복수의 인터넷 쇼핑몰에서 통용되는 안전한 전자상거래 지불수단으로서 로열티시스템

윤 혜 숙[†] · 김 영 국[††] · 최 훈[†††] · 홍 승 재[††††]

요 약

전자상거래가 활성화됨에 따라 다양한 지불시스템이 연구되고, 상용화되고 있다. 고객 확보 차원에서 점차 보편화되고 있는 기존의 로열티는 지불 수단이라기보다는 고객 서비스의 일종으로 볼 수 있다. 그러나 본 논문에서 제안하는 로열티 시스템은 로열티 즉, 보너스 포인트 개념에 화폐 기능과 보안 체계를 지원하고, 각 상점마다의 개별적인 로열티 운영이 아닌 포괄적인 활용을 가능하게 함으로써 전자지불시스템으로서의 역할을 수행할 수 있다. 본 논문에서는 이러한 로열티시스템의 구조를 소개하고 지불시스템으로 활용할 수 있는 특성인 보안체계와 익명성에 중점을 두어 논의한다.

Loyalty System as a Secure Payment Scheme in Multiple Internet Shopping Malls

Hye-Suk Yoon[†] · Young-Kuk Kim[††] · Hoon Choi[†††] · Seung-Jae Hong[††††]

ABSTRACT

The growth of the Internet has brought many kinds of electronic payment schemes that can be applied to electronic commerce applications. Generally speaking conventional loyalty system is not a payment system but a part of customer service. Our loyalty system, however, adds monetary functions and security mechanism to the concept of bonus point, so it can make the electronic markets use entire bonus system as an electronic payment scheme. First, we introduce the organization and the protocol structure of the loyalty system. Next, we describe monetary characteristics, security scheme and anonymity to show our loyalty system can be used a functionally complete payment system.

1. 서 론

인터넷 환경이 계속 확장함에 따라 네트웍을 통해 상품을 팔고 사는 전자상거래에 대한 요구도 점점 커지고 있다. 전자상거래는 크게는 기업간 거래에 해당하는 CALS(Computer Aided Logistic Support)를 포함한 네트웍 상의 모든 거래를 의미하기도 하고 좁게는 소비자와 상인 간의 상거래를 의미하기도 한다. 이런 범위의 상거래든지 물건을 팔고 사기 위해서는 실세계의 화폐 기능을 대신할 수 있는 수단인 전자화폐 혹은 지불시스템이 필요하다.

로열티(loyalty) 시스템은 고객관리 차원에서 상거래에 부수되어 고객에게 보너스 포인트를 제공함으로써 고객에 대한 충성도를 높이는 방식으로 이미 보너스 카드(bonus card), 쿠폰(coupon), 할인카드(discount card), 마일리지 등의 형태로 운영되는 지불 수단이다[12]. 이러한 보너스 포인트를 이용한 로열티 시스템은 일반상

※ 본 논문은 한국과학재단이 지정한 지역협력연구센타(RRC)인 충남대학교 소프트웨어 연구센터의 지원으로 1999년도에 수행한 과제(과제번호 99 11 12-09-a-1)의 연구 결과임
† 준 회 원 충남대학교 대학원 컴퓨터과학과
†† 종신회원 충남대학교 정보통신공학부 교수
††† 정 회 원 충남대학교 정보통신공학부 교수
†††† 정 회 원 씨그미네크(주) 연구소 소장
논문접수 2000년 3월 23일, 심사완료 2000년 5월 3일

거래는 물론이고 전자상거래에서도 많이 활성화되고 있으나 아직은 그 배타적인 성격 때문에 지불수단으로의 관심은 높지 않다. 그 이유는 첫째, 보너스 포인트의 사용처가 보너스 포인트를 발행한 특정 상점이나 쇼핑 몰로만 제한되어 있어 보너스 사용자는 지급 업체마다 별도의 보너스 포인트를 가지고 있어야 하고, 둘째 보너스 포인트 자체가 지불수단으로써 사용될 수 없고 타인에게 양도가 어려워 구매 욕구가 커지지 않으며, 셋째, 보너스 포인트 판매 업체도 보너스 관리 비용이라는 부담과 소비자 확보의 어려움을 겪고 있기 때문이다.

이것은 보너스 포인트가 화폐적인 기능을 가지고 있지 않아서 발생하는 문제로 보너스 포인트에 화폐적 특성이 결합된 로열티 시스템은 인터넷 전자상거래나 실 상거래에서 완벽한 제 2의 지불수단으로 사용될 수 있을 것이다. 화폐적 특성이란 현금성, 유통성, 양도성, 분할성과 같은 원활한 교환가치를 갖는 것이며 이외에도 위조, 정보 누출 및 통신장애(communication failure)와 같은 문제에 견고한 보안 체계와 익명성 등이 제공되어야 한다[3, 6]. 상품이나 서비스의 소비자나 제공자는 어떠한 지불 시스템이 사용이 제한되어 있다거나 신뢰할만하다고 믿지 못한다면 그 지불시스템을 사용하는 전자상거래 응용을 폭 넓게 사용하지 않을 것이다.

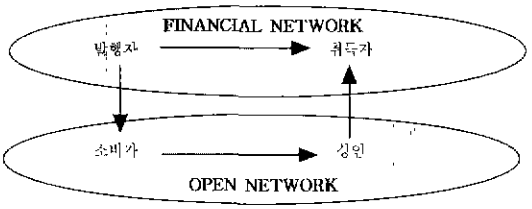
본 논문에서 제안하는 로열티 시스템은 우선 로열티 풀(loyalty pool)을 통한 범용 보너스 포인트를 다수의 인터넷 쇼핑몰에 제공하고, 각자의 보너스 포인트를 전자지갑(electronic wallet)의 형태로 로열티 회원 자신이 관리하며, 로열티 시스템의 모든 가맹점과 거래할 수 있도록 함으로써 이러한 문제를 해결한다. 일반적으로 단독 운영하는 기존의 로열티시스템은 사용자가 로열티를 사용하지 않을수록 로열티 발행자인 가맹점이나 운영자가 유리하게 되는 반면에 로열티의 현금화가 쉽지 않기 때문에 사용자의 관심이 멀어져, 얻어진 로열티는 폐기되고 사용자는 굳이 특정 가맹점을 찾지 않는 악순환이 되풀이될 수 있다. 그러나 본 로열티시스템을 사용하는 가맹점은 로열티 관리비용 절감 뿐 아니라 사용자가 대금으로 지불한 로열티를 로열티 풀에 되팔 때 가격 차이로 인한 수익을 얻을 수 있어 적극적인 로열티 정책을 펼 수 있는 장점이 있다. 한편, 본 로열티시스템은 지불 수단으로서의 안전성 확보를 위해 세션 키를 사용한 보안체계를 지원하며, 제공된 전자지갑 내에 사용자 거래내역과 개인 정보를 사용자 자신이 보유하게 함으로써 거래 익명성을 지원한다. 또한 프로토콜이 단순 명료하므로 거래비용이 적게 소요되어 가맹점이 확산된다면 그 내부에서 소액지불수단으로 사용될 수 있다.

본 논문의 구성은 먼저 2절에서는 일반적인 전자지불시스템이 가지고 있는 특성과 현황에 대해 알아보고, 3절에서는 본 논문에서 제안한 로열티시스템의 구조적인 측면을 설명하고, 4절에서는 이 로열티 시스템의 화폐적 특성과 적용된 보안체계 및 그 장점을 제시하며, 5절에서 결론을 맺도록 한다

2. 전자지불시스템의 특성과 현황

2.1 전자지불 시스템 개요

전자상거래에는 돈과 상품을 서로 교환하는 소비자와 상인, 그리고 은행과 같은 재무기관이 적어도 하나 이상 관련된다. 여기서 재무기관의 역할은 소비자가 연관된 발행자(issuer)와 상인이 가입한 취득자(acquirer)로 나눌 수 있으며 소비자가 지불한 대금은 발행자를 통해 상인과 관련된 취득자에게로 흘러간다[3, 10]. (그림 1)은 이러한 전자지불 시스템을 도식적으로 보여 준다.



(그림 1) 전자지불시스템 모델

전자지불시스템은 그 특징에 따라 여러 가지로 분류할 수 있다[6, 8]. 가장 흔한 분류 방식은 상거래 형태에 의해 분류하는 것으로 지불 브로커 형식, 인터넷 뱅킹 및 전자화폐로 나눌 수 있다. 지불 브로커 방식은 네트웍 상에서 결제가 이루어지도록 중개하는 방식으로 지불 브로커가 영수증을 발급하여 대금 지불을 브로커를 통해 하는 방식으로 신용카드 방식의 SET(Secure Electronic Transaction)을 비롯해 First Virtual 등이 이에 속한다[10]. 인터넷 뱅킹은 인터넷을 통해 은행 계좌 이체를 할 수 있어 일반적인 은행업무 뿐 아니라 대금 지불을 계좌 이체를 통해 온라인 상에서 바로 할 수 있어 지불시스템 역할을 대신할 수 있다.

이외에 대부분의 시스템은 전자화폐 형으로 네트웍 상에서 화폐 가치를 전송할 수 있어 소액거래에 유용한 네트웍 형과 IC 카드를 이용해 실세계와 인터넷에서 모두 쓸 수 있는 IC 카드형이 존재한다. 네트웍 형의 예로는 Netbill, Ecash[9] 등이 있으며 IC 카드형은 캐나다의 몬덱스 카드[2]가 있다. 전자상거래가 활성화되기 위해서는 무엇보다도 전자화폐 형태가 널리 통용되어 일반적인 상거래를 지원할 수 있어야 한다.

그 외에도 지불시스템을 분류하는 수단으로 추적 가능 여부를 따져 전자상거래를 구분할 수 있고 또 지불처리방식이나 자금의 흐름에 의해 구분하기도 한다. 지불처리방식은 전자화폐의 유효성 체크 시점에 기준을 맞춘 것으로 온라인과 오프라인 형태가 있다. 온라인의 경우 대금지불로 받은 전자화폐를 승인하기 전에 발행자에 확인하는 방식으로 대부분의 네트웍형 지불방식에 통용된다. 오프라인은 지불 받은 전자화폐를 승인하고 후에 발행자에 확인하는 형태로 IC 카드형 전자화폐가 이에 해당된다[5, 11]. 자금의 흐름은 전자화폐의 형태를 의미하며 현금과 유사한 특성을 갖는 토큰형 현금(Token money)과 계좌 이체를 이용하여 실제적인 지불이 발생하는 기호형 현금(Notational Money)으로 나눌 수 있다. 많은 지불시스템이 기호형 현금 형태를 가지고 있고 몬덱스 카드나 Ecash 같은 시스템은 토큰형 현금으로 볼 수 있다. 지불 시스템은 분류 방식에 따라 여러 형태로 구분할 수 있는데 로열티 시스템은 온라인 전자화폐로 토큰형 현금으로 분류할 수 있다[1].

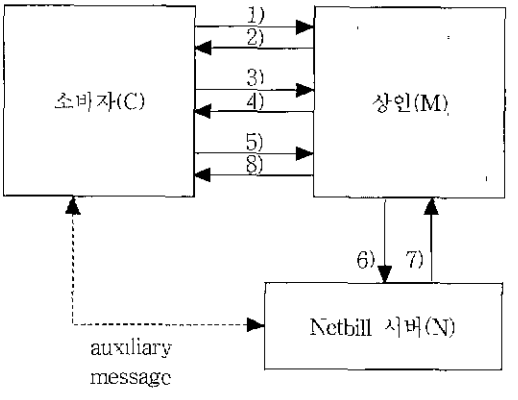
2.2 전자화폐의 고려사항

전자지불수단으로서 전자화폐시스템을 설계할 때는 고려해야 할 요소가 여러 가지 있다. 우선은 지불시스템을 사용하는데 필요한 하부구조에 대한 의존도가 어느 정도인지를 고려해야 한다. 지불 시스템을 개발하여 사용할 때 여러 가지 부대 장비나 네트웍 형태에 대한 요구사항이 많다면 이 요구사항을 쉽게 충족시킬 수 없는 환경 하에서는 사용하기 어려울 것이며 가격 대 성능 비를 충분히 감안해야 한다[9]. 또한 화폐로서의 기능에 충실하기 위해서 현금성, 유통성, 양도성 등을 갖추고 있어야 하며, 복사나 위조가 쉽게 발생하지 않도록 보안 측면을 고려해야 하며 지불시스템을 관장하는 시스템 자체와 전자화폐가 유통되는 통신이 도청되지 않도록 대비해야 한다. 전자상거래에서의 보안은 시스템 운영의 신뢰성이나 시스템의 특성에 따라 차이가 있으나 다른 어떤 요소보다 중요하다. 사실상 익명성의 경우도 보안 요소의 한 부분으로 포함할 수 있으나 여기서는 주로 기밀성, 신원 인증, 무결성 등의 네트웍 보안으로 국한시킬 수 있다[4, 7]. 그리고 상거래 시스템의 보안을 어떻게 유지해야 하는 지에 대해 단일 명세를 제공하기는 불가능하고 어떠한 요구사항이 만족되어야 하는지는 제시할 수 있다. 일단 무결성과 인증을 위해 소비자 계좌로부터의 지불을 승인하는 메시지는 소비자에 의해 실제로 통신은 쉽게 가로채이 메시지나 신원 위조, 변경 등이 일어날 수 있다. 현재 대부분의 전자상거래시스템은 신뢰할 수 있는 인증서 발행과 암호화에 주력하고 있다. 또한 데이터베이스 트랜잭션의 보안은 covert channel의 차단 등을 통해 이루어지고 있다[13]. 지불시스템은 일반 현금 사용과 마찬가지로 거래 주체의 사생활 보호를 위해 자금 흐름의 추적을 할 수 없도록 설계되어야 전자상거래가 활성화될 수 있을 것이다. 이것은 익명성과도 밀접한 관계가 있다. 전자상거래에서 익명성(anonymity)은 어떤 소비자가 자신의 구매 내용을 타인에게 알리고 싶지 않은 요구를 충족시키기 위한 것이다. 익명성을 원하는 이유는 소비자가 구매 내용을 밝히고 싶지 않거나 혹은 자신의 구매로 인해 자신의 이름이 다른 마케팅이나 메일링 리스트에 첨가되지 않기를 바라기 때문일 것이다. 예를 들어, 전자상거래시스템의 지능형 에이전트(Intelligent Agent)의 경우 소비자 개인의 소비 성향을 관찰하여 개개인의 쇼핑도우미 역할로 소비자에게 편리함을 주나 이러한 점이 악용될 경우 구매자가 모르는 사이 소비자의 개인 정보가 다른 곳으로 전이되어 피해를 받을 수 있다. 이러한 문제는 현재 전자상거래 시스템 서버의 신뢰성에 전적으로 의존하고 있으나 전자상거래의 활성화를 위해서는 소비자의 익명성이 보장될 필요가 있다. 익명성은 상거래 상의 전자화폐가 암호화된 토큰 형태로 제공되어, 상인은 이 돈의 유효성(validity)은 체크할 수 있으나 구매자의 신원 확인은 할 수 없어야 하며, 은행 역시 소비자의 이중 지불이나 위조화폐와 같은 문제가 발생한 경우 외에는 자금의 흐름을 추적할 수 없어야 한다. 상인이나 인증기관이 소비자에 대한 개인 정보를 알지 못하도록 해야 개인 정보의 누출이나 불법 사용으로 인한 문제를 줄일 수 있고 소비자도 안심하고 전자상거래에 참여할 수 있기 때문이다. 그밖에도 현금성이나 양도성

및 지불시스템을 손쉽게 사용할 수 있도록 가용성을 고려해야 할 것이다[7]

2.3 지불시스템 사례 연구

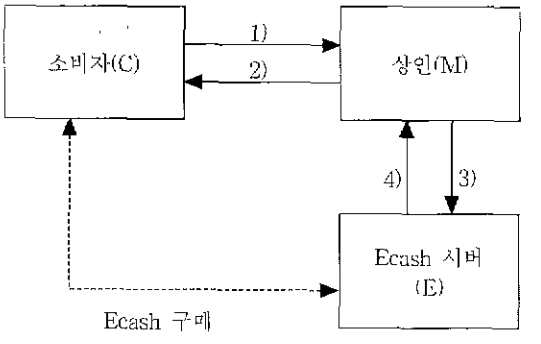
로열티시스템은 완벽한 지불수단으로 사용하기는 어려우나 소액지불(micropayment)이나 부분 지불과 같이 제 2의 지불수단으로 사용할 수 있다. 로열티시스템과 같이 소액지불에 편리한 기존의 네트웍형 전자화폐로 Netbill과 Ecash를 들 수 있다[1, 3, 15]. Netbill은 인터넷 상에서 주로 정보상품(information goods)과 네트웍을 통해 배달 가능한 서비스 판매를 위한 소액지불 수단이다. 정보 상품은 인터넷에 분포한 15,000개 정도의 데이터베이스가 대상이 될 수 있으며 시장 규모가 크며 가격 역시 copy 당 수십 원에서 수백만 원으로 그 범위가 넓으나 증권정보나 기상 등의 소액 지불을 요구하는 상품의 거래가 가장 활성화될 것이다. 이러한 소액 지불은 트랜잭션 비용을 최소화 시키기 위한 방법이 필요하고 잦은 거래가 지원되도록 서버의 트레픽 집중을 피함으로써 많은 고객 처리가 가능한 형태를 취해야 한다. 또한 거래 고객의 익명성과 원자성을 보장하여 고객이 상품 거래에 부담을 느끼지 않도록 구현되어야 한다. Netbill은 이러한 점을 고려하여 트랜잭션의 원자성과 익명성과 더불어 소액지불에 적합한 구조를 제공하고 있다[4]. (그림 2)는 이러한 Netbill 지불 프로토콜이다



(그림 2) Netbill 지불 프로토콜

1) C => M 상품가격 문의
2) M => C : 상품가격 제시
3) C => M : 상품 주문
4) M => C . 암호키 K로 암호화된 상품 배달
5) C => M : 서명된 전자주문서(EPO)
6) M => N : 인증된 EPO(K 포함)
7) N => M : 서명된 결과(K 포함)
8) M => C : 서명된 결과(K 포함)

Ecash는 등록된 일련번호를 부여하여 사용하는 전자 동전(electronic coin) 형태의 소액 지불 수단으로 사용되어 일반상거래 동전역할을 한다고 볼 수 있다[15]. Ecash는 화폐를 디지털 정보의 형태로 다루어 전화나 팩스, 텔레비전 케이블 등 어떤 매체르든지 전송될 수 있는 특징을 가지고 있으며, 화폐 내에 피지불자의 이름을 포함하여 암호화함으로써 보안을 유지한다. (그림 3)은 Ecash를 사용하는 지불 프로토콜이다.



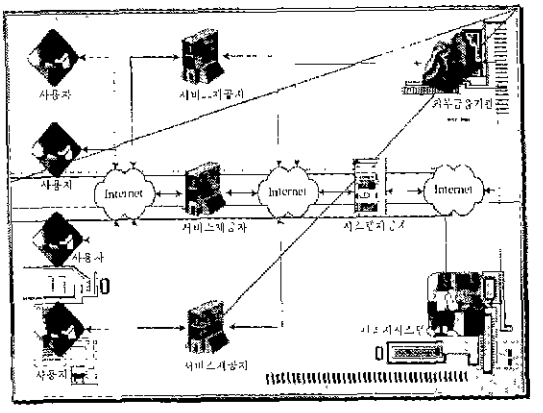
(그림 3) Ecash 트랜잭션 프로토콜

1) C => M : 상품주문 및 대금지불
2) M => C : 상품 제공
3) M => E Ecash 인증요청
4) E => M Ecash 인증 결과

3. 로열티 시스템(Loyalty System)의 구조

3.1 구 성

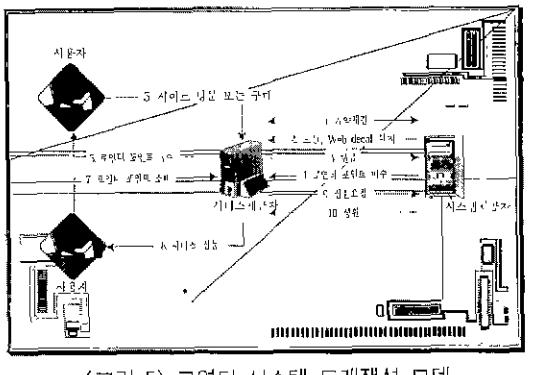
본 논문에서 제안하는 로열티시스템은 크게 사용자, 서비스 제공자, 시스템 제공자, 관리자 시스템으로 구성된다. (그림 4)에서 사용자는 인터넷을 통해 가상 쇼핑몰인 서비스 제공지로 접속하게 되며 서비스 제공지 역시 시스템 제공자와 인터넷으로 연결된다. 또한 시스템 제공자는 원격관리를 위해 관리지시스템과 금융거래를 위해 외부금융기관과도 인터넷으로 연결된다.



(그림 4) 로열티 시스템 구성도

3.2 트랜잭션 모델

(그림 5)에 나타난 로열티 시스템의 트랜잭션 모델은 사용자, 서비스 제공자, 시스템 제공자가 포함되며 시스템 제공자와 서비스 제공자 간에 계약 체결 후 로열티 구매/판매/상환을 위한 프로토콜과 사용자와 서비스 제공자 간에 로열티 수여 및 소비를 위한 프로토콜이 이루어진다. 다음은 각각의 프로토콜 내용이다.



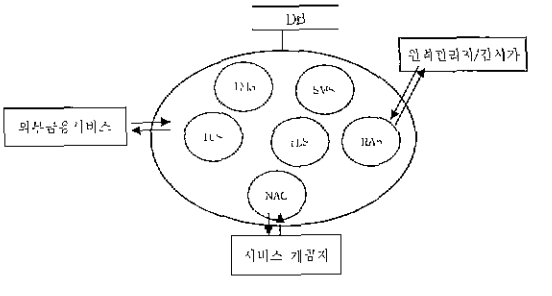
(그림 5) 로열티 시스템 트랜잭션 모델

1. 인터넷 쇼핑몰은 시스템 제공자와 서비스 제공자로서의 계약을 체결한다.
2. 시스템 제공자는 쇼핑몰에 서비스 제공자 모듈과 쇼핑몰 인증을 위한 Web Decal을 설치한다.
3. 서비스 제공자는 사용자에게 지급할 로열티 포인트에 대한 금액을 시스템 제공자에게 지불한다.
4. 시스템 제공자는 서비스 제공자에게 로열티 포인트를 지급한다.
5. 사용자는 쇼핑몰에 접속하여 물품을 구매하거나 서비스를 이용한다
6. 서비스 제공자는 물품구매나 서비스 이용에 대한 로열티 포인트를 사용자에게 지급한다
7. 로열티 포인트를 지급 받은 사용자는 쇼핑몰에 접속하여 자신이 보유하고 있는 로열티 포인트를 현금처럼 사용하여 물품구매나 서비스 이용에 사용한다. 여기서는 로열티 포인트를 지급 받은 쇼핑몰이 아니라도 상관없으며, 로열티 포인트를 사용할 수 있는 서비스 제공자라면 어떠한 쇼핑몰이라도 사용자는 로열티 포인트를 제약 없이 사용할 수 있다.
8. 쇼핑몰은 사용자에게 제시한 로열티 포인트 금액에 대한 물품이나 서비스를 제공한다
9. 서비스 제공자는 사용자들에게서 물품구매나 서비스 이용 대금으로 받은 로열티 포인트를 시스템 제공자에게 판매하여 수익을 얻는다.
10. 시스템 제공자는 서비스 제공자가 제시한 로열티 포인트에 대해 현금으로 지급하게 된다.

각 서비스 제공자는 로열티 포인트를 사용하는 고객이 자신의 회원이 아니더라도 로열티 시스템의 모든 사용자들은 모두 자신의 잠재고객이 될 수 있는 효과를 얻을 수 있으며, 사용자의 입장에서는 일일이 각 서비스 제공자에 회원으로 등록하지 않아도 로열티 시스템의 회원이 된다면 가입된 모든 쇼핑몰에서 로열티 포인트를 아무런 제약 없이 사용할 수 있다는 장점이 있다.

3.3 시스템제공자 구조

(그림 6)은 시스템제공자 구조로 시스템제공자는 보안 처리, 로열티의 판매,구매,상환 및 사용자의 정보 조회 트랜잭션 처리, 트랜잭션 백업, 외부금융서비스와의 인터페이스, 가맹점 정보 DB(Database)와의 인터페이



(그림 6) 시스템제공자 구조

스 역할을 수행하여 로열티를 공유할 수 있는 수단을 제공한다. 이러한 기능을 수행하는 시스템제공자 모듈은 NAC, SMS, TCS, TMS, TLS, RAS로 각 모듈의 역할은 다음과 같다.

• NAC(Network Access Controller)
서비스 제공자와 시스템 제공자 사이의 다중 연결(multi connection) 관리, 통신처리, CRC(Cyclic Redundancy Check) 처리

• SMS(Security Management System)
서비스 제공자, 시스템 제공자 사이의 메시지 암호화, 복호화에 관련된 기능 제공

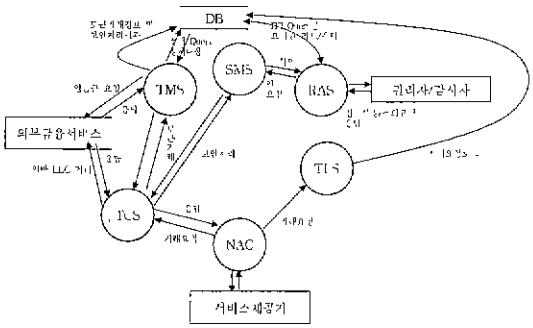
• TCS(Token Capture System)
로열티 관련 데이터와 EDC(Electronic Data Capture) 데이터를 분리하여 로열티 관련 데이터는 TMS로, EDC 관련 데이터는 VAN(Value Added Network)으로 중계

• TMS(Token Management System)
로열티 토큰 구매, 판매 등과 같은 로열티 관련 서비스 제공, DB와의 인터페이스

• TLS(Transaction Log Server)
안정성을 위해 시스템 제공자로 보내진 모든 트랜잭션을 백업

• RAS(Remote Access Server)
관리자나 감사자의 접근 수단을 제공

(그림 7)에 나타난 이들 기능 모듈 간의 DFD(Data Flow Diagram)를 살펴보면, 서비스 제공자로부터 토큰 구매, 판매, 환불, 정보조회 중에서 한 서비스 요청이 NAC로 보내지고, NAC는 요청 메시지를 받아 CRC를 검사한 뒤에 올바른 메시지라고 판명되면 TLS와 TCS로 보내게 된다. CRC 검사를 통해 메시지 형태의 이상 유무를 확인하고 이 메시지가 등록된 서비스 제공자로부터 보내온 것인 지의 여부를 조사한다. TCS에서는 수신된 메시지를 SMS로 보내 복호화하고 로열티 관련 데이터와 EDC(Electronic Data Capture) 관련 데이터를 분류한 후에, 로열티 데이터는 TMS로 전송하고 EDC 관련 데이터는 VAN(Value Added Network)을 통해 외부 금융 서비스로 전달한다. 이와 같이 본 로열티 시스템은 서비스 제공자들이 별도의 통신 수단을 구비하지 않아도 외부 VAN 사업자들과 통신할 수 있는 서비스를 제공한다. 한편, TMS는 메시지를 분석하여, 서비스 제공자, 즉 가맹점 별 로열티 서비스 정책이 저장된 정보 DB를 조회한 후 이에 따라 로열티 처리를 수행한다. SMS는 RAS와 TMS, TCS의 요청에 따라 메시지의 암호화, 사용자 인증 등을 수행한다.



(그림 7) 시스템제공자 DFD

3.4 서비스제공자 구조

서비스제공자는 로열티서비스 가맹점으로 등록한 인터넷 쇼핑몰이나 혹은 PSTN 망으로 연결된 상점에서 수행되는 모듈로 처음 가맹점으로 등록할 때 Web Decal 혹은 터미널 형태로 설치된다. 서비스제공자의 트랜잭션은 로열티 풀로부터 로열티 고객에게 제공할 토큰을 사오거나 혹은 고객에게 대금으로 지불 받은 로열티를 모아 팔거나 상환하는 작업인 토큰 거래 트랜잭션과 DB 정보 조회, 변경작업 트랜잭션으로 구성된다. 서비스제공자의 데이터베이스에는 보안처리를 위한 키 정보 및 로열티 처리를 수행하기 위한 가맹점의 토큰 정보가 저장되어 있다. 서비스 제공자의 구조는 (그림 8)의 형태를 가지며 각 모듈의 기능은 다음과 같다.

• 통신시스템
시스템 제공자와의 연결 관리, 통신처리, CRC(Cyclic Redundancy Check) 체크

• 사용자 및 신용카드 처리
서비스 제공자로 접속하는 사용자 처리, 로열티/신용카드 처리

• 로열티 서비스 처리
사용자 처리로부터 로열티 처리에 대한 요청을 받아

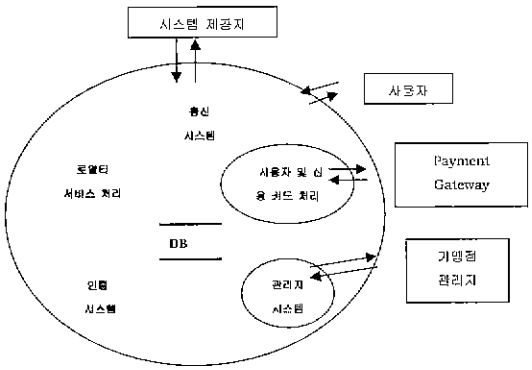
처리, 사용자에게 정책에 따른 로열티 지급

● 인증 시스템

관리자 시스템으로 접속하는 관리자 인증, 사용자 인증 처리

● 관리자 시스템

가맹점 관리자의 서비스 제공자 접근 수단 제공, 서비스 제공자의 로열티 관리에 대한 정책 설정 및 조회, 시스템 제공자와 로열티 거래 요청



(그림 8) 서비스제공자 구조

4. 지불 수단으로서의 로열티시스템

4.1 화폐로서의 특성

● 현금성

기존에 인터넷 전자상거래나 실 상거래에서 통용되는 로열티의 개념은 고객에 대한 보너스 포인트 점수의 개념으로 보너스 포인트 자체는 현금성을 가지고 있지 않다. 즉, 보너스 포인트로 할인을 받거나 사은품은 받을 수는 있지만 보너스 포인트 자체로 물품구매 행위는 할 수 없는 제약이 따른다. 그러나 본 로열티 시스템에서의 로열티의 개념은 완전한 현금성을 가진다. (그림 9)에서와 같이 서비스 제공자로부터 부여 받은 로열티로 물품구매 행위를 할 수 있다는 것은 로열티 자체가 완전한 현금성을 가지고 있다는 것을 의미한다.

● 유통성

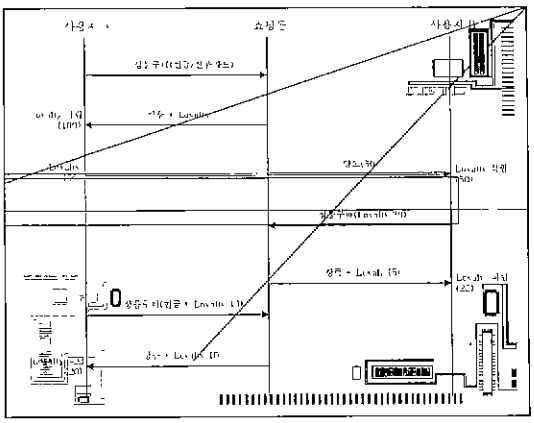
본 로열티시스템에서의 로열티는 로열티 풀에 등록된 서비스 제공자에서는 현금과 동일한 유통성을 지닌다. 역시 기존 로열티의 유통범위는 로열티를 부여한 해당 상점이나 계열사 정도로 제한되었으나 본 시스템에서의 로열티는 풀에 등록된 서비스 제공자라면 모두 자신이 가지고 있는 로열티를 사용할 수 있다. 만일 풀에 많은 서비스 제공자를 유치할 수 있다면 이는 현금과 거의 동일한 수준의 유통성을 지니게 되는 것이다. (그림 9)는 다수의 쇼핑 몰에서 로열티가 유통되는 과정이 나타내고 있다.

● 양도성

일반 화폐는 양도성 즉, 자신이 소유하고 있는 화폐의 가치를 다른 사람에게 줄 수 있는 특성이 있는데, 기존의 로열티는 일반적으로 이것을 허용하지 않는다. 그러나 본 로열티 시스템은 (그림 9)에서 보듯이 자신이 가지고 있는 로열티를 다른 사람에게 줄 수도 있고 또 양도 받은 로열티의 권리를 행사하는데 아무런 제한이 없다.

● 분할성

기존에 사용되고 있는 로열티라고 부르는 보너스 점수의 개념에는 분할성이 포함되어 있지 않다. 즉 로열티가 일정으로 쌓여야만 쌓은 만큼의 권한을 행사할 수 있고 일반적인 화폐처럼 로열티의 일부만을 사용할 수 있는 분할성이 없다. 그러니 우리가 제안한 로열티 시스템에서의 로열티는 현금과 동일한 분할성이 적용되며, 로열티의 현금성과 유통성에 이 분할성과 양도성이 더해져 로열티는 완전한 화폐의 가치를 지니게 된다. (그림 9)에 적립된 로열티를 분할하여 다른 사용자에게 양도하고, 또 물품 구매에 일부를 이용하는 것을 볼 수 있다.

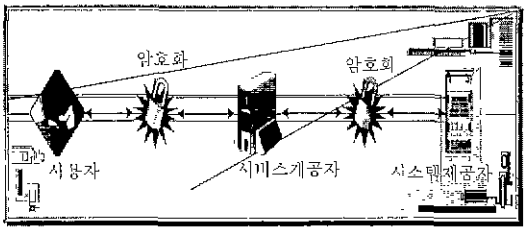


(그림 9) 로열티의 화폐적 특성

4.2 안전한 지불수단으로서의 특성

4.2.1 보안 체계

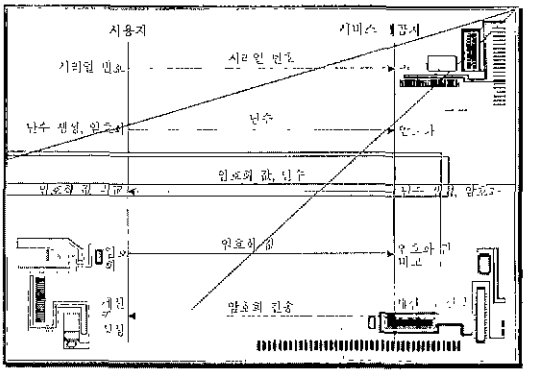
본 로열티 시스템의 사용자와 서비스 제공자 간, 서비스 제공자와 시스템 제공자간, 사용자와 시스템 제공자 간에 네트워크을 통해 전달되는 모든 데이터를 반드시 암호화되어 전달됨으로써 상호간 메시지 인증이 가능하다. 일반적으로 메시지 인증은 수신자에게 송신자의 신원을 증명함으로써 가능하며 공유키 방식이나 공개키 방식이 이용된다. 공유키 방식 암호화 알고리즘은 동일한 영구 키로 암호화와 복호화가 이루어지므로 네트워크을 오가는 패킷을 분석하면 키를 찾아 낼 수 있다는 단점을 가지고 있으며 반면에 공개키에 비해 키 관리가 단순하다[14]. 본 로열티 시스템에서는 기존의 공유키 방식이 가지는 문제점을 보완하기 위해 세션 키라는 임시 키를 이용하는 공유키 방식 알고리즘을 사용한다. 이 방식에서는 모듈 간 트랜잭션이 발생할 때마다 세션 키라는 임시 키를 생성하여 암호화 및 복호화에 이용하므로 네트워크 패킷을 수집하더라도 패킷의 암호화에 이용된 키가 항상 다르기 때문에 키를 찾아내기는 불가능하다. (그림 11)은 사용자와 서비스 제공자 간 세션 키를 만드는 과정을 도식화한 것으로 서비스 제공자와 시스템 제공자 간, 사용자와 시스템 제공자 간의 메시지 인증도 이와 유사한 방식으로 이루어진다.



(그림 10) 로열티 시스템 보안

1 사용자는 자신의 시리얼 번호를 서비스 제공자로 전달한다. 사용자는 시스템 제공자에 등록할 때 자신의 시리얼 번호를 이용하여 Mother Key로부터 파생된 Daughter Key를 가지고 있으므로 서비스 제공자 역시 전달 받은 시리얼 번호로 시스템 제공자로부터 지급 받은 Mother Key Table를 이용하여 그 사용자가 가지고 있는 Daughter Key를 생성할 수 있다

2. 사용자는 난수를 생성하여, 자신의 Daughter Key로 암호화 한 후 저장하고, 서비스 제공자에게 난수를 전달한다.
3. 난수를 전달 받은 서비스 제공자는 사용자가 생성한 난수를 자신이 생성한 Daughter Key로 암호화하고, 자신의 난수를 생성한다. 난수를 생성한 후 서비스 제공자가 사용자의 난수를 암호화한 결과와 자신이 생성한 난수를 사용자에게 전달한다.
4. 서비스 제공자로부터 난수와 암호화 결과를 받은 사용자는 자신이 암호화한 결과와 전달 받은 암호화 결과를 비교하여 같을 경우 서비스 제공자로부터 전달 받은 난수를 자신의 Daughter Key로 암호화한 후 그 결과를 서비스 제공자에게 전달한다.
5. 서비스 제공자는 사용자로부터 전달 받은 암호화 결과와 자신이 암호화한 결과와 비교하여 같을 경우 인증이 성립됐으므로 두 개의 난수와 Daughter Key를 이용하여 세션 키를 생성하고 전달 메시지의 암호화에 이용한다.

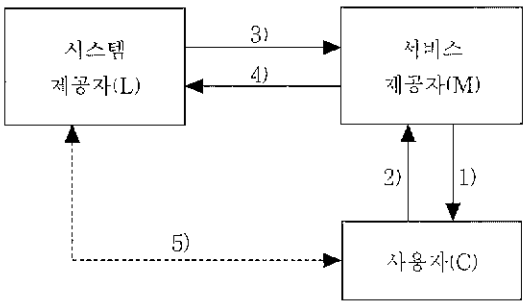


(그림 11) 사용자-서비스 제공자 간 세션 키 생성 방법 (인증과정)

이와 같이 세션 키 방식을 사용하여 메시지 인증과 상호 간 인증이 가능하다. 또한 로열티 포인트는 화폐의 개념을 지니기 때문에 사용자의 로컬 컴퓨터에 그 정보가 저장되는 특징을 가지고 있다 그러므로 사용자의 로열티 포인트에 대한 인증이 필요한데 본 시스템에서는 NONCE(No more than ONCE)를 사용하여 사용자의 로열티 포인트에 대한 인증을 함으로써 부정사용을 피할 수 있다[14].

4.2.2 익명성

본 논문에서 제안한 로열티 시스템의 프로토콜 구조는 (그림 12)에 나타난 바와 같이 지극히 단순하여 낮은 비용으로 트랜잭션 처리가 가능하므로 소액 처리에 적합하다. 사용자가 일단 시스템 제공자에 등록을 마친 경우, 로열티에 가입한 어떤 서비스 제공자와의 트랜잭션도 시스템 제공자와 독립적으로 발생할 수 있다. 이것은 빠른 처리를 가능하게 하는 요인이기도 하며 사용자의 익명성에도 일조할 수 있다. 즉, 사용자는 로열티 회원으로 다양한 쇼핑몰에서 복합적인 거래를 하지만 전체적인 거래내용은 이느 곳에서도 알 수 없으므로 사용자의 사생활 보호에 기여할 수 있다. 만일 백화점 형태의 쇼핑몰에서 여러 가지 물건을 구매했다면 사용자의 거래 내역이 집중되어 누출될 가능성이 크기 때문이다. 사용자의 익명성을 지키기 위해서는 가능한 정보를 적게 노출시킬 필요가 있다. 그러나 악의의 사용자나 트랜잭션에 문제가 생기 복구할 필요가 생길 때 사용자에 대한 정보가 없어 추적이 불가능하다면 이 또한 트랜잭션의 원자성을 지원할 수 없는 문제가 있다. 본 로열티 시스템에서는 사용자 정보를 시스템 제공자와 서비스 제공자에 분산시킴으로써 이러한 문제를 해결할 수 있다.



1) C => M : 물품 구매 요청
2) M => C : 인증 및 거래 결과
3) M => L : 로열티 구매/판매/상환, 정보 조회요청
4) L => M : 인증 및 거래 결과, 조회정보
5) C => L 사용자 정보 등록, 조회, 변경, 삭제

(그림 12) 로열티 시스템 프로토콜

4.3 트랜잭션 특성

본 논문에서 제안하는 범용 로열티시스템은 로열티 사용 영역이 특정 분야의 가맹점이 아닌 본 로열티시스템을 채택한 모든 분야의 쇼핑몰로 확대될 수 있기 때문에 가입한 다중의 쇼핑몰 공간에서 소액 지불이나 부분 지불 수단으로 활용이 가능하다. 가맹점 역시 시스템제공자에서 로열티를 구매할 때와 사용자로부터 대금으로 지불 받은 로열티를 다시 판매할 때 수익이 발생하므로 적극적으로 사용할 수 있다.

그런데 전자화폐가 소액지불수단으로 사용되려면 몇 가지 갖추어야 할 요건이 있다. 첫째로, 트랜잭션 관리 비용을 최소화 시켜 잦은 거래를 지원해야 한다. 트랜잭션 관리비용은 프로토콜 전송횟수와 메시지 길이, 암호화 정도, 내부적인 DB 액세스 횟수 등 여러 가지를 고려할 수 있다. 시스템 내부에서 수행되는 내용은 비슷하다고 가정하고 프로토콜 전송횟수와 암호화 정도만을 비교해보자. 앞서 소개한 Netbill은 Netbill 서버가 소비자와 상인의 계좌를 보유하고 있어 거래가 발생하면 서버 내의 상인의 계좌에서 소비자 계좌로 자금 이체를 하고 정산은 모아서 처리함으로써 트랜잭션 비용을 절감한다 Ecash는 동전 형태로 자신의 PC에 보관하여 사용하고 Ecash를 받은 상점에서 받은 대금의 인증을 위해 Ecash Mint에 확인하는 형태로 트랜잭션이 발생한다. 본 로열티시스템은 자신의 PC에 로열티를 보관하며 로열티 가맹점은 주기별 혹은 비정기적으로 모아 정산하므로 두 시스템에 비해 상대적으로 적은 트랜잭션 비용이 소요된다. 또 암호화 정도의 경우 Netbill과 본 로열티시스템은 128-bit 크기의 키를, Ecash는 768-bit 크기의 키를 갖는다. Ecash는 트랜잭션 비용 면에서는 불리하나 상대적으로 안전한 시스템으로 볼 수 있다.

둘째로 서버의 트래픽 집중을 피하고 많은 고객 처리가 가능한 형태를 취해야 한다. 이것은 전자상거래 시스템의 확장가능성(scalability)을 의미하며 서버가 하나의 트랜잭션을 처리하기 위한 오버헤드(overhead)가 적어야 한다. 서버가 관여하는 프로토콜 횟수만을 고려한다면 Netbill과 Ecash는 인증을 위한 2번의 프로토콜이 발생한다 반면에 본 로열티 시스템은 서비스 제공자가 사용자의 시리얼 번호로 키 확인이 가능하므로 별도의 프로토콜이 필요하지 않다. 이와 같이 본 로열티시스템은 트랜잭션 특성 면에서 소액지불수단으로 적합하다는 것을 알 수 있다

5. 결 론

전자상거래에서는 여러 가지 형태의 지불 수단이 사용되며 새롭게 등장하고 있다. 이들 지불시스템은 제대로 활용되기 위해서는 유통성, 암도성과 같이 현금과 같은 성격과 안전성을 지원하기 위한 보안 체계가

지원되어야 하며 이밖에도 익명성 등이 뒷받침되어야 할 것이다. 본 논문에서 제안한 로열티 시스템은 기존의 개별적인 보너스 포인트 시스템에 비하여 활용성과 관리의 편의성, 확장성 및 경제성 면에서 우수하고, 안전하고 관리가 편리한 보안체계를 제공하며, 사용자가 자신의 PC에 전자지갑 형태로 포인트를 관리하기 때문에 익명성을 지원할 수 있다. 또한 프로토콜이 단순한 특징이 있다. 이러한 점은 앞으로 인터넷 전자상거래에서 많은 가맹점을 확보하게 된다면 그 내부에서 소액지불수단으로 활용될 수도 있을 것이다.

현재 인터넷 전자상거래에서 포탈 사이트(portal site)는 거대 쇼핑몰의 운영이 기본적으로 한계에 부딪치고 있다 이것은 쇼핑몰 내의 많은 상품 소개를 위한 데이터베이스의 비대화로 정보처리 능력이 저하되고 관리가 어려워지기 때문이다. 이러한 문제를 해결할 수 있는 대안으로 다양한 전문 사이트를 묶어 소개하는 허브 사이트(hub site)를 들 수 있다. 앞으로 본 로열티 시스템은 로열티의 제공을 통해 이러한 허브 사이트의 역할을 할 수 있도록 시스템을 확장하고 보완하는 것이 과제라 할 수 있다

참 고 문 헌

[1] L.Jean Camp, Marvin Sirbu, J.D. Tygar, "Token and Notational Money in Electronic Commerce," [http://www.cs.cmu.edu/afs/andrew.cmu.edu/inst/ini/www/NETBILL/pubs/camp/usenix.html]

[2] Felix Stalder, Andrew Clement, "Exploring Policy Issue of Electronic Cash : The Mondex Case," 1998, 7. [http://www fis.utoronto ca/research/iprp/dipcii/workap8.htm]

[3] P.Jason, M.Waidner., "Electronic Payment over Open Networks," 1995,4. [http://www.zurich.ibm com/~sti/g-kk/publications/1995/JaWa95.dir/JaWa95c.html]

[4] J.D. Tygar., "Atomicity in Electronic Commerce," In proceedings of 15-th Annual ACM Symposium on principles of Distributed Computing, pp.8-26, May 1996.

[5] 한국전산원, 전자지불 표준 동향분석에 관한 연구, 1998

[6] 류재철외 5인., "안전한 인터넷 전자지불 프로토콜의 설계 및 구현", 정보처리학회논문지, 1999.

[7] N. Asokan, P A Janson, M. Steiner, M Waidner, "The State of the Art in Electronic Payment Systems," Sept 1997 IEEE Computer.

[8] 김기병, 김수홍., "전자상거래를 위한 지불방법", 정보처리학회지, 1999.

[9] B Cox, J.D. Tygar, M. Sirbu, "Netbill Security and Transaction Protocol."

[10] http://www.fis.utoronto.ca/research/iprp/dipcii/workpap8.htm

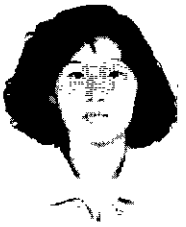
[11] http://www.intertrader.com/library/DigitalMoneyOnline

[12] http://www.gemplus.com

[13] Sang H. Son, Ravi Mukkamala and Rasikan David, "Integrating Security and Real-Time Requirement using Covert Channel Capacity."

[14] William Stalling, "Cryptography and Network Security : Principles and Practice," PrentuceHall.

[15] http://www.ecash.net



윤 혜 숙

e-mail : hsyoon@cs.cnu.ac.kr

1986년 서울대학교 계산통계학과 졸업

1988년 서울대학교 계산통계학과 석사

1988년~1995년 한국통신 진자교환운용연구단 전임연구원

1999년~현재 충남대학교 컴퓨터과학과 박사과정 재학중

김 영 국

e-mail ykim@cs.cnu.ac.kr

1985년 서울대학교 계산통계학과 졸업

1987년 서울대학교 계산통계학과 석사

1995년 버지니아대학교 컴퓨터과학과 박사

1995년 VTT(Technical Research Centre of Finland) 방문연구원

1995년 SINTEF Telecom & Informatics, Norway 방문연구원

1996년~현재 충남대학교 정보통신공학부 조교수

관심분야 : 실시간데이타베이스시스템, 전자상거래시스템, 분산정보시스템

최 훈

e-mail : hchoi@comeng.cnu.ac.kr
1983년 서울대학교 컴퓨터공학과 졸업
1990년 듀크대학교 전산학 석사
1993년 듀크대학교 전산학 박사
1983년~1996년 한국전자통신연구원 책임연구원
1996년~현재 충남대학교 정보통신공학부 조교수
관심분야 : 분산시스템, 컴퓨터네트워크, 이동컴퓨팅

홍 승 재

e-mail : sjhong@sigmatec.co.kr
1994년 콜로라도 테크니컬 대학 전산과학 졸업
1995년 LG정보통신(주) 소프트웨어연구소 연구원
1996년 한국신용통신(주) 연구개발실 연구원
1997년~1998년 BR네트콤 연구개발실 실장
1999년~현재 씨그미테크(주) 연구소 소장
관심분야 : 스마트카드, 전자상거래 보안