http://dx.doi.org/10.3745/KIPSTA.2012.19A.1.051

IC신용카드(EMV)를 이용한 T-커머스 결제처리 모듈 개발

최 병 규[†] · 이 동 복[††] · 김 병 곤[†††] · 허 신[††††]

요 약

일반적으로 스마트카드라고 불리는 IC(Integrated Circuit)카드는 작은 크기의 마이크로칩(MPU)과 메모리, EEPROM, 카드 운영체제(COS) 및 보안 알고리즘을 내장하고 있다. 이러한 IC카드는 금융(카드,은행,증권 등), 교통, 통신, 의료, 전자여권, 멥버쉽 회원관리 등 거의 모든 산업 분야에서 이용되고 있다. 최근 방송통신융합 및 TV의 스마트기기화 추세에 따라 TV전자상거래(T-커머스)가 방송산업의 신성장 동력이 되면서 T-커머스 지불결제 방법으로 IC카드를 이용하는 등 응용분야가 증가하고 있다. 예를 들어, T-커머스에서 IC신용카드(또는 IC현금카드)를 이용하여 결제를 하거나, IC현금카드를 이용하여 ATM과 같은 방식으로 TV뱅킹 서비스를 제공한다. 하지만 아직까지 대부분의 T-커머스 신용카드 결제 서비스는 리모콘을 이용한 카드정보 입력 방식을 이용하고 있기 때문에 고객 편의성이 크게 떨어지고, 카드정보 저장 및 노출 등 보안성에 있어서 취약성을 가지고 있다. 이러한 문제점을 해결하고자, 본 논문에서는 IC신용카드 결제 표준기술인 EMV기술을 이용한 TV전자지불 결제시스템 구현을 위한 결제처리 모듈을 개발하였다.

키워드 : 스마트카드, IC신용카드, T-커머스, EMV

Development of T-commerce Processing Payment Module Using IC Credit Card(EMV)

Choi Byoung Kyu[†] · Lee Dong Bok[††] · Kim Byung Kon[†††] · Heu Shin[††††]

ABSTRACT

IC(Integrated circuits)card, generally be named smard card, embedded MPU(Micro Processor Unit) of small-size, memory, EEPROM, Card Operating System(COS) and security algorithm. The IC card is used in almost all industry such as a finance(credit, bank, stock etc.), a traffic, a communication, a medical, a electronic passport, a membership management and etc. Recently, a application field of IC card is on the increase by method for payments of T-commerce, as T-commerce is becoming a new growth engine of the broadcating industry by trend of broadcasting and telecommunication convergence, smart mechanization of TV. For example, we can pay in IC credit card(or IC cash card) on T-Commerce. or we can be provided TV banking service in IC cash card such as ATM. However, so far, T-commerce payment services have weakness in security such as storage and disclosure of card information as well as dropping sharply about custom ease because of taking advantage of card information input method using remote control. To solve this problem, This paper developed processing payment module for implementing TV electronic payment system using IC credit card payment standard, EMV.

Keywords : Smart Card, IC Credit Card, T-Commerce, EMV

1. 서 론

우리나라 신용카드 보급률과 이용률은 세계적으로 매우 높은 상위권에 속한다. 신용카드는 신용거래(일시불, 할부, 무이자할부 등)나 신용카드 사용액에 대한 세금혜택 등으로 거래가 지속적으로 성장하고 있다. 하지만 POS(Point Of Sale)단말기에 저장된 신용카드정보를 이용한다거나 가맹점의 카드단말기에서 신용카드정보를 저장하였다가 카드를 복제하여 사용하는 등의 위·변조에 의한 부정한 사용이 지속적으로 증가하고 있어 사회적인 문제로 대두되고 있다. 위와 같이 마그네틱 신용카드는 위·변조가 쉽기 때문에 신용카드의 보안성을 강화시키기 위해 2003년 금융감독원의 지침에 의해 마그네틱(Magnetic Stripe) 카드를 IC칩카드로 전환하기 시작하였다. 현재는 90%이상의 신용카드가 IC칩카드로 전환되었고, 현금카드는 100% IC칩카드로 전환되었다.

IC신용카드는 MS신용카드와 동일한 크기의 플라스틱 카드에 IC칩을 부착한 카드이다. IC칩에는 마이크로프로세서, 전용 운영체제, 보안모듈, 메모리 등이 있어 정보의 기밀성과

† 준 회 원 : 한양대학교 컴퓨터공학과 박사과정 수료
†† 정 회 원 : 미디어벨로(주) CEO
††† 정 회 원 : 한국건설기술연구원 건설정보연구실 수석연구원
†††† 정 회 원 : 한양대학교 컴퓨터공학과 교수
논문접수 : 2011년 6월 28일
수 정 일 : 1차 2011년 9월 12일, 2차 2011년 10월 11일
심사완료 : 2011년 10월 18일

보안성을 크게 향상시켰고 많은 양의 정보와 응용프로그램을 저장하고 실행할 수 있는 다양한 기능을 가진 카드이다[1].

초기에 전자지갑용으로 사용되던 스마트카드는 현재 교통, 금융, 통신, 신분증 등 다양한 분야에서 사용되고 있다. 최근에는 가입자 식별모듈(SIM, Subscriber Identif- ication Module)카드가 전체 스마트카드 시장의 50%를 차지하고 있으며, 전자여권과 전자신분증 등 정부의 보안정책으로 사용되는 아이디 카드가 상당한 부분을 차지하고 있다[2].

IC신용카드의 표준으로는 Europay, Mastercard, Visa가 1993년부터 마그네틱 카드의 위·변조를 막기 위해 IC칩을 이용한 신용카드 거래를 위한 공동 규격으로 개발하기 시작하였고, 이에 따라 만들어진 규격이 EMV규격이다. EMV규격은 실질적인 IC신용카드 표준이며, 신용카드외에도 직불, 선불, 로열티 서비스등의 오프라인 지불은 물론 온라인 지불 및 모바일 지불, 모바일 뱅킹 등에까지 확산되어 글로벌한 결제수단으로 확대되고 있다.

유럽, 동남아 등 일부 해외국가에서는 IC신용카드 거래가 의무화되어 있으나 국내에서는 오프라인 가맹점에 있는 결제단말기의 IC카드결제 지원 비율이 25%정도로 낮아 IC신용카드 거래가 활성화되지 않고 있다.

최근 방송산업의 캐시카우(cash-cow)였던 광고매출이 지속적으로 하락하면서 전통적인 방송광고가 아닌 온라인 광고의 특성을 살린 양방향 광고와 T-커머스가 디지털방송 시대의 캐시카우가 되고 있다. 2008년에 시작한 IPTV(인터넷 멀티미디어방송) 방송은 T-커머스 활성화의 중요한 계기가 되었다. 현재 TV홈쇼핑사, 백화점, 마트, 인터넷몰 사업자 등이 T-커머스 시장에 진출하고 있다.

아래의 (그림 1)은 T-커머스 사례들이다.

(그림 1) T-커머스 사례

인터넷전자상거래(e-커머스)와 마찬가지로 T-커머스는 회원가입, 로그인(인증), 주문, 결제라는 과정을 거치게 되며, 이 과정에서 사용하는 입력장치는 리모콘이다. 리모콘을 이용한 회원가입과 결제는 T-커머스 편의성을 크게 저하시키고 있고, 특히 리모콘을 이용한 카드정보 입력과 가맹점의 고객 카드정보 저장은 편리하고 안전한 T-커머스 결제 환경 제공을 위해 개선되어야할 부분이다. 예로 들면, 현재의 T-커머스에서 신용카드 결제를 위해서는 고객의 카드정보(카드번호, 유효기간, 비밀번호)를 리모콘으로 입력해야하는 불편함이 있을 뿐만 아니라, 30만원 이상의 거래에서는 공인인증서를 사용해야 한다.

이에 본 논문에서는 T-커머스 신용결제를 위해 현재 사용하고 있는 카드정보 입력방식이 아닌 IC신용카드를 셋탑박스 카드리더기(외장형, 내장형)에 꽂아 고객이 직접 결제하는 IC신용카드 결제시스템을 개발하였다. 적용된 규격은 IC신용카드 표준인 EMV(Europay, Mastercard, Visa) 규격이며, 상용서비스 중인 KT IPTV(올레TV) 셋톱박스를 타겟으로 T-커머스 EMV결제처리 모듈을 개발하였다.

본 논문에서 제시하는 T커머스 EMV결제 기술은 ATM기에 IC현금카드를 꽂아 조회 및 이체 등의 서비스를 이용하듯이, IC신용카드를 셋탑박스 카드리더기에 꽂아 결제하는 방식으로써, 리모콘으로 카드번호와 유효기간, 비밀번호 등을 입력해야 하는 번거로움과 보안의 취약성을 개선하였다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구로 IC신용카드 기술 동향, EMV표준 및 T-커머스에 대해 설명하고, 3장에서는 T-커머스 EMV결제처리 모듈에 대해 기술한다. 4장에서는 구현모듈에 대한 테스트 결과를 보여준 후, 5장에서 결론을 맺는다.

2. 관련 연구

2.1 IC신용카드 기술 동향

현재 보편적으로 사용하고 있는 신용카드는 플라스틱카드에 부착되어 있는 자기띠에 전자적으로 수록되어 있는 카드정보와 판매정보가 전자적으로 취득되어 컴퓨터 통신망을 통하여 매입사까지 전달, 검증절차를 거친 후 승인이 이루어지는 방식이다. 이러한 마그네틱 카드는 자기띠에 기록되어 있는 정보가 해독, 위변조 되면서 보안성 문제가 제기되었다[3]. 이러한 예로, 쉽게 구입할 수 있는 카드 복제기만 있으면 위조하는 것은 시간 문제이며, 가맹점단말기 또는 서버에 저장되어 있는 정보는 직원이 마음만 먹으면 정당한 방법으로 카드가 발급된 것처럼 언제든지 복제할 수 있다[4].

이러한 문제점을 해결하기 위한 대책으로 IC신용카드 도입을 추진하게 된 것이다.

2.1.1 IC신용카드의 개요

IC신용카드는 기존 신용카드 크기(가로 54mm * 세로 86 mm * 두께 0.76mm)의 플라스틱 카드에 마이크로칩(MPU)

과 메모리, EEPROM, 카드 운영체제(COS) 및 보안 알고리즘을 내장하고 있는 IC칩이 부착된 카드이다. 기존 MS신용카드에 비해 정보의 기밀성과 보안성을 향상시키고, 대용량의 정보를 저장하여 다양한 기능을 수행할 수 있도록 만든 카드이다. IC신용카드는 칩 내부에 저장기능의 메모리만 갖춘 메모리카드와 중앙처리장치인 CPU가 있어 연산 기능도 함께 갖춘 CPU내장카드로 구분된다. 이 두 종류의 IC신용카드를 포괄하여 광의의 IC신용카드라고 하며, 후자만을 일컫어서 협의의 IC신용카드 또는 스마트카드라고 한다[5].

2.1.2 IC신용카드의 특징

IC신용카드의 첫번째 특징은 한 장만으로도 다양한 분야에 적용할 수 있기 때문에 한 장의 카드에 1개의 서비스만 제공할 수 있던 전통적인 마그네틱 카드의 단점을 일시에 보완할 수 있는 상품으로 손색이 없다는 점이다. 두번째로 신용카드정보를 IC칩에 암호화하여 관리하기 때문에 마그네틱 카드보다 보안성이 월등히 우수하다. 또한 마그네틱 카드에서는 도입할 수 없었던 본인 확인방법으로 PIN(Personal Identification Number)이 사용되며, IC신용카드 발급시에 IC칩에 고객이 정한 PIN을 등록해 두고, 고객인증(Cardholder verification)에 PIN을 이용한다. 마지막으로 연산기능과 메모리를 가진 반도체 칩을 이용하므로 마그네틱 카드에 비해 대량의 정보를 저장할 수 있다는 점이다[4].

2.1.3 IC신용카드 운영체제

IC신용카드의 운영체제는 크게 단일 목적으로 사용되는 폐쇄형과 카드발급 후 어플리케이션을 쉽게 추가할 수 있는 개방형 플랫폼으로 구분된다. 개방형 플랫폼은 표준 언어와 개방형 API를 사용하여 응용 프로그램을 개발하기 때문에 스마트카드 칩에 대해 독립적이어서 다른 IC신용카드 칩에 적용하기 쉽고, 폐쇄형과 달리 재활용성이 매우 뛰어나다. 대표적인 개방형 운영체제로는 MULTOS(Multi-Application Operating System)와 자바카드가 있다[6].

- MULTOS

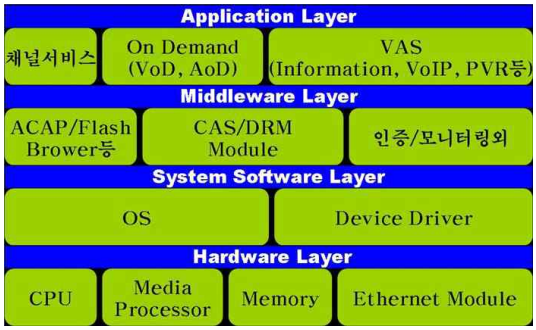
몬덱스에 의해 개발되었고, MAOSCO 컨소시엄에 의해 관리되고 있다. 프로그래밍 언어는 MEL(Multos Excutable Language)이라 불리는 전용 언어에 기반을 두고 MULTOS 가상기계에 의해 처리된다.

- 자바카드

자바카드는 썬 마이크로시스템즈에서 제작한 플랫폼이다. 자바카드의 구조는 운영체제 위에 썬에서 개발한 자바카드 가상머신을 탑재한 형태의 IC신용카드 플랫폼으로 MULTOS와 같이 다중 응용 프로그램 탑재 및 후발급(post-issuance) 형태로 응용프로그램 다운로딩이 가능하다.

2.2 양방향TV 기술 동향

양방향TV는 디지털 기술의 발달에 힘입어 통신망의 양방향성과 방송망의 광대역성이 융합될 수 있는 환경에서 나타난 대화형서비스가 가능한 TV를 통칭하는 개념이다. 대표적인 양방향 TV중 하나가 IPTV(Internet Protocol Television)이다[7].



(그림 2) 셋탑박스 구성도

IPTV는 IP(Internet Protocol)와 TV(Television)의 합성어로 인터넷 프로토콜을 이용해서 TV신호를 전송하는 방송서비스를 말한다.

IPTV 방송을 시청하기 위해서는 IPTV 셋탑박스가 필요하며, 셋탑박스는 TV 및 초고속인터넷망을 연결하여 통신과 방송서비스를 제공한다. 위의 (그림 2)는 셋탑박스의 구성도이다.

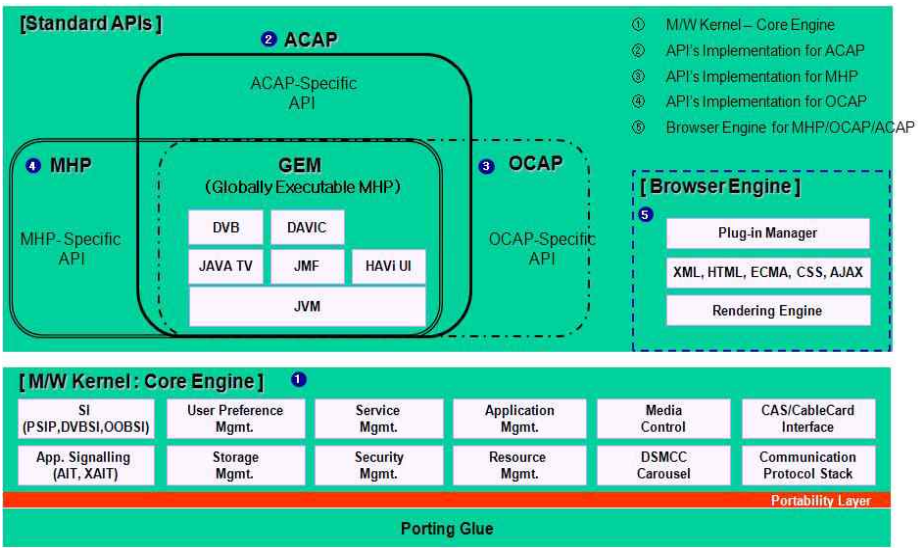
초기 IPTV서비스는 VOD가 주류였으나, 최근 IPTV 서비스는 실시간 고화질 방송서비스와 VOD, T-커머스, TV 앱, 인터넷 서비스 등 방송과 통신을 융합한 서비스를 제공하는 스마트TV로 발전하고 있다.

멀티미디어 콘텐츠 처리를 위한 미들웨어 규격 또한 자바기술을 사용했지만, 현재는 full browser와 flash를 수용하는 등 인터넷표준을 수용하는 추세이다. 향후 디지털TV는 양방향TV를 넘어 스마트TV로 급속히 발전하게 될 것이다. 아래의 (그림 3)은 셋탑박스의 미들웨어 구성도이다.

2.3 EMV(Europay, Mastercard, Visa)

EMV의 유래는 1993년 Europay, Mastercard, Visa 3사가 신용카드 및 직불카드를 IC신용카드화하기 위한 워킹그룹 결성에서 시작된다. EMV는 마그네틱 신용카드의 위·변조를 방지하고, 사기 거래 문제를 해소하기 위하여, 기존 신용카드 처리절차와 달리 서명대신 PIN을 통한 전자서명을 이용하여 처리하는 것을 주요 내용으로 하고 있다. 전자서명 기능을 이용하면 서비스 제공자나 판매업자의 입장에서는 부정카드나 부정단말기의 위협으로부터 보호받을 수 있게 된다.

이러한 EMV규격표준은 국제표준기구와 같은 공식적인 표준화기구에 의해 제정된 것이 아닌, 업체들이 국제표준을 참조하여 특정 어플리케이션을 수용할 수 있는 IC신용카드의 규격을 정한 것이기 때문에 엄격히 말해 EMV는 '표준'이라기보다 '업체규격'이라고 할 수 있다. 그러나 Europay, Mastercard, Visa가 신용카드 업계에서 차지하는 위상을 고려해보면 표준으로 보는데 무리가 없고, 국내외 금융기관들이 세계적으로 호환 가능한 신용, 직불 IC신용카드를 발급



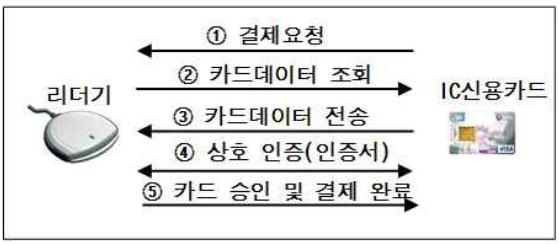
(그림 3) 미들웨어 구성도

하기 위해서는 EMV표준을 준수하는 것이 필수적이라 할 수 있다.

EMV규격은 기본적으로 ISO의 IC카드 표준인 ISO 7816을 참조하고 있으며, EMV규격은 크게 IC카드에 관련된 사항, 보안에 관련된 사항, 신용/직불 응용에 관련된 사항, 단말기에 관련된 사항으로 되어 있다.

1996년 EMV3.0, 2000년에 EMV4.0(통칭 EMV2000)으로 개정되어 현재는 EMV4.2규격에 이르고 있다.

EMV규격의 IC신용카드는 마그네틱 카드와 비교했을 때 가맹점에 설치되어 있는 리더기와 이용자가 소지하고 있는 IC신용카드 간에 거래가 매번 VAN사의 네트워크를 거쳐 카드사의 승인계까지 갈 필요가 없다. 그 이유는 서버에 저장된 비밀번호(온라1인 PIN)가 아닌 IC칩의 PIN(오프라인 PIN)을 통해 고객 검증을 하기 때문이다. 아래의 (그림 4)는 오프라인 가맹점에서 리더기와 EMV규격 IC신용카드간의 결제 흐름을 도식화한 것이다[8].



(그림 4) EMV의 결제 시스템 흐름

EMV규격 IC신용카드의 특성을 요약하면 다음과 같다.

- 오프라인 거래

분실카드 관리가 없어지고, 신용카드 사용시 조회 절차가 필요없이 EMV카드를 단말기에 삽입하여 오프라인으로 결제를 할 수 있다. 단 10회 카드거래 또는 일정주기로 사후 정산만 한다.

- 서명대체 PIN

카드 소지자가 신용카드 가맹점의 단말기에서 결제할 때 영수증 서명을 대신하여 PIN입력에 의한 전자서명으로 대체된다.

- PIN 보안성

MS 신용카드 비밀번호는 카드 소지자의 비밀번호를 서버에 기록 관리하기 때문에 금융기관의 내부자가 특정 개인의 비밀번호를 알 수 있으나, EMV 오프라인 PIN은 EMV IC칩 내부에 암호화된 형태로 저장되므로, 금융기관의 내부자나 발급자도 알 수 없고, 카드소지자 본인만이 알 수 있다.

- PIN 보안관리

만일 발급사가 정한 일정 횟수 이상의 PIN오류가 발생하면, EMV카드는 잠기고 발급사의 영업점에 가서 카드 소지자가 본인임을 확인한 후, 창구 직원이 EMV카드의 잠금 해제하고 새로운 PIN을 카드 소지자가 입력하여야 사용할 수 있다.

- 신용/직불/선불 선택

EMV카드내에 신용과 직불, 선불카드가 포함될 수 있어서 카드 소지자가 금액 규모에 따라 선택적으로 지불할 수 있다[5].

- 위/변조 불가

IC칩 기반의 CSN(Card Serial Number), RID(Registered application provider IDentifier), 암호화 알고리즘 등을 사용하기 때문에 카드의 위·변조에 의한 부정거래를 원천적으로 방지할 수 있다[4].

2.4 T-커머스의 개요 및 현황

T-커머스(T-Commerce)는 Television Commerce의 준말로 TV를 기반으로 한 전자상거래를 의미한다. 즉, T-커머스는 TV를 통해 상품 정보를 검색하고 주문 및 결제까지

할 수 있는 신개념 전자상거래이다. 일반적인 T-커머스 프로세스는 아래 (그림 5)와 같다. 이러한 T커머스 과정은 방송채널을 이용하여 T커머스 어플리케이션과 상품정보를 송출하고 고객이 셋탑박스와 리모콘을 이용하여 주문결제를 한다는 것 외에 일반 전자상거래와 동일하다.

(그림 5) T-커머스상에서의 구매 프로세스

T-커머스의 강점은 접근성과 즉시성이다. 거실에 있는 TV는 컴퓨터와는 달리 부팅과정이 없고, 인터넷 주소(URL)가 아닌 채널(숫자)로 서비스에 진입할 수 있기 때문에 접근성이 뛰어나다. 무엇보다 T-커머스는 인터넷쇼핑(공간, 목적구매)과 TV홈쇼핑(방송, 충동구매)의 장점을 모두 가지고 있어 20대 후반에서 40대 초반의 고객층을 새로운 소비자로 흡수 가능하다[9].

이러한 장점에도 불구하고 T-커머스 활성화의 걸림돌은 컴퓨터의 키보드와 마우스 같이 편리한 인터페이스기기 아닌 TV리모콘을 이용하기 때문에 회원가입, 로그인, 결제정보 입력 등에 있어서 매우 불편하고 결제 수단의 다양성이 부족이다. 현재는 신용카드와 가상계좌입금 방식이 이용되고 있다. 신용카드결제는 카드정보(카드번호, 유효기간), 비밀번호를 직접 입력하는 방식이며, 특히 고객의 편의성 문제로 30만원 이상의 거래에서 적용해야 하는 공인인증서를 적용하지 않고 있다.

이러한 카드결제의 문제점을 극복하기 위해서 KT, 신한카드, 미디어벨로 3사가 2008년 6월 제휴를 맺고 T커머스 IC카드 결제 사업을 준비하기 시작하여, 2009년 9월 신한카드, 국민카드, BC카드, 농협, 미디어벨로가 IC카드결제를 위한 T-커머스 컨소시엄을 구성하였으며, IC카드 결제 시장 활성화의 기반을 마련하였다.

T커머스 컨소시엄은 2010년 12월 현대홈쇼핑 T커머스에 IC카드 '간편결제' 서비스를 시작하였고, 2011년 7월 KT 올레TV 오픈마켓에 IC카드결제를 제공하고 있다.

해외에서는 영국의 BskyB가 2005년 SkyCARD라는 자사 브랜드의 IC신용카드를 발급하여 SkyActive(양방향서비스)와 지불결제에 사용하고 있다[10].

3. T커머스를 위한 IC신용카드 결제처리 모듈 구현

3.1 전체 EMV결제시스템 구성 요소

아래의 (그림 6)은 전체 IC신용카드(EMV) 결제 시스템의 구성도이다. 각 각에 대한 모듈 및 기능에 대한 간략한 설명은 다음과 같다.

3.1.1 IC신용카드 애플릿

IC신용카드 애플릿은 IC칩 메모리에 탑재되어 실행되는 소프트웨어를 말한다. IC신용카드 애플릿은 T-커머스 및 TV 기반의 다양한 부가 서비스에 대해 IC신용카드를 이용하여 제공하기 위해 필요하다.

3.1.2 셋탑박스(STB)의 EMV결제모듈

IC신용카드(EMV)결제를 위해서는 IPTV STB에 IC신용카드 리더기를 제어할 수 있는 디바이스 드라이버와 EMV처리를 위한 EMV모듈, 응용 프로그램에서 사용할 수 있는 API등을 STB에 구현해야 한다.

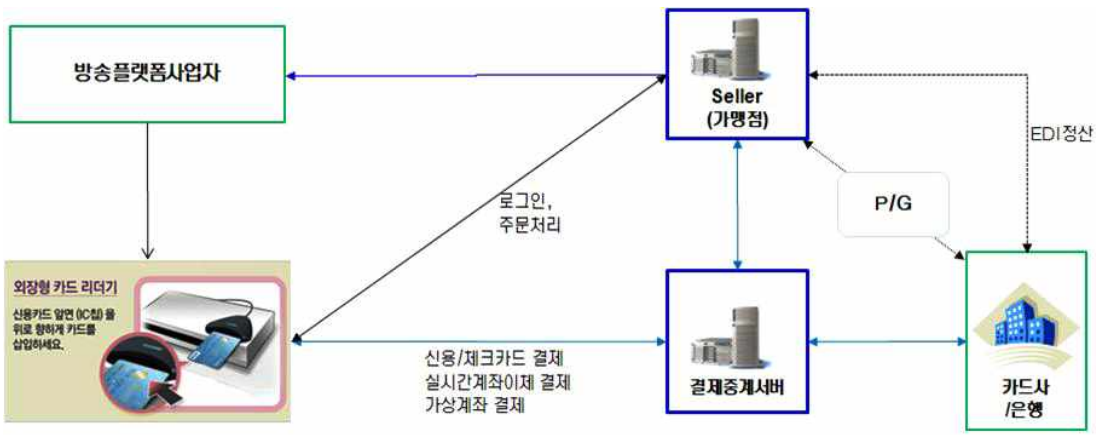
3.1.3 EMV결제 중계서버

EMV결제 중계서버는 IPTV STB의 T-커머스 어플리케이션의 결제 요청을 VAN사와 연동하여 카드사에게 승인을 요청하고 처리 결과를 STB로 전달해주는 중계(Gateway)기능을 수행한다.

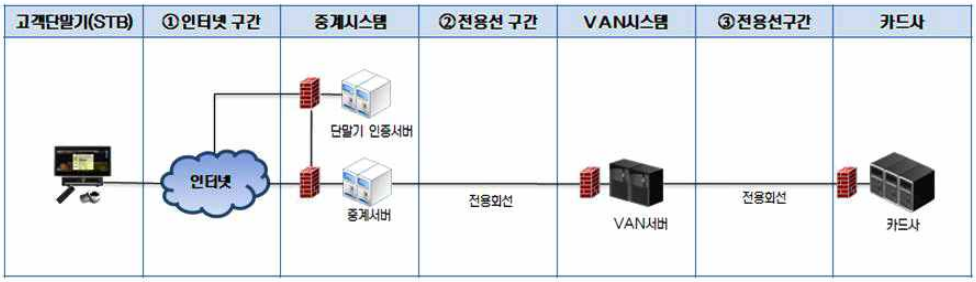
중계서버는 승인처리 외에 셋탑박스 유효성 검증 및 암호화 기능을 수행한다.

3.1.4 망 구성 및 암호화

EMV결제 시스템을 구성하기 위해서 STB와 EMV중계서



(그림 6) 전체 EMV결제 시스템 구성도



(그림 7) 망 구성도

버간의 인터넷 구간 및 EMV중5계서버와 VAN, 카드사를 연결하기 위한 전용선 구간이 있다.

위의 (그림 7)은 EMV결제 시스템을 위한 망 구성도이다. 각 각의 구간에 대한 설명은 다음과 같다.

① 인터넷 구간
- 고객단말기와 중계서버는 세션키 공유 과정을 통해 모든 전문을 암호화 송수신한다.
- EMV거래요청 전문은 중계서버와의 암호화 세션 내에서 PKI 기반의 보안 모듈을 통해 VAN에서만 복호화가 가능하도록 암호화(VAN 공개키)하여 전송한다.
- 전문 종류 : EMV승인 전문, EMV취소 전문, EMV망상취소 전문

② 전용선 구간
- 고객정보가 담긴 EMV거래요청 전문은 고객단말기로부터 암호화된 전문을 전송한다.

③ 전용선 구간
- 기존에 구현되어 있는 구간으로 전용선을 사용하여 전문 암호화 없이 X.25 방식으로 통신한다.

본 논문에서는 이중에서 EMV 결제를 위해 IPTV 셋톱박스용 EMV결제모듈을 개발하였다.

3.2 IPTV셋톱박스 EMV결제 모듈 개발

EMV결제처리를 위해 개발한 모듈과 기능은 다음과 같다.

3.2.1 IC카드리더기용 디바이스 드라이버

IC카드리더기는 셋톱박스에 IC신용카드를 꽂아서 IC칩에 저장된 정보를 읽거나 쓸 수 있는 단말장치로 셋톱박스에 슬롯형태로 내장되거나 USB로 연결되는 동글 형태가 있다.

IC신용카드 결제를 위해서 IC신용카드 EMV애플릿과 셋톱박스의 어플리케이션간 통신시 필요하며, 이를 위해 셋톱박스와 IC신용카드 리더기간의 물리적인 인터페이스를 위한 IC카드리더기 드라이버 및 명령과 데이터를 주고 받는데 필요한 CCID(Chip Card Interface Device), PCSC(Personal Computer Smart Card)드라이버가 필요하다.

기존의 IC카드리더기 드라이버는 pcscd 데몬이 항상 수행되고 있다가 IC카드리더기가 연결되거나 IC카드가 인식되는 경우 곧바로 인식을 하도록 되어 있으나 IPTV 셋톱박스와 같이 사용가능한 자원이 제한적인 경우에는 적용하기 어려운 방식이다. 따라서 IC신용카드 드라이버는 대상 셋톱박스의 운영체제 및 메모리 자원 등을 고려하여 최적화된 모델로 설계하여야 한다. 이에 본 논문에서는 개발용 셋탑박스(올레TV STB)의 메모리 자원을 고려하여, 최소의 리소스만 사용하도록 최적화 모델로 설계하였다.

```
listen
loop begin
    wait for request
    accept
        if pcscd is not running
            execute pcscd
    sleep for PC/SC deamon startup
    execute IC card server
```

(그림 8) 리스너에 대한 의사코드

이를 위해 평상시 메모리 사용량을 고려하여 최소의 메모리만 사용하는 별도의 프로그램(리스너-Listener)이 동작하다가 IC신용카드 결제요청이 발생하면 pcscd 데몬을 수행하여 결제처리를 하고, 요청이 완료되면 데몬 프로세스를 종료하도록 개발하였다.

위의 (그림 8)은 이러한 리스너에 대한 의사코드이다.

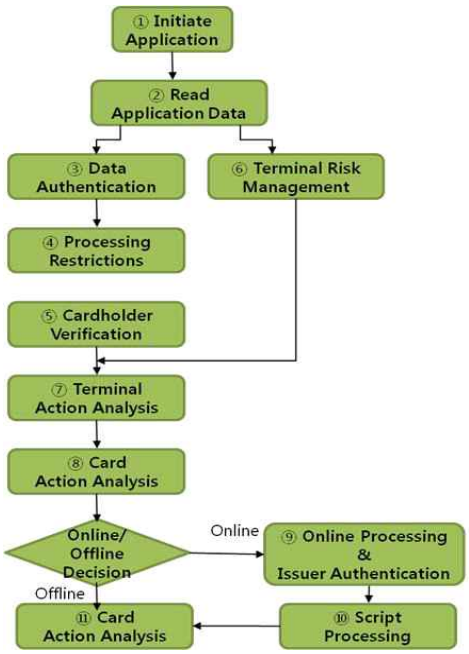
리스너는 서비스를 수행하기 전에 루프를 돌면서 클라이언트의 요청이 오기를 기다린다. 클라이언트로부터 접속 요청이 오면, 클라이언트와 통신할 수 있도록 소켓을 생성한다. pcscd 데몬이 실행 중이 아니라면 데몬을 실행한 후 서비스 처리를 위하여 EMV커널을 실행한다.

3.2.2 EMV모듈

EMV커널이라고 하는 EMV모듈은 단말기(셋탑박스)에 구동되는 EMV어플리케이션 처리 모듈로서, IC신용카드의 IC칩에서 구동되는 EMV애플릿과 통신하여 EMV결제처리를 담당한다. 아래의 (그림 9)는 EMV어플리케이션 처리 절차이다.

(그림 9)에 대한 단계별 처리내용은 다음과 같다[11].

① Initiate Application : 단말기에서 IC카드에 새로운 거래가 시작하는 것을 알리고 거래에 대한 단말기 정보를 IC카드에 제공한다.



(그림 9) EMV어플리케이션 처리절

② Read Application Data : 단말기는 IC카드에 저장된 기본 정보를 읽어 들인다.

③ Data Authentication : 발급기관에 의해 IC카드에 입력된 특정 데이터를 검증한다. 어떤 형태로 인증할지는 발급기관에 의해 결정된다.

④ Processing Restrictions : 어플리케이션 버전, 어플리케이션 사용조건, 어플리케이션 유효/만료일자 검사등과 함께 사용 가능한 IC카드인지를 확인한다.

⑤ Cardholder Verification : 온라인 PIN 검증, 오프라인 PIN 검증, 전자서명 등의 방법을 이용하여 카드소유자가 정당한 사용자인지를 확인한다.

⑥ Terminal Risk Management : 오프라인 방식으로 거래를 처리할 경우에 발생 가능한 여러 가지 위험을 방지하기 위하여 일정금액이나 일정건수를 초과할 경우나 무작위로 특정 거래를 선택하여 발급기관의 승인을 요청하는 것과 같은 위험 관리 기능을 수행한다.

⑦ Terminal Action Analysis : 제반검증이 완료되면 단말기는 거래를 오프라인 또는 온라인으로 처리할지 여부를 결정하기 위해 IC카드와 관련 데이터를 주고 받는다.

⑧ Card Action Analysis : IC카드는 발급기관에서 설정한 방법에 따라 단말기에서와 유사한 위험관리 기능을 수행하고 온라인 또는 오프라인의 거래처리 방법등을 결정한다.

⑨ Online Processing & Issuer Authentication : 거래가 온라인으로 처리될 경우 발급기관에 의한 거래 승인이 이루어진다.

⑩ Script Processing : 발급기관은 거래와 연관된 어떤 기능이나 IC카드에 탑재된 어플리케이션의 기능과 관련된 명령어(Script)를 단말기를 통해 IC카드에 전송한다.

⑪ Completion : 거래를 종료한다.

EMV표준은 공식인증기관으로부터 인증 테스트를 받아야 한다. 인증 테스트는 크게 EMV레벨1과 레벨2의 두 단계로 나뉘어지는데, EMV모듈은 레벨2 인증을 받아야 한다.

EMV결제가 갖는 여러 가지 특성중의 하나는 기존의 신용카드와 달리 결제 승인 시 매번 VAN(Value Added Network)과 카드사 연동이 필요없다는 것이다. 이것은 IC신용카드 내에 관리되고 있는 PIN을 통해 고객 검증(Cardholder verification)을 하는 방법으로 이루어지며 결제 횟수나 결제금액 합계가 카드사가 정한 기준과 부합되는 경우에만 결제처리 정보를 카드사로 전송하게 된다. 이에 따라 EMV결제에서는 VAN과의 통신은 줄어들게 된다.

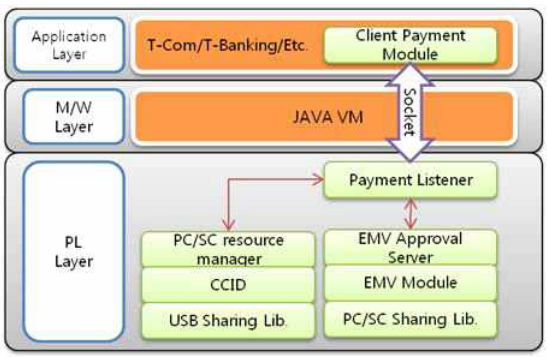
3.2.3 EMV결제 API

EMV결제 API는 T-커머스 어플리케이션이 IC신용카드 결제 방식을 이용할 수 있도록 미들웨어 레벨에서 API형태로 개발되었다.

개발된 EMV결제 API는 IPTV 셋톱박스 미들웨어 표준인 ACAP(Advanced Common Application Platform)의 확장 API형태로 개발 되었다. API 개발시 사용자의 PIN 정보를 입력받는 부분은 API 자체적으로 UI를 구현하여 사용자 PIN 정보가 외부 어플리케이션에서 접근이 불가하도록 설계 및 구현 하였다.

특히, EMV결제기술의 T-커머스 적용 방식에 대해 T-커머스 사업자(대표적으로 홈쇼핑)들의 요구사항이 상이하기 때문에 미들웨어 API 설계시에 유연성과 확장성을 고려하였다.

아래의 (그림 10)은 본 논문에서 구성한 EMV결제를 위한 STB의 계층적인 구성도이다.



(그림 10) STB의 계층적인 구성도

여기서 EMV승인서버(EMV Approval Server)는 EMV모듈의 초기화 및 클라이언트로부터의 서비스 요청(전문) 처리를 위한 부분이다.

T-커머스 서비스와 같은 IPTV 어플리케이션은 미들웨어 위에서 수행되는 반면에 IC카드리더기 드라이버는 미들웨어 하부 레벨인 운영체제에서 수행된다.

EMV모듈 및 EMV승인서버는 클라이언트 지불 모듈과 소켓을 통해 데이터를 주고 받을 수 있다.

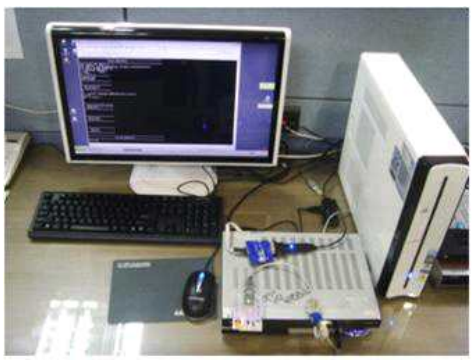
4. 테스트 및 실험결과

본 실험은 IC신용카드 결제 시스템에 대한 테스트를 위해 셋탑박스에서 리스너를 실행한 후, 어플리케이션을 송출하여 실제 IPTV환경과 동일하게 테스트하였다.

〈표 1〉 실행 환경

TV 어플리케이션	eclipse 3.5(갈릴레오), JDK1.5, xletview 사용
셋탑박스	올레TV STB
카드리더기	USB 스마트카드 리더기
IC신용카드	IC신용카드(카드사 발급)
디스플레이	TV 겸용 모니터

위의 <표 1>는 실행 환경을 정리한 것이고, 아래의 (그림 11)은 테스트 환경이다.

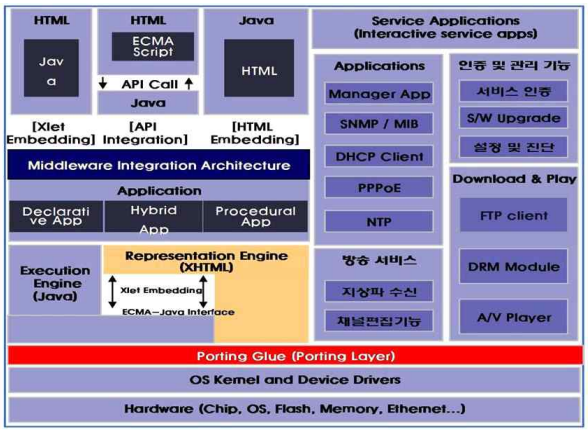


(그림 11) 테스트 환경

4.1 테스트용 셋톱박스의 하드웨어 구성

본 논문에서 사용된 셋탑박스는 이미 상용서비스 되고 있는 올레TV 셋톱박스를 이용하였다. 올레TV 셋톱박스는 ICOD(Internet Contents On Demand), D&P(Download & Play), 스카이라이프 올레TV(위성방송과 IPTV겸용) 3가지가 있다. ICOD 셋톱박스는 실시간 방송 수신, 양방향 서비스(TV앱) 및 TV포털(VOD서비스)이 가능한 셋톱박스이고 D&P 셋톱박스는 양방향 서비스와 TV포털(VOD서비스)이 가능한 셋톱박스이다. 최근에는 위성방송과 IPTV방송 겸용 셋톱박스인 스카이라이프 올레TV가 많이 보급되고 있다.

4.2 테스트용 셋톱박스의 소프트웨어 아키텍쳐



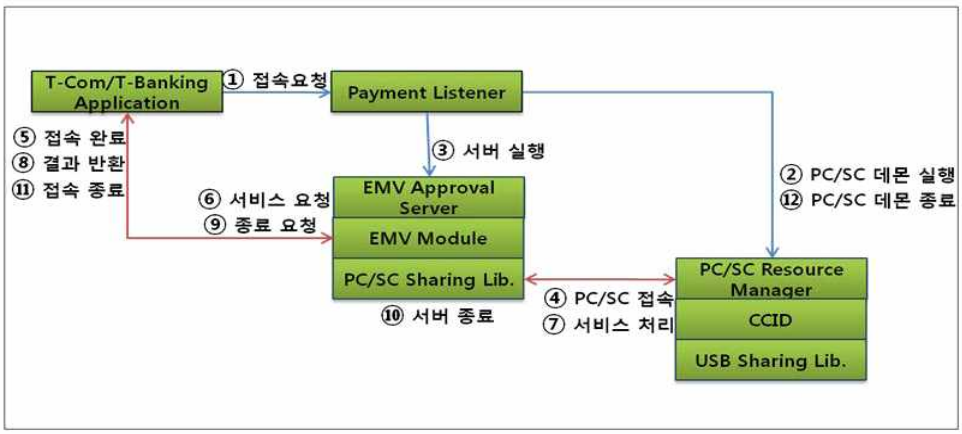
(그림 12) 셋톱박스 S/W 구성도

셋톱박스의 소프트웨어 아키텍쳐를 보면 Linux 운영체제를 사용하고 있으며 미들웨어는 ATSC(Advanced Television System Committee)에서 권고하고 있는 국내 지상파 데이터 방송 디지털TV의 미들웨어 표준인 ACAP (Advanced Common Application Platform)를 기반으로 탑재되어 있다.

위의 (그림 12)은 타겟 STB에 들어있는 소프트웨어 구성도이다.

4.3 STB 결제처리 모듈의 수행과정

EMV결제 리스너는 OS가 부팅되는 시점에서 실행이 되며 아래의 (그림 13)과 같이 서비스 요청이 오는 경우에만 관련 프로세스들을 수행시킨 후, 처리가 완료되면 프로세스를 종료시키도록 하였다.



(그림 13) IC 신용카드 결제처리 모듈의 LifeCycle

위의 (그림 13)의 과정에 대한 설명은 다음과 같다.

1. T-커머스 서비스를 사용자가 이용하면, T-커머스 응용프로그램은 EMV결제 리스너에 접속
2. EMV결제 리스너는 PC/SC 리소스 매니저를 실행
3-4. EMV결제 리스너에서 서버를 실행→서버는 PC/SC 리소스 매니저에 접속
5. 서버에서 응용프로그램에게 실행 준비가 완료됨을 통보
6. 응용프로그램에서 서버에게 서비스 요청
7. 서버는 PC/SC 매니저에 스마트카드 관련 명령 전달→PC/SC 매니저는 드라이버를 통해 스마트카드에 명령 전달 및 응답 수신→PC/SC 매니저는 수신한 응답을 서버에 전달
8. 처리된 결과를 응용프로그램에게 반환
9. 응용프로그램은 작업이 끝났으므로 종료를 서버에 요청
10-11. 서버는 응용프로그램과 접속을 닫은 후 종료
12. EMV결제 리스너는 실행 중인 서버가 일정 시간 존재하지 않을 경우, PC/SC 리소스 매니저에 종료요청→PC/SC 매니저는 드라이버 언로드 및 종료

4.4 EMV결제 모듈 테스트

기존의 IPTV를 통한 IC신용카드 결제는 USB 카드리더기에 IC신용카드를 꽂아서 사용해야 했지만 2010년 말부터 IC카드리더기를 셋톱박스 내장(built-in)하고 있다.

리스너를 사용하지 않을 경우 EMV결제리스너와 커널이 통합된 형태로 항상 메모리에 상주되어 있어, 일반적인 방법에서는 1.3MB가량의 메모리를 점유하게 된다. 하지만 본 논문에서는 다른 어플리케이션에 1MB의 메모리를 더 제공할 수 있도록 하기 위해 EMV결제 리스너와 커널을 분리함으로써 리스너의 크기인 300KB가량의 메모리만 차지하게 된다.

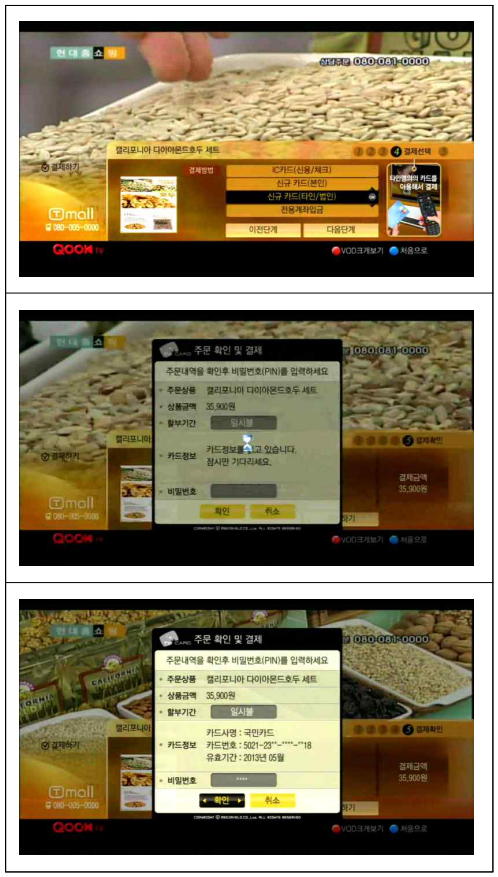
IC신용카드를 리더기에 꽂으면 리스너가 실행되게 되는데, 아래 (그림 14)는 터미널을 통한 EMV결제 리스너의 실행되는 과정을 출력 화면을 통해 확인한 것이다.

```
$ ./tvcard_listener
tvcard_listener[14288] --------------------[ TV*CARD ]--------------------
tvcard_listener[14288] Listener initialization started
tvcard_listener[14288] $ Installing signal handlers
tvcard_listener[14288] Creaing IPv4 stream(tcp/ip) socket for listening
tvcard_listener[14288] Setting FD_CLOEXEC to socket
tvcard_listener[14288] Setting SO_REUSEADDR option to socket
tvcard_listener[14288] Binding 127.0.0.1:2111 to socket
tvcard_listener[14288] Start listening for connections
tvcard_listener[14288] Listener initialization completed successfully
tvcard_listener[14288] Listener is waiting for connections
```

(그림 14) 리스너의 실행 화면

4.5 T커머스 EMV 결제 테스트

EMV결제처리 모듈의 실행을 확인하기 위해서 TV홈쇼핑을 통한 IC신용카드의 사용을 테스트하였다. 기존의 IPTV 상에서 소비자가 홈쇼핑을 보다가 물건을 구매하기 위해서는 상품 선택부터 결제까지 리모콘 key-in방식을 사용해서 40~46회 정도의 키 동작이 필요하다. 하지만 본 논문에서



(그림 15) EMV 결제 과정

제안하는 EMV결제모듈을 이용하면 12~16회의 리모콘 키 동작으로 구매를 완료할 수 있다.

위의 (그림 15)는 IC신용카드를 이용한 EMV 결제 과정을 보여주고 있다.

(그림 15)의 결제 과정에 대한 간략한 설명은 다음과 같다.

① 상품을 결정한 후, 결제 방법을 선택
② 결제버튼을 누르면, IC신용카드에 있는 정보를 불러와 화면상에 표시해준다.
③ 비밀번호(PIN번호)를 입력 후, 일치하면 결제 완료화면을 구매자에게 표시한다.

T-커머스상에서 기존의 IC신용카드의 결제과정과 비교하면, 자신의 카드 정보를 직접 입력하지 않고도 IC신용카드로부터 직접 읽어들이기 때문에 키 입력 횟수가 줄어들게 되고 결과적으로 사용자 편의성이 향상된다.

5. 결론 및 향후 과제

지금까지 마그네틱 카드는 신용카드나 체크카드, 직불카드 등에 오랫동안 사용되어 왔으나 저장되는 정보의 양이 적고, 카드의 위·변조에 취약하다는 치명적인 단점을 가지고 있다. 이에 Europay, Master-card, Visa 3사는 마그네

틱 카드의 위·변조를 막고 글로벌한 결제수단을 제공하기 위해 IC신용카드 결제 방식의 EMV규격을 발표하였다. IC 신용카드는 카드의 위·변조를 방지할 뿐만 아니라, 저장 공간이 크기 때문에 다양한 기능을 한 장의 카드로 해결할 수 있어 금융, 교통, 통신, 의료, 학교등 거의 모든 산업분야에서 이용되고 있다. 또한 신용카드 결제시 PIN 입력방식에 의한 결제가 이루어지기 때문에 사용자 편의성을 제공할 수 있다.

디지털 방송 시장 성장과 함께 T-커머스 라는 새로운 T 전자상거래 시장이 성장하고 있으나, 아직까지는 편리하고 안전한 다양한 TV결제 솔루션이 나오지 않아 성장의 걸림돌이 되고 있다. 이를 극복하기 위한 한 방법으로 본 논문에서는 IC신용카드의 결제표준인 EMV기술을 IPTV환경에 맞도록 개발하기 위해서 IPTV셋톱박스상에 IC신용카드를 이용한 EMV결제처리 모듈을 개발하였다. IPTV셋톱박스에서 IC신용카드를 이용한 EMV결제를 하기 위해서 셋탑박스에 EMV결제처리를 위한 EMV모듈 및 EMV승인 처리를 위한 EMV승인서버를 구현하였다.

또한, 방송용 셋톱박스의 하드웨어 자원에 대한 한계를 극복(메모리의 효율성)하기 위해 결제시에만 해당 모듈이 메모리에 로딩되어 구동될 수 있도록 하였으며, 1MB정도의 메모리 공간을 확보하여 다른 어플리케이션이 구동되는데 문제가 없다는 것 또한 확인하였다. KT Olleh TV 셋톱박스를 이용하여 안정적으로 EMV결제가 이루지는 것과 안정성 확보를 위해 Memory leak 테스트도 시행하였다.

향후 과제로는 IC신용카드를 셋탑박스에 꽂아서 사용하도록 하는 접촉식이 아닌 버스카드나 지하철 패스카드와 같은 비접촉식 결제 방법에 대한 연구 및 스마트폰 등 모바일 기기를 연동한 TV모바일결제, NFC USIM기반의 모바일카드를 이용한 결제 등에 대한 연구가 필요하다.

참 고 문 헌

[1] 박성업, “국내전용 EMVIC칩 신용카드 표준규격 개발 현황 및 발전 방향”, 신용카드, 제42호, pp.51-66, 2007.

[2] 공동현, “스마트카드 산업현황 및 전망”, 한국정보과학회, Vol.28, No.11, pp.49-55, 2010.

[3] 천성록, “비접촉식신용카드 기술의 최근 동향 및 시사점”, 여신금융협회, 2009.

[4] 백미연, “금융IC신용카드 이용동향”, 금융감독원, 2005.

[5] 김요한, “IC신용카드의 현황과 활성화 방안에 관한 연구”, 단국대학교 석사학위논문, 2005.

[6] 공동현, “스마트카드 산업 현황 및 전망”, 정보처리학회지, 제17권 제6호, pp.37-45, 2010.

[7] 권혁주, 김영근, 박진기, 이양선, “양방향 디지털 방송을 위한 Enhanced TV Receiver 설계 및 구현”, 한국정보처리학회 춘계학술대회, Vol.14, No.01, pp.1477-1480, 2007.

[8] 정화용, “모바일 支給決濟의 發展方案에 대한 硏究”, 단국대학교 석사학위논문, 2008.

[9] 김진혁, “TV홈쇼핑의 신성장동력, T-커머스“, 삼성경제연구소, 2006.

[10] 이동복, “T-commerce 현황과 활성화 방안”, 디지털 미디어 트렌드, 9-3호 통권 35호, pp.5-16, 2009.

[11] 장병환, “EMV표준동향”,금융결제원, 2003.

최 병 규

e-mail : mysaint@hanyang.ac.kr
2002년 한양대학교 전자컴퓨터공학부(학사)
2004년 한양대학교 컴퓨터공학과(석사)
현 재 한양대학교 컴퓨터공학과 박사과정 수료
관심분야 : Sensor-network, TMO(Time-triggered Message-triggered Object)

이 동 복

e-mail : dblee@mediavelo.com
1989년 한양대학교 전자계산학과(학사)
1991년 한양대학교 전자계산학과(석사)
1991년~1996년 대영전자공업(주) 기술연구소 주임 연구원
1996년~2000년 삼일데이타시스템(주) 부설 연구소 소장
2000년~2007년 에어코드 DTV연구소 소장(CTO)
2007년~현 재 미디어벨로(주) CEO
관심분야 : 스마트미디어 기반 전자지급결제기술, N-screen payment 기술, T커머스

김 병 곤

e-mail : bkkim@kict.re.kr
1991년 한양대학교 전자계산학과(학사)
1993년 한양대학교 전자계산학과(석사)
2003년 한양대학교 컴퓨터공학과 박사과정 수료
1993년~현 재 한국건설기술연구원 건설정보연구실 수석연구원
관심분야 : 운영체제, 무선센서네트워크(WSN), 건설정보화

허 신

e-mail : shinheu@hanyang.ac.kr
1973년 서울대학교 전기공학과(학사)
1979년 미국 University of Southern California 전산학(석사)
1986년 미국 University of South Florida 전산학(박사)
1980년~1986년 미국 University of South Florida 연구원보
1986년~1988년 미국 The Catholic University of America 조교수
1988년~현 재 한양대학교 컴퓨터공학과 교수
관심분야 : 분산컴퓨팅, 결함허용시스템, 실시간운영체제 등