Java Card를 이용한 인터넷 쇼핑몰 마일리지 통합 관리 시스템에 관한 연구

백장미[0] 강병모 홍인식
순천향대학교 정보기술공학부
bjm1453@hanmail.net kbm1006@hotmail.com ishong@sch.ac.kr

A Study on United Mileage Management System for Internet Shopping-Mall using Java Card

Jang-Mi Baek[0] Byung-Mo Kang In-Sik Hong
Division of Information Technology Engineering, Soonchunhyang University

요 약

인터넷과 전자상거래가 활성화됨에 따라 인터넷상에서의 보다 안전하고 다양한 기능을 수행할 수 있는 지불수단이 필요하게 되었다. 스마트 카드는 안전성과 이동성이 뛰어나기 때문에, 전자상거래상의 일들을 수행하기에 적합하다. 특히, 스마트 카드의 차세대 COS로 주목받는 Java Card는 어플리케이션의 개발의 용이성과, 뛰어난 독립성을 제공하므로, 효율적인 개발을 할 수 있다. 본 논문에서는 지불에 관련된 쇼핑몰 마일리지 통합 관리 시스템의 개발을 제안함으로써 다양한 로열티 서비스 제공에 대하여 연구하였다. 제안된 시스템은 Java Card 내에 저장되는 한 개인의 독립적인 프로그램으로서, Java Card의 연산기능을 이용하여 서로 다른 마일리지 체계를 가지는 이종 쇼핑몰간의 통합마일리지를 직접 계산하고, 적립할 수 있는 카드 어플리케이션을 제안하였다.

1. 서 론

스마트 카드는 반도체와 소프트웨어의 발전된 기술을 바탕으로 현재 인적 거래에 의존하고 있는 모든 경제 활동의 효율성을 제고하고, 정보 기술의 발전상을 도입하여 전자적인 거래의 편리성, 호환성, 정확성, 보안성을 확보하기 위한 매개체로 대두되고 있다. 전자상거래가 활성화됨으로서 카드의 사용이 점점 보편화되고 있으며, 카드를 이용한 어플리케이션의 개발이 활발히 진행중이다.

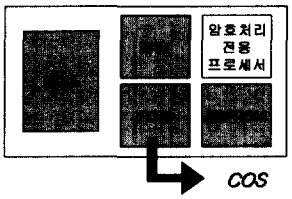
스마트 카드는 COS(Chip Operating System)이라 불리는 32비트 OS가 탑재되며, 64KByte의 저장공간을 갖는다. 따라서, 어플리케이션을 개발하여 저장할 수 있고, 간단한 연산기능을 수행할 수 있다. 전통적으로, SIM(Subscriber Information Manager) 카드의 제조와 카드 소프트웨어의 개발은 칩 카드 벤더들이 담당해 왔으나, 썬 마이크로시스템의 자바카드(Java Card), 마이크로 소프트의 WFSC(Windows for Smart Card), 마스터 카드의 MULTOS와 같은 칩 카드 운영 시스템이 등장하면서 독자적으로 카드 어플리케이션을 개발할 수 있게 되었다. 본 논문은 차세대 COS라 불리는 Java Card에 기반을 두고 어플리케이션을 개발한다. Java Card의 유효성을 입증하기 위하여, 쇼핑몰 마일리지 통합 관리 시스템을 제안하고자 한다. 본 시스템은 GSM(Global System for Mobile Communications) 규격인 ISO 7816 표준과 Java Card를 기반으로 구현된다.[1][2][3]

2. 관련기술

2.1 Smart card

Smart card는 마이크로프로세서와 메모리를 탑재하고 있는 신용카드와 동일한 크기의 카드로서, 전기적 신호에 의해 정보를 저장하며 처리한다. Smart card는 개인휴대성과 간섭에 대한 안정성이 높은 특징을 지닌다. 1968년에 독일에서 처음 소개되었으며, 현재 유럽과 아시아지역에서 활발히 활용되고 있는 추세이다. Smart card는 외부의 자원에 의존하지 않기 때문에, 공격성에 대한 저항력이 크며, 암호화알고리즘을 사용하므로 데이터의 보호성이 높다. [1][3]

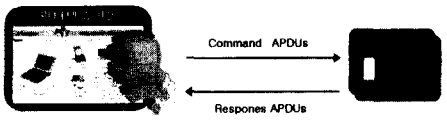
2.1.1 Smart card의 하드웨어



(그림 1) Smart card의 하드웨어 구조

- CPU : 자체연산 기능(8bit-32bit), 모토로라 6805나 인텔 8051사용
- 암호처리 전용프로세서 : 암호화 알고리즘에 의한 연산, Coprocessor
- 메모리
  - ROM : COS 로드,16KB-32KB
  - EEPROM : 데이터 저장 장치(비휘발성)
  - RAM : CPU의 작업 공간(휘발성)

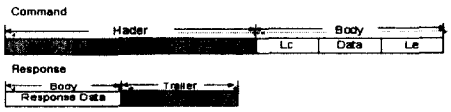
2.1.2 Smart card의 통신



(그림 2) Smart card의 APDU 통신

Smart card와 단말기 사이의 통신은 APDU를 통해 이루어진다. ISO 7816의 스펙을 기준으로 하여, command와 response를 서로 주고받는다. command APDU와 response APDU는 항상 쌍을 이루어 통신을 한다.

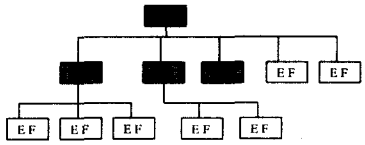
APDU의 command와 response의 구조이다.



(그림 3) APDU의 구조

- CLA : Class Byte (ISO 명령어, 전용 명령어, 암호화 등)
- P1 : Parameter 1 • P2 : Parameter 2
- Lc : 명령어의 Data Byte 수
- Data : Command data block
- Le : 응답 메시지의 예상되는 최대 Byte 수
- Data : Response data block
- SW1 : Status Byte 1 • SW2 : Status Byte 2

2.1.3 Smart card Os의 file 시스템 구조



(그림 4) Samrt card file 시스템 구조

Smart card는 계층적 구조를 지닌다. MF는 Master file로서 루트파일이 되며, 단 하나만 존재한다. DF는 Dedicated file로서, 다른 DF나 EF를 포함할 수 있다. EF는 Elementary file로서 가장 하위계층의 디렉토리로 DF를 각각의 어플리케이션이라 볼 때, EF는 한 어플리케이션에 포함되는 함수들이라 볼 수 있다.

2.2 Java Card

Java Card는 Smart card의 장애요소를 보안하기 위한 기술로서 자바언어로 작성된 Application을 실행하며, 자바언어를 사용하기 때문에, 자바언어가 지니는 특성을 최대한 활용하여 Java Card에 적용할 수 있다. 자바언어로 작성된 어플리케이션은 용량이 작기 때문에, 적은 메모리를 가지는 Java Card에 저장하기 알맞다.[2][4]

2.2.1 Java Card의 장점

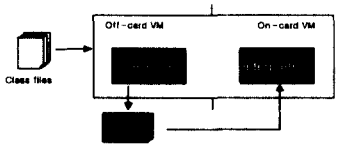
- 어플리케이션의 개발이 쉽다.
- 암호화 알고리즘의 이용으로 안정성이 높다.
- 하드웨어적으로 독립성을 지닌다.
- 다중 어플리케이션을 지원하다.
- 다른 스마트 카드와의 호환성이 뛰어나다.

2.2.2 Java Card의 구조

Java Card는 1K의 RAM과 16K의 EEPROM과 24K의 ROM이 탑재되어 있으며, JCVM(Java Card virtual machine), JCRE(Java Card runtime environment), APIs(Application Programming Interfaces)로 구성되어 있다.

•JCVM(Java Card virtual machine)

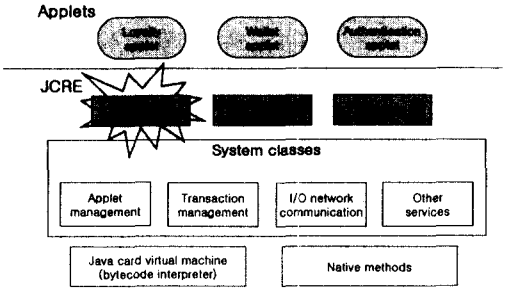
JCVM은 off-card VM과 On-card VM으로 구성된다. 자바언어로 작성하여 생성된 class file을 카드에 로드시키기 위하여, off-card VM의 converter를 이용하여, CAP file을 생성한다. CAP file은 class file을 압축한 형태의 file로서, on-card VM에 load되어, interpreter를 통하여 실행한다.



(그림 5) JCVM의 구조

•JCRE(Java Card Runtime Environment)

JCRE는 Smart card 하드웨어의 상부에 위치한다. Java Card virtual machine은 JCRE 내부에서 실행되며, Java card vendor로 부터 applet을 분리하는 역할을 한다. JCRE는 표준화 시스템과 API 인터페이스를 제공하며, EEPROM에 데이터가 저장되기 때문에, 전원의 공급이 끊어지는 경우라도, virtual machine은 단지 보류되는 상태이며, JCRE의 상태와 모든 데이터 값도 보호된다.



(그림 6) JCRE 의 하드웨어적 구조

•APIs(Applicaton Programming Interface)

API는 Java Card의 어플리케이션을 위한 Java 패키지와 클래스를 정의한다. 자바언어에 지원되는 사항을 제공하는 패키지, Framework class, interface, 전송프로토콜을 지원하는 패키지, 암호화 알고리즘을 위한 패키지로 구성된다.

3. 쇼핑몰 마일리지 통합 관리 시스템

본 연구는, Java Card의 유효성을 입증하기 위하여, Java Card에 저장되는 어플리케이션의 개발을 목적으로 한다. 본 연구에서 제안한 시스템은 서로 제휴되어 있는 각 쇼핑몰에서 축적한 마일리지를 스마트 카드내의 마일리지 시스템을 통해 관리하는 것이다. 기존의 쇼핑몰 관리 서비스는 사용자의 아이디와 패스워드만으로 보안을 하는 수준이므로, 개인 정보 유출의 문제가 발생할 가능성이 높다. 그러나, 스마트 카드를 이용하면 보다 더 안전하게 데이터를 보호할 수 있다. 본 연구의 핵심은 소정의 프로그램을 카드 내에 저장하여, 카드 자체의 연산을 통하여 마일리지를 관리한다는 점이다. 시스템이 카드 내에 저장됨으로서 보다 안전하며, 사용자 이점에서 편리하게 사용할 수 있다.[2][3][5]

3.1 쇼핑몰 마일리지 통합 관리 시스템 개발

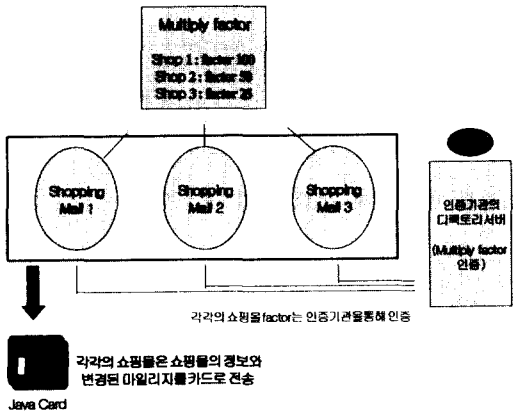
본 논문은, Java Card 내의 통합 관리 프로그램을 이용하여 마일리지를 관리는 시스템을 제안한다. Java Card의 EEPROM에 저장될 프로그램은 자바언어로 작성된다. 자바는 객체지향

형 프로그램으로서, 멀티 스레드 개념을 지니고 있어 다중 작업이 가능하다. 또한 축소형 운영체제인 가상머신을 두어 가상머신이 존재하는 곳이면 어디든지 수행 가능하도록 한다. 자바 언어로 생성된 class file은 cap file로 변형되어, 카드의 EEPROM에 저장한다. cap file은 필요한 정보만을 압축한 file이므로 작은 용량을 지니기 때문에 스마트 카드내의 메모리에 저장하는 것이 가능하게 된다. 한 어플리케이션의 용량은 2k로 정도로 예상할 수 있으며, Java Card에는 여러 개의 어플리케이션을 탑재할 수 있다.

마일리지 통합 관리 서비스 어플리케이션은 각 쇼핑몰에서 마일리지를 받아서 Java Card 내에 저장되어 있는 어플리케이션을 이용하여, 마일리지를 통합하고 축적한다. 각 쇼핑몰이 서로 제휴를 맺었다 하더라도 쇼핑몰마다 마일리지 적용률이 다르므로, 각 쇼핑몰에 대한 정보를 카드에 저장하여야 한다. 카드에는 각 쇼핑몰의 각각 마일리지와 통합적으로 계산된 마일리지가 저장되며, 각 쇼핑몰에서의 회원자격 등을 저장하여, 오프라인 상에서도 저장 내역을 확인할 수 있도록 한다.

각 쇼핑몰에서의 마일리지는 Multiply factor를 이용하여 적용한다. Multiply factor는 각 쇼핑몰의 마일리지에 대한 가중치 값을 의미한다. Multiply factor는 인증기관을 통해 인증을 받고, 인증기관의 디렉토리 서버에 저장이 된다. 사용자는 쇼핑몰을 통해 마일리지를 축적하고, 변경된 마일리지와 쇼핑몰의 정보를 카드로 전송한다. 카드내의 마일리지 통합 관리 어플리케이션을 통해, 각 쇼핑몰의 공인 인증된 Multiply factor를 적용하는 단계를 수행한다.

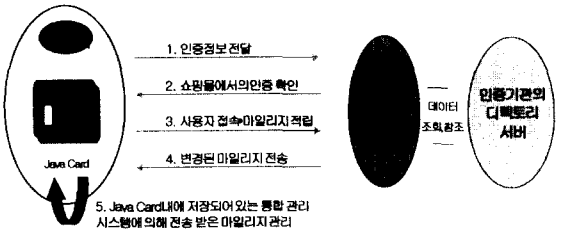
Java Card에 저장된 마일리지는 현금화가 가능해야 한다. 즉, Java Card에 저장되어 있는 또 다른 전자지갑과 같은 어플리케이션과의 데이터 공유를 통해, 현금화할 수 있도록 한다. 각 쇼핑몰마다 적용률의 변동이 발생하는 경우, 쇼핑몰에서 쉽게 Java Card에 변동된 사항이 저장될 수 있도록 구현한다.



(그림 7) 쇼핑몰 마일리지 통합 관리 시스템

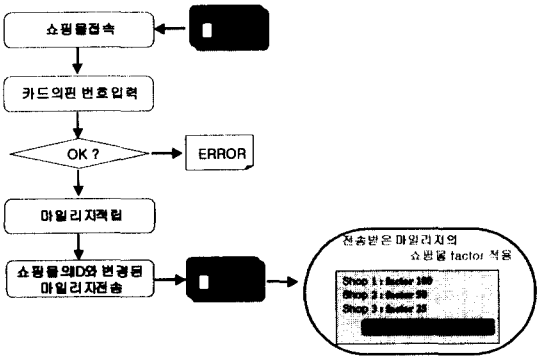
3.2 통합 마일리지 어플리케이션

사용자는 웹사이트를 접속하기 위하여 Java Card에 저장되어 있는 인증정보를 전송한다. 웹사이트는 각 인증정보를 확인한 후, 사용자의 접속을 허용한다. 웹사이트를 접속한 사용자는 쇼핑몰의 마일리지를 적립한다. 적립된 결과는 Java Card로 전송되어, Java Card 내의 마일리지 통합 관리 어플리케이션을 통해 관리된다. 일정량의 마일리지가 축적되면 현금화하여 사용할 수 있도록 한다.



(그림 8) 쇼핑몰 마일리지 통합 관리 시스템 사용 과정

웹사이트를 접속하기 위해서는 카드의 핀 번호를 입력하여야 한다. 입력된 핀 번호와 인증정보를 통해 사용자 인증을 할 수 있다. PIN number는 유효숫자로 지정할 수 있으며, 유효숫자 이상의 입력을 받을 경우에는 에러 메시지를 전송하고, 접속을 거부한다. 이와 같은 인증 단계를 통해 보안적인 요소를 높일 수 있다.



(그림 9) 쇼핑몰 마일리지 통합 관리 시스템 흐름도

4. 결론

본 논문은, 자바카드를 이용한 어플리케이션의 개발을 제안하였다. 스마트 카드의 차세대 COS로 주목받는 Java Card는 어플리케이션의 개발의 용이성과, 뛰어난 독립성을 제공하므로, 효율적으로 어플리케이션을 개발할 수 있다. 본 논문에서 제안된 쇼핑몰 마일리지 통합 관리 어플리케이션은 기존의 웹사이트를 통한 서비스와는 다른 카드 자체 내에 저장되는, 한 개인의 독립적인 프로그램으로서, 적립된 마일리지의 현금화를 가능하게 한다. Java Card의 CPU를 통한 연산작용을 이용하여, 마일리지를 직접 계산하고, 적립할 수 있는 프로그램을 제안하였다. 스마트 카드의 시장은 아직 초기 단계로서, 활성화되고 있는 추세이기 때문에, 국제적이 규격과 카드에 저장될 다양한 어플리케이션의 개발이 뒷받침되어야 할 것으로 본다.

참고문헌

[1] Rankl, W "Smart Card Handbook" Wiley 2000
[2] Chen "Java Card Technology for Smart Cards" Addison Wesley 2000
[3] Hansmann, Uwe (Edt) / Nicklous, Martin S. / Schack, Thomas / Seliger, Frank / Hansmann, Uwe / Springer Verlag "Smart Card Application Development Using Java" Springer Verlag 1999
[4] Ivor Horton "Begining Java2" WROX 1999
[5] Hendry, Mike " Smart Card Security and Applications" Artech House 2001