공학석사 학위논문

P2P 방식을 이용한 안전한 e-Commerce 설계 및 구현

지도교수 이 경 현

이 論文을 工學碩士 學位論文으로 提出함

부경대학교 산업대학원

전 산 정 보 학 과

위 성 균

이 논문을 위성균의 공학석사
학위논문으로 인준함

2004년 12월 18일

주 심 이학박사 윤 성 대 

위 원 이학박사 신 상 욱 

위 원 이학박사 이 경 현 

<차 례>

<표 차례>

<그림 차례>

A secure e-Commerce design and implementation using P2P scheme

Sung-Kyun Wee

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

Abstract

The P2P service can share and exchange the resource with only related program in a different way of client/server method, which the P2P is the method of sharing with resource and service by exchanging them between computer and computer that are connected on network each other directly without via server computer.

We would like to suggest the secure model that is possible to operate the e-Commerce by a direct communication between a seller and buyer, which is using this kind of the characteristics and techniques of P2P method to the e-Commerce that the server takes a role of the middleman.

The suggested model guarantees the fairness of the exchange and payment of digital contents between a seller and buyer, and also guarantees the trust of the contents which is provided by a seller getting the reputation value from the buyer who has already used the contents.

1. 서 론

인터넷의 급속한 발전과 확산으로 인터넷 이용자 수가 증가하고, 인터넷 이용을 위한 기반 환경의 확충 및 개인용 컴퓨터의 이용 증가로 인터넷을 통한 각종 서비스 이용 및 활용 범위가 점차적으로 증가하고 있다. 그 중 인터넷을 통한 상거래 활동이 점차적으로 증가하면서 기존의 오프라인 상의 상거래가 단순히 온라인 적용을 넘어 급속한 속도로 변형 또는 이식되거나 여러 형태의 상거래 모델들이 결합하여 새로운 모델이 탄생하는 등 다양한 형태로 발전하고 있다[12]. 현재 전자상거래는 클라이언트-서버 방식으로 동작하므로 사용자들은 특정 서버에 의존하여 상거래 활동을 수행하며, 정보의 공유 영역 또한 제한적이며, 해당 서버에 문제가 생길 경우 더 이상 상거래를 유지하기 어려운 단점이 있다. 클라이언트-서버 방식이 가지고 있는 이러한 문제점을 보안하기 위해 등장한 P2P 기술은 서비스에 참여하는 각각의 컴퓨터들이 서버인 동시에 클라이언트로 동작하면서 중앙 서버 없이 직접 연결을 통해 서로의 자원에 대한 공유 및 교환을 할 수 있다[2].

이와 같은, P2P 기술을 전자상거래에 적용 시 상거래 서비스 이용자들은 중앙 서버 없이 직접 통신하면서 언제, 어디서나, 제약 없이 개인별 상거래나 경매를 수행할 수 있지만, 별다른 거래 안전장치가 제공되지 않아 피해가 우려되고 있는 실정이다. 이에 본 논문에서는 P2P 방식을 이용한 안전한 e-Commerce의 설계를 제안하고 구현 하고자 한다.

제안하는 설계에서 상거래 대상은 디지털 컨텐츠이고, 컨텐츠 교환 및 지불시 보증 서버를 통하여 거래 당사자들 간의 공정성(fairness)을 보장해 주고, 구매한 컨텐츠를 이용한 피어들로부터 받은 해당 컨텐츠에 대한 평판값을 기반으로 컨텐츠 구매에 대한 신뢰성을 향상시킬 수 있다.

본 논문의 구성은 다음과 같다. 제2장에서 관련 연구로 P2P와 e-Commerce의 개요에 대해 살펴보고, 제3장에서 P2P 방식을 이용한 e-Commerce 모델의 설계를 설명하며, 제4장에서는 본 논문에서 제안하는 안전한 P2P e-Commerce의 구현을 설명한 후 제5장에서 결론을 맺는다.

2. 관련 연구

2.1. P2P (Peer-to-Peer) 개요

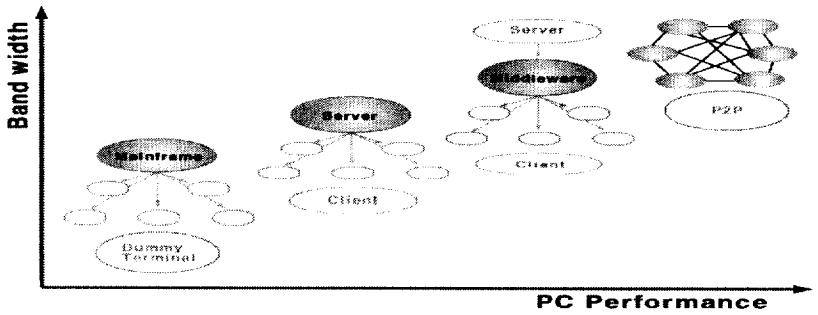
P2P 기술은 고성능 중앙서버나 광대역 네트워크 없이도 정보를 찾는 사람과 정보를 가진 사람의 컴퓨터 간에 직접적인 연결을 통해 다양한 정보를 공유할 수 있도록 하는 기술과 그 기술을 응용하여 제공되는 서비스들의 집합을 의미한다.

소리바다와 Napster, e-Donkey와 같은 파일 공유 서비스와 인스턴트 메신저 같은 실시간 커뮤니케이션 서비스 등을 통해 기술적 잠재력을 입증했던 P2P 기술은 저비용과 고효율로 정보 확산에 편리하고, 파일공유 뿐만 아니라 CPU나 디스크와 같은 컴퓨팅 자원의 공유, 온라인 협업, 전자거래 등으로 응용 분야가 확대되고 있다[4].

P2P 기술을 이용한 서비스 형태는 비슷한 성능을 가진 컴퓨터끼리 연결되어 동작하는 순수P2P(Pure P2P) 방식과 컴퓨터간의 상호 작용을 원활히 해주기 위한 서버가 개입되어 있는 혼합형 P2P(Hybrid P2P) 방식이 있다[7]. P2P 서비스 이용에 있어 장점은 특정 서버에 문제가 발생하더라도 모든 사용자에게 서비스가 중단되는 경우가 발생하지 않으며, 네트워크에 연결되어 있는 여러 사용자들이 가진 정보에 대하여 손쉬운 공유가 가능하다. 한편, 피어 프로그램의 유지 보수 부담이 있고, 시스템 운영의 안정성과 신뢰

도 문제, 그리고 개방되고 분산되어 있는 만큼 P2P 작업을 수행하는 사용자들의 책임성이 요구된다. 또한, P2P서비스를 이용하는 참여자가 항상 온라인 상태로 유지되어야 하고, 악의적인 소프트웨어의 손쉬운 분배로 인하여 보안 문제를 야기 시키는 단점이 있다[4].

P2P 기술은 컴퓨터와 다른 디바이스 간에 서버 없이 직접적인 교환을 통해 디지털 자원(예: CPU, 하드디스크, 파일 등)을 함께 공유하는 기술로 자원 공유(파일공유: 디지털콘텐츠, 장치공유: 하드디스크, CPU)와 이니셜 커뮤니케이션(서버 중개의 커뮤니케이션은 물론 개인간 직접적인 커뮤니테이션도 가능) 및 인프라스트럭쳐(모든 네트워크:WAN/NAN/PAN, 인터넷, 인트라넷, 홈 네트워킹) 등에 활용할 수 있다. P2P 기술의 발전이 있기까지의 네트워크의 변화단계는 [그림 1]과 같다[14].



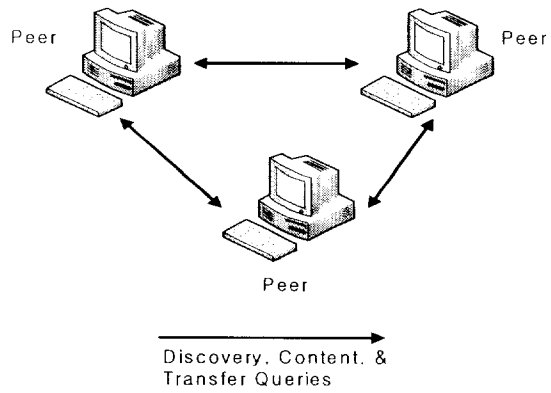
[그림 1] 네트워크의 변화 (Source: EON Group)

2.1.1. P2P 서비스 모델

P2P 서비스 모델은 구현 구조에 따라 순수 P2P 모델(Pure P2P)과 혼합형 P2P 모델(Hybrid P2P)로 구분할 수 있다[6][14].

(1) 순수 P2P 모델(Pure P2P)

이 모델은 피어들 간의 정보교환을 위해 중앙 서버에 의존하지 않고 동작하는 완전 분산형 모델로 관리 역할을 담당하는 중앙 서버가 없기 때문에 네트워크에 연결된 피어들을 스스로 동적으로 찾아야 하지만 서버에 지정된 규칙에 의해 실행되는 전통적인 서버/클라이언트 모델과는 달리 사용자들 자신이 나름대로의 규칙을 자율적으로 지정할 수 있고, 그들 자신의 네트워크 환경을 설정할 수 있게 해준다. 순수 P2P 모델은 필요한 정보의 검색을 위해 피어들간에 질의를 보내는 작업이 중복해서 발생하므로 네트워크 트래픽의 과부하로 인해 전체 대역폭이 증가하여 네트워크 전체의 효율성과 피어 검색의 효율성을 저하시킬 수 있다. 이와 같은 방식으로 동작하는 P2P 모델로 Gnutella와 FreeNet이 대표적이다. 순수 P2P 모델의 구성은 [그림 2]와 같다.

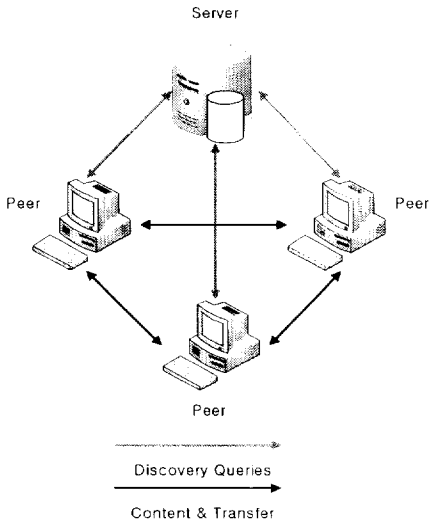


[그림 2] 순수 P2P (Pure P2P)

(2) 혼합형 P2P 모델(Hybrid P2P)

중앙 서버를 통해 각 피어들에게 자원 공유 기능을 지원하는 모델로 서비스를 제공할 수 있는 중앙 서버(centralized server)와 실질적인 공유 자원을 가지고 있는 피어들로 이루어진다. 중앙 서버는 각 피어들로부터의 네트워크 연결 세션을 유지함으로써 각 피어들 간의 통신에 대한 중재 역할을 수행하고, 연결되어 있는 피어들의 GUID(Global Unique IDentifier), 공유 자원들에 대한 메타데이터 등을 유지할 수 있고, 자원의 검색 기능과 기타 통신 기능 등을 제공할 수 있다. 피어들은 서비스를 제공하는 중앙 서버에 접속하여 원하는 자원을 보유한 피어를 검색하게 되지만, 일단 다른 피어와의 네트워크 세션이 성립되면 중앙 서버의 참여 없이도 상호간 정보 교환을 진행할 수 있다. 또한, 기존 클라이언트-서버 네트워크 구조에서 사용자들이 특정 파일을 중앙 서버로부터 받아감으로써 발생되는 네트워크 트래픽을 일반 피어들에게 분산시키기 때문에 각 피어들의 자원을 빠른 속도로 공유할 수 있다는 장

점을 가지고 있지만, 자원의 공유를 위해서는 모든 피어들이 일단 중앙서버에 연결해야 하기 때문에 클라이언트-서버 모델의 중앙서버로 인한 단점을 일부분 가지게 된다. 이와 같은 방식으로 동작하는 P2P 모델로 Napster가 대표적이다. 혼합형 P2P 모델의 구성은 [그림 3]과 같다.



[그림 3] 혼합형 P2P (Hybrid P2P)

2.1.2. P2P 활용

P2P 서비스의 활용 분야를 다음과 같이 분류할 수 있다[14].

(1) 기존의 엔터프라이즈 분야

피어(peer)의 권한과 성질, 능력에 따라 기능을 분산함으로써 비용 절감효과를 가져온다.

(2) 사용자 중심의 End-User 및 서비스 분야

컨텐츠 비즈니스(file sharing), 분산 컴퓨팅(grid), 커뮤니티 서비스, 게임 등에 사용된다. 커뮤니티 서비스의 예로 ICQ는 전 세계 6200만 명의 사용자를 가지고 있는 대표적인 인스턴트 메신저이다. 사용자가 ICQ를 자신의 PC에 설치하고, 이메일 주소나 ID, ICQ 번호 등을 이용하여 통신할 상대자를 자신의 PC에 있는 ICQ 프로그램에 저장하면, 상대자가 허용할 경우 상대자 IP 주소를 이용하여 직접 메시지 통신할 수 있게 된다.

(3) 전자 상거래 분야

P2P를 통한 완전한 공급망을 구축해주며, 콘텐츠, 정보, 소프트웨어의 분산 및 분산관리를 통해 전자상거래의 복잡성을 단순화시켜준다. 현재 알려진 P2P 방식을 이용한 최초의 전자상거래 방식으로 Open4u가 있다. 이 서비스는 사용자가 Open4u 서버에 접속하여 P2P 프로그램인 오프너를 다운로드 받아 설치하고, 구매자의 경우 이 프로그램을 이용해 자신이 구매하고 싶은 물품의 사양을 적어 메시지를 보내면 중앙 서버인 Open4u 서버가 이 사양의 물품을 제공할 수 있는 판매자의 IP 주소를 구매자에게 전달한다. 이 정보를 가지고 구매자는 P2P 방식으로 각 판매자에게 견적 요구서를 보낸다. 견적 요구서를 받은 판매자는 견적서를 구매자에

게 보내며 구매자를 여러 견적서 중 적합한 하나를 고르게 된다. Open4u의 서버는 최종 거래가 어느 조건으로 성립되었는지에 대한 정보만 확보하고 두 당사간의 거래에는 개입하지 않는다.

2.2. e-Commerce 개요

e-Commerce(Electronic Commerce)는 인터넷이 보편화되기 이전에도 기업간 문서를 전자적 방식으로 교환하거나, PC통신의 홈쇼핑, 홈뱅킹 등 다양한 형태로 존재해 왔으나, 인터넷이 대중화되면서 전자상거래는 인터넷상에서의 거래와 관련지어 생각하게 되었다. e-Commerce는 최근 빠른 속도로 발전하고 있는 인터넷 관련 전자 정보기술을 활용하여 모든 거래 활동을 전자적으로 수행하고, 신속하고 정확한 정보를 교류함으로써 기업의 이윤을 대화하고 있다.

"전자상거래"라는 용어는 미국 국립 로렌스리 버모어 연구소(Lawrence Livermore National Laboratory)가 미국 국방성의 프로젝트를 수행하면서 처음으로 사용하기 시작하였다. 초기 전자상거래는 일종의 전용망인 VAN(Value Added Network)을 이용해 기업간 또는 정부와 기업간 전자적인 자료를 교환하는 EDI(Electronic Data Interchange)에 대한 연구에 집중되었는데, 전자상거래의 일반적인 확산은 인터넷의 상용화와 밀접한 관계를 갖는다[9]. 그러나, 이러한 e-Commerce용어의 기원뿐만 아니라 전자상거래의 개념 자체에 대해서 현재까지도 많은 논란이 있다. 일

반적으로 전자상거래는 온라인 네트워크를 통하여 이루어지는 모든 형태의 거래를 지칭하며, 최근에는 인터넷을 활용하는 데에만 국한되지 않고 전화, TV, 케이블TV, CD롬 등을 이용한 전자카탈로그, 사내전산망 등 다양한 정보통신매체를 이용하여 상품과 서비스를 전자적으로 유통시키는 모든 유형의 상업적인 행위를 뜻하는 것으로 확대되고 있다[10].

e-Commerce는 기존의 전통적인 상거래와는 다른 많은 차이점을 보이고 있다. 예를 들어 기존의 전통적 상거래의 유통 방법이 기업, 도매상과 소매상을 거쳐 소비자에게 전달되는 방식을 취한다. 그러나 전자상거래는 기업과 소비자를 곧바로 연결시켜주는 체계를 취하고 있다. 또한 전통적인 거래가 일부지역을 대상으로 한정된 범위를 갖고 있다면, 전자상거래는 전 세계적인 네트워크를 바탕으로 소위 "global marketing"이 가능하다는 차이가 있다.

현재 e-Commerce는 컴퓨터통신망을 통해 이루어지는 상품 및 서비스의 판매, 발주, 광고 등을 포함한 모든 경제 활동을 의미하는 것으로 인터넷상에서 기업과 소비자가 상품 및 서비스를 거래하는 것도 전자상거래에 포함된다. 전자상거래의 목적은 상거래의 신속화와 효율화를 실현하고자 하는 것으로 인터넷상에서 거래처의 선택을 비롯한 상품 구매, 가격 교섭, 계약 체결, 대금 결제 등 상거래에 관련된 모든 업무를 전자적으로 처리할 수 있는 환경을 만드는 것이다[3].

2.2.1. 전통적 상거래와 e-Commerce의 비교

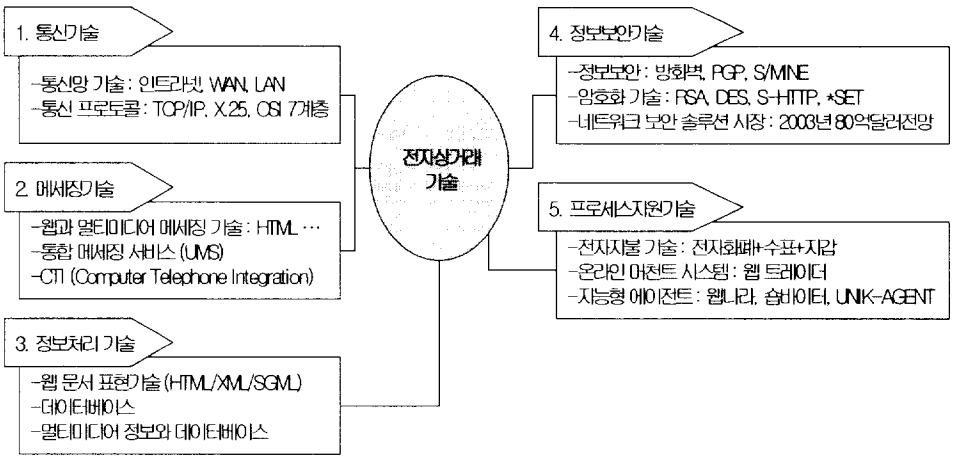
전통적 상거래 방식과 e-Commerce 방식의 차이점을 <표 1> 에서 비교하고 있다[11].

<표 1> 전통적 상거래와 전자상거래의 비교

구 분	전통적 상거래	e-Commerce
유통경로	기업-중간상인(도소매)-최종소비자	기업-최종소비자
거래시간	한정된 영업시간	24시간 가능
거래장소	한정된 물리적 시장 및 점포	인터넷 가상 공간 (사이버쇼핑몰 등)
거래지역	한정된 일부 지역	전세계 (Global Marketing)
거래수단	물리적 장비 및 시설	컴퓨터/통신기기
거래비용	토지, 건물 등 대규모 비용	서버 및 홈페이지 구축 등 상대적으로 적은 비용
마케팅	구매자의 의사와 관계없는 일방적 마케팅	쌍방향 통신을 통한 1:1 상호적 마케팅
고객대응	고객 불만에의 대응 지원 고객의 필요(요구)를 신속히 포착	고객 불만에 즉시 대응 고객 필요(요구) 포착이 느림
고객정보획득	시장조사 및 영업사원이 획득 정보의 재입력 필요	온라인에 의한 수식 회득 재입력이 필요없는 디지털 데이터
결제수단	현금, 수표, 신용카드 등 외상, 연불 허용	신용카드, 전자화폐, 전자수표 및 전자자금이체 등
거래서류	다량 필요	대폭 축소되거나 불필요
거래상 문제점	과다한 거래비용 및 시간소요 거래상의 불편	개인정보 노출 및 악용 우려 지적 재산권의 침해 과세상의 문제 등

2.2.2. e-Commerce 기반기술

전자상거래의 기반기술에는 전자서비스에 있어서 중요한 역할을 하는 네트워크의 통신기술, 웹과 멀티미디어의 메시징 기술과 이의 표현처리에 필요한 정보처리 기술 및 구매자와 판매자의 인증 및 상호 주고받는 정보의 변조가 없는 무결성을 포함한 정보보안 기술이 필요하게 된다. [그림 4]에서 e-Commerce 기반 기술을 나타내고 있다.



[그림 4] e-Commerce 기반 기술

3. P2P 방식의 안전한 e-Commerce 설계

3.1. 제안 모델의 개요 및 목표

본 논문에서 제안하는 e-Commerce의 설계는 P2P 서비스 방식 중 중앙 서버가 존재하는 혼합형 P2P 방식(Hybrid P2P)을 기반으로 한다. 이는 피어들의 중복되는 질의에 의한 네트워크 트래픽의 과부하로 발생하는 전체 대역폭 증가를 없애기 위함이며, 또한 각 피어(peer)간의 공정성 보장을 위한 보증서버(escrow server) 구축에 적합하기 때문에 혼합형 P2P 방식을 기반으로 한다[1][8].

기본 구성은 회원 및 컨텐츠 관리를 위한 서버(CS: Central Server), 컨텐츠 교환 및 지불에 있어 공정성을 보장하는 보증 서버(ES: Escrow Server)와 각 피어들로 구성된다. 제안 e-Commerce의 설계에서 서비스에 참여하는 모든 피어들은 인증된 피어이고, 서비스에 참여하는 개체들 간에 주고받는 모든 메시지는 안전하고 기밀성이 보장되는 채널을 통해 전송되는 것으로 가정한다.

중앙 서버는 서비스에 참여하는 피어들이 등록한 판매하고자 하는 컨텐츠에 대한 목록과 컨텐츠에 대한 신뢰도를 나타내는 평판값(trust)을 저장하고 있다. 컨텐츠 구매를 원하는 피어들은 중앙 서버가 제공하는 평판값을 참조하여 구매를 원하는 대상 피어를 결정할 수 있다. 또한, 본 논문에서는 컨텐츠 교환과 지불에 있어

판매 피어와 구매 피어 상호간에 공정성을 보장해 주기 위해 보증 서버를 사용하고, 이 서버는 신뢰된 서버로 가정한다. 판매 피어는 구매 피어로부터 컨텐츠 요청이 있을 경우 먼저 보증 서버에게 해당 컨텐츠를 전송한 후 구매 피어에게 전송하고, 구매 피어는 컨텐츠의 정당성 확인을 위해 판매 피어에게 받은 컨텐츠와 구매에 대한 지불 정보를 보증 서버로 전송한다. 보증 서버는 판매 피어로부터 받은 컨텐츠와 구매 피어로부터 받은 컨텐츠를 비교하여 일치할 경우 구매 피어에게 올바른 컨텐츠임을 알리고, 판매 피어에게 구매 피어로부터 받은 지불 정보를 전송한다.

지금까지 제안된 P2P 방식의 안전한 e-Commerce 구축의 기반인 P2P 시스템을 구축함에 있어서 보증 서버와 평판값 확인에 따른 사용자들에게 보다 안전한 e-Commercer의 지원에 목표를 둔다.

3.2. 기본 구성 요소

제안된 P2P 방식의 안전한 e-Commerce 구축에 따른 기본 구성 요소는 [그림 5]와 같이 구성되어 있으며 각 구성 요소는 다음과 같다.

1) 관리서버(CS: Central Server)

CS 구성은 회원에 대한 아이디, 비밀번호 및 평판값과 컨텐츠 목록에 대한 정보를 데이터베이스 관리를 통해 피어들의 요구가 있을 때 해당하는 응답 서비스를 제공하기 위한 구성요소이다.

2) 보증서버(ES: Escrow Server)

ES 구성은 거래에 공정성을 부여하기 위한 구성으로 판매피어와 구매피어 사이의 거래에 있어서 공정성 및 신뢰성을 부여해 준다.

3) 각 피어(peer: 판매피어, 구매피어)

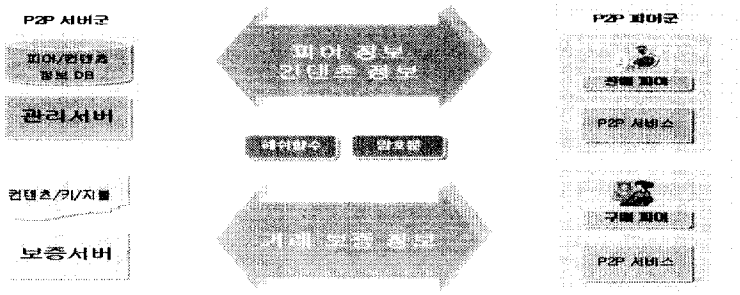
P2P e-Commerce를 이용하고자 하는 일반 사용자 군으로 이루어진다.

4) 해쉬 함수(hash function)

피어들의 로그인 및 피어들 간의 거래에 있어서의 안정성 제공을 위해 사용되는 함수로써 MD5, SHA-1, LMD, ELF 함수가 사용된다[15].

5) 암호문(cipher)

피어들 간의 거래에 사용되는 컨텐츠의 보호를 위해 사용되는 암호문으로써 Blowfish, Blowfish(CBC), DES, DES(CBC), Triple, Triple(CBC), Rijndeal, Rijndeal(CBC) 암호문이 사용된다[15].



[그림 5] 기본 구성 요소

3.3. 요구 사항

P2P 방식의 e-Commerce는 기존의 인터넷 환경에서 일어나는 상거래와 달리 구매자가 구매 의사가 있는 제품을 밝히면 서비스에 가입된 모든 제공자들에게 주문 내용이 실시간으로 전달되고, 해당 제품의 제공자는 견적을 구매자에게 보내며, 구매자는 여러 제공자들로부터 받은 견적 가운데 가장 유리한 업체를 선택하여 직접 연락을 취하는 형태로 이루어진다. 이 경우 구매자는 제품 구매를 위해 들이는 웹 서핑 시간이나 검색 시간을 줄일 수 있고, 중간 브로커를 거치지 않고 제공자와 직접적인 연결을 통하여 거래가 가능하기 때문에 수수료가 들지 않으며, 특정 지역이나 특정 업종을 지정할 수 있는 장점을 가진다[13]. P2P 방식을 이용한 전자상거래는 실제 구현에 있어 다음과 같은 요구 사항을 필요로 한다. [그림 6] 설계 시 요구 사항을 나타내고 있다.

1) 공정성

정보의 신뢰성 및 공정성을 향상시키기 위해, 정보를 이중으로 검사하는 것이 필요하게 된다. SETI@home에서는 같은 데이터에 의한 계산을 이중으로 실시하고 그 사이에 차이가 있는지를 검사해서 정보의 신뢰성 및 공정성을 확보하고 있다. 제안되는 P2P 방식의 e-Commerce에서도 구매자와 판매자간에 서로가 원하는 정보를 모두 다 가질 수 있거나 둘 다 가지지 못함을 보장할 수 있어야 한다.

본 제안 설계에서는 ES에서 판매피어와 구매피어에서 받은 각 컨텐츠 값을(암호화된 컨텐츠 값의 암호처리) 비교 처리함으로써 공정성을 보장하도록 하고 있다. 해쉬 함수는 MD5, SHA-1, LMD 및 ELF을 랜덤하게 선택해서 사용하게 하여 보다 안전한 공정성을 가지게 한다.

2) 기밀성

P2P에서는 파일 접근 제어, 파일의 암호화, 접근 로그 관리의 기능을 어떻게 PC에서 구현할 것인지가 배포의 한 조건이 된다. P2P 소프트웨어는 상황에 따라 사용자를 제한할 수 있어야 한다. 현재의 PC의 기본 소프트웨어에는 이러한 기능이 없거나 또는 불충분하기 때문에 차후에 이에 대한 개선이 필요하며 또한 구매 피어와 판매 피어 간에 주고받는 정보는 허가되지 않은 제 3자로부터 보호되어야 한다.

본 제안 설계에서는 컨텐츠의 암호화에 의해 기밀성을 유지하고 있다. 암호화는 Blowfish, Blowfish CBC, DES, DES CBC, Triple, Triple CBC 및 Rijndael, Rijndael CBC을 랜덤하게 선택해서 사용하게 하여 보다 안전한 기밀성을 가지게 한다.

3) 무결성

P2P에서는 정보의 무결성을 확보하기 위해 네트워크 트래픽의 증가 제어, 바이러스 침입방지, 정보의 신뢰성 향상 등이 과제가 된다.

본 제안 설계에서는 구매 피어와 판매 피어 간에 주고받는 정보는 불법적인 사용자에 의해 변조되어서는 안 되게 하는데 주안점을 두

고 있다. 각 피어의 평판값, 로그인 암호화 및 컨텐츠의 암호화를 중심으로 외부 침입을 방지하고 정보의 신뢰성을 높여주게 된다.

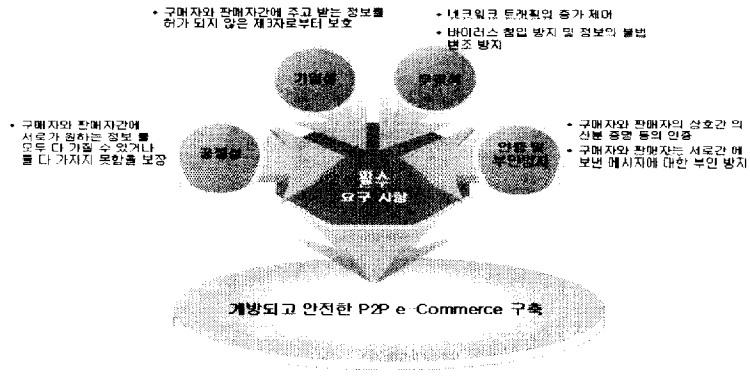
4) 인증

구매 피어와 판매 피어는 상호간에 정보를 전달할 때 자신이 원하는 상대인지를 확인할 수 있어야 한다. 인증에 있어서 컨텐츠 소유권자와 사용자의 신분 증명과 전자 투명을 이용해 정보가 수정되었는지를 검사할 수 있다.

본 제안 설계에서는 CS(Central Server)에서 피어들의 평판값을 활용하여 상대에 대한 신뢰성을 부여하며, 기본 피어정보를 관리하여 피어 인증에 있어서 투명성을 제공해 준다.

5) 부인방지

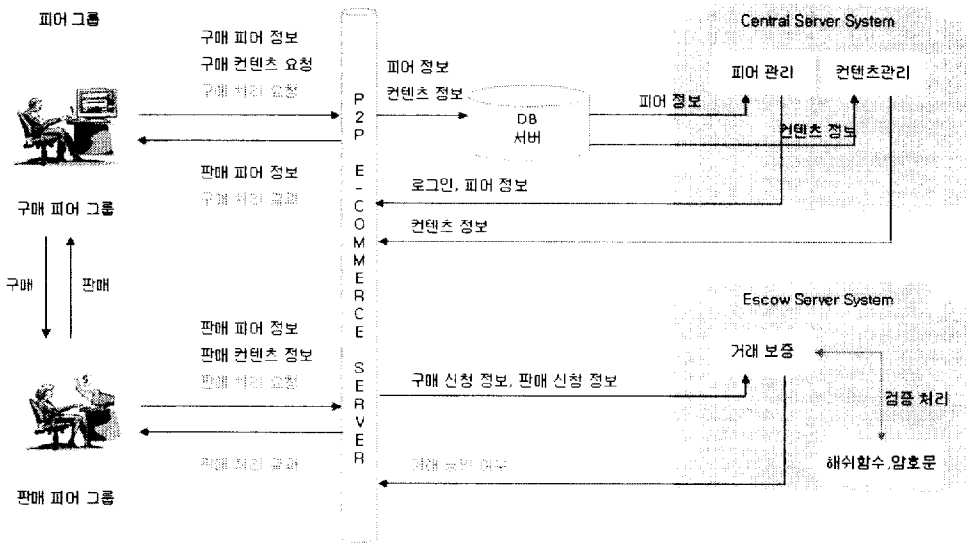
구매 피어와 판매 피어는 서로 간에 보낸 메시지에 대해 부인할 수 없어야 되며, 본 논문 거래 내역을 EC에서 관리함으로써 부인방지를 예방하게 한다.



[그림 6] 설계 시 요구 사항

3.4. 시스템 구성체계 및 연계방안

본 논문에서 제안하는 P2P 방식의 안전한 e-Commerce 설계는 TCP/IP 프로토콜을 중심으로 상호간 동작하게 된다. 기본적인 연계방안 및 구성체계는 [그림 7]과 같이 이루어진다.



[그림 7] 시스템 구성체계 및 연계방안

1) CS와 각 피어간의 연계 및 구성

CS에서는 각 피어들의 정보(아이디, 비밀번호, 평판값 및 컨텐츠 목록)를 보유하고 있으며, 각 피어들은 CS를 통해 로그인 및 컨텐츠들을 등록/검색하게 된다. 사용되는 구성으로는 각 피어들과 CS, 해쉬함수 및 암호문들이 사용되며 초기 피어에서의 CS접속 시 CS에서 사용할 해쉬 함수 색인키(MD5, SHA-1, LMD, ELF)와 암호

문 색인키(Blowfish, Blowfish CBC, DES, DES CBC, Triple, Triple CBC, Rijndael, Rijndael CBC)를 넘겨주게 되며, 넘겨받은 색인키를 이용해서 피어들은 로그인 시 아이디를 암호화(암호화키는 비밀번호를 해쉬한 값으로 처리)하며 비밀번호를 해쉬 함수 처리해서 로그인 승인을 받게 된다. 이는 암호화와 해쉬 함수 처리를 통한 피어들의 정보를 보호기 위함이다. 컨텐츠의 등록 및 검색은 평문을 통해 이루어지게 된다.

2) ES와 각 피어간의 연계 및 구성

ES에서는 각 피어들 간의 거래에 있어서 보증을 위한 정보만을 가지고 있으며, 이 정보를 통해 각 피어들에게 거래의 승인 여부를 부여하게 된다.

판매피어의 경우 구매요청이 일어날 경우 구매피어에게는 공정성 부여에 사용될 컨텐츠 해쉬 값과 해당 컨텐츠 내용을 암호화(Blowfish, Blowfish CBC, DES, DES CBC, Triple, Triple CBC, Rijndael, Rijndael CBC)하여 전송하게 되며, ES에게는 검증에 사용될 컨텐츠 해쉬 값과 복호화에 사용될 암호문의 색인키(Blowfish, Blowfish CBC, DES, DES CBC, Triple, Triple CBC, Rijndael, Rijndael CBC)와 복호화 키를 전송하게 된다.

구매피어의 경우 구매 결정 시 판매피어에게 받은 정보 내용 중 컨텐츠 해쉬 값과 지불 방법을 ES에게 전송하게 된다.

ES에서는 각 판매피어와 구매피어로부터 받은 컨텐츠 해쉬 값을 비교하여 정당성 확인을 하게 되며, 올바른 거래가 이루어질 경우

판매피어에게는 지불 방법을 전송하게 되며, 구매피어에게는 복호화에 사용될 암호문 색인값과 키를 전송하게 된다.

3) 각 피어들 간의 연계 및 구성

각 피어들은 P2P e-Commerce에 있어서 암호화된 정보를 송/수신 함으로써 안전한 거래를 보장 받을 수 있게 된다.

4) 해쉬 함수와 암호문 색인키 적용의 구성

기본적인 해쉬 함수는 MD5, SHA-1, LMD 및 ELF를 사용하게 되며 각 0:MD5, 1:SHA-1, 2:LMD, 3:ELF의 색인 값을 갖게 된다. 각 피어들의 로그인 경우에는 CS에서 랜덤(random)한 색인 값을 각 피어들에게 부여하게 되며, 거래가 이루어질 경우에는 판매피어에서 랜덤하게 값을 부여하여 보증을 위한 컨텐츠 해쉬에 사용하게 된다.

암호문은 Blowfish, Blowfish CBC, DES, DES CBC, Triple, Triple CBC, Rijndael 및 Rijndael CBC를 사용하게 되며 각 0:Blowfish, 1:Blowfish CBC, 2:DES, 3:DES CBC, 4:Triple, 5:Triple CBC, 6:Rijndael, 7:Rijndael CBC의 색인값을 갖게 된다. 암호문 또한 각 피어들의 로그인 경우에는 CS에서 랜덤(random)한 색인 값을 각 피어들에게 부여하게 되며 해당 암호문을 활용하여 피어들의 아이디를 보호해 주게 된다. 거래가 이루어질 경우에는 판매피어에서 랜덤하게 값을 부여하여 컨텐츠를 암호화 하며 구매피어에게는 암호화된 컨텐츠 내용을 전송하게 되며, ES에게는

복호화에 사용될 키를 전송하게 된다.

5) 피어들의 신뢰도를 나타내는 평판값 구성

본 논문에서 제안하고 있는 평판값 생성은 피어들의 신뢰도를 나타내는 척도로 활용된다. 평판값 구성에 있어서 초기값은 0의 값을 가지게 되며 범위는 -50에서 100으로 구성하였다. 평판값 부여 방식은 <표 2>와 같이 부여하기로 한다.

<표 2> 평판값 부여

발 생 구 분	평 판 값 부 여	비 고
거래완료	판매피어: +0.03 구매피어: +0.02	-
구매피어의 거래취소 (수령 후 지불방식 미 수행)	판매피어: +0.00 구매피어: -0.01	암호화된 컨텐츠 자동 삭제
판매피어의 불법거래	판매피어: -1.03 구매피어: +0.00	대칭키 오류
구매피어의 불법거래	판매피어: +0.00 구매피어: -1.02	거래완료 후 대금 미지급
판매피어의 시스템장애	판매피어: -0.01 구매피어: +0.00	거래도중 미 응답
구매피어의 시스템장애	판매피어: +0.00 구매피어: -0.01	거래도중 미 응답
연속적인 불법거래 (3회 초과 시 매회)	판매피어: -10.0 구매피어: -10.0	불법거래 추가 평판값 부여
연속적인 시스템장애 (3회 초과 시 매회)	판매피어: -5.00 구매피어: -5.00	시스템장애 추가 평판값 부여
평판값 -5099 미만 발생	-	해당 피어 거래 중지
평판값 100 초과 발생	-	평판값 변화 없음 (거래 건수 만 추가)

4. P2P 방식의 안전한 e-Commerce 구현

4.1. 개요

본 논문에서 제안하는 P2P 방식을 이용한 안전한 e-Commerce의 설계 방안을 기본으로 CS(Central Server) 프로그램, ES(Escrow Server) 프로그램 및 피어(peer) 프로그램을 구현을 하게 된다. 각 프로그램 이름은 LPPCS.exe, LPPES.exe 및 LPP.exe로 명명하게 된다.

4.2. 표기법

본 논문에서 사용되는 표기법은 다음과 같다.

1) CS(Central Server)

서비스에 참여하는 피어의 ID와 피어들이 등록한 컨텐츠 목록, 피어들의 평판값을 저장하는 서버

2) ES(Escrow Server)

컨텐츠 거래 및 지불에 있어 공정성 보장을 위해 사용하는 서버

3) $I(E), I(H)$

사용할 암호문의 색인값(0:Blowfish, 1:Blowfish CBC, 2:DES, 3:DES CBC, 4:Triple, 5:Triple CBC, 6:Rijndael, 7:Rijndael CBC), 해쉬 함수 색인값(0:MD5, 1:SHA-1, 2:LMD, 3:ELF)

4) P_i, P_{ID}, P_{PASS}

컨텐츠 판매피어 또는 구매피어 식별자, 아이디, 비밀번호

5) K, k

컨텐츠 암호화를 위해 생성한 대칭키

6) $E_k(M)$

개체 M에 대해 대칭키를 사용한 암호화

7) $H(M)$

개체 M에 대해 암호학적 해쉬 함수 처리를 수행

8) L

CS 상태를 나타내는 값(FULL: 접속 피어 초과, LINK: 정상 접속)

9) $desc_{P_i}$

피어들이 등록한 컨텐츠 정보

10) *trust*

피어들의 평판값

11) C

거래 대상 컨텐츠(이미지, 음악파일 등의 디지털 컨텐츠)

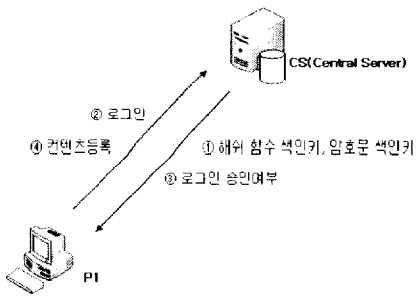
12) $pay\_info_{P_i}$

구매 피어가 제공하는 지불 정보

4.3. 운영절차 및 동작과정

제안 설계의 운영절차 및 동작과정은 [그림 8], [그림9]와 같은 절차를 통해 발생하게 된다.

1) 초기 CS 접속, 로그인 및 컨텐츠 등록



[그림 8] CS 접속, 로그인 및 컨텐츠 등록

① CS → P1: $Connect(I(E), I(H))$

CS 서버와 피어간의 접속이 이루어지게 되면 초기 CS 서버와 피어 사이에서 사용될 암호화 인덱스 지정 값과 해쉬 함수 지정 값을 해당 피어에게 전송한다.

② P1 → CS: $Login(Ek(P_{ID}), H(P_{PASS}))$

P1은 지정받은 암호문과 해쉬 함수를 사용하여 CS에 로그인 정보(피어 ID, 피어 비밀번호)를 전송한다. 기본적인 대칭키는 피어 사용 포트 값으로 설정한다.

③ CS → P1: $Link(L)$

CS는 P1에게 사용 가능 여부를 전송한다.

④ P1 → CS: $Register(P_{1,}, desc_{P_1})$

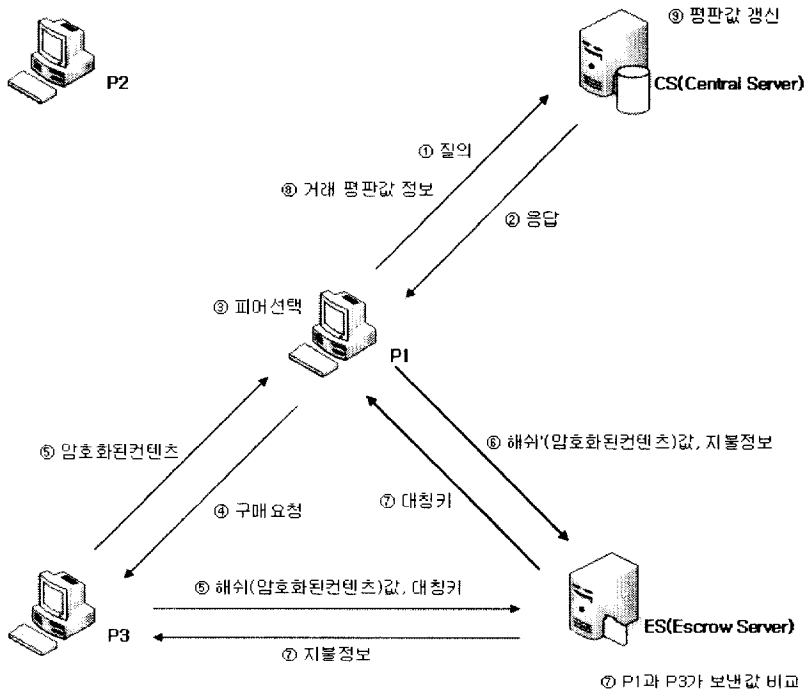
서비스에 참여하는 피어들은 자신이 가진 컨텐츠 중 판매하고자 하는 컨텐츠 목록을 CS에 등록한다. CS가 관리하는 피어들에 대한 정보는 다음과 같다.

$< P_{1,} desc_{P_1}, trust >$

각 항목은 컨텐츠 목록을 등록한 피어의 ID, P1이 등록한 컨텐츠 정보 그리고 P1의 평판을 나타내는 값으로 서비스 이용을 위해 처음 로그인한 피어들의 trust 값은 0으로 초기화되고, 컨텐츠를

구매한 피어들이 컨텐츠 확인 후 서버에게 trust 값을 전송한다. trust 값은 컨텐츠 구매를 원하는 피어들이 해당 컨텐츠에 대한 신뢰도를 참조하도록 하기 위해 사용된다.

2) 구매(판매) 피어의 컨텐츠 구매(판매)



[그림 9] 구매(판매) 피어의 컨텐츠 구매(판매)

① P1 → CS : *Query(desc)*

P1는 컨텐츠 구매를 위해 필요로 하는 컨텐츠에 대한 질의를 CS에게 전송한다.

② CS → P1 : $Response(P_i, trust)$

CS는 P1가 요청한 컨텐츠를 가지고 있는 피어 ID와 해당 피어가 제공하는 컨텐츠에 대한 평판값을 함께 전송한다.

③ P1 : *Select*

P1는 CS로부터 받은 목록 중 컨텐츠에 대한 평판값을 나타내는 "trust" 값을 참조하여 하나의 피어 P3을 선택한다.

④ P1 → P3 : $Request(C)$

선택한 피어 P3에게 컨텐츠 구매 의사를 알린다.

⑤ P3 → ES : $Send(P_3, P_1, H(E_k(C)), K)$

⑤ P3 → P1 : $Send(E_k(C))$

P3은 P1의 요청에 따라 컨텐츠를 판매하기 전 컨텐츠 거래와 지불에 대한 공정성을 보장 받기 위해 먼저 판매할 컨텐츠를 암호화하여 해쉬한 값과, 컨텐츠 복호화에 필요한 키를 ES에게 전송한 다음 암호화된 컨텐츠를 P1에게 전송한다.

⑥ P1 → ES : $Send(P_1, P_3, H'(E_k(C)), pay\_info_{P_1})$

P1은 컨텐츠에 대한 정당성 확인과 지불을 위해 P3으로부터 받은 암호화된 컨텐츠에 해쉬한 값과 컨텐츠 판매 피어의 ID 및 지불 정보를 ES에게 전송한다.

⑦ ES : $Compare(H(E_k(C)), H'(E_k(C)))$

⑦ ES → P3: $Send(pay\_info_{P_1})$

⑦ ES → P1: $Send(K)$

ES는 P1과 P3으로부터 받은 $H(E_k(C))$값과 $H'(E_k(C))$값을 비교하여 해쉬 값이 동일할 경우 P3으로부터 올바른 컨텐츠 전달이 이루어진 것으로 보고 컨텐츠를 복호화 할 수 있는 키를 P1에게 전송하고, P1이 보낸 지불 정보를 확인하여 유효하면 P3에게 컨텐츠에 대한 지불 정보 $pay_info_{P_1}$을 전송한다. 만약 P1과 P3으로부터 받은 해쉬 값이 동일하지 않을 경우 AS는 컨텐츠 교환이 제대로 수행되지 않은 것으로 판단하여 P1과 P3에게 통보하고 작업은 종료된다. 지불의 경우에도 동일하다. 이와 같이 ES는 판매 피어와 구매 피어 간의 컨텐츠 교환 및 지불에 있어 어느 한 피어가 컨텐츠를 받고 지불을 하지 않거나 반대의 경우가 발생하는 것에 대해 중재자 역할을 수행하며 피어간의 공정성을 보장해 준다.

⑧ P1 → CS : $Send(P_1, P_3, trust)$

P1는 구매한 컨텐츠를 사용한 후 컨텐츠의 정확성 여부에 따라 CS에게 해당 컨텐츠에 대한 신뢰도에 해당하는 "trust" 값을 전송한다. "trust" 값은 현재 거래 상태값을 뜻하며 상태 값에 따라 CS에서 자동 갱신하게 된다.

⑨ CS : $Update(trust)$

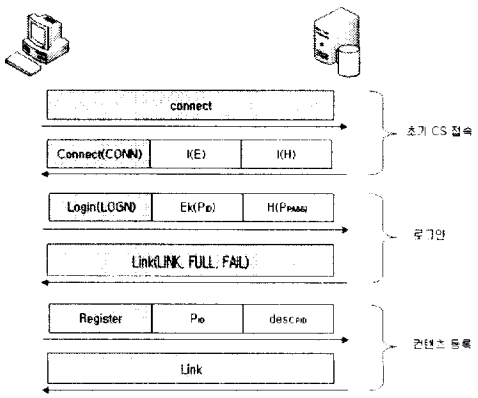
CS는 컨텐츠를 구매한 피어들로부터 받은 “trust”(현재 거래 상태) 값을 이용하여 <표 2> 에 해당하는 값을 갱신하고 새로운 컨텐츠 교환이 발생할 경우 항상 최신의 평판값을 참조할 수 있도록 제공해 준다.

4.4. 주요 흐름도 및 프로토콜

구현에 있어서 주요 흐름도 및 프로토콜은 제안하는 설계에 따라 다음과 같이 구성되어 지며, 표기 방식은 차례 4.2 표기법을 적용해서 나타낸다.

1) 초기 CS 접속, 로그인, 컨텐츠 등록 및 검색(CS에서 처리)

개별 피어에서의 초기 접속, 로그인 과정 및 상품 등록에 있어서의 CS흐름도 및 프로토콜 정의는 다음과 같이 구성된다. [그림 10]은 기본 프로토콜을 나타내고 있다.



[그림 10] 초기 접속, 로그인 및 컨텐츠 등록 프로토콜

- 초기 CS 접속

피어 프로그램에서 CS로 초기 접속이 이루어지게 되면 CS에서는 사용할 암호문 색인 키와 해쉬 함수 색인 키를 전송하게 된다. 암호문 색인키는 0:Blowfish, 1:Blowfish CBC, 2:DES, 3:DES CBC, 4:Triple, 5:Triple CBC, 6:Rijndael, 7:Rijndael CBC로 구성되며 해쉬 함수 색인키는 0:MD5, 1:SHA-1, 2:LMD, 3:ELF 로 구성되어진다. [그림 11]에서 프로그램 소스에 적용된 부분을 보여준다.

```
procedure TFComm.IdTCPServerIConnect(AThread: TIdPeerThread);
{*****************************************************************************}
{* 초기 피어 접속
{*****************************************************************************}
var
  Peer: TOPeerData;
  ListItem: TListItem;
  SendMsg: string;
begin
  if PubPeerData.Count >= MAX_PEER then begin
    AThread.Connection.WriteLn(CMD_FULL);
    AThread.Connection.Disconnect;
    Exit;
  end;

  Randomize;
  Peer := TOPeerData.Create;
  Peer.ID := 'Idleing...';
  Peer.IP := AThread.Connection.Socket.Binding.PeerIP;
  Peer.Host := 0;
  Peer.Session := AThread.Connection.Socket.Binding.PeerPort;
  Peer.Trust := 0;
  Peer.Encrypt := Random(8);
  Peer.Hash := Random(4);
  Peer.Link := PubPeerData.Count; //LisvPeer.Items.Count;
  Peer.Thread := AThread;

  SendMsg := CMD_EKEY+IntToStr(Peer.Encrypt)+IntToStr(Peer.Hash);
  AThread.Connection.WriteLn(SendMsg);

  AThread.Data := Peer;
  PubPeerData.Add(Peer);

  ListItem := ListView1.Items.Add;
  ListItem.Caption := Peer.ID;
  ListItem.SubItems.Add(Peer.IP);
  ListItem.SubItems.Add(IntToStr(Peer.Host));
  ListItem.SubItems.Add(IntToStr(Peer.Session));
  ListItem.SubItems.Add(IntToStr(Peer.Trust));
  ListItem.SubItems.Add(TxtEncrypt[Peer.Encrypt]);
  ListItem.SubItems.Add(TxtHash[Peer.Hash]);
end;
```

[그림 11] CS 소스 (CS 초기 접속)

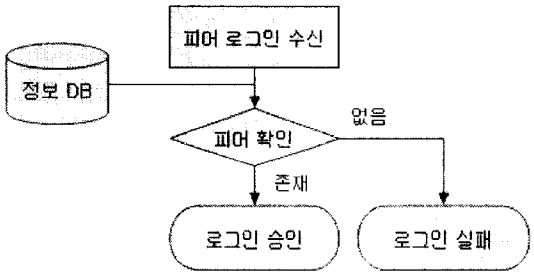
- 로그인

CS로부터 받은 색인키를 이용해서 암호화 및 해쉬 함수 처리로 안전한 로그인이 가능하도록 한다. [그림 12]에서 프로그램 소스에 적용된 부분을 보여준다.

```
procedure TFLogin.Timer1Timer(Sender: TObject);
{*****************************************************************************}
{* TCP/IP
{*****************************************************************************}
begin

  ...

 else if Cmd = CMD_CONN then begin
    Desc := Copy(Msg,8,1);
    SendMsg := SendMsg + FDM.EncryptString(UpperCase(Trim(EditPeer.Text)), UpperCase(Trim(EditPass.Text)), StrToIntDef(Desc,0));
    Desc := Copy(Msg,9,1);
    SendMsg := SendMsg + CMD_TABS + FDM.MakeHash(UpperCase(Trim(EditPass.Text)), StrToIntDef(Desc,0));
    ItccCentral.WriteLn(CMD_LOGN+SendMsg);
   end

  ...

end;
```

[그림 12] LPP 소스 (색인키 수신 후 로그인 정보 전송)

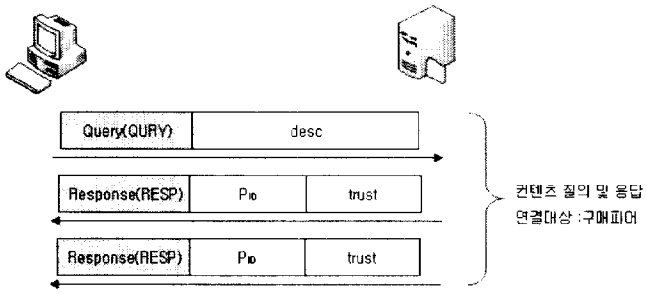
암호화된 로그인 정보를 가지고 CS에서 로그인 승인을 하게 된다. 기본 흐름도는 [그림 13]과 같다.



[그림 13] CS 에서의 로그인 흐름도

- **컨텐츠 검색**

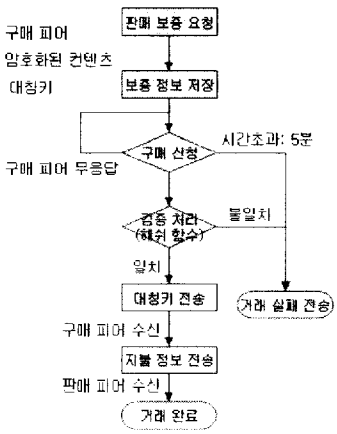
구매피어에서 CS로 검색 요청을 하게 되면 CS에서는 해당 피어 정보 및 평판값을 전송하게 된다. 기본 프로토콜은 [그림 14]와 같다.



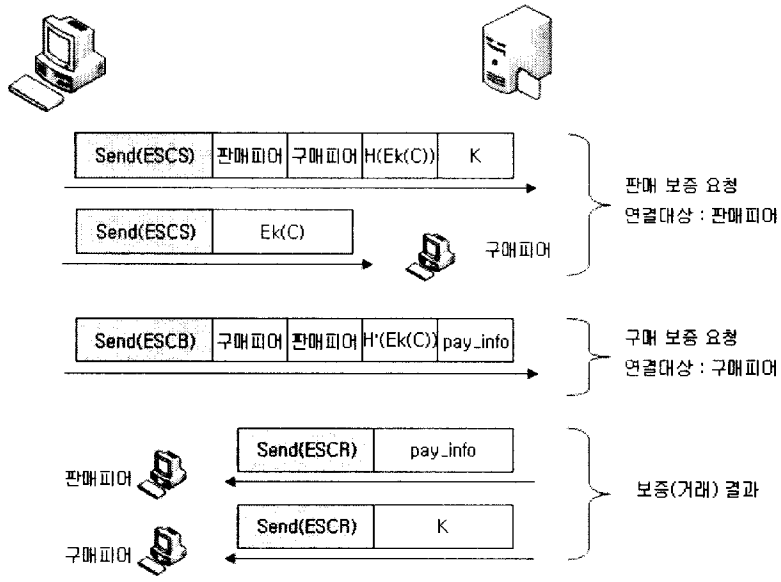
[그림 14] 컨텐츠 검색 프로토콜

(2) 구매/판매 피어의 컨텐츠 구매/판매(ES에서 처리)

거래 승인을 위한 ES에서의 업무 흐름도 및 프로토콜 정의는 다음과 같이 구성된다. 기본 흐름도는 [그림 15]와 같으며, 기본 프로토콜은 [그림 16]과 같다.



[그림 15] ES에서의 보증 흐름도



[그림 16] ES 보증 서버와의 프로토콜

(3) 구매 프로토콜

- Peer-to-Peer Protocol (P2가 P1에게 구매 요구)

  P1: SEDB #P1ID #CONTENT ... P2전송

  P2: SEDS Ek(#CONTENT) ... P1에 전송

(4) 기타

- CS Protocol

  Port = 8249

  Defalt Address = 210.110.177.72

- ES Protocol

  Port = 8289

  Defalt Address = 210.110.177.72

- Peer Protocol

  Server Port = 8989 (Default)

  Client Port = 4949 (Default)

4.5. 구현 환경

기본적인 구현은 윈도우 환경에서의 적용되도록 개발되어 있으며, 웹(Web) 프로그램이 아닌 일반 응용(Application) 프로그램으로 개발되어 구현 하였다.

(1) 구현환경

본 논문에서 제안하는 e-Commerce 모델은 소켓(Socket)을 이용한 TCP/IP로 구축되어 운영되며 기본적인 구현 환경아래 <표 3>과 같다.

<표 3> 개발환경

항 목		내 용
서 버 CS/ES	운영체제	Windows 2000 Pro
	데이터베이스	Paradox 7.x, MySQL 4.0.18
	Socket	Indy 9.00.17
	Spec	p-III 700, 384M, 160G HDD
Peer Program		Application Program
개발도구(언어)		Delphi 6.0
암호화 도구		해쉬 함수(5종) 암호문 (8종)

4.6. 고려 사항

P2P 시스템의 서밴트(Server+Client) 자신은 클라이언트인 동시에 서버로 동작하므로 언제라도 다른 피어의 서비스 요청에 대해 클라이언트에서 서버로 전환하기 위한 메커니즘이 필요하며 P2P 시스템의 구성을 제일 하부의 물리적 인프라 계층과 중간의 미들웨어 계층, 그리고 상부의 응용계층으로 구분 할 때, 서밴트는 미들웨어 계층에서 이러한 역할을 담당하게 된다[5]. <그림 15>에서 보여주듯이 미들웨어 계층은 시스템의 자원 관리, 다른 피어들에 대한 검색, 식별 및 통신하기 위한 기능과 접근제어와 같은 보안 기능 등을 지원하게 된다. P2P와 미들웨어의 관계에 있어서 다음과 같은 점을 고려해야 할 것이다.

Trust 문제: 서로 인증되지 않은 사용자 간에 접근과 리소스가 공유되게 되면 피어 건 신뢰 문제가 발생할 수 있다.

서로 다른 하드웨어: 전체 환경이 완전한 다른 컴포넌트들로 구성에 따른 각각의 피어는 다양한 프로세스, 메모리 사이즈의 차이 및 다른 내부 구조의 지원이 필요하게 된다.

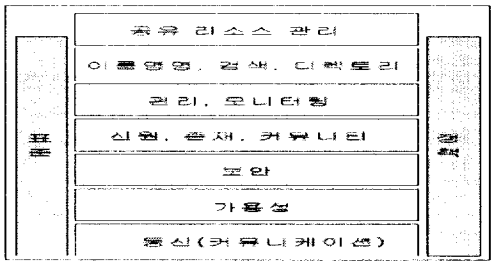
서로 다른 소프트웨어: P2P 가 적용되는 OS 환경은 매우 다양하며 P2P 프로그램은 모든 OS에서 작동해야 한다.

이기종 네트워크: 각각의 피어 연결은 다른 네트워크 환경을 가질 수 있으며, CDMA, 인터넷 환경에 관계없이 다른 대역폭과 연결성 의 제한을 포함, 이런 모든 환경에 대한 고려가 필요하다.

스케일: 하나의 피어 네트워크에 참가하는 인원은 다양하며, 적

게는 두 명에서 동시에 수백 명의 연결자수를 가져갈 수 있으므로, 네트워크 상황에 대한 고려가 필수적이다.

연결의 일시성 : P2P에 참가하는 모든 피어는 시스템과 환경이 항상 유동적으로 들어오고 빠져나갈 수 있으므로 피어의 존재 유무에 대한 고려가 필요하다. [그림 17은] P2P 미들웨어 계층 구성을 나타낸다.



[그림 17] P2P 미들웨어 계층 구성

4.7. 구현 결과

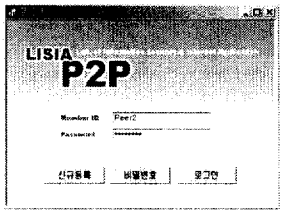
위에서 사항을 바탕으로 구현한 결과는 다음과 같다[그림13-16]. 구현을 위해 사용자를 각 Peer1, Peer2, Peer3으로 등록시켰으며 기본 컨텐츠 목록은 CS(Central Server)에 등록이 되어 있는 상태다.

운영 서버로는 보안을 위해 CS(Central Server)와 ES(Escrow Server)가 각각 별도의 서버를 운영해야 하지만, 구현을 위해 하나의 서버(IP: 210.110.177.72)로 운영하였다. 각 피어들은 로그인을 통해 CS에서 인증을 받은 후 컨텐츠 등록 및 검색을 할 수 있으

며, ES의 검증을 통해 P2P e-Commerce를 수행할 수 있게 된다.

(1) 로그인

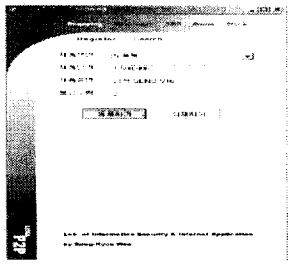
P2P e-Commerce 사용을 위한 초기 로그인 화면으로 아이디 및 비밀번호를 입력 후 승인 과정을 수행하도록 한다. [그림 18]은 로그인 화면을 나타내고 있다.



[그림 18] 로그인

(2) 상품 등록 및 삭제

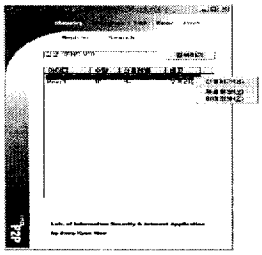
로그인 승인 후 상품을 등록 및 삭제를 하고자 할 경우 CS 에 변경 정보를 전송하게 된다. 로컬에서(각 피어)는 .ini 의 파일 데이터베이스로 처리 되며 서버에서는 Paradox 7.x 데이터베이스에 저장되게 된다. [그림 19]는 피어들이 CS에 목록을 등록하는 화면은 나타내고 있다.



[그림 19] CS 목록
등록

(3) 상품 검색

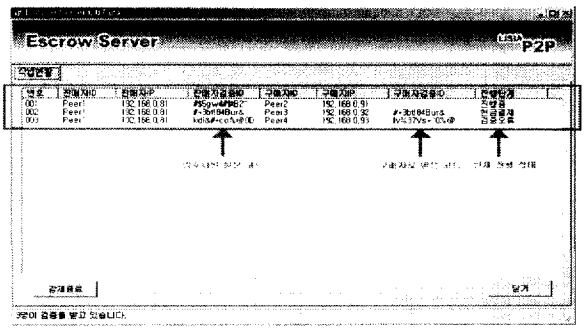
구매자의 구매 상품 요청에 의해 CS 에서의 검색 후 해당 상품 소유자의 정보를 전송하게 된다. [그림 20]은 피어에서 컨텐츠를 검색 및 신청하는 화면을 나타낸다.



[그림 20] 컨텐츠
검색 및 신청

(4) 보증 처리

거래 요청 시 구매자와 판매자의 거래 보증/승인을 위한 해쉬 함수 처리 결과를 전송하게 된다. [그림 21]에서는 ES에서 보증 처리하는 화면을 나타내고 있다.



[그림 21] ES에서의 보증 처리

5. 결론 및 향후 연구

본 논문에서는 서버가 개입되어 동작하는 기존의 e-Commerce 방식에 서버 없이 서비스 이용자(피어)들 간의 직접적인 통신에 의해 구매 및 판매가 가능한 P2P 서비스를 적용한 새로운 e-Commerce를 제안하였다. 제안된 P2P e-Commerce는 컨텐츠 교환과 지불에 있어 공정성을 보장해 줄 수 있고 또한, 피어들이 제공한 컨텐츠에 대한 평판값을 참조하여 신뢰성 보장과 안전하고 정확한 컨텐츠 구매가 가능한 이점을 가진다.

그러나 기본 설계를 혼합 P2P 방식을 이용하여 컨텐츠 목록을 CS(Central Server)에서 관리하다 보니 많은 컨텐츠 정보량과 서버에서의 검색에 따른 부하가 발생될 수 있다는 단점이 있다. 이를 보안하기 위해 서버의 분배 및 목록들을 각 피어들에서 관리하여 서버의 부하를 덜어줄 수 있는 연구가 필요할 것으로 판단되며, 이 또한 피어의 부하를 부여할 수 있기에 계속적인 추가 보안이 필요할 것이다. 또한, 본 연구는 최근 인터넷 기술의 발전으로 P2P를 이용한 전자상거래를 통한 상업 활동이 많이 이루어지는데 있어서 판매자의 평판값(trust)를 이용한 신뢰도 확보 보증 서버(ES: Escrow Server)를 통한 상호간에 공정성을 보장해 주기 위해 제안 한 것으로, 평판값의 레벨부여에 있어서 상호간 신뢰할 수 있는 표준안이 추가로 연구되어질 필요가 있을 것으로 판단한다.

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 표준화, 그리고 디지털 컨텐츠 보호와 관련된 추가적인 연구가 필요할 것으로 판단된다.

<참 고 문 헌>

[1] Bill Horne, Benny Pinkas, Tomas Sander, "Escrow Services and Incentives in Peer-to-Peer Networks", EC'01, 2001

[2] DIOGO R.FERREIRA, J.J.PINTO FERRERIA, "Building an e-marketplace on a peer-to-peer infrastructure", INT.J. COMPUTER INTEGRATED MANUFACTURING, APRIL - MAY 2004, VOL.17, NO.3, 254-264

[3] D.S. Milojicic, et. al., "Peer-to-Peer Computing," HP Technical Report. HP Labora-tories, Mar. 2002

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

[5] Jonas Aslund, "Authentication in peer to peer systems", Lith - ISY - EX - 3153 - 2002, 2002.

[6] K. Aberer and M.Hauswirth, "An Overview on Peer-to-Peer Information System." Workshop on Distributed Data and Structures(WDAS-2002), Paris, France, 2002

[7] Krishna Kant, Ravi Iyer, "A Framework for Classifying Peer-to-Peer Technologies", CCGRID'02, 2002

[8] SAI HO KWOK, KARL R. LANG AND KAR YAN TAM, "Peer-to-Peer Technology Business and Service Models: Risks and Opportunities", Electronic Markets,

[9] 산업자원부, 한국전자거래(CALS/EC)협회, 전자상거래백서

2000, 2000.6. p26.

[10] 산업자원부, 한국전자거래(CALS/EC)협회, 전자상거래백서 2000, 2000.6. p27.

[11] 신현종, '세계통산과 인터넷 전자상거래' 및 노재범, '인터넷의 대두와 기업의 대응', 삼성경제연구소 1996.5. 수정보완.

[12] 이만영, 김지홍, 류재철, 송유진, 염흥열, 이임영 공저, "전자상거래 보안 기술", 1999

[13] 정유진, "P2P의 현황 및 전망", 지급결제와 정보기술, 2001

[14] 최현우, Penta System 고등기술연구소, Next Generation Peer-to-Peer, 2002.10

[15] 한국정보보호센터 편, 정보보호개론 - 알기쉬운 정보보호 기술 , 2000

감사의 글

석사과정동안 많은 지도와 관심으로 부족함이 많은 저를 학문의 길로 이끌어 주시고 지도해 주신 이경현 교수님께 깊이 감사드립니다.

또한, 논문이 완성되기까지 바쁘신 와중에도 귀중한 시간을 내어주시어 논문에 대한 충고와 조언을 해주신 윤성대 교수님, 신상욱 교수님께도 감사드립니다.

그밖에도 지난 2년간의 대학원 과정에서 많은 가르침을 주신 전산정보산업대학원 교수님들께도 감사의 마음을 전합니다.

석사과정동안 많은 격려와 지도 그리고 따뜻함과 편안함을 제게 주신 LISIA 연구실 여러 선배님과 동기님들, 후배님들께도 감사의 마음을 전합니다.

직장 생활과 학교생활을 겸하는데 크나큰 도움을 주신 신상건 사장님과 파인텍(주) 임직원분들 그리고 (주)켄비텍 임직원분들과 R&D 여러분들께도 감사의 마음을 전합니다.

이밖에도 저를 아시는 모든 분들께 감사의 마음을 전하며 항상 웃음과 즐거움이 함께하시는 하루하루 되시기를 기원합니다.

그리고 제게 있어서 가장 소중한 사람들이며 항상 힘이 되어주신 아버님, 어머님, 장인어르신, 장모님, 누나, 자형, 동생 그리고 형님(아들 외삼촌입니다. ^0^)께 감사의 마음을 전합니다.

끝으로 어려운 가운데에서도 항상 웃음으로 힘이 되어준 제가 가장 아끼고 사랑하는 아내 김경남 氏에게 감사의 글을 전합니다. 그리고 사랑하는 아들 동건이에게도 아빠의 사랑을 전하며 이글을 마칩니다.

2004년 12월 위 성 균 올림