지불 트랜잭션 비용 감소를 위한 전자상거래 지불프로토콜에 관한 연구

정 헌°, 서영수, 강병욱
영남대학교 컴퓨터공학과
e-mail: law1207@neolife.net

A study on electronic commerce protocol for reducing cost of payment transaction

Hun Jung°, Yeung-Su Suh, and Byung-Ug Kang
Dept. of Computer Engineering, Yeungnam University

요약

기존의 쇼핑몰에 비해 창고비, 인건비 등과 같은 부대비용을 상대적으로 줄일 수 있는 인터넷 쇼핑몰이 증가 추세에 있다. 그러나 인터넷 쇼핑몰의 운용과 관련된 문제점들은 여전히 해결되지 않은 상태이며, 특히 개인의 보안문제, 상품 구매 시 상품가격이외에 소요되는 비용으로 암호화비용, 통신비용, 트랜잭션비용으로 나타나는 거래비용 등은 최우선적으로 개선되어야 할 중요한 과제다. 본 논문에서는 전자상거래와 관련된 기존의 기술들을 분석하고 이를 이용하여 전자화폐를 이용한 지불방식, 거래비용의 감소를 특징으로 하는 전자지불시스템을 제안한다.

I. 서론

인터넷은 정보의 보고로서 사용자들이 급증하고 있으며 이로 인해 인터넷은 학술·연구적인 목적에서 상업적인 형태로 변화되어, 최근 인터넷 쇼핑몰의 운영이 증가하고 있다[1][2][3]. 인터넷을 이용한 전자상거래가 발달함에 따라 새롭고 다양한 지불방식이 요구되며, 특히 지불방식과 보안문제는 전자상거래를 성공적으로 발전시키는 필수요소다. 인터넷을 이용한 지불방법에는 신용카드 기반형, 전자화폐 기반형, 전자적 자금이체형이 있다[2][4]. 이중에서 전자화폐 기반형은 실제 화폐와 같이 물품 구매자에 대한 익명성을 보장하므로 인터넷상에서 이용하기에 가장 이상적인 전자지불시스템이다.

전자지불시스템은 상품 구매 시 소요되는 거래비용에 따라서 거액지불시스템과 소액지불시스템으로 나눌 수 있으며, 같은 상품을 적은 거래비용으로 구매할 수 있는 소액지불시스템이 보다 이상적이다.

본 논문에서는 지불방식으로 전자화폐를 사용하며, 거래비용을 줄일 수 있는 전자지불시스템을 제안 할 것이다. 2장에서 기존의 전자지불시스템의 종류, 인터넷상에서의 지불시스템의 처리 흐름, 지불시스템에 필요한 암호화 및 인증 기술을 살펴본다. 3장에서는 제안된 전자화폐 기반 소액지불시스템을 설계할 것이며, 4장에서 결론을 맺는다.

II. 전자지불시스템

2.1 전자지불시스템 분석

현재 인터넷상에서 사용되는 전자지불시스템은 전자화폐 기반형 시스템, 신용카드 기반형 시스템, 전자적 자금이체형 시스템으로 나누어 볼 수 있다[2][4].

또한 지불 시 제3자의 개입여부에 따라 온라인 시스템과 오프라인 시스템으로 나누어 볼 수 있으며[5], 거래 시 지불비용에 따라 거액지불시스템과 소액지불시스템으로 나눌 수 있다. 다음의 [표 1]은 지불방식에 따른 전자지불시스템의 종류를 나타내며, [표 2]에서는 전자지불시스템을 거래 시 소요되는 지불비용에 따라 거액지불 방식과 소액지불 방식[7]으로 나누며, 각각을 다시 비 전자화폐형과 전자화폐형으로 나누어 분석한다[6][12].

[표 1] 지불방식에 따른 분류

	전자화폐형	신용카드 기반형	전자적 자금이체형
기밀성	상	중	하
익명성	상	하	하
부인방지	중	상	상

[표 2] 거래 시 지불비용에 따른 분류

	거액지불		소액지불	
	비 전자 화폐형	전자 화폐형	비 전자 화폐형	전자 화폐형
보안성	상	상	하	중
거래비용	하	하	상	중
익명성	하	상	하	상

2.2 전자지불시스템 암호화 및 인증 기술

전자지불시스템의 효율적이고 신뢰성 있는 운용을 위해 요구되는 조건들 중에서 가장 중요한 기밀성(security), 신뢰성(reliability), 익명성(anonymity)을 보장하는 방법으로 암호화 알고리즘, 인증 시스템이 이용된다[8]. 이러한 암호화 알고리즘으로 관용 암호방식과 공개키 암호방식이 있다[9][10]. 다음의 [표 3]은 전자지불시스템에서 사용되는 암호방식을 나타낸다.

[표 3] 암호방식

	관용암호방식	공개키 암호방식
키의 수	1개	2개
암호/복호화 속도	빠르다	느리다
부인방지	없다	있다

고객이 인터넷 쇼핑몰로부터 물건을 구매하기 위해서는 해당 고객의 구매 자격을 사전에 인증해야 하며, 이를 위해 여러 가지 기술이 개발되었다[3][9]. 아래의 [표 4]에서는 과거로부터 발전해온 주요 인증 기술의 장단점을 비교 분석한다.

[표 4] 인증 기술

인증 기술	요건	구매가능범위	고객 작업공간
로그인 방식	고객명과 패스워드	고객이 등록된 쇼핑몰	영향 없음
디지털 서명	디지털 서명	고객이 등록된 쇼핑몰	영향 있음
인증 기관	개인 인증서	인증기관에 등록된 모든 쇼핑몰	영향 없음

전자상거래의 신뢰성과 구매자의 익명성을 보장하는 것은 전자지불시스템에 필수 요건이다. 따라서 전자지불시스템을 위해 다양한 보안기능이 개발되었으며, 특히 기밀성, 인증, 무결성, 부인방지는 보안기능에 반드시 포함시켜야하는 가장 중요한 요소다. [표 5]는 이러한 주요 보안기능에 대한 특징을 설명한 것이다[8].

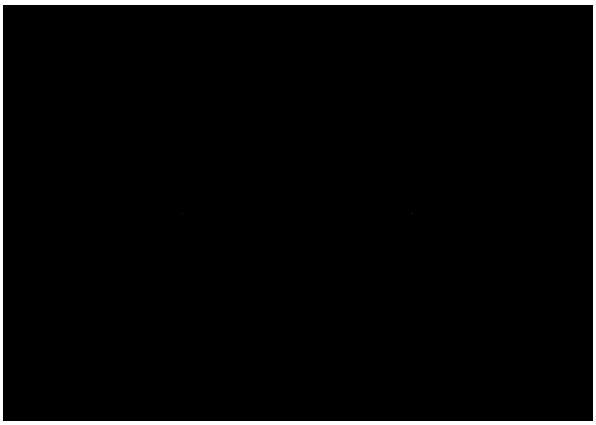
[표 5] 전자상거래에 필요한 보안기능

보안기능	특징
기밀성	전달내용을 제3자가 사용하지 못하도록 방지
인증	정보를 보내온 사람의 신원을 확인
무결성	정보 전달 도중 훼손되지 않았는지를 확인
부인방지	정보제공자가 정보제공사실을 부인하는 것을 방지

III. 전자화폐 기반 소액지불시스템 설계

제안된 전자화폐 기반 소액지불시스템 모델의 전체 구성을 살펴보면 아래 [그림 1]과 같다. 거래에 참여하는 객체는 고객, 인터넷 쇼핑몰, 그리고 인증기관 등이다. 고객은 인터넷 쇼핑몰 연결을 통하여 상품·서비스를 검색하고 주문하기 위해 웹브라우저

를 이용하고 지불처리를 위해 고객의 개인정보, 전자화폐 등과 같은 고객의 정보를 안전하게 관리하는 전자지갑으로 구성된다. 전자지갑은 인증기관에서 암호화키와 함께 고객에게 전달되며, 인증기관에서 발행된 고객 인증서 및 전자화폐가 등록되어 있다. 마지막으로 인터넷 쇼핑몰에 위치한 전자지불서버는 고객과 인터넷 쇼핑몰사이에서 지불처리를 중개하며, 이를 위해 암호화키와 영수증을 발급하게 되며, 고객 인증서의 유효성을 검증하기 위해 인증기관으로부터 발급 받은 고객 인증서 목록을 저장하게된다.



[그림 1] 제안된 전자지불시스템의 전체 구성도

3.1 프로토콜 메시지 형식 및 전자화폐의 구조

제안된 전자지불시스템에서 사용되는 메시지들의 모든 필드 구조는 [표 6]과 같다. 메시지 형식은 크게 헤더와 전자화폐 데이터 부분으로 구분된다. 헤더는 소액전자지불 프로토콜의 버전 정보, 프로토콜의 다음 갱신일, 오류메시지의 식별자, 메시지 타입 정보를 포함한다. 메시지 타입은 크게 고객 등록 메시지, 전자화폐 발행 메시지, 지불처리 메시지로 나뉜다. 고객 등록 메시지는 다시 고객 등록 요청, 고객 등록 허가 및 고객 등록 실패의 경우로 구분할 수 있다. 전자화폐 발행 메시지는 전자화폐 요청, 전자화폐 허가, 전자화폐 실패의 경우로, 마지막으로 지불처리 메시지는 CRL, 실제화폐 교환, 지불요청, 지불정보 전송, 지불처리 요청, 지불처리 응답, 영수증 전달의 경우로 나누어 볼 수 있다. 전자화폐 데이터 부분은 ID 타입, 서버 타입, 화폐의 구체적인 정보를 포함하는 몸체 부, 전자화폐의 인증 부분으로 나눌 수 있다. ID 타입의 일련번호 항목은 전자화폐 발행 시 생성되는 정수형태의 값이며, 서버 타입의 항목들은 각각 인증기관의 도메인명과 IP 주소, 인터넷 쇼핑몰의 도메인명과 인터넷 쇼핑몰에서 운영하는 전자지불서버 포트 번호를 나타낸다.

[표 6] 지불 처리 시 사용되는 메시지 형식

헤더 데이터 구조 : header_type		
protocolversion 소액 전자지불 프로토콜의 버전 정보		
protocoldate 프로토콜의 다음 갱신일		
errmsgid 오류메시지 ID		
cmdtype 고객등록메시지, 전자화폐발행메시지, 지불처리메시지로 구분		
전자화폐 데이터 구조 : money_type		
ID Type	serialnumber	일련번호
Server Type	dnsname	인증기관의 도메인
	ipaddr	인증기관의 IP주소
	servername	인터넷 쇼핑몰 도메인
	port	지불서버포트번호
money Body Type	currency	화폐단위
	value	전자화폐의 금액
	vendorid	servertype의 데이터 구조
	moneyid	idtype으로서 화폐발행정보 식별자
	customid	idtype으로서 고객 인증서 발행정보
	ad	광고, 설문 등을 이용했을 때 얻은 전자화폐금액
	expirationdate	전자화폐의 유효기간
전자화폐 인증부	hashalgorithm	해쉬알고리즘 식별자
	money	moneybodytype의 데이터 구조
	certificate	전자화폐의 인증서

전자화폐 몸체 부의 항목들 중에서 화폐단위 항목은 실제화폐로부터 파생된 전자화폐인지 광고나 설문을 통해 획득된 전자화폐인지를 구분하는 정보를 가진다. 이어서 전자화폐의 금액 항목은 상품 구매

시 지불 금액을 나타내며, 계속해서 인증기관의 서버 타입 정보, 전자화폐 발행 정보, 고객 인증서 발행 정보가 저장된다. 전자화폐 몸체 부의 마지막 두 항목에는 각각 광고나 설문을 통해 획득된 전자화폐의 금액과 전자화폐의 유효기간이 기록된다. 전자화폐 데이터 부분을 구성하는 마지막 구조인 전자화폐 인증부의 각 항목들은 사용하고 있는 해쉬함수의 종류, 해쉬함수를 통해 변형된 전자화폐 몸체 부의 정보, 전자화폐의 인증 여부 정보가 등록된다.

3.2 각 단계에서의 프로토콜과 메시지 형식

고객이 인터넷 쇼핑몰을 통해 물품을 구매하기 위해서는 우선 인증기관으로부터 인증서를 획득해 둘 필요가 있다. 일단 인증서를 획득하고 나면 인증기관으로부터 전자화폐를 발급 받고 클라이언트의 전자지갑을 이용하여 실제 구매행위를 할 수 있다. 고객의 구매 요청 이전 단계에 대한 프로토콜과 메시지 형식을 3.2.1 절에서 설명하며, 구매 요청 단계의 프로토콜을 3.2.2 절에서 제시한다.

3.2.1 구매 요청 이전 단계

고객의 구매 요청이 일어나기 전에 선행되어야하는 두 가지 조건은 인증기관으로부터 고객의 인증서를 발급 받는 것과 전자화폐를 발행 받는 것으로 나눌 수 있다.

(1) 인증서 발행 시의 프로토콜

아래에 고객과 인증기관 사이의 프로토콜을 다이어그램으로 나타낸다.

[그림 2] 고객과 인증기관 사이의 프로토콜

고객은 인터넷 쇼핑몰에 접속하여 거래가 이루어지기 이전에 인증기관으로부터 거래 시 필요한 고객 인증서를 발급 받아야 한다. 먼저 고객은 인증기관으로부터 전자지갑과, 전자서명용 공개키와, 암호용 공개키를 전송 받아 전자지갑을 클라이언트 컴퓨터에 설치한다. 설치 후 고객은 자신의 정보를 암호화하여 인증기관에 보내며, 고객의 정보를 받은 인증기관은 그 정보를 이용하여 고객 인증서를 발급하며 발급된 인증서는 고객의 전자지갑에 저장되어 이후 인터넷 쇼핑몰과의 거래 시 사용된다. 이때 일정한 시간이 지난 고객 인증서는 인증기관으로부터 재발급 받아야 한다.

(2) 인증서 발행시의 메시지 형식

아래의 [표 7]은 고객 등록 요구 메시지의 형식을 나타내며, [표 8]에 고객 등록 허가 메시지의 형식을 보인다. 각 표의 헤더는 메시지의 흐름 방향을 나타낸다.

[표 7] 고객 등록 요구 메시지 형식

전자지갑 → 인증기관	
Header_Type	고객 등록 요구
ID	고객 전자지갑 식별자
NAME	고객 이름
ADDRESS	고객 주소
E-mail	전자우편 주소
ETC	기타 고객 정보
session_key	고객 등록 허가 메시지를 암호화하기 위한 비밀키

[표 8] 고객 등록 허가 메시지 형식

인증기관 → 전자지갑	
Header_Type	고객 등록 허가
E_session_key	고객 인증서를 고객이 보내온 세션키로 암호화 후 전송

(3) 전자화폐 발행 시의 프로토콜 및 메시지 형식

고객은 인증기관으로부터 고객 인증서를 발급 받은 이후부터 인증기관에서 일정금액의 전자화폐를 발급 받을 수 있다. 발급 받은 전자화폐는 전자화폐가 발급된 시간과 함께 자신의 전자지갑에 저장되어 고객 인증서와 함께 인터넷 쇼핑몰에서 물건을 구매 후 지불 시 전달된다. 발행된 전자화폐는 고객 인증서와 동일하게 일정기간동안만 이용되며, 사용기간

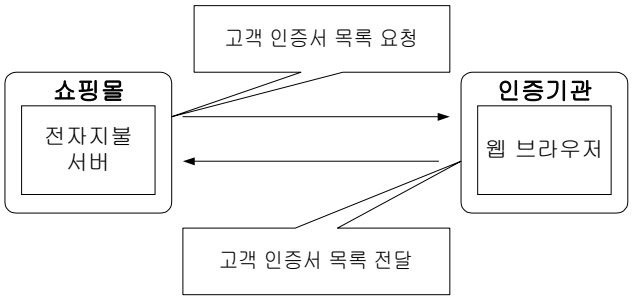
이 지난 전자화폐에 대해서는 인증기관으로부터 재발급 받아야 한다. [표 9]는 전자화폐 발행 시 메시지 형식을 보여준다.

[표 9] 전자화폐 발행 시 메시지 형식

전자지갑 → 인증기관	
Header_Type	전자화폐 발행 요청
ID	고객 전자지갑 식별자
Value	화폐금액
Header_Type	전자화폐 발행 불가
HTML 문서	화폐발행 불가 사유 전달

(4) 전자지불서버와 인증기관간의 프로토콜

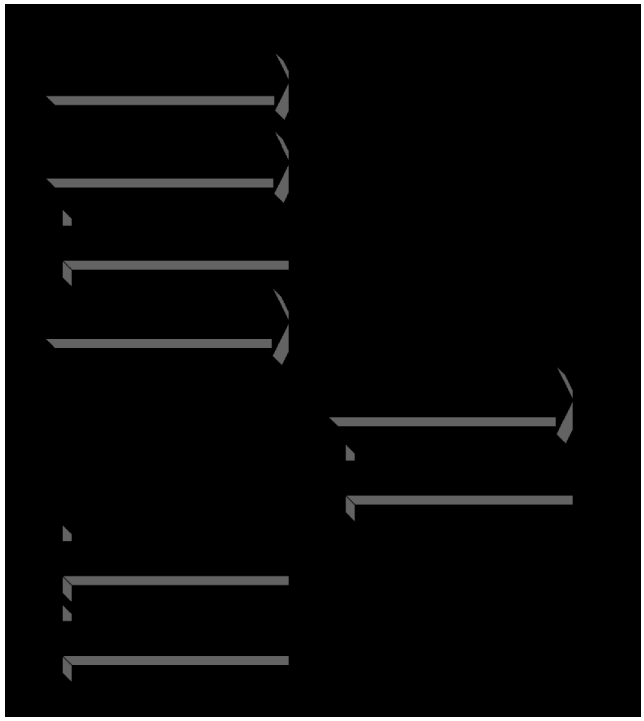
전자지불서버와 인증기관사이에는 고객 인증서의 유효함을 검사할 수 있도록 인증기관에서 무효화된 고객 인증서들의 목록인 CRL(Certificate Revocation List)및 전자화폐정보를 상호 교환함으로써 고객에 대한 인증서와 전자화폐의 유효성을 검사할 수 있다. [그림 3]은 전자지불서버와 인증기관 사이의 프로토콜을 보여준다



[그림 3] 인터넷 쇼핑몰과 인증기관간의 프로토콜

3.3.2 구매 요청 단계

위에서 언급한 바와 같이 일단 고객이 인증서와 전자화폐를 획득하게되면 고객은 같은 인증기관에 소속된 인터넷 쇼핑몰에서 상품을 검색하고 구매할 수 있다. [그림 4]에서 고객이 상품을 검색하고 구매하기 위해 요청을 하고 인터넷 쇼핑몰은 이에 대해 지불처리 절차를 수행하는 프로토콜을 각 단계별로 나누어 설명한다.



[그림 4] 지불단계 흐름

(0) 상품검색 단계

고객은 웹 브라우저를 이용하여 인터넷 쇼핑몰에 접속한 뒤, 구매 대상물을 검색하게된다.

(1) 상품주문 단계

구매할 상품을 선택한 고객은 다음 단계로 인터넷 쇼핑몰에 주문서를 전송하게 된다. 이때 고객의 인증서도 함께 전송된다.

(2) 지불요청 단계

고객이 주문한 상품에 대해 인터넷 쇼핑몰은 고객의 구매 요청 메시지로부터 지불처리 요청정보를 생성한다. 이때 인터넷 쇼핑몰은 정보의 암호화를 위해 전자지불서버로부터 생성된 세션키를 지불처리 요청정보와 함께 고객에게 발송한다.

(3) 지불정보전송 단계

고객은 인터넷 쇼핑몰이 보내온 지불 요청 메시지를 확인하고 지불정보를 전송해 줌으로써 지불을 시작한다. 이때 고객은 자신의 정보를 암호화하기 위해 전자지갑으로부터 세션키를 생성하고 이 정보를 지불정보와 함께 전송한다.

(4) 지불처리 요청 단계

인터넷 쇼핑몰은 고객이 전송해온 지불정보를 전

자지불서버에 전달하여 지불처리를 요청하는 단계다. 전자지불서버에서는 고객이 보내준 고객 인증서의 유효성 유무를 인증기관으로부터 미리 획득한 CRL목록에서 살펴보고 해당 고객의 전자화폐 유효성을 검사한다.

(5) 지불처리 응답 단계

전자지불서버는 지불처리를 완료한 후 영수증을 생성한다. 이때 영수증은 고객과 인터넷 쇼핑몰이 각각 생성한 세션키들로 암호화하여 인터넷 쇼핑몰로 전송된다.

(6) 영수증 발급

인터넷 쇼핑몰은 지불처리를 완료하고 고객의 정보에 대한 유효성이 만족되면 전자지불서버가 발행한 영수증을 고객에게 전송해 준다.

(7) 상품배달 단계

구매요청 단계의 마지막 과정으로 인터넷 쇼핑몰은 지불처리가 성공적으로 끝난 상품에 대해 고객에게 배달 서비스를 수행한다.

IV. 결론

인터넷 쇼핑몰을 이용하는 고객의 수는 매년 급증하고 있으며 따라서 효율적이고 신뢰성 있는 전자지불 시스템의 필요성은 주지의 사실이다.

본 논문은 기존의 전자지불시스템을 지불방식, 지불비용, 암호화방식, 인증기술 등에 따라 분석함으로써 최선의 관련 기술들을 선택하고, 이를 이용하여 지불 트랜잭션 비용을 감소시킬 수 있는 지불프로토콜을 제안했다. 결론적으로 고객의 익명성을 보장하기 위해 전자화폐형 지불방식을 선택했으며, 거래시 발생하는 지불비용을 줄이기 위해 소액지불방식을, 암호화 및 복호화 속도를 향상시키기 위해 관용암호방식을 택했다. 인증 기술로는 가장 최근에 나온 인증기관을 이용하는 방식을 이용함으로써 전자상거래에 필요한 신뢰성과 효율성을 높였다. 특히 고객과 인터넷 쇼핑몰 사이의 거래 시 고객 인증서를 확인하기 위해 매번 인터넷 쇼핑몰에 있는 전자지불서버에서 인증기관으로 데이터를 전달할 필요없이 고객 인증서 및 전자화폐의 사용유무가 담겨진 정보(CRL)를 인터넷 쇼핑몰의 전자지불서버에 저장해둠으로써 거래비용을 상당히 줄일 수 있다.

앞으로 고객의 구매 인터페이스를 도울 수 있도록 에이전트 기술을 도입하는 방향과 보다 안전하고 효율적인 암호화 기법을 접목하는 것도 고려해볼 수 있는 사항이다.

V. 참고문헌

1. 정보통신정책 연구원 국제협력팀,
"The Emerging Digital Economy," 1998. 4. 30.
2. 성기윤, 인터넷 전자지불시스템의 현황.
http://mis.cau.ac.kr/market/mis/ec/ec_re_paper/ec15.html.
3. 송용욱, 전자상거래 보안과 SET.
4. 김기병,지정권,김형주, “전자상거래를 위한 지불방법 및 보안”, 정보과학회지 제16권 제5호, pp19-25, 1998.5.
5. Berry Schoenmakers, Basic Security of the ecash Payment system.
6. 송익진, 인터넷 전자상거래 지불시스템[특집원고], 정보통신연구 제12권 제1호 1998.3.
7. M . Hallam-Baker, "Electronic Payment Schema," World Wide Web Consortium ,1995 http://www.w3.org/ECommerce/roadmap.html.
8. 강신각, Web Security and Payments .
9. 김철, 암호학의 이해, pp.55-84, 109-133, 135-161, 165-203, 1996.10.
10. Douglas R. stinson, Cryptography - Theory and Practice pp.70-110, 114-157, 223-256, 1995.
11. S.Garfinkel, PGP:Pretty Good Privacy, O'Reilly & Associates, Inc., 1995.
12. 권도균, “WWW보안과 전자화폐”, WWW-96-1, 웹코리아 제3회 WWW WorkShop, 1996.
13. Matthew K.Franklin, Michael K.Reither, "Fair Exchange with a semi-Trusted Third Party," 1996.