이동통신단말기를 이용한 안전한 온라인 금융거래 기법

정종근, 하추자, 김철원

Secure On-line Financial Business Method Using on Wireless Terminal

Jong-Geun Jeong, Chu-Ja Ha, Cheol-Won Kim
Dept of Computer Engineering, Honam University

요 약

이 논문에서는 이동통신단말기를 이용한 신용카드 및 온-라인 금융거래에 관한 방법을 제안한다. 제안한 방법은 먼저, 신용카드 회원이 신용카드사 거래승인시스템으로부터 보안코드를 이동통신단말기로 수신 받는 보안코드수신단계, 보안코드를 가맹점의 인증 단말기에 입력하는 단계, 입력된 보안코드의 일치여부를 비교하는 단계 및 최종 승인단계의 과정으로 구성된다.

I. 서 론

일반적으로 신용카드 승인 시스템은 카드 이용자가 소정의 물품에 대한 금액을 지불하기 위해 신용카드를 제시하게 되면 각 가맹점에서는 신용카드회사에 신용카드의 승인여부를 인증단말기를 통해 요청하게 된다. 신용카드회사는 가맹점의 신용카드 인증단말기로부터 전송되어온 신용카드 이용자의 거래 상태 및 신용상태를 조회한 후 거래정지나 기타 불승인 내역이 없으면, 신용카드 가맹점의 인증 단말기에 카드 이용자의 거래 내역에 대한 승인결과를 통보하고, 다음으로 신용카드 가맹점의 단말기는 신용거래에 대한 매출전표를 출력하고, 마지막으로 카드 이용자는 본인에 거래한 매출전표에 서명을 하는 단계로 이루어진다. 그림 1은 일반적인 전화망과 패킷망을 이용한 신용카드 거래 승인시스템의 구성도로서, 신용카드 이용자, 신용카드의 가맹점 및 신용카드 거래 승인시스템과 신용카드 가맹점과 신용카드 거래 승인시스템을 통신매체로 연결하는 VAN사로 구성된다. 그림1과 같이 구성된 시스템에서 신용카드를 이용하려면, 먼저 신용카드 소지자가 소정의 물품이나 용역을 구입하거나 이용한 대가로서 대금을 결재하기 위해 신용카드 가맹점에 자신의 신용카드를 제시하며 결재요구를 하면, 신용카드 가맹점은 신용카드 소지자의 신용카드에 기록되어 있는 이용자 정보와 거래내역 및 금액을 신용카드 가맹점에 설치되어 있는 신용카드 거래 승인 단말기를 통해 거래내역 및 가맹점 정보를 조합하여 거래 승인요구 전문을 작성하여 유무선 통신망을 통해 신용카드사에 승인을 요청한다. 이때, 신용카드 가맹점으로부터 발생한 거래 승인요구 전문(사용자 정보, 거래내역, 가맹점 정보의 조합)은 유무선 통신망을 통해 VAN사의 중계시스템으로 전송된다. 이때 신용카드 거래 승인 단말기에는 특정 VAN사의 중계시스템으로만 정보를 전송하게 하는 장치가 내장되어 있기 때문에, 특정 신용 카드 거래 승인 단말기에서 발생한 승인 요구는 특정 VAN사의 중계시스템으로만 전송된다. 거래 승인 요구 전문을 수신한 VAN사의 중계 시스템은 거래 승인 요구 전문내의 사용자 정보에 수록된 신용카드사 정보를 판독하여 해당 신용카드사의 거래 승인시스템으로 승인요구와 관련된 자료의 조합을 전송하는데, VAN사의 중계시스템과 해당 신용카드사의 거래시스템은 전용 패킷망으로 연결되어 있다.

거래 승인 요구를 수신 받은 신용카드사의 거래 승인시스템은 거래 승인 요구내역에 포함된 사용자 정보, 거래내역, 가맹점 정보를 각각 자사의 회원자료 또는 가맹점 자료와 비교하여 사용자와 가맹점 양자가 거래 구성원으로서 결격사유 및 양자간에 거래가 타당한가를 검사한다. 이어서 신용카드사는 거래 승인요구에 대한 결과를 패킷망을 통해 거래 승인요구를 중계한 VAN사로 회송한다. 신용카드사는 VAN사로부터 거래 승인 요구를 받을 때 중계 VAN사와 관련된 정보를 함께 수신 받아 저장하며, 거래 승인 결과를 거래 승인 요구 중계 내역에 수록된 VAN사의 중계시스템으로 회송한다. 거래 승인 결과를 회송 받은 VAN사의 중계시스템은 거래 승인 결과 내역에 포함된 가맹점 정보를 판독하여 전화망을 통해 거래 승인 요구가 최초로 발생된 가맹점에 거래 승인 결과를 회송한다.

II. 제안된 신용카드 및 금융거래 승인 방법

본 연구에서는 기존의 신용카드 분실시 또는 위조시 발생되는 문제점을 해결하기 위한 방법으로서, 신용카드 이용자가 물품대금 또는 기타 용역의 대가를 지불하기 위해 신용카드 가맹점에 결재 승인을 요청할 때 신용카드 소유주의 이동통신단말기에 합법적인 신용카드 소유주인지를 확인하는 보안코드를 미리 전송하여 신용카드 결재 승인시 이를 확인할 수 있게 하여 안전한 신용카드 거래를 위한 이동통

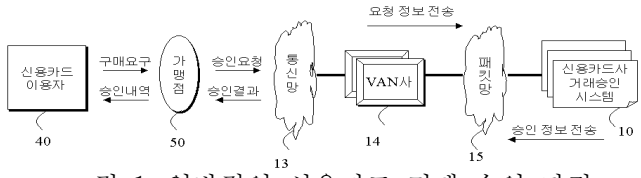

그림 1. 일반적인 신용카드 거래 승인 과정

신단말기를 이용한 신용카드 및 온-라인 금융거래 방법을 제공하고자 한다.

또한 금융거래 승인단계를 다음과 같이 구성할 수 도 있다. 먼저, 소정의 약정 절차를 밟아 금융거래 승인서비스의 이용 회원이 된 후 신용카드사 거래승인시스템으로부터 보안코드를 이동통신단말기로 수신 받는다. 다음으로 신용카드 가맹점의 인증요청이 있을 경우 신용카드사에서 전송된 보안코드 가맹점의 인증 단말기로부터 출력한다. 마지막으로 신용카드 이용자가 제시한 보안코드와 인증 단말기에서 출력된 보안코드의 일치 여부를 확인하여 보안코드가 일치할 경우에만 최종 거래 승인을 한다.

Ⅲ. 신용카드 및 금융거래 승인 시스템의 구성

그림 2에서 보안코드는 안전한 신용카드 거래를 위해 신용카드 비밀번호 이외에 신용카드 거래승인시스템의 보안코드 발생 및 관리모듈에서 발생시키는 코드로, 이 때 발생된 보안코드는 신용카드 소지자의 이동통신단말기에 전송되고, 동시에 신용카드사 회원데이터베이스에 저장된다. 이 때, 신용카드 이용자의 이동통신단말기 번호, 이동통신서비스회사 등의 정보는 필수적으로 신용카드 회사의 회원 데이터 베이스에 저장되어 있어야 한다. 보안코드를 이용한 신용카드 거래시, 신용카드 이용자는 가맹점에 보안코드를 먼저 제시해야 하며, 보안코드는 가맹점의 인증 단말기를 통해 거래승인시스템으로 전송되며, 거래승인시스템은 전송된 보안코드와 신용카드 회사의 회원 데이터베이스에 저장된 회원의 보안코드를 비교한 후 거래 승인을 하게된다. 보안코드 갱신은 주기적 또는 수시로 하거나, 신용카드 거래 직후 다음 거래를 위해 갱신될 수 있다.

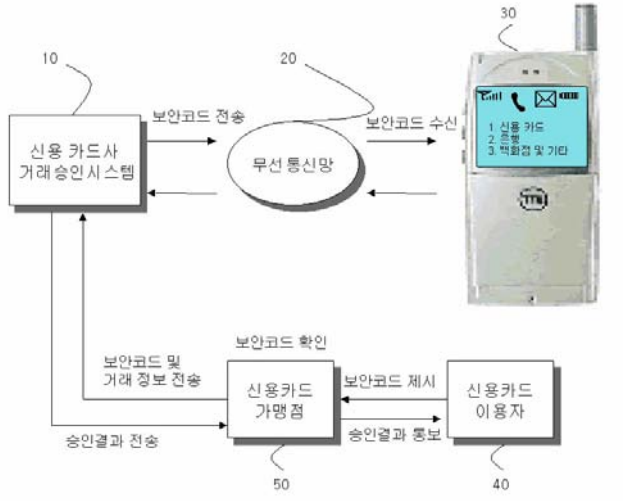

그림 2. 이동통신단말기를 이용한 신용카드 및 온-라인 금융거래의 개략적인 구성

그림 3은 보안코드를 수신할 수 있는 이동통신단말기 내부의 블록구성도 이다. 신용카드사 거래승인시스템에서, 암호화를 거친 후 무선통신망을 통해 전송된 보안코드를 수신하는 수신부와, 이동통신단말기의 데이터를 전송하는 송신부와, 베이스밴드 처리부와, 디스플레이부, A/D 변환기, 단말기 키 입력부, 제어부, 보안처리부, 응용프로그램(보안수첩), 메모리부로 구성된다.

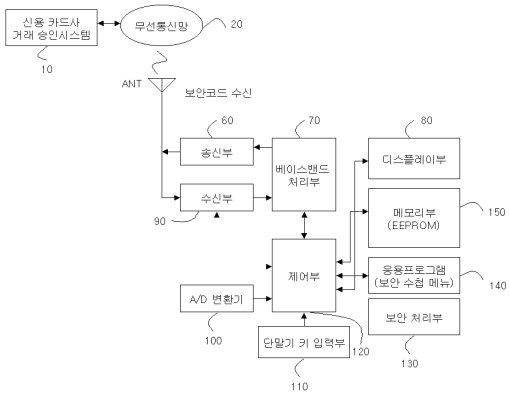

그림 3 이동 통신 단말기 내부의 구성도

수신부는 무선통신망과 안테나에 유기되는 신호를 동조하여 일정 주파수 대역의 RF 신호를 검출하여 증폭하는 증폭부와 복조부로 구성되어 있고, 베이스밴드처리부는 송수신되는 데이터에 대해 인터리빙(Interleaving)과 블록코딩(Block Coding) 및 컨볼루션 코딩(Convolution Coding)을 실행하도록 구성되어 있고, 제어부는 수신된 보안코드를 이후에 설명할 메모리부에 저장하도록 구성되어 있고, 응용프로그램 내의 보안수첩은 신용카드 이용자가 단말기 키조작을 통해 메모리부에 저장된 보안코드를 디스플레이부를 통해 확인할 수 있도록 구성되어 있고, 보안 처리부는 암호화된 채 수신된 보안 코드를 처리하거나 보안수첩 기능에 대한 보안처리를 하도록 구성되어 있고, 메모리부는 수신부로 수신된 보안코드를 저장할 수 있도록 EEPROM을 포함하여 보안코드를 저장하는 영역을 할당하게 된다.

그림 3에서 보안수첩이란, 보안코드를 관리하기 위한 이동 통신 단말기 내의 응용프로그램으로서 보안수첩을 이용하면, 신용카드사별, 은행별, 증권회사별, 백화점별, 기타 등으로 분류하여 보안코드를 관리할 수 있다. 보안수첩 서비스를 이용하려면 신용카드사 또는 은행 등에 서비스를 신청해야 하는데, 서비스 신청 항목에는 은행 및 신용카드사의 기존 회원 가입양식에 이동통신단말기 번호, 이동 통신단말기 전화번호 등이 필수적으로 포함되어야 한다.

보안코드를 전송하기 위한 신용카드사 거래승인시스템은 그림4에 도시된 바와 같이 신용카드 회원데이터베이스를 포함하여 기존의 신용카드 거래승인 과정의 전반적 모듈에 이 발명에 의한 보안코드 서비스 모듈이 추가하여 구성된다. 그리고 보안코드 서비스모듈은 보안코드 발생 및 관리 모

듈, 암호화 모듈, 무선통신망 접근 모듈로 구성된다.

보안코드 서비스모듈에서 보안코드 서비스 이용을 약정한 회원에 한정하며, 신용카드사 거래승인시스템은 보안코드 발생 및 관리 모듈을 제어하여 보안코드를 발생시킨 후 암호화 모듈로 전송하고, 암호화 모듈은 발생된 보안코드를 암호화 한 후 카드사 회원데이터베이스에 저장하고, 이 때 발생된 코드와 동일한 보안코드를 무선통신망 접근모듈에 전송하고, 무선통신망 접근모듈은 암호화된 보안코드를 무선통신망을 통해 신용카드 회원의 이동통신단말기에 전송한다.
보안코드 관리는 기존 신용카드사의 회원관리 방법에 위해 관리하거나, 정보가 위조 또는 유출되는 것을 방지하기 위해 에서 설명한 암호화 통신을 수행할 수 있으며, 이를 위해 암호화 모듈에서는 단일키 암호화방식(예:DES, RC5, SEED) 또는 공개키 암호화(예: RSA)방식 등을 이용하여 암호화를 할 수 있다.

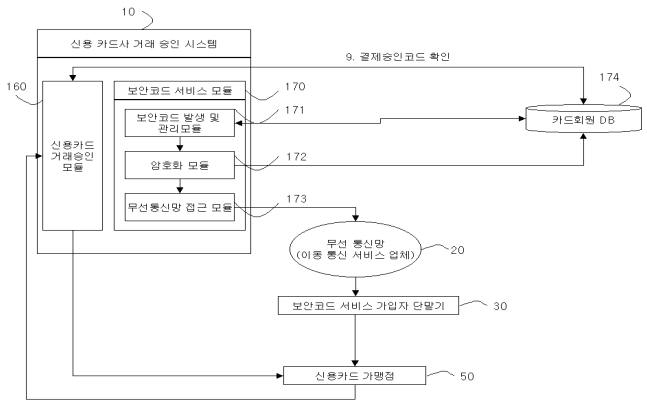

그림 4 보안코드 서비스를 위한 신용카드사 승인 시스템 구성

단일키 암호화 알고리즘을 통한 인증은 온라인 상에서 인증키를 상호 공유하기 위해 전송시 인증키가 공격자로부터 다시 사용될 수 있는 것을 방지하기 위해, 챌린지 리스펀스 스킴(Challenge Responce Scheme) 등의 방법을 이용할 수 있고, 공개키 기반 구조의 인증 방식은 인증기관에 자신의 공개키를 보내어 인증을 요청하는 방식이다.
정한다.

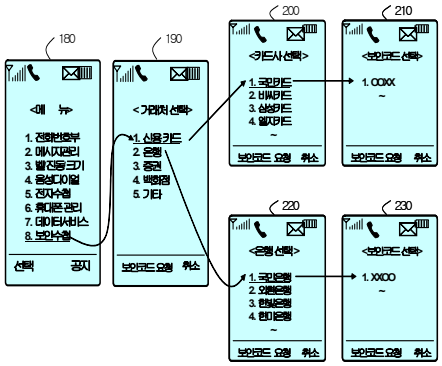

그림 5 이동통신단말기에서 보안코드 확인 과정

위의 방법을 이용하려면 신용카드사의 기존 회원은 신용카드사에 방문하거나 인터넷 사이트에 접속하여 이동통신가입회사, 이동 통신단말기번호, 이동통신 전화번호 등의 추가 항목을 작성하여 제시하고, 본 서비스이용 약정, 즉 일정요금 또는 이에 상응한 대가를 지불할 것 등에 대한 소정의 약정서에 약정하거나, 또는 신규회원의 경우 신용카드 가입 양식에 추가 항목을 작성한 후 서비스 이용 약정을 하게되면 신용카드사는 작성된 정보를 신용카드사 거래 승인시스템의 신용카드 회원데이터베이스에 등록하게 된다.

그림 5는 보안코드 확인 과정의 화면을 보여주고 있다., 이전의 일반적인 이동통신단말기의 메뉴화면에 보안수첩이 추가된 메뉴화면에서 "8. 보안수첩"을 선택하면, 거래처 선택 메뉴화면이 나타나며, 거래처 선택 메뉴에서 "1. 신용카드"를 선택하고, 카드사 선택 메뉴에서 "1.국민카드"를 선택하면 최종적으로 보안코드 선택화면에서 보안코드 "1.OOXX"를 선택 할 수 있다. 또한 거래처 선택 화면에서 "2. 은행"을 선택하면 은행선택화면이 나타나고, "1.국민은행"을 선택하면, 보안코드 선택화면에서 "1.XXOO"를 선택할 수 있다.

그림 6에 나타난 바와 같이 미리 소정의 약정 절차를 밟아 서비스의 이용회원이 되어 신용카드사 거래승인시스템으로부터 보안코드를 수신받아, 신용카드 이용자가 신용카드 가맹점)에서 물품 또는 용역의 대가로 신용카드 거래를 요구하면, 가맹점)은 이용자로부터 보안코드를 입력받기 위해 신용카드 이용자의 이동통신단말기에 비밀번호를 입력하고, 신용카드, 은행, 증권, 백화점, 기타 등의 거래처를 선택하여, 거래승인시스템에서 송신되어온 보안코드를 확인한 후, 보안코드, 거래일시, 거래내역, 할부내역 등의 정보를 취합한 후 가맹점의 인증 단말기를 통해 신용카드사 거래 승인 시스템에 전송하게 되고, 거래승인시스템은 보안코드가 일치하는지의 여부를 확인한 후, 이를 토대로 최종승인 결과를 가맹점에 전송하여 승인이 완료되며, 매출전표를 작성하게 된다. 또한, 승인이 되지 않은 경우에는 승인거부사유를 전송하게 된다. 거래처선택 후에 선택된 신용카드나 은행 등의 보안코드에 접근할 경우 한 번 더 비밀번호를 입력받을 수 있도록 하여 이동통신단말기의 분실에 대해 보안코드의 불법사용을 한 번 더 방지할 수 있도록 할 수도 있다.

보안코드 선택 화면에서 보안코드는 한 개 또는 다중으로 수신이 가능하도록 구성되며, 보안코드는 신용카드 승인을 위한 용도 이외에 인터넷 뱅킹, 폰뱅킹, 홈뱅킹, 전자상거래, 모바일뱅킹, 인터넷 금융백화점 또는 전자화폐, 사이버카드 또는 자동화기기(CD/ATM 기기) 거래 등과 같이 보안코드가 필요한 거래에 이용될 수 있다. 또한 이동통신단말기 이외에 핸드폰, PDA, IMT-2000 서비스를 위한 단말기 등을 통해서도 제안한 서비스를 이용할 수 있다.

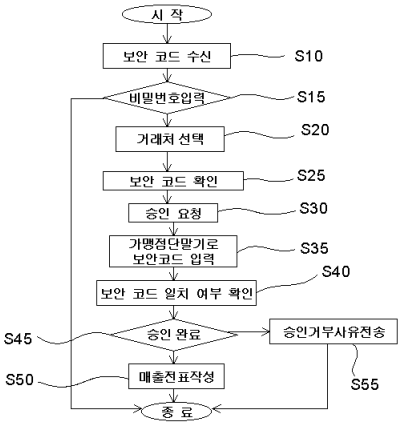

그림 6 이동통신단말기를 이용한 신용카드 및 온-라인 금융거래 방법의 동작

Ⅳ. 결론

본 논문에서는 이동통신단말기의 보안코드를 이용한 신용카드 거래승인방법을 제안하였다. 거래승인과정에서 고객이 자신의 이동통신단말기의 보안코드를 제시하여 직접 참여함으로써 신용카드 소지자가 신용카드를 분실한 경우 또는 불법 신용카드 복제 이용 등이 발생하여도 타인은 보안코드를 알 수 없기 때문에 신용카드를 사용할 수 없게 된다. 즉, 신용카드 분실시 발생되는 여러 문제점을 해결함으로써 신용사회 정착 및 보다 건실한 신용카드 거래 문화를 창출 할 수 있고, 신용카드 범죄 예방에 많은 효과를 발휘할 수 있다.

참고문헌

[1] TurePosition Co, Ltd, Time difference of arrival technology for locating narrowband cellular signals.

[2] 이석준, 원유재, “ 무선인터넷 보안 기술의 동향과 향후 전망”, 주간기술동향, 963호, 2000

[3] M. Hanaoka, S. Kaneshige, N. Hagiya, K. Ohkubo, K. Yakura and Y. Kikuta, "Network System," NTT DoCoMo Technical Journal, vol. 1, no. , pp. 14-!9, oct. 1999

[4]Mobile Information Device Profile(JSR-37): Specification(JCP Public Draft), Java 2 Platform Micro Edition, Draft 0.9, Sun Microsystems, MAy 5, 2000

[5] WAP WTLS Spec. version 1.2, http://www.wapforum.org