

Millicent를 이용한 웹 상에서의 소액지불 시스템 활용방안

The Practical Usage of Inexpensive Payment System Using Millicent on the WWW

박정선* · 김동우** · 유명종** · 정우필**

* 명지대학교 산업공학과

Abstract

최근 인터넷이 확산되면서, 전자상거래 규모와 분야도 점점 확대되어 가고 있고, 이에 따라 전자상거래에 대한 모든 정의는 전자상거래 영역을 바라보는 시각에 따라 다를 수 있다. 광범위하게 말한다면, 전자상거래는 새로운 비즈니스 기회에 대한 창출과 개척, 그리고 '비즈니스 가치 창출' 혹은 '최소의 비용으로 최대 효과'를 의미하는 수단일 수도 있다.

이렇게 전자상거래의 규모와 분야가 점점 확대되어 감에 따라 전자상거래의 분야는 기업 영업의 보조적인 역할과 제한적인 쇼핑물에서 시작되어 정보서비스, 온라인 출판, 오락 방송 등으로 점차 확대되어 가고 있다. 전자상거래의 거래 규모에 있어서 현재의 규모는 실세계의 거래규모에 비교되지 않을 만큼 미미하지만, 갈수록 규모가 기하급수적으로 증가할 것으로 예상되고 있다.

이에 따라 전자상거래가 부각되면서 구매자의 욕구를 충족시키기 위해 전자 쇼핑물이 등장하게 되었고 이러한 인터넷을 통해 이루어지는 전자상거래인 전자쇼핑물은 고객과 기업간에 물건을 판매하고, 상품대금을 지불하는 두 가지 형태로 나타나며, 가장 중요한 문제는 지불 방법을 선택하는 것이다. 또한 이러한 전자상거래의 활성화를 위해 고려되어야 할 사항은 상품에 대한 안전한 대금결제이다.

기존의 대금결제는 소비자가 직접 은행지로를 통해 이루어지고 있고 이 방식은 소비자가 직접 은행에 가야하는 불편으로 인해 전자상거래 활성 저해요인으로 지적되고 있다. 따라서, 네트워크를 통해 안전하게 대금을 지불하는 수단이 대두하게 되었다.

인터넷상에서 일반적으로 사용할 수 있는 방법은 전자화폐방식과 지불브로커 방식으로 나눌 수 있다. 다시 지불방식으로 구별하자면, 크게 가입자 기반(Account)의 방식, 트랜잭션을 모아서 처리하는 방식(Aggregation), 신용카드를 활용하는 방식(Credit Cash), 전자 화폐 방식(Digital Cash System) 등으로 구분해 볼 수 있다.

전자화폐를 이용하는 방식은 화폐가치를 디지털 정보의 형태로 발행하여 이를 지불수단으로 이용하는 것이다. 전자화폐를 이용하는 방식은 다시 전자현금(Electronic Cash, Digital Cash) 기반 지불 시스템과 전자수표(Electronic Cheque) 시스템, 그리고 소액 전자지불을 목적으로 설계된 소액 전자지불(Micro-Payments) 시스템으로 구분해 볼 수 있다. 지불브로커 방식은 신용카드 기반의 지불중개자(Payment Broker) 시스템이 있다.

이 중 소액 전자지불은 비록 거래 단위가 작지만 실생활에서 많은 부분을 차지하고 있다. 소액 전자지불 시스템의 이점은 웹상에서 잡지, 만화, 음악, 비디오, 소프트웨어 등의 판매가 가능하고 구매자로 하여금 원하는 부분에 대해서 구매할 수 있으므로 불필요한 구매를 방지할 수 있다.

가입자 기반 방식은 사용자와 상인간의 가장 간단한 모델로서 사용자가 상인과 거래를 하기 위해 상인에게 등록을 하고 자신의 ID와 계좌를 만들어서 거래하는 방식이며 트랜잭션 처리방식(Aggregation)은 가입자 기반 방식과 유사하지만 계좌 관리에 있어서의 오버헤드를 감소시키기 위해 상인과의 거래가 어느 정도의 금액에 이르면 결제를 하는 방식이다. 다음으로 신용카드 방식은 현재 가장 널리 사용되고 있는 신용카드를 이용하는 방법으로 사용자가 물건 구입 시 상인에게 자신의 신용카드 정보를 넘겨주면 상인이 카드 회사에 연락을 해서 지불을 요청하는 구조를 가지고 있다. 그리고 전자화폐 시스템(Digital Cash System)은 화폐를 비트 스트림(Bit Stream)의 형태로 구현한 것으로 전자 화폐는 인증 된 중앙의 서버에 의해 발행되며, 전자 화폐의 인증은 화폐 발행기관의 전자 서명으로 이루어진다. 또한 전자화폐 시스템(Digital Cash System)은 온라인 전자화폐 시스템과 오프라인 방식이 있다.

현실세계에서의 거래가 가상세계의 거래로 이전함에 따라, 10달러 미만의 거래가 전체 거래에서 차지하는 비중이 높아질 것이라고 예상되고 있는데, 이러한 인터넷 상에서의 잡지, 신문, 참고서적 구독 등과 같은 온라인 서비스에 이용되는 거래 금액은 그 단가가 기존의 신용카드나 기타 전자지불 프로토콜을 사용하기에는 너무 적기 때문에 서비스하기에 적합하지 못하며 소액 거래를 취급하기 위한 필요성에서 개발된 프로토콜이 필요하게 되었는데 이러한 진정한 의미의 소액 상거래를 이루기 위해 Millicent가 발표되었다.

이 Millicent System의 특성으로는 과도한 암호화 트랜잭션의 부담을 가볍게 함으로써 높은 전산 처리비용을 획기적으로 낮추고 모든 금액 처리 및 계정 관리를 브로커가 대신함으로써 소프트 상품 공급업자의 계정관리비가 획기적으로 절감된다. 또한 선불 계정 방식이므로 신용거래에 대한 부담이 없고 사용자의 계정의 확인이 공급자 사이트에서 즉각적으로 이루어지기 때문에 통신비용이 대폭 줄어들게 된다.

본 연구에서는 소액 전자지불 시스템인 Millicent 프로토콜에서 문제시 되어왔던, 사용자의 금융정보를 안전하게 전송해 줄 수 있는 대칭키 암호화 방식(DES)과 MD5를 이용한 각각의 전자서명을 구현해 보았다.