신용카드 리더에 기반한 전자지불 승인시스템

장시웅, 박민석
동의대학교 전산통계학과

An Electronic Payment System based on a Magnetic Card Reader

Si-Woong, Jang, Min-Suk Park
Dept. of Computer Science&Statistics, Dongeui University
E-mail : swjang@dongeui.ac.kr, pmsw01@cssbbs.dongeui.ac.kr

요 약

현재 전자상거래에서 가장 많이 사용되는 전자지불 방법은 신용카드를 이용한 방법이다. 그러나 신용카드를 이용한 결제는 해킹과 spoofing등의 방법을 통해 신용카드 정보를 해킹 당할 수 있다. 본 연구에서는 종래의 전자 지불 승인의 약점을 개선하기 위한 방법으로 인터넷상에서도 신용카드를 소지한 사람만이 신용카드 결재를 수행할 수 있도록 하는 방법을 제시하고, 컴퓨터 부착용 신용카드 리더와 전자지불 시스템을 구현하였다. 본 연구에서 구현한 전자지불 승인시스템은 Windows-2000, Windows-98 및 Windows-me에서 동작 가능하며, 50명 이상의 동시 사용자를 지원할 수 있다.

1. 서론

전자상거래는 기업간 또는 기업과 개인, 정부간에 컴퓨터 네트워크를 통해서 다양한 거래를 수행하여 기업의 경영 효율을 높이고 국제시장에서 경쟁력을 강화할 수 있는 수단이다[1]. 전자상거래가 활성화되기 위해서는 선결해야 하는 중요한 문제가 전자지불(Electronic Payment) 문제이다.

현재 전자상거래에서 가장 많이 사용되는 전자지불 방법은 신용카드를 이용한 방법이나 타인의 신용카드 번호와 유효기간을 알면 신용카드가 없어도 쇼핑몰을 통해 물건 구입을 도용할 수 있는 약점을 가지며, 키보드 해킹 등의 방법을 통해 신용카드 정보를 해킹 당할 수 있다. 본 연구에서는 종래의 전자 지불 승인의 약점을 개선하기 위한 방법으로 인터넷 상에서도 신용카드를 소지한 사람만이 신용카드 결재를 수행할 수 있도록 하는 방안을 제시하고 이를 구현하였다.

본 연구는 과학기술부·한국과학재단 지정, 부산광역시 지원 지역협력연구센터인 동의대학교 전자세라믹스연구센터의 지원에 의한 것입니다.

전자지불 설계 과정에서 고려되어야 할 대표적인 요소들은 안정성, 이중사용 방지, 분쟁해결성, 효율성, 사생활 보호 등이다[2,3]. 즉 안정성은 프로토콜이 외부의 공격으로부터 안전해야 한다는 가정이 있어야 하며, 이중사용 방지는 같은 지불 데이타를 두 번 사용할 수 없어야 한다는 것이며, 분쟁해결성은 지불과정에서 생길 수 있는 분쟁 유형에 대해 효과적으로 대처할 수 있어야 한다는 것이다. 효율성은 지불 처리 비용이 저렴해야 한다는 것이고, 사생활 보호는 거래과정에서 거래자의 개인정보가 노출되는 것을 막을 수 있어야 한다는 것이다[4,5].

전자상거래에서 활용하고 있는 전자지불의 형태로는 전자화폐(Electric Cash), 스마트카드를 통한 결제, 신용카드를 통한 전자결제, 제3자 결제방식 등이 있다[6,7].

기존의 방식에서는 안전한 전자지불을 구현하기 위해 마스터카드, 비자 등의 대규모 신용카드와 금융회사를 중심으로 마련된 SET을 이용해서 암호화 작업을 하는 실정이다. 그러나 본 논문에서는 컴퓨터 부착용 신용카드 리더를 이용하여 하드웨어에서 암호화

작업을 마친 후 인증 서버에 넘겨주는 방식을 이용하므로 기존의 소프트웨어로만 암호화 작업을 한 것보다 훨씬 암호화를 효율적으로 수행할 수 있다.

2. 전자 지불 승인 시스템의 관련 연구

전자 지불 승인 시스템에 대한 연구는 지금까지 다양하게 이루어져 왔으며, 실제로 전자 지불 승인 시스템에 대한 서비스도 많이 이루어지고 있다. 기존에 연구되어진 전자 지불 승인 시스템의 사례들을 살펴보면 데이콤 전자지불 시스템, EasyPay, PayGate, SET/SSL Protocol을 이용하는 방식, PGP를 이용한 WWW 기반에서의 전자지불 프로토콜, 웹 브라우저와 CGI 프로그램 사이의 보안통신 방법, 독립된 고유번호 서비스를 이용한 전자화폐 대금 결제 시스템 등이 있다.

데이콤 전자지불 시스템은 PC Banking 서비스를 이용하는 천리안 PPP 고객을 대상으로 하여 서비스(계좌이체)를 처음 개시하였으며, 1999년 9월 국내 전 신용카드에 대한 대금결제 서비스를 개시하였다. 이 시스템은 SET Protocol을 적용한 신용카드 전자지불 시스템을 기반으로 하고 있다[8].

EasyPay는 카드소지자와 지불 GateWay 전구간 128bit SSL 구현하였으며, 세계적으로 공인된 암호화 Key를 사용하고 있으며 별도의 인증(Certificate)을 필요로 하지 않는다는 장점이 있다.

PayGate은 신용카드 전자지불 시스템으로서 실시간으로 VAN을 거쳐 신용카드 승인을 획득하는 방식의 서비스를 제공하고 있으며, 신용카드 승인을 획득한 이후에도 지불을 취소할 수 있는 서비스를 제공하고 있다. 이 시스템의 지불 데이터는 128bit의 암호 알고리즘으로 보호하고 있다.

SET/SSL Protocol을 이용하는 방식은 SET과 SSL을 결합하여 전자 지불 보안을 높인 것이다[9].

PGP를 이용한 WWW 기반에서의 전자지불 프로토콜은 신용카드를 이용하는 시스템에서 독립적으로 작동하고, 공개키 인증이 현실적이어서 단지 전자우편이라는 제한된 분야에만 사용되는 것은 아니다[10].

웹 브라우저와 CGI 프로그램 사이의 보안통신 방법은 웹 브라우저와 웹 서버 사이의 통신뿐만 아니라 Internet에서도 보안을 지원할 수 있는 시스템을 구현한 것이다. 이 시스템은 PKI 기반의 SSL을 이용하여 보안을 지원한 것이 특징이다. 그러나 브라우저 사용자와 CGI 개발자는 같은 PKI 제품을 사용해야 한다는 제약사항이 있는 것이 단점이다[11].

독립된 고유번호 서비스를 이용한 전자화폐 대금결제 시스템은 이중 지불검사를 담당하는 고유번호 관리 서버를 은행과 독립적으로 구성하여 익명성을 보장하며, 고유번호 관리 서버는 데이터베이스에 현재 통용중인 전자화폐들의 고유번호를 저장하고, 고유번호 데이터베이스의 크기는 일정하게 유지되어 이중지불 검사를 효율적으로 수행하는 것이 이 시스템의 특징이다. 그러나 전자화폐가 다량 존재하게 되어 관리가 어렵고 대금 지불시 지불에 필요한 전자화폐를 직접 선택해야 한는 단점이 있다[12].

지금까지 살펴본 연구에서의 전자 지불 승인 시스템은 보안에 상당한 비중을 두고 있으며, 다음으로 사용자에게 간편하게 서비스하는 것이 요구되고 있다. 보안은 대부분 SSL이나 SET과 같은 Protocol을 이용하여 암호화를 하였으며, 간혹 특정의 CGI를 이용하거나 PGP와 같은 메일 기반의 색다른 방법을 이용하는 것도 있지만 현실적으로 적용하기에는 미흡한 부분이 많이 있다.

본 논문에서는 전자상거래에서 신용카드 결제 문제를 해결하기 위해 개인용 컴퓨터에 신용카드 리더를 부착하여 인터넷에서 신용카드 결제 시에도 신용카드를 소지한 사람만이 신용카드를 결재할 수 있도록 구현한 것이다.

3. 전자 지불 승인 시스템의 구조 및 설계

본 장에서는 전자 지불 승인 시스템의 전체적인 구성 및 자료흐름에 대해 기술한다.

3.1 전자 지불 승인 시스템의 전체 구성

전자 지불 승인 시스템은 신용카드를 이용하여 카드번호 및 거래관련번호를 전송하여 인터넷상에서 거래를 하는 것이다. 신용카드를 이용할 경우 신용카드에 대한 보안이 마련되어야 가능하다. 현재 신용카드 정보에 대해서 암호화를 통해 데이터를 보호하고 있는 실정이고, 마스터카드, 비자 등의 대규모 신용카드와 금융회사를 중심으로 마련된 SET을 통해서 전자지불 승인 시스템을 구성하고 있다. 본 논문에서 제안하는 시스템은 기존의 전자 지불 승인 시스템에 신용카드 리더를 결합하여 신용카드의 보안 및 편리성을 향상 시켰다.

본 연구에서 제안하는 전자 지불 승인 시스템은 HTTP Protocol을 기반으로 한 클라이언트 서버 모델을 기반으로 한다. 서버는 Windows 2000의 IIS Server를 이용하고, 클라이언트는 인터넷이 가능한

PC로 구성한다. Web 프로그램의 특징인 Request /Response 의 구조를 이용하여 다중 사용자(Multi User)가 사용 가능하며, 서버의 부하를 줄이기 위해서 DCom 기술을 이용하였으며 ActiveX 기술을 이용하여 하드웨어와 서버간의 통신 기술을 구현하였다. 신용카드 리더와 서버간의 통신은 윈속(Winsock)을 이용하였으며, 데이터 전송 프로토콜은 TCP/IP를 사용하였다. 네트워크 통해 클라이언트의 신용카드 리더의 신용카드 정보를 읽어서 서버로 전송하여 안전하게 정보를 보호할 수 있도록 설계하였다.

3.2 전자 지불 승인 시스템의 자료흐름

본 연구에서 제안하는 전자 지불 승인 시스템과 외부 요소들과의 관계를 간단하게 살펴보면 다음과 같다.

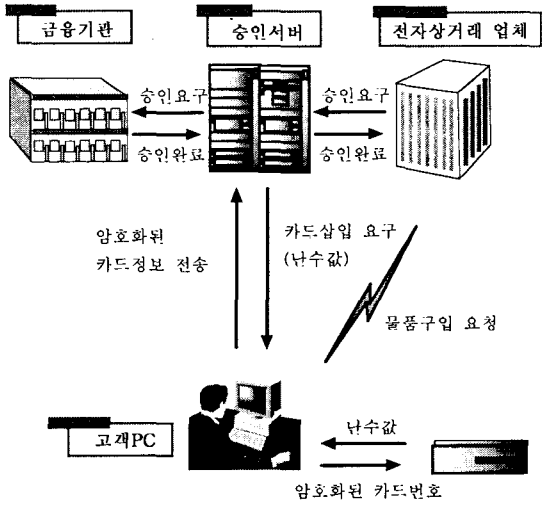

그림 1. 전자지불 승인시스템과 외부요소와의 관계

그림 1에서 처럼 고객이 전자상거래 업체로부터 물건을 구입하고, 신용카드 결재를 선택하게 되면, 전자상거래 업체의 서버는 고객의 신용카드 결재를 위해서 승인서버에게 결재 요구를 요청한다. 승인 시스템은 난수값(암호키값)을 생성한 후 카드삽입요구정보로서 난수값을 고객 PC에 부착된 신용카드 리더에 전달한다. 신용카드 리더는 사용자가 삽입한 카드로부터 카드번호를 읽은 후 승인서버에서 전달받은 난수를 암호화키로 이용하여 카드번호를 암호화하고 암호화된 카드 정보는 승인서버에 전달된다. 전달된 카드정보는 승인서버에서 복호화 과정을 거친 후 복호화된 원래 정보를 금융기관이 요구하는 암호체계로 바꾼 후에 금융기관에 해당 정보를 전송한다. 승인 서버는 금융기관으로부터 승인 결과를 통보 받은 후 전자상거래 업체에 신용카드 승인 결과를 최종적으로 통보하고 전자 상거래 업체는 신용카드의 승인 결과에 따라 승인작업을 종료하고 다른 서비스를 제공한다

전자지불 승인시스템의 외부 요소는 구매자, 상인 서버, 승인 시스템 및 금융 기관으로 이루어져 있다. 구매자는 상품을 구매하거나 판매하는 주체로서 구매자는 쇼핑 도중에 구입하려는 물건을 선택한 후, 지불 페이지 요청을 한다. 상인 서버는 물건을 판매하는 주체로서 일반적으로 쇼핑몰을 들 수 있다. 승인 시스템은 신용카드 번호 인증 및 관리를 수행한다. 금융기관은 신용카드의 신용내역 판별 및 결과를 전송한다. 구체적인 자료흐름 과정은 다음과 같다.

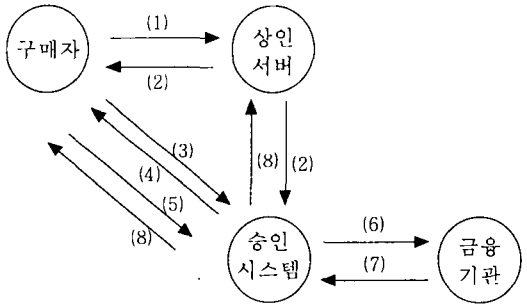

그림 2. 전자지불 승인시스템과 외부요소와의 자료흐름

그림 2처럼 구매자는 상인 서버에서 물건을 선택한 후 대금을 지불하기 위해서 지불페이지를 요청한다(1). 상인서버는 구매자의 구매내역을 제시하고 승인시스템으로의 연결 버튼을 제공한다(2). 구매자가 선택한 상품 목록을 확인하면 연결버튼을 통하여 승인시스템에 연결된다(3). 승인 시스템은 난수번호를 생성한 후 난수번호를 담아 카드 삽입 요구 메시지를 전송한다(4). 사용자가 신용카드를 카드 리더에 삽입하면 카드 리더는 승인시스템으로부터 받은 난수번호를 암호화키로 하여 신용정보를 암호화한 후 승인 시스템에 전송한다(5). 승인 시스템은 카드 리더로부터 받은 암호화된 신용정보를 복호화한 후 다시 금융기관이 원하는 암호체계로 암호화한 후 금융기관에 신용정보를 전송한다(6). 금융기관은 승인 시스템으로부터 받은 신용정보를 체크하여 구매자의 신용내역 판별 결과를 승인 시스템에 전달한다(7). 승인 시스템은 금융기관으로부터 받은 판별 내역을 확인한 후 전자 영수증을

발행하여 구매자와 상인서버에 전자 영수증을 전송한다.

4장 전자지불 승인 시스템의 구현

전자지불 승인시스템은 ASP 모듈, 난수생성 모듈(dll), 복호화 모듈(dll), Active-X 컴포넌트, DB 데몬 서버로 구성되어 있다. 그림 3은 전자지불 시스템의 컴포넌트간 호출관계 및 파라메터 전달 관계를 나타낸다. 각 컴포넌트간의 상세한 통신 관계를 설명하면 다음과 같다.

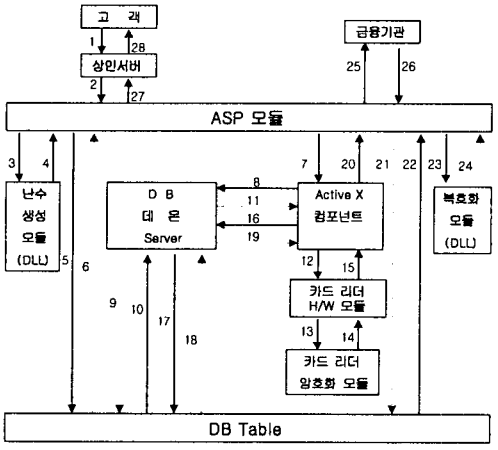

그림 3 전자지불 시스템의 컴포넌트간 관계

1. 고객이 물건을 구입한 후 카드결재를 선택한다.
2. 상인서버에서는 전자결재 승인시스템의 ASP 모듈에 카드 결재를 요구한다.
3. 전자지불 승인시스템의 ASP 모듈은 결재를 요구한 고객의 카드번호를 암호화하기 위해 난수생 성 모듈에 난수값(Encrypting key)발생을 요구한다.
4. 난수발생 모듈은 난수 값을 생성하여 ASP 모듈에 전달한다.
5. ASP 모듈은 난수 값을 DB Table에 저장한다.
6. DB Table에 저장한 결과를 Return한다.
7. session id를 파라메터로하여 Active-X 컴포넌트를 호출한다.
8. session id를 파라메터로하여 난수 값 읽기를 요구한다.
9. DBMS에 난수값 읽기를 요구한다.
10. DBMS는 읽은 난수값을 DB 데몬서버에 전송한다.
11. DB데몬 서버는 읽은 난수값을 Active-X 컴포넌트에 전달한다.
12. 난수 값을 카드 리더 모듈에 전달한다.
13. 난수 값과 읽은 카드 정보를 카드 리더 암호화 모듈에 전달한다.
14. 암호화한 카드 정보를 카드 리더에 전달한다.
15. 암호화한 카드 정보를 Active-X 컴포넌트에 전달한다.
16. 암호화된 카드 정보를 DB 데몬 서버에 전달
17. 암호화된 카드 정보를 DB Table에 저장
18. DB 저장결과를 전송
19. DB 저장결과를 전송
20. 암호화된 카드 정보를 읽은 결과 전달
21. 암호화된 카드 정보 읽기를 요구한다.
22. 암호화된 카드 정보를 읽는다.
23. 암호화된 카드 정보를 파라메터로 복호화 모듈을 호출한다.
24. 복호화된 카드 정보를 ASP 모듈로 리턴한다.
25. 복호화된 카드 정보를 가지고 카드번호 조회 요구
26. 카드번호 조회 결과를 전달한다.
27. 카드번호 조회 결과를 전달한다.
28. 카드결재 종료를 알린다.

5. 성능분석

본 연구에서는 신용카드 리더를 이용한 전자 지불 승인 시스템을 인터넷 환경에서 구현하였다. 구현한 전자지불 승인시스템을 테스트하기 위해서 인트라넷 환경을 구성하였다. 성능 분석은 메인 서버(IIS Server + DB Server)와 클라이언트를 표 1과 같은 환경으로 구성하였다. 다수의 클라이언트로 구성하여 테스트할 필요가 있으므로 여러 대의 클라이언트로 구성하였고, 클라이언트의 시스템 환경도 다양하게 구성하였다.

표 1. 테스트 환경 구성표

구분	OS	CPU
서버 (IIS + DB)	Windows 2000 Server	Pentium III 1G Mhz
클라이언트	Windows 2000 Server	Pentium III 1G Mhz
	Windows Me	Pentium III 800 Mhz
	Windows 98	Pentium II 600 Mhz

그림 4는 클라이언트 수에 따른 전체 수행에 대한

평균전송 시간을 나타낸 것이다. 전체적으로 1.2초 이내에 모든 수행이 이루어지고 운영체제별로 살펴보면 Windows 2000은 0.5~1 초 이내로 응답이 나왔으며, Windows Me는 0.55~1.1 초 이내로 응답이 나왔으며, Windows 98은 0.6~1.2초 이내로 응답이 나왔다. 그림 4의 결과와 같이 응답시간이 1.2초 이내로 응답이 가능하므로 신용카드 리더에 대한 서비스를 원활히 수행할 수 있다.

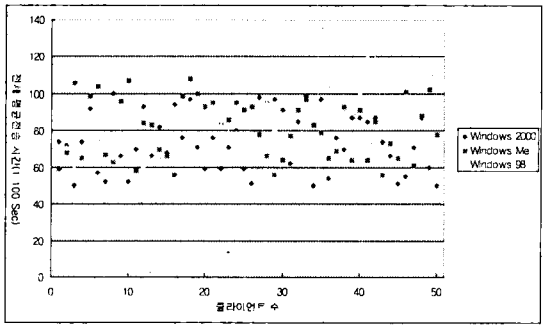

그림 4. 전체 수행에 대한 전송 시간 비교

6. 결론

본 연구에서는 종래의 전자 지불 승인의 약점을 개선하기 위한 방법으로 인터넷상에서도 신용카드를 소지한 사람만이 신용카드 결재를 수행할 수 있도록 하는 방안을 제시하고, 컴퓨터 부착용 신용카드 리더와 전자지불 승인 시스템을 구현하였다.

컴퓨터 부착용 신용카드 리더의 보안을 위해 암호화를 수행하였으며, 암호화된 신용카드 정보는 서버의 복호화 모듈에 의해 해독된다. 본 연구에서는 신용카드 리더내에 암호화 모듈을 탑재하여 사용자가 신용카드를 읽는 즉시 암호화하여 컴퓨터에 전달함으로써 각종 해킹에도 안전하게 하였다. 신용카드 리더는 서버로부터 부여받은 난수 값과 자체 생성한 난수 값을 조합하여 신용카드로부터 읽은 정보를 암호화하고, 서버는 암호화된 신용정보를 받아 복호화를 수행한다.

전자상거래에 있어서의 철저한 보안 체계의 확립은 전자상거래의 활성화에 반드시 필요한 요소이다. 개발된 시스템은 홈쇼핑(home Shopping), 홈뱅킹(Home banking) 및 전자결재 시스템 등의 네트워크 상에서 이루어지고 있는 모든 사용자 인증 보안 시스템에 응용 될 수 있다.

[참고문헌]

[1]송용욱, "지불기술, 시스템 동향," 인터넷백서, forthcoming.

[2]손은경, 김태윤, "재사용 가능한 전자화폐 일련번호와 지불 트랜잭션 메커니즘" 정보과 학회 논문지, 제 4권, 제 6호 1998. 12.

[3]P Putland, J Hill, D Tsapakidis, "Electronic payment systems" BT Technology Journal, V.15 N.2 , 1997. 4. 1.

[4]박현동.이은성.송상헌.강신각.박적수.류재철, "안전한 인터넷 전자지출 프로토콜의 설계 및 구현", 한국정보처리학회 논문지 제 6권 제 8호,1999.8

[5]주미리, 이보영, 양형규 원동호, "전자상거래 인증서비스를 위한 검증 가능한 자체인증 방식", 정보처리논문지, 2000.9

[6]김정은, 이형우, 김태윤, "스마트 카드를 사용한 오프-라인 전자 지불 기법", 정보과학회 논문지(A) Vol.26, No.11, November 1999.

[7]Michael Peirce, Donal O'Mahony, "Flexible Real-Time Payment Methods for Moble Communications", IEEE Persional Commnications. Dec 1999.

[8]Lucas de Carvalho Ferreira, Ricardo Dahab "A scheme for Analyzing Electronic Payment Systems" Proceedings of the Fourteenth Annual Computer Security Applications Conference, pp137-146, 1998. 12. 7.

[9]M.H.Sherifa.Serhrouchni,A.Y.Gaid,F.Farazmandnia, "SET and SSL : Electronic payments on the Internet" Proceedings of the Third IEEE Symposium on Computers and Communications, 1998

[10]박현동, 강신각, 박성열, 류재철, "PGP를 이용한 WWW 기반에서의 전자지불 프로토콜 개발" 한국정보처리학회 논문지, 제 4권, 제4호 1997. 4.

[11]이준석, "웹 브라우져와 CGI 프로그램 사이의 보안 통신을 지원하는 시스템 설계 및 구현" , 정보처리 논문지, 제 6권 제3호 1999.3.

[12]조지용 외 4인, "독립된 고유번호 서비스를 이용한 전자화폐 대금 결제 시스템의 설계 및 구현", 정보과학회논문지(C) 제4권 제5회, 1998.10