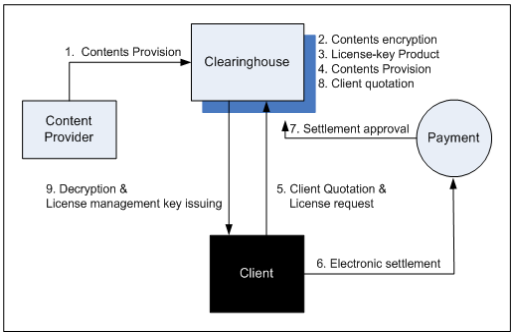

그림. 1 개선된 P2P네트워크 기반 DRM 시스템
Fig. 1 Improved DRM System based on P2P Network

DRM 서버는 암호화/복호화 모듈, 라이선스 관리 모듈, 키 관리 모듈, 거래 관리 모듈 등으로 구성되며, DRM 클라이언트는 라이선스 키 관리 모듈, 복호화 모듈 등으로 구성된다. DRM 서버는 콘텐츠 제공자로부터 받은 콘텐츠의 암호화, 라이선스 키 작성, 온라인을 통한 전송을 담당한다. 클라이언트로부터 콘텐츠 요청이 있을 경우 결제를 통하여 승인 여부를 체크한 다음 콘텐츠는 암호화 모듈을 이용하여 암호화하고 이 정보를 DB에 기록한다. DRM 클라이언트는 DRM 서버에서 다운로드 받은 암호화된 파일을 라이선스 획득 여부에 따라 복호화하며 동시에 사용자 시스템의 정보를 서버로 전송한다. 전송된 사용자의 시스템 정보를 통해 콘텐츠의 사용 여부와 사용자 관리를 가능하게 한다.

3.1 인증 프로토콜

개선된 P2P 기반 DRM 시스템에서는 기존 시스템과의 호환성을 높이기 위하여 표준화되어 있고 범용으로 쓰이는 RSA, SEED, AES, SHA-1 등의 알고리즘을 이용하였다. 그리고 안전하고, 신뢰성 있는 디지털 콘텐츠 유통 및 인증을 위해 공개키 암호 알고리즘을 적용하여 비밀 키의 분배와 서명에 사용하였다. 최소한의 정보만을 공개키 암호 알고리즘을 이용하여 암호화 하고, 콘텐츠 및 다른 정보들은 범용 암호 알고리즘을 사용하여 효율성을 고려하였다.

일반적으로 사용자 인증은 회원 가입을 통해 이루어지지만 본 논문에서는 하드웨어 바인딩 기법을 사용하여 불법 사용자가 정당한 사용자의 정보를 획득하여 손쉽게 복호화 하지 못하도록 한층 더 보안 강화하였다. 정당한 사용자의 컴퓨터의 하드웨어 정보까지 인증하도록 하는 하드웨어 바인딩 기법을 사용하기 때문에 회원 가입과 동시에 클라이언트 네트워크 카드 주소까지 함께 전송을 시켜 인증을 하도록 하였다. 콘텐츠를 다운로드 받은 사용자만이 회원에 가입할 수 있도록 하였으며 이를 위해서 PKI 기반의 인증서를 통한 로그인을 사용하였다. 그림 2는 인증 프로토콜을 나타낸 것이다.

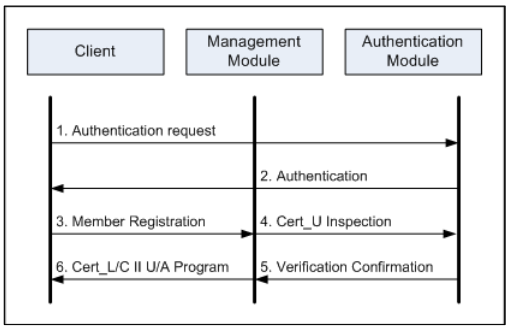

그림 2. 인증 프로토콜
Fig. 2 Authentication Protocol

3.2 라이선스 프로토콜

사용자는 콘텐츠를 복호화하기 위하여 라이선스를 발급받아야 한다. 라이선스가 없을 경우 서버에 접속하여 서버에서 사용자 인증과정 수행 후 라이선스를 발급한다.

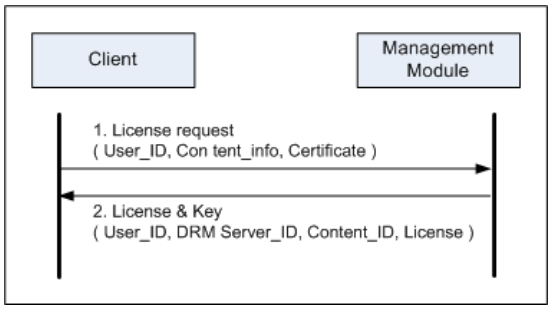

그림 3. 라이센스 프로토콜
Fig. 3 License Protocol

사용자는 콘텐츠의 라이선스를 발급 받기 위해 라이선스 요청 메시지를 서버에 전송한다. 라이선스 요청 메시지에는 사용자 ID, 라이선스 ID, 유효기간, 라이선스 검증 주기, 사용자의 공개키 정보, 서버 식별 정보 및 권한 등 인증서를 사용자의 개인키로 서명하고 이를 서버의 공개키로 암호화 값을 전송하여 라이선스 발급 요청을 한다. 서버는 해당 인증서의 정보에 의하여 공유키에서 개인 정보를 추출하고 추출된 개인 정보와 암호화된 콘텐츠의 비밀 키와 공유 키 그리고 라이선스를 함께 사용자에게 전송하고 라이선스 다운로드 받은 사용자는 복호화와 실행을 동시에 수행하도록 한다. 그림 3은 라이선스 프로토콜 수행 과정을 나타낸 것이다.

V. 성능 평가

제안된 시스템의 성능을 측정하기 위하여 네트워크 대역폭 측정을 하였다. 그림 4는 클라이언트들이 다운로드 시작 후 60초 동안 네트워크 대역폭을 사용한 평균 비율을 측정한 결과이다. 실험에 참여한 모든 클라이언트가 동시에 다운로드를 시작하여 측정한 결과 개선된 시스템은 평균 1%~4%사이의 대역폭을 점유하고 있으며, 기존 시스템에 비해 일정한 네트워크 대역폭을 이용하고 있음을 알 수 있다. 이는 안정된 스트리밍 서비스를 제공하며 부하의 증가에 따른 중단 현상이 최소화되었음을 알 수 있다.

본 논문에서 제안한 개선된 DRM 시스템에 대한 성능 평가를 위해 지속적인 스트리밍 서비스를 요구하는 영상 데이터를 기준으로 실험하였다. 암호화되어 있는 비디오 데이터 파일의 복호화를 먼저 수행한 후 재생하는 기존 DRM 방식과 실시간으로 복호화를 하면서 재생하는 개선된 DRM 방식에 대해 각각 수행 시간을 측정하였다.

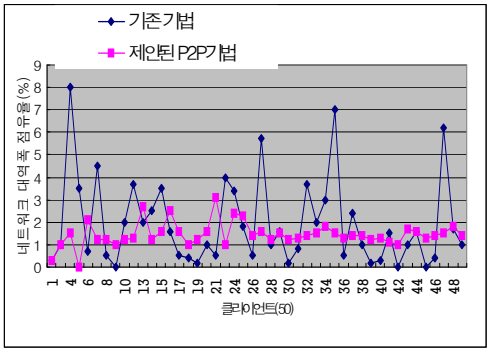

그림 4. 평균대역 비교
Fig. 4 Comparison of bandwidth Averages

사용자가 영상 데이터 파일을 실행할 경우 복호화와 실행이 동시에 수행되므로 재생지연시간에서 복호화 시간을 분리하여 정확하게 계산하기 어려우므로, 암호화 시간을 측정하고 복호화와 실행시간을 동시에 측정하여 복호화 시간과 동영상 파일의 로딩시간이 포함된 지연시간을 계산하였다.

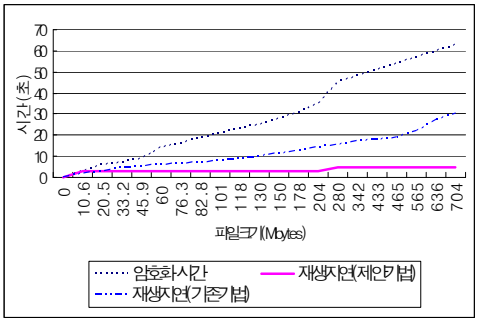

그림 5. 암호화 시간 과 재생지연 시간 비교
Fig. 5 Comparison of encryption time and delayed time

재생 지연 시간과 암호화 시간의 차이로 파일 재생

을 위한 로딩 시간을 측정할 수 있었다. 그림 5는 기존시스템과 개선된 시스템의 암호화 시간과 재생 지연 시간을 측정한 후 결과를 나타낸 것이다.

기존 시스템은 콘텐츠의 크기에 비례하여 암호화 시간이 늘어나며 지연시간 역시 비례하여 늘어나는 것을 알 수 있다. 기존의 시스템을 대용량의 영상 데이터에 사용할 경우 많은 지연시간이 발생하여 사용자에 대한 서비스 지연 시간이 늘어나는 반면 개선된 시스템은 영상 데이터의 크기에 비례하여 암호화 시간이 증가하지만 복호화와 동시에 재생하므로 실제 지연 시간은 감소하는 것을 확인할 알 수 있다.

Ⅵ. 결 론

본 논문에는 P2P 환경의 DRM 시스템을 개선하여 분산컴퓨팅의 성능을 최대화하고 사용자 증가와 콘텐츠 공유 증가에 비례해 발생되는 부하를 최소화함으로써 디지털 콘텐츠의 스트리밍 서비스를 개선하고자 하였다.

이를 위해 인증 프로토콜과 라이센스 프로토콜을 개선하여 콘텐츠를 사용하고자 할 경우 라이선스만을 다운로드 받은 다음 복호화와 실행을 동시에 수행하도록 함으로써 기존 DRM 시스템보다 한층 강화된 스트리밍 지원을 하도록 하였다.

성능 평가를 위해 암호화되어 있는 영상 데이터 파일의 복호화를 먼저 수행한 후 재생하는 기존 DRM 방식과 실시간으로 복호화를 하면서 재생하는 개선된 방식에 대해 각각 수행 시간을 측정하였다.

개선된 시스템은 평균 1%~4%사이의 대역폭을 점유하고 있으며, 기존 DRM 시스템에 비해 일정한 네트워크 대역폭을 유지하고 있음을 알 수 있다. 이는 안정된 스트리밍 서비스를 제공하며 부하의 증가에 따른 중단 현상이 최소화되었음을 알 수 있다. 또한 개선된 시스템은 동영상의 크기에 비례하여 암호화 시간은 증가하지만 복호화를 수행하면서 동시에 재생하므로 실제 지연 시간은 감소하는 것을 확인할 알 수 있다.

본 논문은 한국건설교통기술평가원에서 위탁시행한 2005년도 건설기반구축사업(05기반구축D02)의 지원으로 이루어졌습니다.

참고 문헌

[1] Hauser, T. and Wenz, C. (2003): DRM Under Attack : Weaknesses in Existing Systems, In Digital Rights Management-Technological, Economic, Legal and Political Aspects. LNCS 2770, Springer, pp.206-223.

[2] Lei Li. and Ian Horrocks, "A software framework for matchmaking based on semantic webtechnology", In Proceedings of the Twelfth International World Wide Web Conference (WWW2003), ACM, pp.331-339, 2003.

[3] Pinar Yolum and Munindar P. “Singh. Dynamic communities in referral networks”, Web Intelligence and Agent Systems, pp.105-116, 2003.

[4] S. Guth., “Digital Rights Management”, Number in LNCS. Springer-Verlag Heidelberg, pp.150-161, 2003.

[5] Biddle, P., England, P., Peinado, M. and Willman, B., "The Darknet and the future of content protection", In Digital Rights Management-Technological, Economic, Legal and Political Aspects. LNCS 2770, Springer, pp. 344-365.

[6] Peinado, M. Chen, Y. et al., NGSCB: A Trusted Open System. In Proceedings of 9th Australasian Conference on Information Security and Privacy ACISP, Sydney, Australia, pp.13-15, July 2004.

[7] Nelson Minar, Marc Hedlund, Clay Shirky, and Tim O’Reilly, “Peer-to-Peer: Harnessing the Power of Disruptive Technologies”, pp. 109-122, 2001.

저자 소개

이정기(Jeong-gi Lee)

2006년 조선대학교 컴퓨터공학과 졸업 (공학박사)
2006년~현재 전자부품연구원 재직
※ 주관심분야 : 시스템보안, Embedded, 운영체제

정양권(Yang-kwon Jeong)

1988년 조선대학교 대학원 졸업 (공학석사)
1996년 조선대학교 대학원 졸업 (공학박사)
동신대학교 컴퓨터공학과 부교수
광주광역시 남구청 정보화 위원
전남도청 정보화 위원
※ 주관심분야 : 지문기반 사상체질 인식 시스템, 가상현실 자가치유 영상 시스템, 원격 기공 공유기반 치료 시스템, 교통사고자동기록시스템, 자동차 번호인식 시스템

김동현(Dong-hyun Kim)

1992년 공학석사(컴퓨터공학)
2002년 이학박사(컴퓨터응용)
2006년 행정학석사(부동산학)
2007년~현재 부동산학 박사 과정
1996년~현재 순천청암대학 교수
벤처정보연구소장
정보처리 기술지도사
※ 주관심분야 : 컴퓨터응용, 부동산조사분석, 전자상거래, 부동산정보, U-city