공학석사 학위논문

P2P 기반의 신뢰성 있는 디지털 콘텐츠 판매 시스템 설계 및 구현

이 論文을 工學碩士 學位論文으로 提出함

2005년 8월

부경대학교 산업대학원

전산정보학과

서 선 희

서선희의 공학석사 학위논문을 인준함

2005년 6월 17일

주 심 이학박사 윤 성 대 

위 원 공학박사 여 정 모 

위 원 이학박사 이 경 현 

<차 례>

<표 차례>

<그림 차례>

Design and Implementation of a Reliable Digital Content Delivery System Based on Peer-to-Peer

SunHee Seo

Det. of Computer & Information, Graduate School.
Pukyong National University

Abstract

Nowadays P2P(Peer to Peer) service is widely used and different from the classical client/server service. It's a new service that two computers can communicate to share the information without intervening the central computer. If P2P service is used in internet purchases, the service users could communicate without the central server and can do many personal purchases and auctions anytime and anywhere. However there is one problem; there are not enough secure systems that can protect the P2P service from the hackers. Hence this thesis proposes the e-Commerce system that is based on the P2P system and the purchasing protocol that provides the fairness between two peers on the purchase of digital contents. The designed

e Commerce system also provides the reliability by adopting user reputation certificate for guaranteeing credibility of providing information.

I. 서 론

인터넷 이용을 위한 기반 환경의 확충 및 네트워크 환경이 계속적으로 발전하면서, 기업 간 또는 기업과 소비자 간의 상거래 활동을 통신 네트워크를 통해 수행하는 전자상거래가 활발하게 이용되고 있다. 전자상거래는 네트워크를 통해 판매자와 구매자를 직접 연결하므로 물리적인 판매 거점이 불필요하며, 기업 활동에 있어 시간과 공간의 제약이 사라져 기업은 언제, 어디서나 상품 판매가 가능하고, 소비자는 언제, 어디서나 상품 구매가 가능한 이점을 가진다. 인터넷 쇼핑몰을 중심으로 거래가 발생하는 기존의 전자상거래 방식은 클라이언트-서버 방식으로 동작하므로 사용자들은 특정 서버에 의존하여 상거래 활동을 수행하며, 정보의 공유 영역 또한 제한적이고, 해당 서버에 문제가 생길 경우 더 이상 상거래를 유지하기 어려운 단점이 있다[8].

클라이언트-서버 방식이 가지고 있는 이러한 문제점을 보완하기 위해 등장한 P2P(Peer to-Peer) 기술은 서비스에 참여하는 각각의 컴퓨터들이 서버인 동시에 클라이언트로 동작하면서 중앙 서버 없이 직접적인 연결을 통해 서로의 자원에 대한 공유 및 교환이 가능하다. P2P 기술을 전자상거래에 적용하는 경우 상거래 서비스 이용자들은 특정 중앙 서버에 의존하지 않고, 개인별 상거래나 경매가 가능하므로 P2P 방식을 이용한 전자상거래 시스템 개발에 관한 연구가 급증하고 있다[1]. 그러나, 신뢰할 수 있는 관리 서버의 부재로 인해 P2P 네트워크는 신뢰성(reliability)이나 공정성(fairness)과 같은 전자상거래에 필요한 서비스를 효과적으로 제공하지 못하고 있는 실정이다. 공정성은 전자상거래에서 중요한 보안 서비스로서 거래 종료 후, 거래에 참여했던 모든 사용자들은 자신이

원하는 것을 받거나 혹은 어떤 개체도 원하는 것을 받지 못함을 보장하는 것을 말한다[2]. 또한, P2P 시스템에서는 사용자의 익명성 때문에 그들이 제공하는 자료들에 대한 신뢰성 또한 부족하다.

이에 본 논문에서는 디지털 콘텐츠의 판매의 안전한 거래를 위해, 판매자의 평판 값을 이용하여 신뢰도를 확인 할 수 있도록 평판 관리 서버를 두어 평판 인증서를 발행하도록 하였다. 또한, 지불문제와 공정한 교환 문제를 해결하기 위해 지불 중개 서버를 두어 지불과 교환에 관계된 문제를 해결하고자 하였으며, ElGamal 암호기법을 사용하여 지불 중개 서버가 콘텐츠를 획득하여 복호화 할 수 있는 방법을 차단 하고자 하였다.

본 논문의 구성은 다음과 같다. 2장에서 관련연구로 P2P 서비스 방식과 P2P 전자상거래 개요, 평판(Reputation), 에스크로 서비스(Escrow Service)에 대해 살펴보고, 3장에서 제안 시스템의 설계 및 구현으로 시스템의 개요, 시스템 구성 요소, 시스템의 설계, 시스템의 구현, 그리고 시스템의 분석에 대해 살펴보고, 4장에서 결론 및 향후 연구에 대해 살펴본다.

II. 관련 연구

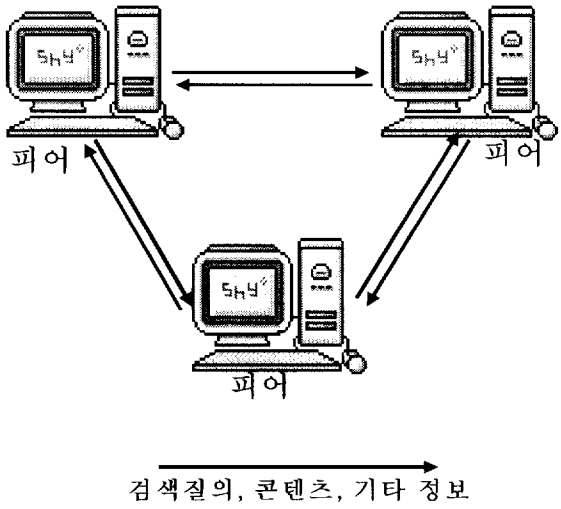
본 장에서는 관련연구로서 P2P 서비스 방식과 P2P 전자상거래 개요, 평판, 그리고 에스크로 서비스에 대해 살펴본다.

2.1 P2P 서비스 방식

P2P 서비스 방식은 크게 피어 간에 공유가 이루어지는 순수(Pure) P2P 서비스와 서버를 통해 공유가 이루어지는 혼합형(Hybrid) P2P 서비스로 구분할 수 있다.

1) 순수 P2P 서비스

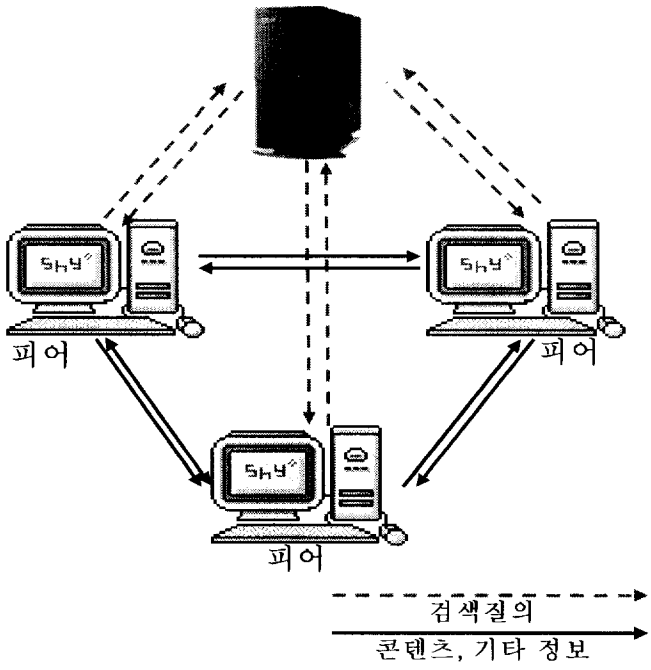
순수(Pure) P2P 서비스[9]는 전적으로 개별의 컴퓨터들에 의존한다. 피어들 간의 정보교환을 위해 중앙서버에 의존하지 않고 동작하는 완전 분산형 모델로 관리 역할을 담당하는 중앙 서버가 없기 때문에 네트워크에 연결된 피어들은 스스로 다른 피어들을 찾아야 한다. 순수 P2P 모델은 필요한 정보의 검색을 위해 피어들 간에 질의를 보내는 작업이 중복해서 발생하므로 네트워크 트래픽의 과부하로 인해 전체 대역폭이 증가하여 네트워크 전체의 효율성과 피어 검색의 효율성을 저하 시킬 수 있다. 대표적인 모델로 Gnutella와 FreeNet이 있다.



[그림 1] 순수 P2P 방식

2) 혼합형 P2P 서비스

혼합형(Hybrid) P2P 서비스[9]는 현재 네트워크에 접속되어 있는 피어들의 식별정보나 공유자원/파일들의 목록과 같은 메타정보들을 관리하는 서버를 포함시켜 피어들의 검색을 용이하게 하기 위한 방식으로 실질적인 통신을 수립하고 필요한 정보에 대한 교환은 개별 피어들이 담당한다. 중앙 서버는 전체 네트워크의 성능이나 연결 상태 파악, 검색에 있어 효율성을 제공하기 위한 인덱스 서버의 역할을 하거나 트랜잭션, 과금, 인증 등을 처리하는 역할을 수행할 수 있다. 대표적인 모델로 Napster, 소리바다가 있다.



[그림 2] 혼합형 P2P 방식

2.2 P2P 전자상거래 개요

디지털 경제의 본격적인 도입으로 초기 인터넷 기업들이 향유하던 거래비용의 감소와 선점효과 등 전략적 우위를 가능하게 하는 많은 요소들이 이제 더 이상 의미를 갖기 어렵게 되었다. 디지털 경제의 속성은 콘텐츠의 디지털화를 통한 제작비용, 유통비용, 보관비용, 탐색비용, 복제비용 등의 절감과 이를 기업경영에 반영한 거래비용의 감소에 있다[10]. 하지만 이러한 거래 비용의 절감은 치열한 경쟁구조를 도입하게 되었고 온라인과 오프라인 기업들은 엄청난 경쟁 환경 하에서 구체적인 대안을 찾지 못하고 있다. 또한 네트워크 효과와 수확 체증의 효과를 이용한 선점

선략에 기초하여 기업의 독점적 이익을 보장해 줄 것으로 판단하고 상당한 규모의 시스템 구축 및 마케팅비용을 수반한 투자는 수익성 모델을 요구하는 시장의 논리에 의거하여 주춤거리고 있는 실정이다[10].

이러한 시점에서 인터넷 비즈니스의 새로운 모델로 등장하고 있는 P2P는 차세대 인터넷의 대안으로 상당한 의미를 갖는다. P2P는 원래 'Peer to Peer'의 약자로서, 개인 대 개인의 커뮤니케이션을 가능하게 해주는 다양한 기술의 총칭으로 일종의 분산컴퓨팅, 분산처리 기술방식을 일컫는다. 현재는 기술적인 측면보다는 소비자 각 개인이 중심이 되는 'Person to Person'의 개념으로 빠른 속도로 발전하고 있다.

국내의 '오픈포유(open4u.co.kr)' 에서는 P2P 방식을 이용한 전자상거래 서비스를 제한하고 있다. 이 모델의 동작 방식을 살펴보면, 우선 사용자는 오픈포유에 접속하여 P2P 프로그램을 다운로드 받아 설치한다. 구매자는 이 프로그램을 이용해 자신이 구매를 원하는 물품의 사양을 적어 메시지를 전송하면 중앙서버인 오픈포유 서버가 구매자가 요청한 사양의 물품을 제공할 수 있는 판매자의 IP주소를 구매자에게 전송한다. 구매자는 이 정보를 이용하여 P2P 방식으로 각 판매자에게 견적요구서를 요청하고, 견적서 요청을 받은 판매자는 견적서를 구매자에게 전송한다. 구매자가 여러 견적서 중 적합한 하나를 선택하여 거래를 수행한다. 오픈포유의 서버는 최종 거래가 어느 조건으로 성립되었는지에 대한 정보만 확보하고 두 당사자 간의 거래에는 개입하지 않는다. 오픈포유의 주요 목적은 소매상 또는 도매상간, 도매상과 제조업간, 소매상과 제조업 사이에 개입해 B2B 네트워크를 형성시키는 데 있다. 오픈포유 서비스의 장점은 역경매와 같이 구매자 중심의 비즈니스 모델을 적용한 사례로 서버의 개입 없이 네트워크만을 제공한다는 데 있다. 그러나 P2P의 본질적인 문제점인 거래의 신뢰성 보장에 대한 해결책이 아직까지 마련되지 않고 있

으며, 결제, 배송 등 전자상거래 인프라 시스템이 제공되지 않아 실제적인 상거래 발생 가능성이 작다고 볼 수 있다.

전자상거래 시 요구사항으로는 공정성, 신뢰성, 인증, 기밀성, 무결성 그리고, 부인방지를 들 수 있으며, 디지털 콘텐츠 판매를 중심으로 살펴보면 다음과 같다[3]

공정성(Fairness)은 구매자와 판매자 간 거래에 있어 자신이 원하는 콘텐츠를 둘 다 가질 수 있거나 가지지 못함을 보장 할 수 있어야 한다.

신뢰성(Trustiness)은 구매자가 판매자의 평판 값을 활용하여 상대에 대한 신뢰성을 판단하여 판매자를 선택 할 수 있어야 한다.

인증(Authentication)은 구매자와 판매자간에 디지털 콘텐츠를 전달할 때 서버에 의해 인증 된 정당한 상대인지를 확인할 수 있어야 한다.

기밀성(Confidentiality)은 구매자와 판매자간에 주고받는 콘텐츠는 허가 되지 않은 제3자로부터 보호 될 수 있어야 한다.

무결성(Integrity)은 구매자 판매자 간에 주고받는 콘텐츠는 불법적인 사용자에 의해 변조될 수 없어야 한다.

부인방지(Non-Repudiation)는 구매자와 판매자가 서로 간의 콘텐츠 거래 요청 메시지에 대해 부인 할 수 없어야 한다.

2.3 평판

평판(Reputation)이란 세상에 널리 퍼진 소문, 또는 명성을 말한다.
소리바다, Napster, eDonkey 등의 P2P 프로그램에서 특정 노래를 찾고자 할 때 사용자는 사전 정보 없이 파일 제공자가 제공하는 정보만으로

파일에 대한 모든 것을 판단한다. 파일이 실제로는 바이러스나 웜 등을 포장해 놓은 것일 수도 있고, 매우 질이 낮은 것일 수도 있지만 실제 사용자들은 그것을 판단할 수 있는 어떠한 사전 정보도 가지고 있지 않다. 이러한 문제점에 대한 일차적인 해결 방안으로 사용자들의 경험에 의한 의견이나 소문 등을 생각할 수 있으며, 실제로 여러 인터넷 사이트에서 사용되고 있다. 예를 들면, 사용자가 외식을 하고자 할 때 인터넷 상의 여러 외식업체들에 대한 평가와 경험담들을 소개해놓은 사이트를 참고할 것이고, 인터넷 쇼핑몰을 이용하여 물건을 구매하고자 할 때는 물건에 대한 품평들을 참조하여 구매를 결정할 것이다. 또한, eBay나 옥션 등에서 거래를 할 때는 판매자와 구매자에 대한 평가가 거래에 대한 큰 판단기준이 되고 있다. 반면, 그러한 의견이나 소문들의 신뢰도 혹은 위조 가능성이 문제가 될 수 있다. 이러한 문제점에 대한 해결 방안으로 몇 가지 방법이 제시되고 있는데, 그 중 평판에 기반한 시스템이 가장 주목할 만하다[4].

1) Xrep 시스템

Xrep-시스템 **[6]**은 Damiani 등에 의해 2002년 발표되었다. Xrep-프로토콜에서는 각 개인이 다른 사용자들에 대한 경험과 정보를 저장하고 이에 대하여 사용자의 요구가 있을 시 이를 공유하도록 한다. 이 때 각 사용자(서밴트:servent)는 자신의 공개키를 해쉬한 값을 $servent_{id}$ 로 사용하고, 자료의 내용을 해쉬 한 값을 $resource_{id}$ 로 사용한다. 그리고, 각 사용자는 두 가지의 평판을 관리하는데 하나는 사용자 평판으로 $servent_{id}$에 대응되는 값이고, 다른 하나는 자료에 대한 평판으로 $resource_{id}$에 대응되는 값이다.

이 시스템은 다음과 같은 순서로 각 사용자와 자료에 대한 평판을 알아내고 자료를 공유한다.

① 사용자 p가 자신의 주변에 있는 사용자에게 찾고자 하는 자원의 질의(Query)를 브로드캐스트 하고, 질의를 받은 서밴트 중 자료를 가지고 있는 서밴트는 자료의 수, 최적 속도, IP, 포트 등의 정보를 대답한다.

② 받은 응답(QueryHit)에 대하여 질의자 p가 자원(resource_id)과 자원을 제공할 사람(servent_id)에 대한 평판을 주변 사람들에게 묻고 그 응답을 받는다.

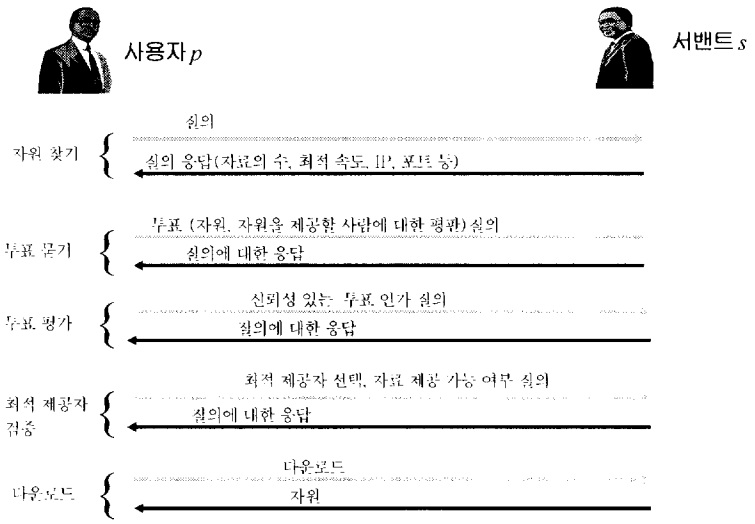
③ 받은 투표응답(PollReply)에 대하여 실제로 해당하는 노드에 의해서 투표 된 것 인지를 묻고 응답하는 과정이다. p는 투표결과를 바탕으로 자신의 잣대에 맞는 자료의 제공자와 자료를 선택한다.

④ 선택된 자료의 제공자와 자료에 대하여, 제공자에게 자료를 제공 가능한지 묻고 답을 받는 과정이다. 이 때 최적 제공자를 유일하게 선택한다면, 대부분 좋은 평판 제공자에게 집중되어 실행 효율에 있어 병목현상을 일으키게 된다. 그래서 먼저 선정된 최적제공자에게 자료의 제공여부를 질의하고, 만약 현재 제공이 불가능하다는 응답이 오면, 다른 제공자를 다시 찾게 된다.

⑤ 최적 제공자가 자료 제공이 가능하다고 응답을 하게 되면, 받은 응답

의 <IP, port>를 이용하여 직접 최적 제공자로부터 자원을 다운로드 한다.

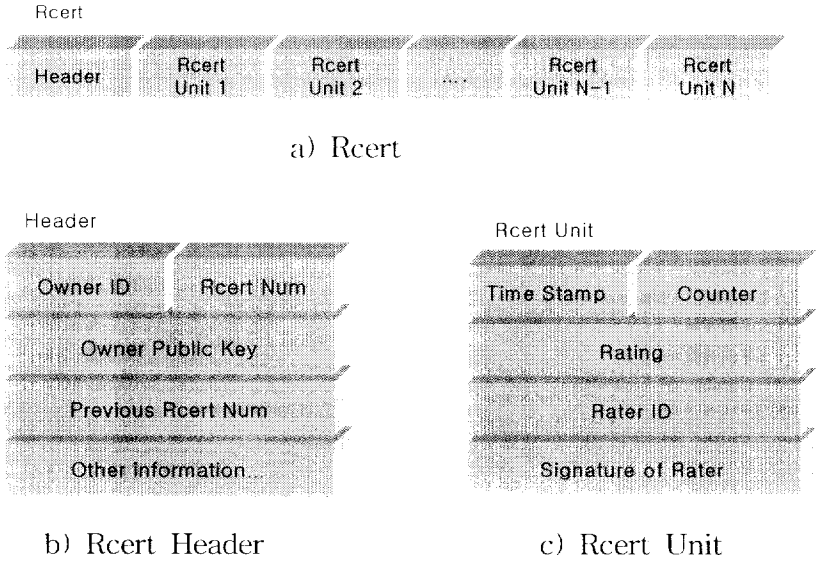
[그림 3]은 Xrep 프로토콜을 나타낸다.



[그림 3] Xrep 프로토콜

2) Rcert 시스템

2003년에 제안된 시스템으로 Rcert(Reputation Certification)시스템[7]는 PKI를 사용하고 서명의 안전성을 이용하여 평판의 위조를 방지한다. 또한, 서명의 임의적인 추가와 삭제를 방지하기 위해 타임스탬프를 이용한다. Rcert 시스템에서 rater는 피어에 의해 제공된 서비스를 이용한 피어를 말하며 ratee와 상호 작용의 경험을 기반으로 ratee를 평가한다. ratee는 서비스를 제공하는 피어를 말한다.



[그림 4] RCert형식

[그림 3]의 a) Rcert는 Rcert의 형식을 나타내며, b) Rcert Header는 Rcert의 소유자에 관한 정보를 제공하며, Rcert에 관한 정보를 포함(Rcert's currenID, previous ID)한다. Rcert의 크기가 커질 때, 소유자는 새로운 Rcert를 생성하고, header에서 old Rcert에 대한 참조를 제공한다. c) RcertUnit에서 타임스탬프는 거래가 시작되기 전에 Rcert의 소유자가 발행하며, Rating는 소유자와 거래를 가진 피어에 의해 주어진다. Rater ID는 rating(RcertUnit)을 생성한 피어를 말한다. 그리고, Signature는 rater에 의해 생성되며 Rcert의 무결성을 위해 전체 Rcet에 대한 서명이다.

Rcert시스템의 순서는 다음과 같다.

① 자료를 얻고 싶은 Rater가 다른 사용자의 평판을 알고 싶으면, ratee에게 질의를 보낸다

② 질의를 받은 ratee는 자신의 평판을 모아놓은 Rcert를 보내준다
이것의 확인과정은 ③, ④의 두 가지 과정을 거치게 된다

③ 검증은 서명자체를 확인하는 과정이다.

④ 평판의 추가와 삭제여부를 확인한다. 이 과정은 이전의 ratee의 평판을 작성한 사용자(이전 Rater)에 의해 이루어진다. 서명에 타임스탬프를 포함시키고, 이 타임스탬프를 이전의 rater에게 인증을 받는 형식이다. 가장 최근의 rater가 연결이 되지 않을 경우는 그 이전의 rater들 중 에서 연결이 되는 rater를 찾을 때까지 거슬러 올라간다.

⑤ 모든 확인과정이 완료되었다면, 자료를 받을 ratee를 선정하고 그 ratee에게 응답을 보낸다.

⑥ 응답을 받은 ratee 는 자신의 타임스탬프를 보내준다

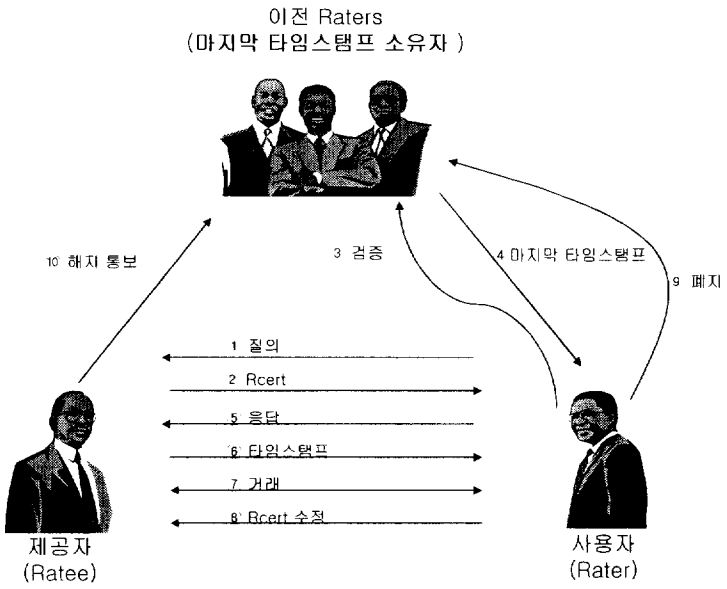
⑦ 타임스탬프가 현재시간과 일치하면 자료의 전송을 시작한다.

⑧ 자료의 전송 이후에 타임스탬프를 포함하는 서명을 만들어 ratee에게 보낸다

⑨ 최근의 rater에게 폐지 신호를 보낸다.

⑩ ratee는 해지 통보를 역시 rater에게 보낸다. 양쪽의 신호를 모두 받

으면 rater는 자신이 폐지되었다는 사실을 알게 되고, 자료를 전송 받은 사용자가 최근의 rater가 된다.



[그림 5] RCertPX 프로토콜

2.4 에스크로 서비스

세계 인터넷 사용 인구가 급증함에 따라 인터넷을 이용한 여러 형태의 전자상거래가 두드러지게 증가하고 있다. 그러나 아무리 전자상거래가 발달하더라도 전자상거래에 참여하는 이해 당사자들의 기본적인 신뢰가 제공되지 않는 한, 전자상거래의 발전은 곧 한계에 다다를 수밖에 없다. 더구나 직접 사람을 대하면서 서명을 하지 않는 비대면성과 익명성을 가지고 있는 전자상거래, 특히 먼저 결제를 하고(선 결제) 나중에 상품을 보내는 방식의(후 배송) 사이버쇼핑몰이나 인터넷 경매 사이트, 멀리 떨

어진 해외 바이어들과의 전자상거래에서 지급결제와 물품인도에 대한 신뢰는 전자상거래의 활성화를 위하여 필수적이다. 전자상거래를 통한 거래가 증가하고 이에 따른 여러 부작용이 사회적 문제로 대두됨에 따라 온라인에서의 거래를 보호해 주는 서비스의 필요성이 크게 부각되었다. 이 때문에 구매자와 판매자 사이에 보이지 않는 신뢰를 시스템적으로 보장해주는 도구의 등장은 필연적이라 할 수 있다. 이처럼 전자상거래의 이해 당사자들 중간에서 대금결제와 물류서비스의 문제를 해결해 주는 역할을 하는 것이 바로 인터넷 에스크로 서비스(internet escrow service)이다[11].

에스크로(escrow)란 원래 법률용어이다. 특정물을 제3자에게 기탁하고 일정한 조건이 충족된 경우에 상대방에게 교부할 것을 약속하는 조건부양도증서로 정의된다. 인터넷 에스크로 서비스를 다시 풀이하자면 '매매보호 서비스'로 해석할 수 있다. 구매자와 판매자가 서로 만나지 않고 거래하기 때문에 발생할 수 있는 거래 불이행 위험을 회피하기 위해 신뢰성 있는 제3자 (trusted third party)가 상품대금을 대신 받아서 보관하다가 서로의 거래가 원만히 이뤄졌음을 확인하고 대금결제를 해주는 서비스이다. 즉, 구매자와 판매자가 제3의 에스크로 업체에게 결제와 물품인도 보증서비스를 맡길 경우, 구매자가 인터넷을 통해 에스크로 업체 사이트에 상품의 종류와 가격, 결제방법 등 거래정보를 통보하고 상품대금을 에스크로 업체에 입금하면, 에스크로 업체는 판매자에게 상품대금이 입금되었음을 통보하고, 배송을 지시한 후 소비자가 주문한 상품이 아무 이상 없이 배달될 때까지 전적인 책임을 진다. 이때 에스크로 업체는 상품이 아무 이상 없이 배달됐음을 확인한 뒤 판매자에게 물품 대금을 결제한다. 거래가 아무런 문제없이 완결됐을 때 에스크로 업체는 구매자와 판매자 양측으로부터 혹은 어느 한쪽으로부터 일정 수수료를 받

을 수 있다. 또한, 상품에 이상이 있거나 거래하기로 한 상품과 다른 상품이 배송되는 경우 구매자는 반품을 할 수 있으며 거래대금을 안전하게 돌려받을 수 있다. 따라서, 에스크로 서비스가 활성화 될 경우 국내 전자상거래 시장 활성화에 큰 영향을 미칠 것으로 기대된다[11].

인터넷 에스크로 서비스의 장점은 다음과 같다[11].

첫째, 매매행위의 신뢰성을 높여준다는 것이다. 온라인 거래는 익명의 상태에서 거래자간의 신용만으로 이루어지기 때문에 온라인 경매를 통해서 물품거래를 하는 경우 구매자는 "원하는 물품을 확실히 받을 수 있을까?", 판매자는 물건을 보내 후 "물품대금을 확실히 받을 수 있을까? " 라는 의구심을 가질 수 있다. 인터넷 에스크로 서비스는 구매자의 대금이 입금된 것을 확인한 후 판매자에게 물품배송 요청을 하고 구매자가 물품을 수령하였는지를 확인하여 주므로 양측 모두 안전하게 거래를 보호 받을 수 있게 된다. 즉, 에스크로 서비스는 구매자 입장에서는 무엇보다 돈을 입금하고 물품을 받지 못하는 경우가 없고, 판매자 입장에서는 구매자가 안심하고 상품을 구매 할 수 있는 환경을 제공하므로 매출이 증대된다는 장점이 있어서 비대면 거래에 따르는 위험 요소들을 제거할 수 있다.

둘째, 인터넷 에스크로 서비스가 판매자에게 줄 수 있는 혜택은 구매자의 물품대금이 입금된 것을 확인한 후에 배송을 하므로 대금 지급을 완벽하게 보장 받을 수 있고, 거래의 안전성을 높여주므로 판매자가 새로운 고객과 시장을 개척할 수 있어 매출 증대의 효과가 있다. 또한 거래시간을 단축시킬 수 있고, 에스크로 사업자를 통하여 주문의 진행상황을 온라인으로 언제든지 확인 할 수 있게 해준다.

셋째, 에스크로 서비스가 구매자에게 주는 혜택은 구매대금을 지불하기 전에 물품을 먼저 검수할 수 있는 기회가 있으므로, 구매자가 새로운

판매자를 선택할 수 있는 기회가 주어지는 것이며 거래의 위험을 제거하여 거래를 신속히 진행할 수 있고 온라인으로 주문의 진행 상황을 24 시간 확인할 수 있다 .

넷째, 다양한 지급 결제 수단을 활용할 수 있다는 것이다. 개인 간의 거래에 있어서 이용이 가능한 지급 결제 수단은 현금, 수표 등으로 제한되어 있지만, 에스크로 업체를 이용하는 경우에는 에스크로 업체가 제공하는 모든 지불 결제 수단을 이용할 수 있으므로 신용카드, 전자화폐, 사이버 머니 등의 다양한 지불 결제 수단을 이용할 수 있게 된다 .

III. 제안 시스템의 설계 및 구현

본 장에서는 제안 시스템의 설계 및 구현으로, 시스템의 개요, 시스템 구성 요소, 시스템 설계, 시스템 구현 그리고, 시스템 분석에 대해 살펴본다.

3.1 시스템 개요

제안 시스템은 전자상거래에 참여하는 피어에 대한 신뢰성과 거래에 대한 공정성을 보장하기 위해, 판매자와 구매자의 거래에 직접 관여하지는 않지만 P2P 기반의 가상의 상거래 공간을 제공하는 마켓 매니저(MM : Market Manager)를 가정하며, 마켓 매니저는 공정한 거래를 위한 매매 보증 서버와 거래에 대한 피어들의 신뢰도를 평가하기 위해 평판 관리 서버를 운영한다. 또한, 판매와 지불의 공정성을 위해 조건 암호 기법[5]을 이용하여 구매자가 올바른 지불 단계를 수행하지 않으면 디지털 콘텐츠를 획득하지 못하도록 한다.

3.2 시스템 구성 요소

제안된 P2P기반의 신뢰성 있는 디지털 콘텐츠 판매 시스템을 구축하기위해 필요한 개체와 시스템 설정은 다음과 같으며, 표기법은 [표 1]을 따른다.

1) MM(Market Manager)

P2P 기반의 가상의 상거래를 위한 공간이다.

2) RMS(Reputation Management Server)

상거래 서비스를 이용한 피어들로부터 평판 값을 받아 그 값을 취합하고 계산하여 평판 인증서(RC : Reputation Certificate)를 발행하는 서버이다.

3) ES(Escrow Server)

개인 간 거래에서 구매 피어로부터 지불이 올바르게 이루어질 때 구매 피어에게 콘텐츠 복호화 키를 얻을 수 있는 정보를 전달하고, 판매 피어에게 대금을 지불하는 서버로 구매 피어와 판매 피어 모두 자신들이 원하는 정보를 제대로 받을 수 있도록 공정성을 보장해 주는 서버 이다.

4) P_i

콘텐츠 거래에 참여하는 판매 피어, 구매 피어를 나타낸다.

5) RD(Reputation Data)

구매한 콘텐츠에 대한 확인 후 구매 피어가 RMS에게 전송하는 평판 값으로 RMS는 이 값을 취합하고 계산하여 평판 인증서(RC)를 발행한다.

■ RD 형식

Target PeerID	Voting PeerID	Rating	Time stamp	Voter Signature

① Target PeerID

평판 대상(판매피어)에 대한 정보를 제공한다.

② Voting PeerID

Target PeerID에 대해 평판을 한 피어에 대한 정보를 제공한다.

③ Rating
Target PeerID에 대한 평판정보이다.

④ Time Stamp
RD의 발행시간을 나타낸다.

⑤ Voter Signature
RD의 무결성을 위한 투표자(Voter)의 서명이다.

6) RC(Reputation Cerificate)

평판 값을 취합하고, 계산하여 RMS가 발행하는 평판 인증서이다. 거래에 있어 판매 피어의 신뢰성을 판단하는 기준이 된다.

■ RC 형식

판매 PeerID	Rating	Time Stamp	Valid Period	RMS Signature

① 판매 PeerID
판매 피어에 대한 정보를 제공한다.

② Rating
콘텐츠 구매 후 판매 PeerID에 대한 평판 값을 나타낸다.

③ Time Stamp
RC의 발행시간을 나타낸다.

④ Valid Period
평판 인증서인 RC의 유효한 기간을 나타낸다. 이 기간이 지나면

평판인증서의 효력을 상실한다.

⑤ RMS Signature
RC의 무결성을 위한 RMS의 서명이다.

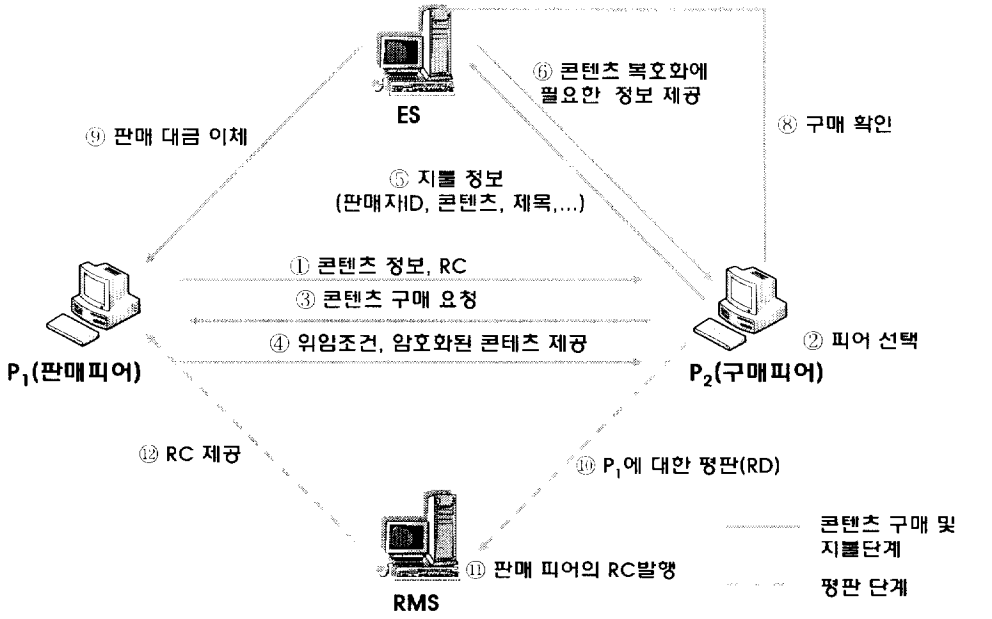
[표 1] 표기법

*	모든 피어	$Cert_{P_i}$	공개키에 대한 인증서
q	충분히 큰 소수	$E_{y_i}(\bullet)$	ElGamal 공개키를 이용한 암호화
x_i	i의 ElGamal 타입 개인키 $x_i \in Z_q$	$D_{x_i}(\bullet)$	ElGamal 개인키를 이용한 복호화
y_i	i의 ElGamal 타입 공개키 $y_i=g^{x_i}$	$Sig_{x_i}(\bullet)$	전자서명 생성
P_1	판매 피어(Seller)	$Ver_{y_i}(\bullet)$	전자서명 검증
P_2	구매 피어(Buyer)	$Enc_K(\bullet)$	비밀키를 이용한 암호화
MM	마켓 매니저	$Dec_K(\bullet)$	비밀키를 이용한 복호화
K_{xy}	피어 X와 피어 Y의 공유키	VP	RC의 유효기간

3.3 시스템 설계

제안 시스템은 크게 가입단계, 콘텐츠 구매 및 지불 단계 그리고, 평판 단계로 나뉘어 동작한다.

[그림 5]는 동작 단계 중 가입단계를 제외한 콘텐츠 구매 및 지불 단계와 평판 단계를 도식화 한 것이다.



[그림 6] 제안시스템 모델

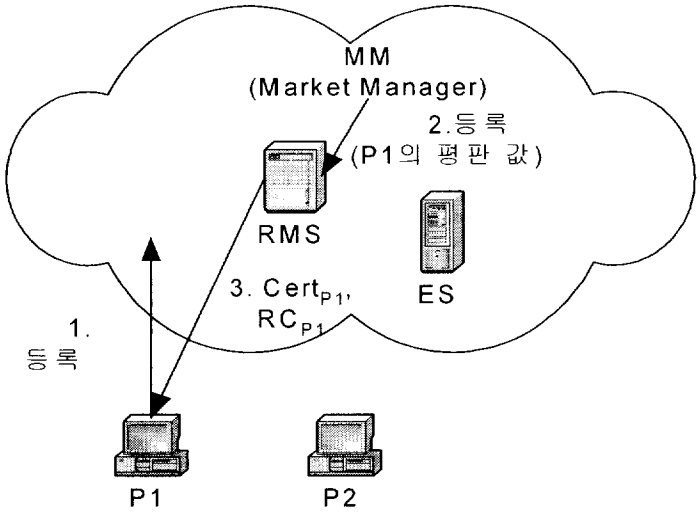
다음에서는 각 단계별로 나뉘어 살펴본다.

1) 가입 단계

① 각 피어 P_i는 시스템에 가입한다.

② MM은 RMS에 P_i의 기본 평판 값을 등록한다.

③ P_i의 공개키 PU_i에 대한 인증서 $Cert_i$와 평판에 대한 RC_i를 피어에게 발급한다.



[그림 7] 가입 단계

2) 콘텐츠 구매 및 지불단계

① 콘텐츠 판매를 원하는 피어(P_1)는 자신이 판매하고자 하는 콘텐츠에 대한 정보(콘텐츠 종류, 가격 등)와 자신의 평판을 나타내는 평판 인증서 RC_{P_1}를 P2P 네트워크로 발송한다. 판매 피어가 P2P 네트워크로 발송하는 메시지 형식은 식(3.1)에서 계산한 m_1과 같다. 이때, 전송 메시지에 대한 무결성 보장을 위해 메시지에 대한 서명값도 함께 전송한다.

$$m_1 = \{P_1, Cert_{P_1}, Item\_Info, RC_{P_1}\} \quad (3.1), \qquad Sig_{x_{P_1}}(m_1)$$

② 구매 피어(P_2)는 P2P 네트워크를 통해 구매하고자 하는 콘텐츠에 관한 정보를 검색하고, 여러 판매 피어들이 네트워크로 발송한 메

시지에서 평판 인증서의 평판 값을 확인하여 하나의 판매 피어(P_1)를 선택한다. 선택한 판매 피어가 P2P 네트워크로 발송한 공개키 인증서에 대한 검증과 메시지에 대한 서명 검증을 통해 신뢰할 수 있는 피어인지 확인한 후, 선택한 판매 피어로부터 구매를 결정하게 되면, 판매 피어와 안전한 메시지 전송을 위해 공유할 비밀키 K_{12}를 생성하여, 판매 피어의 공개키로 암호화하고, 구매하고자 하는 콘텐츠에 대한 정보와 함께 식(3.2)에서 m_2와 같은 형식의 메시지를 계산하여 판매 피어로 전송한다. 전송 메시지에 대한 무결성 보장을 위해 메시지에 대한 서명 값을 함께 전송한다.

$$m_2 = \{Item\_Info, P_1, P_2, C = E_{x_{P_1}}(K_{12})\} \quad (3.2), \quad Sig_{x_{P_2}}(m_2)$$

③ P_1는 P_2가 전송한 구매 요청 메시지에 대한 서명 검증을 수행하여, 구매를 요청한 콘텐츠를 확인한 후 해당 콘텐츠의 안전한 전송을 위해 랜덤키(K)를 생성하여 콘텐츠를 암호화하고, 거래 대상자들과 거래하는 콘텐츠에 대한 정보들로 구성되는 거래명세서 ϕ를 식(3.3)과 같이 작성한다. 거래 명세서는 ES가 구매 피어에게 콘텐츠 복호화 키를 전송할 때 거래에 대한 정확성을 확인하기 위해 사용된다.

$$\phi = \{\text{거래정보}\ (P_2, P_1, Item\_Info, pay\_info, Date)\} \quad (3.3)$$

식(3.3)에서 P_1는 판매 피어의 ID이며, P_2 는 구매 피어의 ID, *Item_Info*는 판매하는 콘텐츠에 대한 정보, *pay_info*는 판매 콘텐츠에 대한 가격 및 지불과 관련된 정보 그리고, *Date*는 거래 명세서 발급 일자이다.

콘텐츠 복호화 키의 안전한 전달과 구매자로부터의 올바른 지불을 위해 조건 암호 기법을 이용한다. 조건 암호 기법에 따라, 임의의 난수 $r \in Z_q$를 선택하여, 콘텐츠 암호화에 사용되는 키에 대하여 ElGamal 암호 기법을 적용하여 식(3.4)와 같이 c_1을 계산하고 식(3.5)와 같이 c_2를 계산한다. c_1과 c_2는 구매자에게 콘텐츠 복호화 키 정보를 전달하는 보증 서버에게 콘텐츠 복호화 키가 노출되지 않도록 하기 위해 사용된다.

$$C_1 = g^r \quad (3.4), \qquad C_2 = (y)^r \cdot K \quad (3.5)$$

구매자가 지불을 올바르게 해야만 콘텐츠 복호화 키를 얻을 수 있도록, 임의적으로 n 비트 메시지 v를 선택하여 식(3.6)과 같이 u_1을 계산하고 식(3.7)과 같이 u_2를 계산한다.

$$u_1 = E_{y_{ES}}(v) \quad (3.6), \qquad u_2 = x_{P_1} - H(\phi, v) \quad (3.7)$$

P_1은 P_2에게 식(3.8)과 같이 계산한 메시지 m_3를 전송한다. 전송 메시지에 대한 무결성 보장을 위해 메시지에 대한 서명 값을 함께 전송한다.

$$m_3 = \{c_1, c_2, \phi, Enc_{K_{12}}(u_1, u_2), Enc_K(item)\} \quad (3.8), \quad \mathrm{Sig}_{x_{P_1}}(m_3)$$

④ P_2는 P_1으로부터 받은 메시지에 대한 서명 검증 후 식(3.9)를 계산하여 콘텐츠 복호화 키를 얻기 위해 ES에 해당 콘텐츠에 대한 지불 정보인 m_4와 전자서명, 인증서를 함께 전송한다.

$$m_4 = \{c_1, u_1, \phi, pay\_info\} \quad (3.9), \; Sig_{x_{P_2}}(m_4), \; Cert_{P_2}$$

⑤ ES는 인증서 검증을 통해 P_2에 대한 신원을 확인하고, P_2가 전송한 거래 명세서에 대하여 P_1의 공개키로 서명 검증을 수행하여 이상이 없을 경우 V를 식(3.10)과 같이 계산하여 콘텐츠 복호화에 필요한 정보인 C_B를 식(3.11)와 같이 계산하고, 식(3.12)와 같이 m_5을 계산하여 P_2로 전송한다.

$$v = D_{y_{ES}}(u_1) \quad (3.10), \qquad C_B = C_1^{H(\phi, v)} \quad (3.11)$$

$$m_5 = E_{y_{P_2}}(c_B) \quad (3.12), \qquad Sig_{x_{ES}}(m_5)$$

⑥ P_2는 ES로부터 받은 정보와 이전 단계에서 P_1으로부터 받은 정보를 이용하여 콘텐츠 복호화 키를 식(3.13)과 같이 계산하여, 판매 피어로부터 받은 암호화된 콘텐츠를 식(3.14)와 같이 복호화 하여 확인한다.

$$K = C_2 \cdot C_1^{-u_2} \cdot C_B^{-1} \quad (3.13)$$

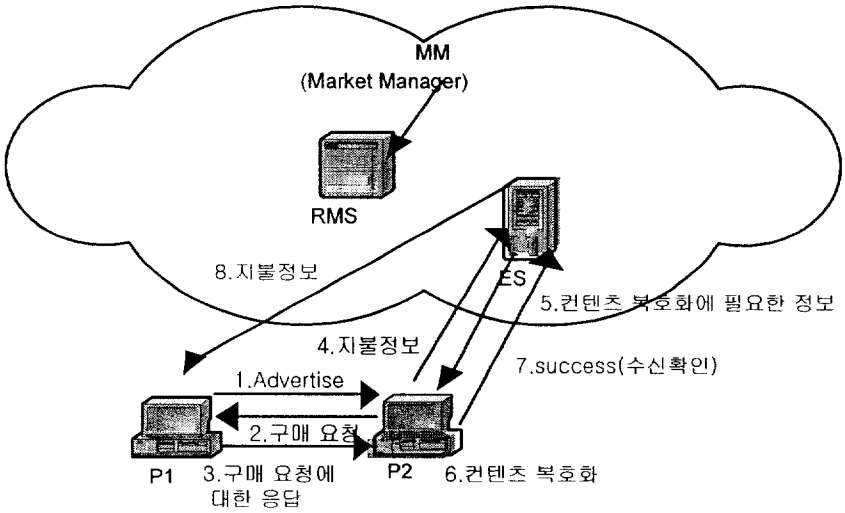
$$item = Dec_K(Enc_K(item)) \quad (3.14)$$

⑦ P_2는 콘텐츠 확인 후 ES에게 콘텐츠 수신에 대한 메시지를 전송한다.

SUCCESS

⑧ ES는 P_2로부터 확인 메시지를 받은 후 P_1에게 해당 콘텐츠에 대한 지불 정보를 전송한다.

$$E_{y_{ES}}(pay\_info)$$



[그림 8] 콘텐츠 구매 및 지불단계

3) 평판단계

① P_2는 자신이 구매한 콘텐츠에 대한 정확성 등을 확인한 후, 식(3.15)와 같이 m_6을 계산하여, P_1에 대한 신뢰도를 나타내는 평판값인 RMS를 식(3.16)과 같이 계산하여 전송한다. 본 논문에서는 신뢰할 수 있는 경우에는 +1, 신뢰할 수 없는 경우에는 -1을 전송한다.

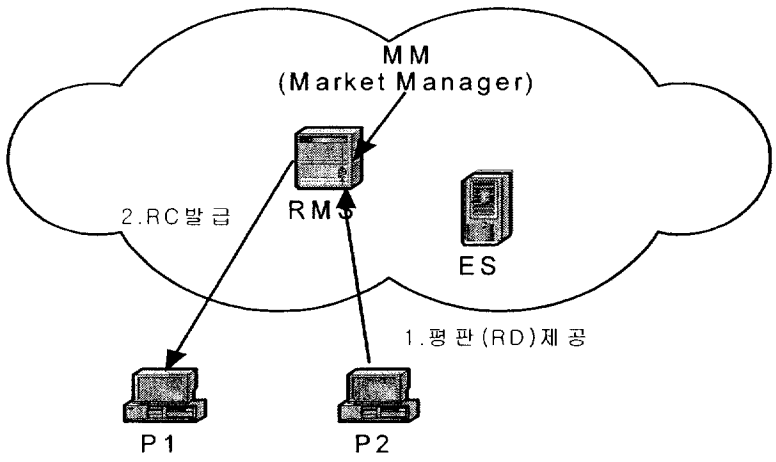
$$m_6 = \{ P_1, P_2, rating(+1 or -1), T \} \quad (3.15)$$

$$RD = m_6, \; Sig_{x_{P_2}}(m_6) \quad (3.16)$$

② RMS는 P_1에 대해 수집된 평판 값들을 취합하고 정리하여(취합된 평판 값을 누적) 식(3.17)과 같이 m_7을 계산하여, 해당 판매 피어의 평판 인증서에 대한 유효기간이 만료되면 수집된 평판 값을 이용하여 새로운 평판 인증서인 RC를 식(3.18)과 같이 계산하여 전송한다.

$$m_7 = \{ P_1, rating, T, VP \} \quad (3.17)$$

$$RC = m_7, \; Sig_{x_{P_2}}(m_7) \quad (3.18)$$



[그림 9] 평판 단계

3.4 시스템 구현

본 절에서는 실제 시스템을 구현 하는데 필요한 환경과 구현 내용에 대해 살펴본다.

3.4.1 구현 환경

본 논문에서 제안하는 P2P 기반의 신뢰성 있는 전자상거래 시스템은 소켓(Socket)을 이용한 TCP/IP로 구축되어 운영되며, 기본적인 구현 환경은 다음과 같다.

1) 사용언어

- Java 2 Platform, Standard Edition SDK(JDK 1.4.2)
- 암호알고리즘 : ElGamal 암호기법, ElGamal 전자서명, DES 암호기법

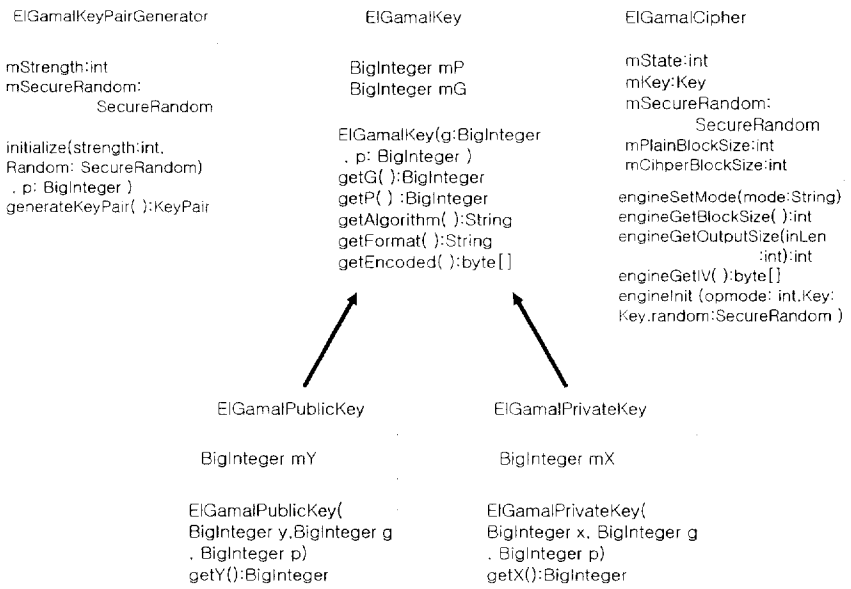
2) 시스템 환경

- CPU : Pentium IV 1.0GHz
- Memory : 256M
- OS : Windows 2000 Pro
- Editor : Jdeveloper 9.0

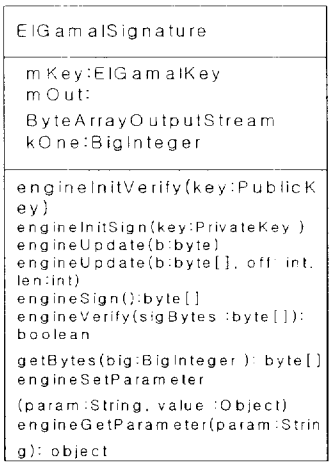
3.4.2 구현

1) 암호화 클래스 UML 설계

[그림 10]는 ElGamal 암호 기법을 적용하기 위한 클래스의 UML을 나타내며, [그림 11]은 ElGamal 전자서명을 위한 클래스 UML을 나타낸다.



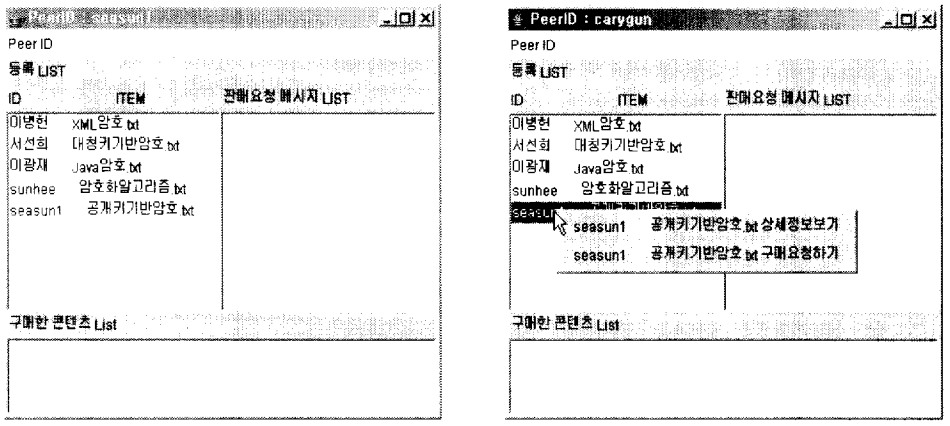
[그림 10] ElGamal 암호화를 위한 클래스 UML



[그림 11] ElGamal 전자서명을 위한 클래스 UML

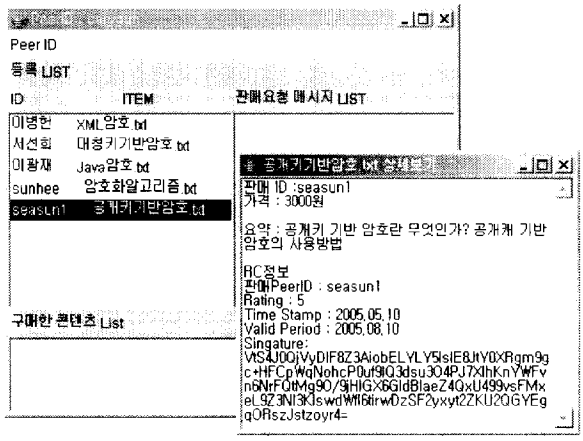
2) 구현 화면

- [그림 12]은 서비스 이용을 위해 접속한 피어들의 디지털 콘텐츠 판매 리스트를 보여 준다.



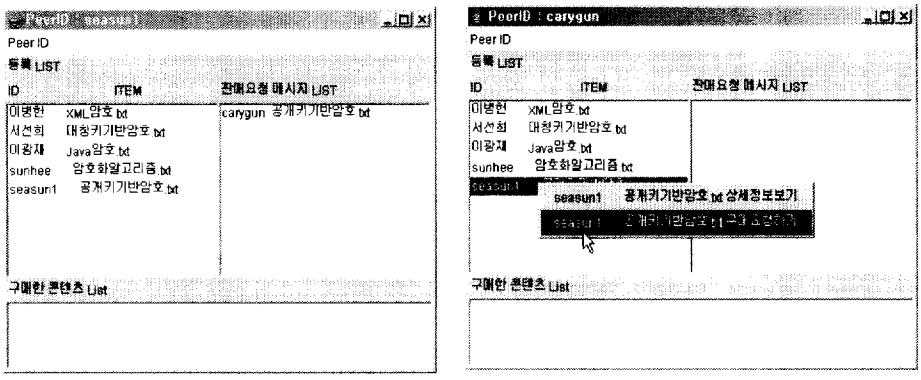
[그림12] 접속한 피어들의 디지털 콘텐츠 리스트 화면

- [그림 13]은 구매 피어가 구매를 원하는 콘텐츠의 "상세정보 보기"를 선택하여 콘텐츠 가격, 요약, RC정보를 보고 자신이 원하는 콘텐츠가 맞는지 확인한다.



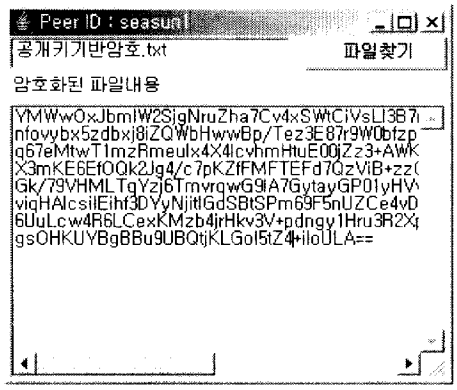
[그림 13] 구매 결정을 위하여 선택한 디지털 콘텐츠의 상세정보

- [그림 14]는 콘텐츠의 상세정보를 확인한 후 콘텐츠를 소유하고 있는 피어로 구매요청을 한다



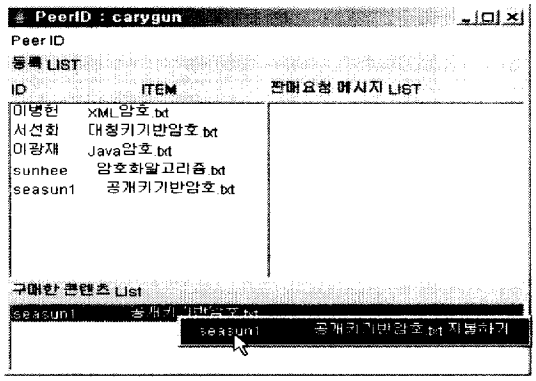
[그림 14] 디지털 콘텐츠 구매요청

- [그림 15]는 판매 피어가 구매를 요청한 피어에게 안전한 콘텐츠 전송을 위해 디지털 콘텐츠를 암호화 한다.



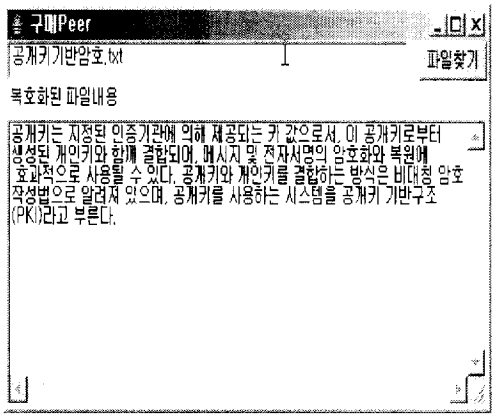
[그림15] 디지털 콘텐츠 내용의 암호화

- [그림 16]는 구매 피어가 구매한 디지털 콘텐츠에 대한 결제를 한다.



[그림16] 구매한 디지털 콘텐츠에 대한 결제

- [그림 17]는 구매 피어가 지불정보를 ES 서버에게 전달하고 ES 서버로부터 받은 정보를 이용하여 콘텐츠 복호화에 필요한 키를 획득하여 콘텐츠 내용을 복호화 한다.



[그림 17] 구매한 콘텐츠의 복호화

3.5 시스템의 분석

본 논문에서의 제안시스템에서는 다음과 같은 요구 사항을 만족한다.

첫째, 매매중개 서버인 ES를 두어 구매자가 올바른 지불 단계를 수행하지 않으면 디지털 콘텐츠를 획득하지 못하도록 하였으며, 구매자가 디지털 콘텐츠에 대한 확인 결과를 ES에게 보낸 후 판매자에게 대금이 지불되도록 하여 디지털 콘텐츠거래에서의 공정성 문제를 해결하고자 하였다. 또한 조건암호기법을 이용하여 ES가 복호화에 필요한 정보를 제공하지만 ES에게 주어지는 정보만으로는 ES가 암호화된 콘텐츠를 복호화하는데 필요한 키를 획득할 수는 없으므로 판매자는 올바른 가격을 지불

한 정당한 구매자만이 콘텐츠를 획득할 수 있도록 하였다.

둘째, 평판 관리 서버인 RMS를 통해 구매자가 판매 피어에 대한 신뢰성을 평가할 수 있도록 하였다. 또한, 평판에 있어서 평판 값의 위조방지를 위해 평판 값을 보낼 때, 구매 피어의 서명을 포함하고, voting의 임의적인 삭제, 추가와 악의적인 사용자들(임의의 제3자)에 의한 평판 조작은 RMS에서 평판 값을 수렴하여 평판 인증서를 발행하게 하므로 신뢰성을 보장할 수 있는 '평판' 정보가 되도록 하였다.

셋째, 디지털 콘텐츠 거래 시 암호화된 콘텐츠를 제공 하여 불법적인 사용자들에 의해 변조되는 것을 막을 수 있다.

넷째, 모든 정보 거래 시 자신의 전자 서명을 이용하여 상호간에 보낸 메시지에 대해 부인 할 수 없도록 하였으며, 자신이 원하는 상대인지를 확인 할 수 있도록 하였다.

Ⅳ. 결론 및 향후 연구

본 논문에서는 최근 인터넷 기술의 발전으로 서버 중심으로 동작하는 기존의 전자상거래 방식에 중앙 서버 없이 서비스 이용자들 간의 직접적인 통신에 의해 거래가 이루어지는 P2P 서비스를 적용한 새로운 상거래 모델을 제안하였다.

제안 모델은 P2P 기반의 디지털 콘텐츠 판매의 안전한 거래를 위해, 판매자의 평판 값을 이용하여 신뢰도를 확인할 수 있도록 RMS 서버를 두어 평판 인증서를 발행하는 방안을 설계하고 이를 구현하였다. 또한, P2P에 있어서 지불 문제와 공정한 교환 문제를 해결하기 위해 지불 중개 서버인 ES를 두어 지불에 관계된 문제를 해결하고자 하였다. 그리고, ElGamal 암호기법을 사용하여 ES가 복호화 키가 아닌, 키에 대한 정보 중 일부를 가지고 있으므로, 콘텐츠를 획득하여 복호화 할 수 있는 방법을 차단하였다. 따라서, 올바른 지불을 행한 구매자만이 콘텐츠를 복호화 할 수 있도록 하였다.

향후 연구과제로 P2P 기술의 계속적인 발전으로 파일 공유 분야로 제한되었던 P2P 기술의 응용 분야가 점점 다양해지면서 응용 분야에 따라 필요한 보안 요구 사항에 대한 연구와 P2P 기술의 표준화와 관련된 추가적인 연구가 필요할 것이며, 평판인증서인 RC에 대해서도 적용 분야에 따라 좀 더 추가적이고 세밀한 표준안과 연구가 필요할 것이다.

<참고문헌>

[1] Diogo R.ferreira, J.J.Pinto Ferreria, "Building an e marketplace on a Peer-to-Peer infrastructure", International Journal Computer Integrated Manufacturing, 2004.

[2] Petros Daras, Despoina Palaka, Venetia Giagourta, "A novel Peer-to-Peer payment", IEEE, 2003.

[3] Ji Won Jung, "A Fair and Reliable e-commerce Model InP2P Network", master's thesis Pukyong Nat'l Unvi., 2004.

[4] Fabrizio Cornelli, Ernesto Damiani, Sabrina De Capitani De Vimercati, "Choosing Reputable Servents in a P2P Network", WWW2002, 2002.

[5] Y. Watanabe, M. Numao, "Conditional Cryptographic Delegation for P2P Data Sharing", In Proceedings of International Security Conference(ISC 2002), LNCS 2433, pp.309-321, 2002.

[6] E. Damiani, S. Vimercati, S. Paraboschi, P. Samarati, F. Violante, "A Repuatation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Network." Conference on Computer and Communications Security archive Proceedings of the 9th ACM conference on Computer and communications security, pp.207-216, 2002.

[7] B. Ooi, C. Liau, K. Tan, "Managing Trust in Peer-to-Peer Systems Using Reputation-Based Techniques", The 4th International Conference on Web Age Information Management (WAIM), August 2003, Keynote Paper.

[8] 이만영, 김지홍, 류재철, 송유진, 염홍열, 이임영 공저, "전자상거래 보안 기술", 1999.

[9] (주)컨설팅베이, "P2P 차세대 인터넷의 대안", 2000.

[10] 김희락, "P2P 결제서비스의 현황과 전망", 대우경제리뷰, 2001.

[11] 김정곤, "전자상거래상의 인터넷 에스크로 서비스의 규제에 관한 연구", 정보기술과 데이타베이스 저널, pp.215 226, 2004.

[12] 전현성 외 4인역, "차세대 인터넷 P2P", O'REILLY, 한빛미디어.

[13] 서수석, 임규홍, 이종호, "P2P의 전자상거래 응용 및 발전방향에 관한 연구", 한국경영정보학회 춘계학술대회 논문집, pp.865-875, 2002.

감사의 글

논문의 완성을 앞둔 지금 대학원에 들어올 때부터 지금까지의 일들이 주마등처럼 지나갑니다. 힘들기도 하고 또 뿌듯하기도 한 시간들이었습니다. 지금 이렇게 생각해보니 도움을 받았던 사람들이 참 많았던 것 같습니다.

우선, 석사과정동안 알게 모르게 신경을 써주시면서 학문에 열중하도록 지도하고 이끌어주신 이경현 교수님께 누구보다 감사드립니다. 또한, 논문이 완성되기까지 아낌없는 충고와 조언을 해주셨던 윤성대 교수님과 여정모 교수님께도 감사드립니다. 그 밖에도 석사 과정동안 많은 가르침을 주신 전산정보학과 교수님들께 감사의 마음을 전합니다.

대학원 생활을 하는 동안 많은 도움을 주었던 종필선배, 철이선배, 혜란선배에게 고마운 마음을 전합니다. 특히, 제 논문이 완성되기까지 너무도 많은 도움을 주었던 영호선배와 정화선배 그리고 재귀선배에게 정말 감사하다는 말을 전하고 싶습니다. 그리고 연구실에 오는 걸 즐겁게 만들어 주었던 채덕이와 윤희에게도 고마운 마음을 전하며, 더불어 음으로 양으로 많은 도움을 받았던 학부생인 봉기, 민현이, 광규, 희숙이에게도 고마움을 전합니다. 지금은 졸업하고 없지만 항상 마음 편하게 대해 주었던 영경이와 지원이, 미선이에게도 또한 고마움을 전합니다.
그 밖에도 석사과정 동안 많은 격려와 따뜻함을 주었던 여러 선배, 동기, 후배들에게 감사의 마음을 전합니다.

공부하느라 제대로 돌보지 못하는 아들 민제를 사랑으로 돌보아 주셔서 걱정 없이 공부하고 일 할 수 있게 해주셨던 사랑하는 엄마, 아빠에게 감사의 마음을 전하며, 더불어 알게 모르게 도움을 주셨던 시어머니께도 감사의 마음을 전합니다.

끝으로, 결혼생활을 하면서 공부 할 수 있도록 누구보다 아낌없는 격려와 도움을 준 사랑하는 남편 김우경씨에게 감사의 마음을 전합니다. 또한,

엄마가 제대로 돌보아 주지 못했는데도 건강하게 자라준 나의 사랑하는 아들 민제에게도 미안하면서도 고마움을 전하며 이 글을 마칩니다.