Gateway를 이용한 온라인 전자지불 방식의 개선*

김상윤 신준범 이광형
305-701 대전시 유성구 구성동 한국과학기술원 전산학과

Enhancement of On-line Electronic Payment System using Gateway

S. Y. Kim J. B. Shin H. Lee-Kwang
CS Dept. KAIST Kusong-dong Yusong-gu, Taejon, 305-701, Korea

요 약

전자지불 시스템은 여러 조건을 필요로 하지만 그 중에서도 이중사용의 방지는 전자현금의 구현을 위해 꼭 갖추어야 할 조건이다. 이러한 이중사용의 방지를 위해 안전한 하드웨어를 사용하거나, 중앙서버에서 확인을 해주는 방법이 제안되고 있다. 중앙서버에서 확인을 해주는 방법은 기반 시스템이 없어도 사용이 가능하고 더 안전하다고 여겨지고 있다. 그러나, 중앙서버에서의 병목현상이 문제가 되며, 중앙서버가 외부의 침입에 의해 사용할 수 없게 되면 전체 시스템을 사용할 수 없게 된다. 본 논문에서는 중앙서버와 상점의 사이에 Gateway를 두어 이러한 문제를 줄일 수 있는 구조를 제안하고자 한다.

1. 서론

인터넷 전자상거래에 있어서 대금결제의 문제는 가장 중요하면서도 취약한 항목으로 여겨지고 있다. 인터넷을 통해 대금을 결제하는 전자지불 시스템은 금액이 큰 경우에 특별한 하드웨어를 사용하거나 온라인으로 중앙서버에서 전자현금을 확인하는 방법이 제안되고 있다. 그 중에서도 중앙서버를 통하는 지불방식은 기반 시스템이 없어도 사용가능하고, 더 안전하다고 여겨지고 있다. 그러나, 실제 시스템에 적용될 경우 프로토콜 자체에서 분산 환경을 지원하지 않으면 중앙서버에서의 병목현상이 생길 수 있다. 또, 중앙서버를 사용할 수 없게 되면 전체 시스템을 사용할 수 없으므로 중앙서버의 안전이 중요하다. 이 문제를 해결하고자 본 논문에서는 상점과 중앙서버 사이에 Gateway를 두는 방법을 제안하고자 한다.

2장과 3장에서는 일반적인 전자지불 시스템의 구조, 온라인 지불 방식에서의 문제점을 각각 알아보고, 4장과 5장에서는 Gateway를 적용한 구조에 대해 설명한 뒤 6장에서 결론을 맺는다.

*본 연구는 인공지능 연구센타에 의해 지원되고 있습니다

2. 전자지불 시스템의 구조

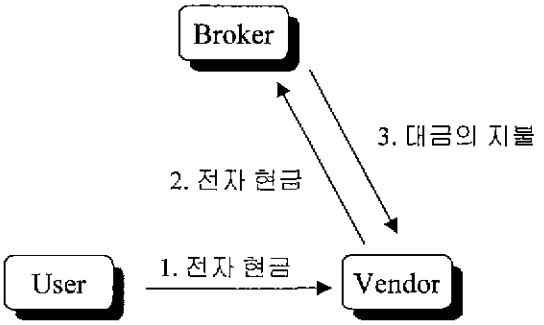

그림 1 전자지불 시스템의 흐름도

전자지불 시스템은 사용자, 상점, 중개인으로 이루어지며 사용자가 상점에 전자화폐를 지불하면 상점이 다시 중개인에게 전자화폐를 주고 그 금액만큼의 실제 대금을 돌려 받는 방식을 사용하고 있다[1]. (그림 1.)

대금의 지불은 사용자의 계좌에서 상점의 계좌로의 이체에 의해 이루어진다.

사용자가 상점에게 전자화폐를 지불하는 과정에 중개인이

개입해야 하는 지불 방식을 온라인 지불 방식이라 하며, 사용자와 상점 사이의 거래가 완료된 후 중개인이 상점에게 대금을 지불하는 방식을 오프라인 지불 방식이라 한다.

전자화폐는 일반 화폐와는 달리 디지털 정보로 이루어져 있으므로 암호학적 방법을 사용하면 위조나 변조는 막을 수 있다. 그러나, 복사는 방지할 수가 없으며, 복사 화폐와 진짜 화폐와의 구별 또한 불가능하다. 따라서, 전자지불 시스템은 이중사용과 막기 위한 방법을 갖추어야만 한다. 이중사용을 막는 방법은 이중사용을 하면 후에 불이익을 주는 방법과[2], 이중사용을 힘들게 하는 방법이 있을 수 있다. 그 중에서도 이중사용을 힘들게 해서 이중사용을 막는 방법은 크게 3가지로 나눌 수 있다.

- 이중사용으로 얻을 수 있는 이득보다 이중사용을 위한 비용을 더 크게 하는 방법 : 소액지불 시스템에서 많이 사용하는 방식이다. [3][4].
- 안전한 하드웨어를 이용한 방법 . 특별한 하드웨어를 사용하여야만 지불이 가능하도록 하는 방법이다 [5][6][7].
- 중앙서버를 통해 이중사용 여부를 확인하는 방법: 중앙서버에 전자화폐의 사용 기록을 남겨두고 사용자가 화폐를 사용할 때마다 상점이 중앙서버에 접속해서 이중사용의 여부를 확인하는 방식이다[8][9][10][11].

이중사용을 위한 비용을 더 크게 하는 방법은 시스템 유지 비용을 저렴하게 하면서 적당한 정도의 안전성을 제공하는 것을 목적으로 한다. 안전한 하드웨어를 이용한 방법은 오프라인 방식으로 시스템을 만들 수 있는 장점이 있으나 기반 시스템이 갖추어져야만 사용이 가능하다. 중앙서버를 통해 확인하는 방법은 기반 시스템이 없어도 사용이 가능하고, 일반적으로 더 안전하다고 여겨지고 있다.

3. 온라인 시스템 구축에 있어서의 문제점

온라인 방식의 전자지불 시스템은 앞서 말한 바와 같은 장점을 가지고 있다. 그러나, 사용자측에서 상점측에 지불을 할 때마다 중앙서버에 접속하여 확인을 해야하므로 중앙서버에서의 병목 현상이 큰 문제가 될 수 있다. 현재 제안된 온라인 지불 시스템 중 어떤 것은 프로토콜 자체에서 분산 환경을 지원하는 것도 있으나[12][13] 대부분의 프로토콜은 분산 환경에 대한 고려를 하지 않고 있다. 이러한 프로토콜은 대규모 시스템의 구현에 있어서 중앙서버의 부하 집중은 큰 문제가 될 수 있으며 이를 줄일 수 있는 방법이 필요하다.

또한 중앙서버가 외부의 침입에 의해서 사용할 수 없게 되면, 전체 시스템을 사용할 수 없게 되므로 중앙서버의 안전성이 상당히 중요하다.

4. Gateway

본 논문에서 제안하는 Gateway는 상점과 중앙서버 사이에 위치하면서 여러 상점이 중앙서버에 보내는 데이터들을 모아서 한번에 중앙서버에 전달해 준다. 본 장에서는 일반적인 온라인 전자 지불 시스템과 Gateway를 이용한 구조에서의 전체 흐름에 대해 설명한다.

4.1 일반적인 온라인 전자지불 시스템에서의 전자현금 확인 절차

일반적인 온라인 전자지불 시스템(그림 2)과 본 논문에서 제안하는 구조를 사용한 전자지불 시스템의 흐름(그림 3.)은 다음과 같다.

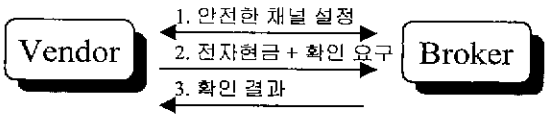

그림 2 일반적인 온라인 시스템에서의 전자현금 확인 과정

일반적인 전자지불 시스템은(그림 2.) 상점이 중앙서버에 접속한 후, 중앙서버에 전자현금의 확인을 요구하면 중앙서버가 확인하고 그 결과를 상점측에 넘겨준다.

4.2 제안된 구조에서의 전자현금 확인 절차

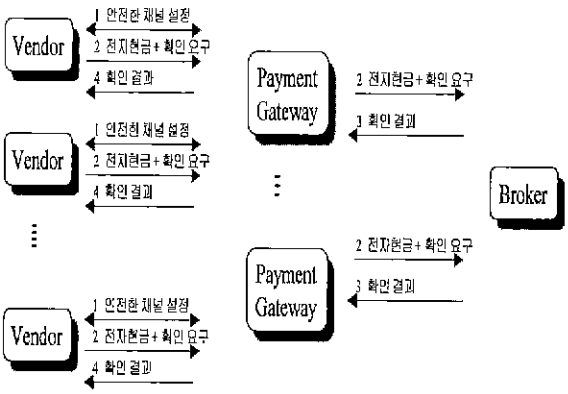

그림 3. 제안된 구조에서의 전자현금 확인 과정

Gateway를 이용한 방식은 우선 상점이 임의의 Gateway에 접속을 한다. 상점이 확인을 요구하는 전자현금을 Gateway에 보내면 Gateway는 여러 상점에게서 오는 전자현금들을 모아서 일정량이 되거나 일정한 시간이 되면 중앙서버에 보낸다. 중앙서버는 이들을 받아서 확인 후 Gateway에 결과를 돌려준

다. Gateway는 확인 결과를 돌려 받아 다시 상점들에게 나누어준다

5. 분석

제안된 구조의 장점은 효율성의 측면과 중앙서버의 안전성 측면으로 나누어 볼 수 있다.

5.1 효율성

Gateway는 여러 개의 전자 현금 확인 요구를 한번에 중앙서버로 보내주어 중앙서버의 네트워크 부하를 줄여준다. 상점이 중앙 서버에 전자현금 확인 요구를 보내고 받을 때 접속을 위해 걸리는 시간은 상당히 커서 약 250ms 정도가 된다. 전자현금의 확인에 필요한 다른 연산들과 비교해 보면, RSA 전자서명 확인의 경우 약 50ms, 중앙서버의 DB 검색이 약 5~50ms, 데이터의 전송이 약 100ms 정도가 걸린다. 이들과 비교해 보았을 때 접속을 위해 필요한 시간은 상당히 길다는 것을 알 수 있다[14].

Gateway에서 n개의 확인 요구를 한 번에 보내준다고 할 때 중앙 서버의 네트워크 접속과 데이터 전송을 위한 부하는 1/n로 준다. 위에 보인 바와 같이 전자현금 확인에서 가장 많은 시간을 필요로 한 것이 접속과 데이터 전송이다. 따라서 이것은 중앙 서버의 부하 집중을 줄이는 데에 상당히 효과적이다.

5.2 안전성

중앙서버에는 전자현금의 확인을 위한 접속만을 허용한다고 할 때 고의적으로 많은 수의 현금 확인을 보내는 공격방법을 생각할 수 있다. 제안한 방식을 사용한 경우 중앙서버는 Gateway의 접속만을 허용하고 있고, IP 인증을 통해 쉽게 방화벽을 만들 수 있다. 따라서 나쁜 의도를 가지고서 보내는 현금 확인 요구를 중앙서버에 직접 보낼 수 없다. 전자현금에 다이제스트나, 체크섬을 일부로 두어서 Gateway에서 확인 절차를 거친 후 중앙서버로 보내어지게 하면 이러한 나쁜 의도의 전자현금 확인 요구가 중앙서버로 보내지는 것을 방지할 수 있다. Gateway는 침입자에 의해 사용할 수 없게 되어도 다른 Gateway를 사용하면 되므로 전체 시스템에 큰 영향을 미치지 못 한다.

6. 결론

현재 온라인 전자지불 시스템에서 이중사용의 방지를 위해 안전한 하드웨어를 사용하거나 중앙서버를 통해 확인하는 방법이 제안되고 있다. 그 중에서 중앙서버를 통해 확인하는 방법은 기반시스템이 없어도 사용가능하고, 보다 더 안전하다고 여겨지고 있다. 이러한 전자지불 시스템 많은 수의 상점이 중앙서버에 접속해 이러한 확인 과정을 거치게 될 것이므로 중앙서버에서의 병목현상은 시스템 구축에 있어서 문제가 될 가능성이 높다. 본 논문에서는 온라인 전자지불 시스템에서 중앙서버로의 부하 집중을 덜기 위하여 중앙서버와 상점 사이에 Gateway를 두는 방법을 제안하였다. 이러한 구조는 중앙서버로의 부하 집중을 상당히 막아줄 뿐만 아니라 중앙서버의 안전성 측면에서도 많은 기여를 할 수 있을 것으로 보인다.

7. 참고 문헌

[1] N Asokan, Phil Janson, Michael, Michael Steiner, Michael Waidner, "Electronic Payment Systems " IBM Research Report, RZ 2890(#91033), 1996

[2] David Chaum, Amos Fiat, Moni Naor, "Untraceable Electronic Cash," Crypto '88, LNCS 403, Springer-Verlag, Berlin 1990, 319-327

[3] R. L. Rivest and A. Shamir, "Payword and micromint - Two simple micropayment schemes," tech. rep , MIT LCS, May 1996

[4] S. G Mark S. Manasse, "The Millicent protocols for inexpensive electronic commerce," in 4th International World Wide Web Conferences, Dec. 1995.

[5]J.-P., Boly et al., "The ESPRIT Project CAFE - Hight Security Digital Payment Systems," ESORICS '94, LNCS 875, Springer-Verlag, Berlin 1994, 217-230

[6] Mondex, http://www.mondex.com

[7] EUROPAY. CLIP http.//www europay.com/

[8] Marvin Sirbu, J. Douglas Tygar, "Netbill'An Intermet Commerce System Optimized for Network Delivered Information and Services," In Proceedings of IEEE Compcon '95, March 1995

[9] DigiCash. ECash http.//www.digicash.com/ 1994

[10] FristVirtual http://www.fv.com

[11] CyberCash http://www.cybercash.com

[12] Gennady Medvinsky, Clifford Neumann, "NetCash:A design for practical electronic currency on the Internet," 1st ACM Conference on Computer and Communications Security, Proceedings, Faifax , November 1993, acm Press, New York 1993, 102-106

[13] Michael Peirce Donal O'Mahony Scaleable., "Secure Cash Payment for WWW Resources with the PayMe Protocol Set," http.//www.w3.org/Conferences/WWW4/Papers/228

[14] A. Herzberg. "Safeguarding Digital Library Contents," D-Lib Magazine, January, 1998, ISDN 1082-9873