초소액 지불 시스템 비교 및 분석*

신준범, 김상윤, 이광형
305-701 대전시 유성구 구성동 한국과학기술원 전산학과

An Analysis of Microment Systems

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

본 논문에서는 기존에 제안된 초소액 지불 시스템들의 성능을 비교 분석한다. 비교 대상 시스템으로는 μ-iKP, PayWord, CAFE(phone call), MPTP, NetBill, Mini-Pay, Millicent를 선택하였고, 비교 항목으로는 효율성, 안전성, 그리고 분쟁 해결성등의 요소를 고려하였다.

1. 서론

최근 전자 상거래의 활성화와 더불어 네트워크를 통하여 안전하게 지불을 할 수 있는 여러 종류의 전자 지불 프로토콜들이 제안되고 있다. 그 중, 지불 처리비용을 최소화 하여 적은 금액의 지불에 사용될 수 있는 것을 초소액 지불 시스템(MicroPayment System)이라 한다. 초소액 지불 시스템은 신문, 저널 등의 기사 및 주식 정보와 같은 특정 서비스에 대한 요금 지불이나, 자바 애플릿 등 작은 소프트웨어의 구입 등에 사용할 수 있다.

지금까지 여러 종류의 초소액 지불 시스템이 제안되었다. 이들은 각각 여러 가지 장단점을 갖는다. 본 논문에서는 제안된 초소액 지불 시스템 중, 다음의 시스템들을 비교하였다 : μ-iKP[1], PayWord[2], CAFE(phone call)[3], MPTP[4], NetBill[5], Mini-Pay[6], Millicent[7]. 비교 요소로는 시스템의 안전성, 분쟁 해결 능력, 효율성, 그리고 확장성등을 고려하였다.

* 본 연구는 한국과학기술원 인공지능연구센타에 의해 지원되고 있습니다.

본 논문의 구성은 다음과 같다. 2장에서는 초소액 지불 시스템의 기본 구조에 대해서 언급하고, 3장에서는 세부적인 비교 요소들을 기술한다. 4장에서는 이러한 비교 요소를 기준으로 각 시스템을 비교한다. 그리고 5장에서 끝을 맺는다.

2. 초소액 지불 시스템 기본 구조.

초소액 지불 시스템의 구성원으로는 사용자, 상점, 그리고 지불 관리 서버(브로커)가 있다(그림 1 참조). 사용자는 브로커에게서 초소액 지불 시스템을 사용할 수 있는 일종의 쿠폰 묶음을 구입하고, 실제 지불에서는 그 쿠폰을 사용하는 방식

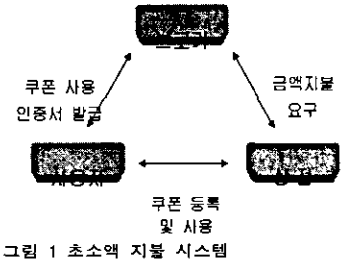

그림 1 초소액 지불 시스템

이다.

현재 제안된 초소액 지불 시스템은 사용자, 상점, 그리고 브로커의 관계에 따라 다음의 4가지로 구분할 수 있다.
type-1 : 사용자는 상점과 거래하기 이전에 미리 쿠폰 사용 인증서를 발급 받는다. 그리고 사용자는 쿠폰을 온라인 방식[1]으로 사용한다.
type-2 : 사용자는 상점과 거래하기 이전에 미리 쿠폰 사용 인증서를 발급 받는다. 그리고 사용자는 쿠폰을 오프라인 방식[2]으로 사용한다.
type-3 : 사용자는 상점과 거래를 시작하면서 쿠폰 사용 인증서를 발급 받는다. 그리고 사용자는 쿠폰을 온라인 방식으로 사용한다.
type-4 : 사용자는 상점과 거래를 시작하면서 쿠폰 사용 인증서를 발급 받는다. 그리고 사용자는 쿠폰을 오프라인 방식으로 사용한다.

기존 시스템들의 유형을 분류하면 NetBill, Mini-Pay[3]는 type 1이고, PayWord, CAFE(phone call), MPTP등은 type 2이다. 그리고 *Millicent*은 *type-3*이고, μ-*iKP*은 *type-4*이다.

3. 기반 암호 기술

초소액 지불 시스템들은 안전성 및 분쟁 해결을 위하여 각기 다른 암호 기술을 사용한다. 대표적인 암호 기술로는 Kerberos[8], 공개키 전자 서명, 비밀키 전자 서명, 그리고 S/KEY[9]방식을 응용한 해쉬 체인(hash chain)이 있다. 이들 중, 해쉬 체인을 사용한 방식은 실제 지불 과정에서는 해쉬 체인만을 사용하여 이루어지나 이를 등록하는 과정에서 지불을 보증할 수 있는 공개키 전자 서명과 함께 사용된다. 각 암호 기술에 대한 자세한 내용은 [10]을 참조 바란다.

μ-iKP, PayWord, CAFE, MPTP는 해쉬 체인을 사용하였고, NetBill은 공개키 전자 서명과 kerberos를 부분적으로 사용했다. *Mini-Pay*는 공개키 전자 서명을 사용하고, *Millicent*는 비밀키 전자 서명을 사용했다.

4. 비교 항목

본 논문에서는 기존의 초소액 지불 시스템들을 다음의 항목에 따라서 평가하였다. 이들 항목은 안전성, 분쟁 해결 능력, 그리고 효율성은 비교 항목을 다음과 같이 세분화 하였다.

효율성 : 효율적 초소액 지불 시스템 설계를 위하여 다음의 사항들이 권장된다.
- **Req. 1** : 오프라인 시스템 : 온라인 방식의 지불 시스템의 경우는 브로커의 병목현상(bottleneck)이 생길 가능성이 크다.
- **Req. 2** : 메시지 전달 회수의 최소화 : 네트워크 지연을 최소화 하여야 한다.
- **Req. 3** 공개키 서명 알고리즘 사용의 최소화 : 공개키 서명 알고리즘은 생성 및 확인에 많은 시간이 소요된다. 따라서 상점 및 브로커의 병목 현상을 막기 위하여 상점 및 브로커가 확인 하여야 하는 공개키 서명 알고리즘의 사용을 줄여야 한다.

안전성 및 분쟁 해결 기능 : 다음의 위험 요소를 해결할 수 있어야 한다.
- **Risk 1** : 사용자가 사용한 데이터를 도청하였다가 다시 사용하는 행위.
- **Risk 2** : 공격자가 상점인 것처럼 가장하여 데이터를 얻는 행위이다.
- **Risk 3** : 사용자가 보낸 데이터를 가로채어 사용하는 행위.
- **Risk 4** : 사용자가 물품을 구매하였을 때, 사용자 계좌의 감소분과 상점 계좌의 증가분이 다름.
- **Risk 5** : 사용자가 상점으로부터 상품을 받고 대금을 지불하지 아니함.
- **Risk 6** : 상점은 사용자로부터 상품 금액을 받고 상품을 제공하지 아니함.
- **Risk 7** : 사용자가 구매한 상품과 받은 상품이 다름.
- **Risk 8** : 사용자는 상점으로부터 상품을 받은 다음에 받지 않았다고 주장.

초소액 지불 시스템을 평가할 수 있는 또 다른 중요한 측면으로는 시스템의 확장성 및 지불 데이터의 이중 사용 방지 등이 있다. 그러나 고려한 모든 종류의 초소액 지불 시스템은 이중 사용 방지 기능을 갖으며, 또한 원 자료에 기술되어 있지는 않더라도 확장성을 갖도록 변형이 가능하므로 비교 대상에서는 제외하였다.

5. 초소액 지불 시스템 비교

μ-iKP, PayWord, CAFE, MPTP와 같이 해쉬 체인에 기반하는 시스템은 효율성 측면에서 부족하다. NetBill은 안전성 및 분쟁 해결 기능과 관련된 모든 요구조건을 충족한다. 그러

1) 쿠폰의 유효성을 브로커의 도움을 받아야 확인할 수 있는 방식
2) 쿠폰의 유효성을 브로커의 도움 없이 상점 자체적으로 확인할 수 있는 방식
3) 분쟁 해결 기능을 최대로 하였을 경우를 고려하였음

나 Req. 2를 고려하지 않았으므로 효율성 측면에서는 가장 떨어진다. Mini-Pay는 여러 선택기능을 가지고 있어 엄밀한 비교는 힘들지만 분쟁 해결 기능을 최대한도로 하였을 경우 온라인 지불 방식이므로 효율성 측면에서 조금 떨어진다. 그리고 분쟁 해결 기능이 부족하다. Millicent은 Req. 3의 만족을 위주로 설계되었으며 안전성 및 분쟁 해결 기능 전반에 걸쳐 미흡하다. 각 세부 항목에 대한 자세한 비교는 표 1을 참조 바란다.

		μ-iKP[1]	PayWord[2] MPTP[4]	CAFE[3]	NetBill[5]	Mini-Pay[6]	Millicent[7]
구성원		type-4	type-2	type-2	type-1	type-1	type-3
기반 암호기술		해쉬체인	해쉬체인	해쉬체인	공개키 서명 +Kerberos	공개키	비밀키서명
효율성	Req. 1	○	○	○	×	×	×
	Req. 2	○	○	○	×	○	○
	Req. 3	○	○	○	×	×	○
안전성	Risk 1	○	○	○	○	○	○
	Risk 2	○	○	○	○	○	○
	Risk 3	×	○	×	○	○	○
분쟁해결기능	Risk 4	○	○	○	○	○	×
	Risk 5	○	○	○	○	×	×
	Risk 6	×	×	×	○	×	×
	Risk 7	×	×	×	○	×	×
	Risk 8	×	×	×	○	×	×

표 1. 초소액 지불 시스템 성능비교

6. 결론

전자 상거래의 활성화에 따라 많은 종류의 초소액 지불 시스템들이 제안되었다. 본 논문에서는 이러한 시스템들을 효율성, 안전성, 그리고 분쟁 해결 기능 측면에서 비교하였다. 안전성 및 분쟁 해결 기능 측면에서는 비교된 시스템 중, NetBill[5]이 가장 뛰어나나 효율성 측면에서 결함을 갖는다. μ-iKP[1], PayWord[2]등과 같이 해쉬 체인에 기반한 시스템은 효율성 측면에서는 가장 뛰어나나 안전성 및 분쟁 해결 기능 측면에서 부족함하다.

향후 연구 과제로는 보다 엄밀한 요구 사항의 분석이 요구된다. 또한 본 논문에서 제안된 모든 요구 조건을 만족하는 초소액 지불 시스템의 개발이 요구된다.

7. 참고 문헌

[1] Micro-Payments based on iKP, Ralf Hauser, Michael Steiner and Michael Waidner, IBM Research, 12 February 1996, Research Report 2791 (\# 89269), presented at SECURICOM96.

[2] R.L. Rivest and A. Shamir, PayWord and MicroMint--Two Simple Micropayment Schemes, presented at RSA Security conference, 1996.

[3] T. Pederson, Electronic Payments for Small Amounts, Proc. Security Protocol Workshop, LNCS. 1189, pp. 59-68, 1997

[4] Phillip M. Hallam-Baker, Micro Payment Transfer Protocol (MPTP), W3C Working Draft WD-mptp-951122 (22-Nov-95). at http://www.w3.org/TR/WD-mptp

[5] Benjamin Cox, J. D. Tygar and Marvin Sirbu, NetBill Security and Transaction Protocol, in Proceedings of the First USENIX Workshop on Electronic Commerce, 1995.

[6] Amir Herzberg and Hilik Yochai, Mini-Pay : Charging per Click on the Web, IBM Research. at http://www.hrl.il.ibm.com/mpay/docs/papers/mpay

[7] S. Glassman, M. Manasse, M. Abadi, P. Gauthier, and P. Sobalvarro, The Millicent Protocol for Inexpensive Electronic Commerce. In World Wide Web Journal, Fourth International World Wide Web Conference Proceedings, pages 603-618. O'Reilly, December 1995.

[8] B. C. Neuman and T. Ts's, Kerberos : An authentication service for computer networks, TEEE Communications, v. 32, n. 9, Sep. 1994

[9] N. M. Haller. The S/KEY one-time password system, In ISOC, 1994

[10] B. Schneier, Applied Cryptography(Second Edition), John Wiley & Sons, 1996