

GVM 과 모바일 C 를 이용한 무선 결제 시스템

엄은배^o, 신흥섭, 오세만
동국대학교 컴퓨터공학과
e-mail : {ketty03, s4064, smoh}@dongguk.edu

Wireless Payment System using GVM and MobileC

Eun-Bae Eom^o, Hong-Seob Shin, Se-Man Oh
Dept. of Computer Engineering, Dongguk University

요 약

무선인터넷의 비약적인 발전에 힘입어, 이동통신 단말기를 위한 이동통신서비스가 급격히 증가하고 있다. 특히 온라인이나 오프라인상에서 물품을 판매하거나, 정보서비스를 제공하는 무선전자상거래 시장이 빠른 속도로 성장하고 있으며, 무선전자상거래가 성공적으로 이루어지기 위한 무선 결제 시스템이 요구되기 시작하였다. 기존의 무선 결제 시스템은 스마트 카드를 이동통신 단말기에 탑재하여 결제하는 방식이었으며, 반드시 스마트 카드를 이동통신 단말기에 탑재해야 하는 번거로움과 제 3 자에 의한 오남용을 막을 수 없는 단점을 지니고 있다.

본 논문에서는 소프트웨어 다운로드 솔루션을 기반으로 한 GVM(General Virtual Machine)상에서 실행될 수 있는 모바일 C 기반의 무선 결제 시스템을 제안하고자 한다. 제안하는 무선 결제 시스템은 모두 3 개의 모듈로 구성되어 있으며, 개인 정보 관리 모듈에서는 공인인증서와 개인의 신용정보를 단말기에 다운로드 받아 저장한다. 사용자 상호 작용 모듈에서는 유저 인터페이스를 통하여 결제 금액과 개인 인증 번호를 입력 받으며, 암호화 모듈에서는 공인인증서의 암호화 알고리즘을 적용하여 결제금액과 개인 인증 번호를 암호화한 후 서버로 전송한다.

1. 서론

무선인터넷의 비약적인 발전에 힘입어, 이동통신 단말기를 위한 이동통신서비스가 급격히 증가하고 있다. 특히 온라인이나 오프라인상에서 물품을 판매하거나, 정보서비스를 제공하는 무선전자상거래 시장이 빠른 속도로 성장하고 있으며, 무선전자상거래가 성공적으로 이루어지기 위한 무선 결제 시스템이 요구되기 시작하였다.

무선 결제 시스템이란, 온라인과 오프라인 상에서 이루어지는 서비스와 재화 구매 시, 이동통신 단말기를 이용하여 대금을 지불하는 결제 서비스이다.[2] 기존의 무선 결제 시스템은 신용카드, 직불카드, 마일리지 등의 다양한 신용정보가 저장된 스마트 카드를 이동통신 단말기에 탑재하여 결제 서비스를 처리하는 방식이었다. 그러나 이동통신 단말기에 반드시 스마트 카드를 탑재해야 하는 번거로움과 제3자에 의한 오남

용을 막을 수 없는 단점을 지니고 있다.

본 논문에서는 소프트웨어 다운로드 솔루션을 기반으로 한 GVM 상에서 실행될 수 있는 모바일 C 기반의 무선 결제 시스템을 제안하고자 한다. 스마트카드가 탑재되지 않은 이동통신 단말기에서도 모바일 C 기반의 무선 결제 시스템을 다운로드 하여 결제 서비스를 처리할 수 있으며, 반드시 개인의 신용 정보를 입력해야 하기 때문에 제 3 자의 오남용을 방지할 수 있다.

모바일 C 기반의 결제 시스템은 모두 3 개의 모듈로 구성되어 있다. 개인 정보 관리 모듈에서는 공인인증서와 개인의 신용정보를 단말기에 다운로드 받아 비휘발성 메모리에 저장한다. 사용자 상호 작용 모듈에서는 무선 결제 시스템의 유저 인터페이스를 통하여 결제 금액과 개인 인증 번호를 입력 받으며, 암호화 모듈에서는 공인인증서의 암호화 알고리즘을 적용하여 결제금액과 개인 인증 번호를 암호화한 후 서버로 전송한다.

2. 관련연구

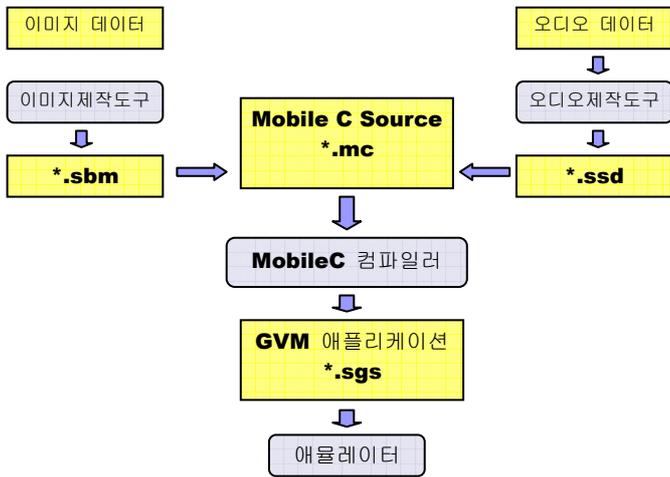
2.1 GVM 과 모바일 C

2.1.1 GVM

GVM 은 이동통신 단말기상에서 동적으로 응용프로그램을 실행할 수 있는 가상기계 플랫폼이다. GVM 은 무선 인터넷 미들웨어 솔루션으로 무선망을 통하여 애플리케이션을 다운로드하여 필요한 시점에 단말기상에서 실행할 수 있게 하는 기능을 제공한다.

GVM 시스템은 GVM SDK, GVM 서버, GVM 모듈이 내장된 단말기로 구성되어 있다.

GVM SDK 는 GVM 애플리케이션을 작성하는 프로그램 개발도구를 총칭하며 모바일 C 컴파일러, Media Tool Kit, GVM 에뮬레이터의 세가지로 구성되어 있다. [그림 1]은 GVM SDK 를 이용한 애플리케이션 개발과정을 보여준다.



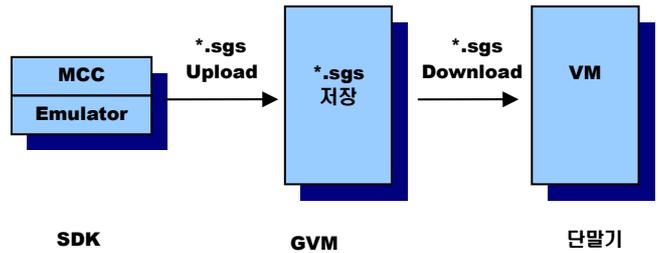
[그림 1] GVM SDK 의 구성

GVM 서버는 애플리케이션 다운로드를 수행하는 다운로드서버와 네트워크 클라이언트 애플리케이션의 연결을 수행하는 커넥션서버로 구성된다.

GVM 모듈은 이동통신 단말기에 탑재되는 가상기계와 관련된 라이브러리 모듈(Library Module)을 뜻하며 SVM(Swap Virtual Machine), MIL(Mobile Interface Library), MIDD(Mobile Interface Device Driver)로 구성된다.

2.1.2 GVM 서비스 구성

제작된 이미지와 사운드를 GVM SDK 의 이미지와 사운드 저작도구를 통해 GVM 규격으로 변환하여 모바일 C 소스파일(*.mc)에 포함시킨 후 컴파일하여 *.sgs 파일을 생성한다. 이렇게 작성된 모바일 응용프로그램은 에뮬레이터와 실제 단말기에서 테스트를 거친 후 서버에 업로드 시킨다. 사용자는 GVM 이 내장된 단말기로 모바일 응용프로그램을 다운로드 받아 실행하게 된다. [그림 2]는 이와 같은 과정을 도시한 것이다.



[그림 2] GVM 의 실행 모델

2.1.3 모바일 C

모바일 C 는 표준 C 언어를 기반으로 제한된 모바일 플랫폼에 맞추어 응용프로그램을 작성할 수 있는 언어이다. 표준 C 언어와 동일한 문법구조를 가지고 있으며 192 개의 문법이 있다. 최적화된 코드 생성으로 열악한 컴퓨팅 환경에 적합한 언어이다. 모바일 C 프로그램은 모바일 C 컴파일러를 통해 가상기계인 GVM에서 실행될 수 있는 코드(*.sgs)로 변환된다.

모바일 C 는 모바일 디바이스의 하드웨어 제약을 반영한 언어의 특성을 가지고 있으며, 따라서 부동소수점을 지원하지 않는다. 하지만 이미지, 사운드 등 멀티미디어 자료형을 지원하여, 모바일 디바이스에서 멀티미디어 프로그래밍을 하기에 적합하게 설계되었다.

2.2 결제 시스템

2.2.1 하드웨어 방식

스마트 카드와 같은 물리적 기억공간을 이동통신 단말기에 탑재하여, 온라인, 오프라인상에서 재화 구매에 대한 결제가 가능하도록 하는 결제 방식이다. 이동통신 단말기에 반드시 스마트 카드를 탑재해야 하는 단점이 있으며, 제 3 자로 인한 오남용을 막을 수 없다. 구현방식으로는 직불식, 후불식과 선불식 3 가지의 방식이 있다.

직불식 결제방식은 예금의 사용한도 내에서 물품의 구매나 기타 서비스 이용과 같은 상거래 발생 즉시 고객의 예금계좌에서 해당 금액이 차감되는 방식을 말하며[6], 후불식 결제방식은 우선 여러 가지의 상거래를 발생시키고 일정 기간 이후에 해당 거래의 사용 금액을 지급하는 방식이다[6]. 선불식 결제방식은 고객이 일정한 금액을 미리 지불하고, 재화를 구매할 때마다 구매 금액만큼 차감되는 방식이다.

2.2.2 소프트웨어 방식

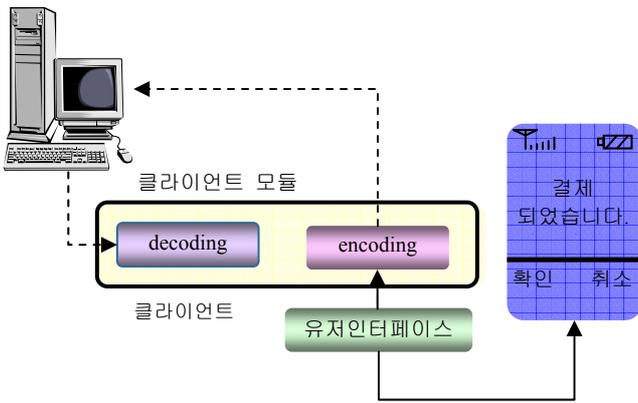
이동통신 단말기 자체에 전자지갑 소프트웨어를 저장함으로써 온라인과 오프라인에서도 활용할 수 있는 결제 방식이다. 재화 구매에 대한 결제 금액의 제한이 있으며, 구현 방식으로는 선불식과 후불식 2 가지가 있다.

선불식 결제방식은 일정한 금액을 미리 지불하고, 재화를 구매할 때마다 구매 금액만큼 차감 되는 방식이다. 후불식 우선 여러 가지의 상거래를 발생시키고

일정 기간 이후에 해당 거래의 사용 금액을 지급하는 방식이다.

2.2.3 서버 중심 시스템

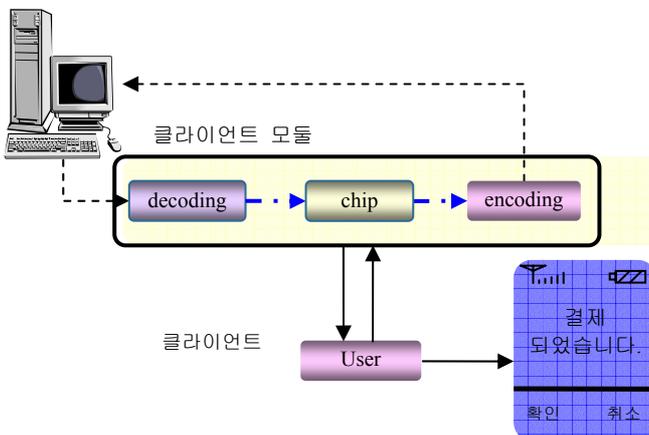
서버 중심 시스템은 이동통신 단말기(Client)와 서버가 지속적으로 연결된 상태에서, 이동통신 단말기의 인터페이스를 통하여 결제 정보가 서버로 전송되는 결제 시스템이다. 모든 정보는 서버가 관리하며, 이동통신 단말기는 유저 인터페이스 부분만을 처리한다. [그림 3]은 서버 중심의 결제 시스템을 도시한 것이다.



[그림 3] 서버 중심 결제 시스템

2.2.4 클라이언트 중심 시스템

클라이언트 중심 시스템은 이동통신 단말기(Client)에 탑재된 스마트 카드를 이용하여 결제를 처리하는 방식이다. 사용자 인터페이스로부터 입력 받은 결제 정보와 스마트 카드에 저장된 사용자 정보를 암호화하여 서버로 전송한다. 서버 중심 시스템과 달리 사용자의 개인 정보들은 스마트 카드에 탑재되어 있으며, 암호화된 결제정보만을 서버로 전송하는 결제 시스템이다. [그림 4]는 클라이언트 중심의 결제 시스템을 도시한 것이다.

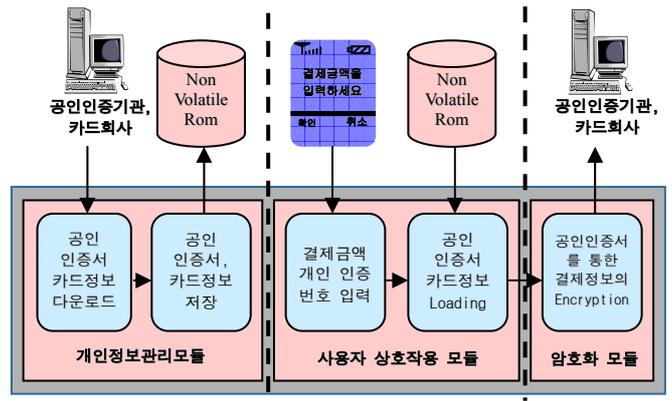


[그림 4] 클라이언트 중심 결제 시스템

3. 무선 결제 시스템의 설계

3.1 시스템 구성도

본 논문에서 제안하는 무선 결제 시스템은 소프트웨어 다운로드 솔루션을 기반으로 한 GVM 상에서 실행될 수 있는 모바일 C 기반의 무선 결제 시스템이다. 세부 모듈로는 개인 정보 관리 모듈, 사용자 상호작용 모듈, 암호화 모듈로 구성되어 있다. 본 논문에서 제안하는 무선 결제 시스템의 시스템 구성도는 [그림 5]와 같다.



[그림 5] 시스템 구성도

3.2 개인 정보 관리 모듈

개인 정보 관리 모듈은 무선 결제 시스템에 필요한 개인의 신용 정보와 결제 정보를 관리하는 모듈이다. 공인인증기관의 서버로부터 개인의 결제 정보를 암호화하기 위한 공인인증서를 다운로드하여 이동통신 단말기의 비 휘발성 메모리에 저장한다. 또한, 카드회사의 서버로부터 결제에 필요한 개인의 결제 정보를 다운로드하여 비 휘발성 메모리에 저장한다. 모바일 C의 NetConnect()함수를 적용함으로써 공인인증기관이나 카드회사의 서버에 접속이 가능하며, PutUserNV()함수를 적용하여 다운로드 받은 공인인증서와 개인의 결제 정보를 이동통신 단말기의 비 휘발성 메모리에 저장할 수 있다. 이동통신 단말기의 비 휘발성 메모리에 공인인증서와 개인의 결제 정보를 저장함으로써, 단 1회의 다운로드를 통하여 사용자가 폐기하기 전까지 영구적으로 사용이 가능하며, 추가 및 삭제가 가능하다.

3.3 사용자 상호 작용 모듈

사용자 상호 작용 모듈에서는 무선 결제 시스템의 사용자 인터페이스를 이용하여 결제 금액과 개인 인증 번호(비밀번호)들을 입력 받는다. 모바일 C의 StrInput()함수와 StrInput2()함수를 적용하여 결제에 필요한 정보들을 입력 받으며, GetUserNV()함수를 적용하여 비 휘발성 메모리에 저장되어 있는 공인인증서

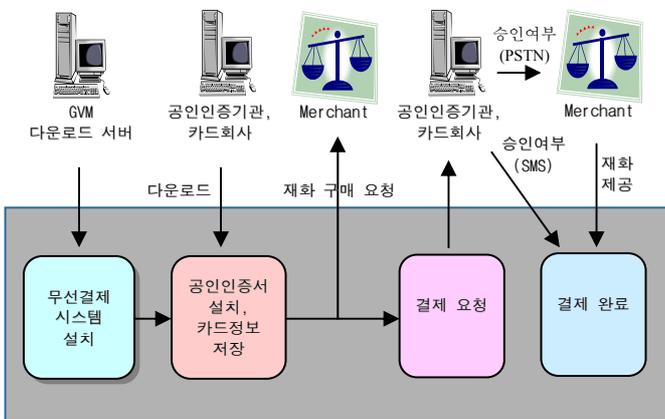
와 개인 결제 정보들을 읽어 들인다. 입력 받은 결제 금액과 개인 인증 번호들은 공인인증서와 개인 결제 정보와 함께 암호화 모듈로 전송된다.

3.4 암호화 모듈

암호화 모듈에서는 사용자 상호작용 모듈로부터 입력 받은 결제 금액, 개인 인증 번호, 공인인증서와 개인 결제 정보들을 공인인증서의 암호화 알고리즘을 적용하여 암호화한다. 공인인증서에서 제공하는 암호화 알고리즘은 대칭 키 암호 알고리즘, 공개키 알고리즘, 공개키 서명 알고리즘, 해시 알고리즘이 있다. 대칭 키 암호 알고리즘은 DES, Triple-DES, SEED 등을 지원하며, 공개키 암호 알고리즘은 RSA, ECC 등을 지원한다. 공개키 서명 알고리즘은 RSA, KCDSA 등을 지원하며, 해시 알고리즘은 SHA-1, HAS-160 등을 지원한다. 암호화 모듈을 통하여 암호화된 결제 정보들은 모바일 C 의 NetConnect()함수와 NetSend()함수를 적용하여 서버로 전송되며, 서버에서는 가맹점과 사용자에게 승인정보내역을 전송한다.

3.5 구현 모델

본 논문에서 제안하는 모바일 C 기반의 무선 결제 시스템은 GVM 이 탑재된 이동통신 단말기에서 실행되는 시스템이다. GVM 다운로드 서버로부터 모바일 C 기반의 무선 결제 시스템을 다운로드 받은 후, 무선 결제 시스템을 이용하여 공인인증서와 개인 결제 정보를 다운로드 받는다. 가맹점으로부터 재화를 구매할 경우, 무선 결제 시스템을 적용하여 서버에 승인을 요청하며, 서버에서는 가맹점과 무선 결제 시스템 이용자에게 승인여부를 전송한다. 가맹점에게는 PSTN 을 통하여 카드 단말기로 승인여부를 전송하며, 무선 결제 시스템 이용자에게는 SMS 를 통하여 승인여부를 전송한다. [그림 6]은 GVM 다운로드 서버로부터 무선 결제 시스템을 다운로드하여 결제가 완료되기까지의 과정을 도시한 것이다.



[그림 6] 구현 모델

4. 결론 및 향후 연구

본 논문에서 제안하는 무선 결제 시스템은 GVM 과 모바일 C 를 기반으로 설계되었으며, 개인 정보 관리 모듈, 사용자 상호 작용 모듈, 암호화 모듈로 구성되어 있다. 소프트웨어 다운로드 방식인 GVM 기반의 무선 결제 시스템이며, GVM 이 탑재된 이동통신 단말기에서 사용이 가능하다. 개인의 신용정보가 저장된 스마트 카드 기반의 무선 결제 시스템과는 달리 특정한 하나의 카드에 대해 구매를 받지 않으며, 개인의 결제 정보와 신용 정보의 보안을 위하여 공인인증기관의 공인인증서를 적용하였기 때문에, 이동통신 단말기 분실에 따른 제 3 자의 오남용을 방지할 수 있다. 또한, 본 논문에서 제안하는 무선 결제 시스템을 통하여 저장된 공인인증서와 개인 결제 정보들은, 단 1 회의 다운로드를 통하여 사용자가 직접 폐기 하기 전까지 지속적으로 사용할 수 있기 때문에, 영구적으로 사용할 수 있는 장점을 가진다. 결제 금액과 개인 결제 정보들은 무선 결제 시스템의 편리한 유저 인터페이스를 통하여 입력 받는다. 이동통신 단말기의 키 패드를 무선 결제 시스템의 유저 인터페이스로 사용하고 있기 때문에, 누구나 쉽게 사용할 수 있는 장점을 가지며, 다양한 종류의 이동통신 단말기에서도 적용이 가능하다.

본 논문에서 제안하는 무선 결제 시스템은 서버와 클라이언트로 나뉘어 설계되었으며, 클라이언트의 구조와 각각의 모듈에 관하여 설명하였다. 모바일 C 의 함수들을 적용하여 구현이 이루어져야 할 것이며, GVM 에뮬레이터와 이동통신 단말기에서의 테스트를 필요로 한다. 향후 무선 결제 시스템의 서버 역할을 수행할 수 있는 커넥션 서버(Connection Server)의 설계와 구현에 대해서도 지속적인 연구가 계속되어야 한다.

참고 문헌

- [1] Data Monitor, "Mobile Payment System", White Paper, 2001.
- [2] Krueger, M., "The Future of M-payment: Business Options and Policy Issues", e-POS Background Paper, No. 2, 2001.
- [3] Mobile Payment Forum, Mobile Payment Forum White Paper, 2002.
- [4] 김필진, GVM 과 Mobile C 를 이용한 모바일 콘텐츠의 개발, 동국대학교 컴퓨터공학과 석사학위 논문, 2002.
- [5] 남동근, 나승원, 오세만, "GVM 기반 모바일 GIS 를 위한 XML 파서의 설계 및 구현", 정보처리학회논문지, 제 9 권 2 호, pp. 2277~2280, 2002.
- [6] 성원, 인터넷 상거래를 위한 소액대금결제 시스템의 설계 및 구현, 충남대학교 컴퓨터공학과 석사학위 논문, 1999.
- [7] 정찬주, 이용, 이재일, "무선 PKI 에서 WIM, USIM 등의 스마트카드를 사용하지 않는 인증서 및 키 로밍", TELECOMMUNICATIONS REVIEW, pp. 495~503, 2003.