(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년07월14일
(11) 등록번호 10-0968941
(24) 등록일자 2010년07월01일

(51) Int. Cl.
G06Q 20/00 (2006.01)
(21) 출원번호 10-2007-0028792
(22) 출원일자 2007년03월23일
심사청구일자 2007년03월23일
(65) 공개번호 10-2008-0086733
(43) 공개일자 2008년09월26일
(56) 선행기술조사문헌
KR100412986 B1*
KR1020070016893 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
(주)에이티솔루션
서울특별시 마포구 상암동 택지개발지구 E3-2 DMC산학협력연구센터 12층 1204호
(72) 발명자
김덕상
서울 강남구 역삼동 682-1 효신빌라 106
(74) 대리인
유경열, 특허법인 신지

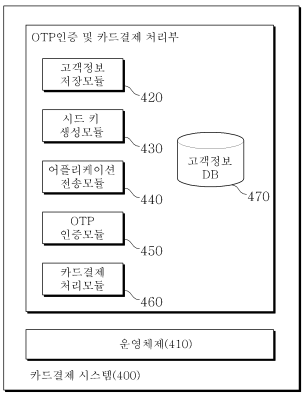
전체 청구항 수 : 총 3 항 심사관 : 두소영

(54) ＯＴＰ를 이용한 금융거래 시스템

(57) 요 약

본 발명은 일회용 비밀번호(One-Time Password)를 이용하여 금융거래를 수행하는 시스템에 관한 것으로, OTP(One-Time Password) 생성을 위한 시드(SEED)키를 카드정보 혹은 계좌정보와 같은 금융거래정보에 기초하여 생성하기 위한 시드키 생성모듈과; 상기 시드키를 고객 단말기측으로 전송하기 위한 어플리케이션 전송모듈과; 고객의 금융거래정보와 시드키 정보를 고객정보 DB에 저장하기 위한 고객정보 저장모듈과; 고객 단말기에서 생성된 OTP와 고객식별정보를 네트워크를 통해 전송받아 해당 OTP를 인증하기 위한 OTP 인증모듈과; 상기 OTP 인증결과에 따라 전송받은 고객식별정보를 가지는 고객의 금융거래정보에 기초하여 금융결제 승인처리하는 금융결제 처리모듈;을 포함함을 특징으로 한다.

대 표 도 - 도3



특허청구의 범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

고객의 금융거래정보와 그 금융거래정보에 기초하여 생성된 시드(SEED)키 정보 및 이벤트 인덱스 정보를 고객정보 DB에 저장하기 위한 고객정보 저장모듈과;

고객의 금융거래정보에 기초하여 OTP 생성을 위한 시드키를 생성하는 시드키 생성모듈과;

상기 시드키를 고객 단말기측으로 전송하기 위한 어플리케이션 전송모듈과;

고객 단말기에서 생성된 OTP를 고객식별정보와 함께 네트워크를 통해 전송받아 인증하되, 그 전송받은 OTP에 부가된 이벤트 인덱스 정보를 포함하는 하나의 완전한 이벤트 인덱스 정보를 순차적으로 생성해 가면서, 순차적으로 생성되는 각 이벤트 인덱스 정보와 금융거래 고객의 시드키 정보를 해시함수 인자로 설정하여 해쉬함수값을 계산하고, 계산된 해쉬함수값과 전송된 OTP에 포함된 해쉬함수값을 비교하는 방식으로 OTP 인증하는 OTP 인증모듈과;

OTP가 유효한 것으로 인증되면 그때 이용된 이벤트 인덱스 정보를 저장된 이벤트 인덱스 정보와 비교하여 OTP 생성 어플리케이션의 복제 여부를 판단하는 OTP 생성 어플리케이션 복제 판단모듈과;

상기 OTP 인증결과에 따라 네트워크를 통해 전송받은 고객식별정보를 가지는 고객의 금융거래정보에 기초하여 금융결제 승인처리하는 금융결제 처리모듈;을 포함함을 특징으로 하는 OTP를 이용한 금융거래 시스템.

청구항 5

청구항 4에 있어서, 상기 금융결제 처리모듈은 카드정보 혹은 계좌정보중 하나의 금융거래정보를 이용하여 금융결제 승인처리함을 특징으로 하는 OTP를 이용한 금융거래 시스템.

청구항 6

청구항 4에 있어서, 상기 어플리케이션 전송모듈은 OTP 생성어플리케이션 데이터를 고객 단말기측으로 추가 전송함을 특징으로 하는 OTP를 이용한 금융거래 시스템.

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0005] 본 발명은 금융거래 시스템에 관한 것으로, 특히 일회용 비밀번호(One-Time Password)를 이용하여 금융거래를 수행하는 시스템에 관한 것이다.

[0006] 금융거래 시스템으로서 일반화되어 있는 것이 바로 카드 결제 시스템과 계좌이체 및 조회업무를 담당하는 폰 뱅킹 혹은 인터넷 뱅킹 시스템이다. 카드결제는 주로 오프라인상에서 많이 이용되었으나, 최근에 전자상거래가 활성화되면서 온라인에서도 수많은 카드결제가 이루어지고 있다. 아울러 폰 뱅킹 및 인터넷 뱅킹 역시 그 이용자 수가 폭발적으로 증가하고 있다.

[0007] 일 예로 온라인상에서의 카드결제 처리과정을 살펴보면, 카드소지자는 쇼핑몰을 통해 물품을 구매하고 그 결제 수단으로서 카드정보, 보다 구체적으로는 카드명, 카드번호, 유효기간, CVC와 같은 정보를 입력하여 승인요청한다. 이러한 카드정보는 밴(VAN)사를 통해 카드사측으로 전송되고, 카드사측에서는 전송된 카드정보를 조회하여 신용승인 처리함으로서 카드결제 프로세스가 종료된다. 보다 강화된 방안으로 카드 소지자의 인증 혹은 비밀번호의 입력 등이 추가되기도 하나 이에 대한 부연 설명은 편의상 생략하기로 한다.

[0008] 설명한 바와 같이 온라인을 통한 카드결제 과정에서는 카드번호, CVC, 카드명 등의 정보가 통신망을 통해 직접적으로 전송되는 관계로 고도화된 해킹기술 등에 의해 악의의 제3자에게 노출될 소지가 많다.

[0009] 더 나아가 기존의 온라인을 통한 카드결제 과정에서는 카드번호, 카드명, CVC 정보 등을 입력하는 방식이기 때문에, 카드결제 과정에서 너무 많은 정보의 입력이 수반되는 관계로 그만큼 사용이 번거롭다는 단점이 있다.

[0010] 이러한 문제 및 번거로움은 폰 뱅킹 혹은 인터넷 뱅킹과 같은 금융거래 시스템에서 공히 나타나는 문제이기도 하다.

발명이 이루고자 하는 기술적 과제

[0011] 이에 본 발명의 목적은 상술한 문제점을 해결하기 위하여 안출된 것으로서, 계좌정보 혹은 카드정보와 같은 금융거래정보의 온라인 전송 없이 단순히 OTP를 이용하여 금융거래가 정상적으로 이루어질 수 있는 OTP를 이용한 금융거래 시스템을 제공함에 있으며,

[0012] 더 나아가 금융거래를 수행함에 있어 입력정보를 최소화하여 사용상의 편의를 제공코자 한 OTP를 이용한 금융거래 시스템을 제공함에 있다.

발명의 구성 및 작용

[0013] 상기 목적을 달성하기 위한 본 발명의 일실시예에 따른 OTP(One-Time Password)를 이용한 금융거래 시스템은,

[0014] 고객의 금융거래정보와 그 금융거래정보에 기초하여 생성된 시드(SEED)키 정보를 고객정보 DB에 저장하기 위한 고객정보 저장모듈과;

[0015] 고객 단말기에서 생성된 OTP를 고객식별정보와 함께 네트워크를 통해 전송받아 그 OTP(One-Time Password)를 인증하기 위한 OTP 인증모듈과;

[0016] 상기 OTP 인증결과에 따라 전송받은 고객식별정보를 가지는 고객의 금융거래정보에 기초하여 금융결제 승인처리하는 금융결제 처리모듈;을 포함함을 특징으로 한다.

[0017] 상술한 구성에 따르면, 본 발명은 카드정보 혹은 계좌정보와 같은 금융거래정보에 기초하여 시드키를 생성하여 고객 단말기에 제공하고, 고객 단말기에서는 상기 시드키를 이용하여 생성한 OTP를 고객식별정보와 함께 금융거래 시스템으로 전송함으로서, 금융 거래 시스템에서는 해당 고객에게 발급된 시드키를 이용하여 OTP를 생성하고 이를 전송받은 OTP와 비교하여 일치할 경우에만 정상적으로 금융결제 승인처리하여 주기 때문에, 결국 통신망을 통해 금융거래정보가 전송됨으로서 발생할 수 있는 정보의 노출을 사전 차단할 수 있는 효과를 가지게 되는 것이다.

[0018] 더 나아가 본 발명의 또 다른 실시예에 따른 OTP를 이용한 금융거래 시스템은,

[0019] 고객의 금융거래정보와 그 금융거래정보에 기초하여 생성된 시드키 정보를 고객정보 DB에 저장하기 위한 고객정보 저장모듈과;

[0020] 고객 단말기에서 생성된 OTP와 고객식별정보 및 금융결제를 위한 비밀번호를 네트워크를 통해 전송받아 해당 OTP를 인증하기 위한 OTP 인증모듈과;

[0021] 상기 OTP 인증결과에 따라 전송받은 고객식별정보를 가지는 고객의 금융거래정보와 상기 비밀번호를 이용하여 금융결제 승인처리하는 금융결제 처리모듈;을 포함함을 특징으로 한다.

[0022] 이러한 시스템 역시 통신망을 통해 OTP와 고객식별정보를 전송하여 금융거래 고객을 식별하고, 비밀번호를 이용하여 해당 고객의 진위 여부를 판단함으로서, 금융거래정보를 전송하는 종전 시스템들에 비해 안전하게 금융거래정보를 보호할 수 있는 실익이 있다.

[0023] 이하 본 발명의 바람직한 실시예들을 첨부 도면을 참조하여 상세히 설명하기로 한다. 본 발명을 설명함에 있어 관련된 공지 기능 혹은 구성에 대한 상세한 설명은 생략하기로 한다. 예를 들면, 카드결제를 위해 필요한 카드 리더기, 카드 리더 방식, 밴(VAN)사 등에 대한 설명은 생략하기로 한다. 더 나아가 하기에서의 카드라 함은 MS 타입의 신용카드는 물론 체크카드와 같이 선불 및 후불식 결제카드 모두를 포함하는 것으로 가정하기로 한다. 그리고 하기에서는 카드 결제 시스템을 가정하여 본 발명의 실시예에 따른 금융거래 시스템의 구성 및 동작을 부연 설명하기로 한다.

[0024] 도 1은 본 발명의 일실시예에 따른 금융거래 시스템의 하나인 카드 결제 시스템의 주변 구성도를 예시한 것으로, 본 발명의 실시예에 따른 카드결제 시스템(400)은 예를 들어 쇼핑몰 서버(300)와 연결될 수 있다. 쇼핑몰 서버(300)는 온라인상에서 각종 물품을 판매하는 판매자 역할을 수행하며, 물품 구매자가 카드결제를 선택한 경우 결제에 필요한 정보를 전송받아 카드결제 시스템(400)으로 전송하는 역할을 한다.

[0025] 한편 카드 소지자인 구매자들은 자신의 컴퓨터(200)를 통해 온라인상에서 물품을 구매하고 그 결제 수단으로 선불식 혹은 후불식 카드 정보에 기초하여 만들어진 OTP를 이용하여 결제 수행한다. 도 1에 도시한 휴대폰은 물품 구매자, 즉 카드 소유자가 이용하는 무선 단말기(이하 고객 단말기라 함)(100)로서 OTP 생성에 이용된다.

[0026] 이하 고객 단말기(100)에 설치되어 실행되는 OTP 생성 어플리케이션과 OTP를 이용한 카드 결제 시스템의 구성을 도 2와 도 3을 참조하여 보다 구체적으로 설명하기로 한다.

[0027] 도 2는 본 발명의 실시예에 따라 고객 단말기(100)에 설치되는 OTP 생성 어플리케이션(120)의 프로그램 모듈 구성도를 예시한 것이다. OTP 생성 어플리케이션(120)은 예를 들어 MS 방식의 신용카드를 발급받은 자가 온라인 혹은 오프라인상에서 OTP 생성을 위한 시드(SEED)키의 발급을 요청한 경우에 카드결제 시스템(400)으로부터 발급되는 응용 프로그램이다.

[0028] 참고적으로 카드결제 시스템(400)은 카드를 발급받은 자 온라인상에서 혹은 오프라인상에서 관리자가 시드키의 발급을 요청하면 해당 카드정보(카드번호, 유효기간, CVC, 카드명)를 정해진 내부 알고리즘을 이용하여 시드키를 생성하고, 이러한 시드키가 포함된 OTP 생성 어플리케이션 데이터를 해당 고객 단말기로 다운로드하여 준다. 물론 시드키 발급 이전에 개인인증이 요구될 것이며, 해당 어플리케이션은 이동 통신망을 통해 다운로드될 것이다. 그리고 시드키와 OTP 생성 어플리케이션은 하나 이상의 서로 다른 주체에 의해 각각 생성되어 서로 다른 시점에 다운로드될 수도 있을 것이다.

[0029] 도 2를 참조하여 상술한 OTP 생성 어플리케이션(120)에 대해 부연 설명하면, 우선 유저 인터페이스 모듈(140)은 주민등록번호와 같은 고객식별정보, 카드 비밀번호와 같은 사용자 데이터를 입력받거나 OTP와 같은 표시 데이터를 출력하기 위한 유저 인터페이스 화면을 제공하여 준다.

[0030] 이벤트 인덱스 갱신모듈(150)은 사용자 로그인시마다, 비밀번호 갱신요구시마다 이벤트 인덱스 정보를 갱신하여 SEED 저장부(130)에 저장한다. 상기 이벤트 인덱스 정보는 최초 사용자 로그인시에 "0"으로 초기화된후 이벤트 발생시마다 하나씩 증가하는 일련번호의 값을 가진다. 그리고 정해진 값에 도달하면 다시 "0"으로 초기화된다.

[0031] OTP 생성모듈(160)은 갱신 저장된 이벤트 인덱스 정보와 저장된 시드키 정보를 해쉬함수 인자로 설정한후 일방향 해쉬함수(f(x))에 의거하여 해쉬함수값을 계산한다. 그리고 계산된 해쉬함수값에 이벤트 인덱스 정보(의 일부)를 조합하여 완전한 하나의 OTP를 생성하고 이를 유저 인터페이스 모듈(140)을 통해 표시 출력한다.

[0032] 이상에서 설명한 OTP 생성 어플리케이션(120)은 단말기 VM(Virtual Machine) 프레임워크상에서 구동 가능한 어플리케이션이다. 본 실시예에서는 이벤트 인덱스 정보와 시드키 정보를 해쉬함수 인자로 설정하여 OTP를 생성하

는 것으로 설명하였지만, 시드키를 이용하여 OTP를 생성하는 이미 공지된 알고리즘을 이용하여 본 발명을 실시할 수도 있을 것이다.

[0033] 이하 상술한 구성을 가지는 OTP 생성 어플리케이션(120)의 동작예를 설명하면,

[0034] 우선 카드를 발급받은 자(이하 카드 소유자라 함)는 카드사에서 지정하는 시스템(예를 들면 카드 결제 시스템)에 접속하여 OTP 생성을 위한 시드키의 발급을 요청한다. 시드키 발급요청을 받은 시스템, 예를 들면 카드 결제 시스템(400)은 카드 소유자의 고객식별정보(주민등록번호)와 발급받은 카드의 비밀번호를 요청한다. 이는 원 카드 소유자인지를 체크하기 위함이다. 만약 원 카드 소유자에 의한 발급요청이라면 카드 결제 시스템(400)은 카드 소유자에게 발급된 카드번호, CVC 정보, 카드명, 유효기간 정보에 기초하여 OTP 생성을 위한 시드키를 생성한다. 그리고 생성된 시드키를 OTP 생성 어플리케이션 데이터와 함께 혹은 시드키만을 카드 소유자의 고객 단말기로 전송하여 준다. 이에 카드 소유자의 고객 단말기에는 도 2에 도시한 바와 같은 구성을 가지는 어플리케이션(120)이 설치 완료된다. 참고적으로 시드키는 미리 정해진 알고리즘에 기초하여 생성될 수 있으며, 고객 단말기 정보는 시드키 발급시 혹은 저장된 고객 정보를 활용한다. 만약 카드 결제 시스템(200)으로부터 시드키만을 전송받는 경우라면 OTP 생성 어플리케이션은 다른 시스템, 예를 들면 통신사 서버 혹은 본 서비스를 이용하기 위해 링크 가능한 서버로부터 전송받아야 할 것이다.

[0035] 이하 고객 단말기에 설치된 OTP 생성 어플리케이션에 의해 OTP가 생성되는 과정을 설명하기로 한다. 하기설명에서 OTPGA(OTP Generation Application)는 OTP 생성 어플리케이션(120)을 나타내는 것으로 정의한다.

[0036] 우선 PC(200)를 통해 쇼핑몰 서버(300)에 접속하여 소정의 물품을 구매한 카드 소유자는 결제 수단으로 카드 결제를 선택한다. 이러한 카드 결제 선택에 따라 카드 소유자는 카드 정보의 전송을 요청받는다. 이에 카드 소유자는 자신의 단말기에 설치된 OTPGA를 실행한다. OTPGA가 실행되면, 우선 이벤트 인덱스 갱신모듈(150)은 최초 사용자 로그인에 따라 이벤트 인덱스 정보를 "0000"으로 초기화 갱신한다. 이벤트 인덱스 갱신모듈(150)은 이후의 이벤트 발생시마다 상기 이벤트 인덱스 정보를 0001, 0002,0003과 같이 하나씩 증가시켜 갱신한다.

[0037] 이벤트 발생에 따라 이벤트 인덱스 정보가 갱신되면 OTP 생성모듈(160)은 갱신된 이벤트 인덱스 정보와 저장된 시드키 정보를 해쉬함수 인자로 설정한후 일방향 해쉬함수에 의거하여 해쉬함수값을 계산한다. 그리고 OTP 생성모듈(160)은 갱신된 이벤트 인덱스 정보, 바람직하게는 이벤트 인덱스 정보의 일부 정보를 상기 계산된 해쉬함수값에 부가하여 하나의 완전한 OTP를 생성하고 이를 유저 인터페이스 모듈(140)을 통해 표시 출력한다. 본 발명의 실시예에서는 이벤트 인덱스 정보의 일련번호중 십단위 두 자리값을 OTP에 부가하는 것으로 가정한다. 이러한 가정하에 따라 최종적으로 생성 표시되는 OTP 정보의 산출근거를 예시하면 하기와 같다.

[0038] OTP = f(시드, 이벤트 인덱스 정보)*100 + ((이벤트 인덱스 정보) mod 100)

[0039] 상기 수식에서 f(x)는 OTP 생성을 위한 일방향 해쉬함수를 나타낸 것이다. 해쉬함수로서 MD4, MD5, SHA 등을 이용할 수 있으며, 해쉬함수에 인자로 넘기는 x값을 상기 수식에서와 같이 시드와 이벤트 인덱스 정보이다. 예를 들어 시드값은 "1qaz"이고, 이벤트 인덱스가 "1234", 해쉬함수의 결과가 "495724"라 하면,

[0040] OTP = f(1 qaz, 1234)*100 + (1234 mod 100) = 49572434가 된다. 즉, 최종적으로 표시 출력되는 OTP는 f(x)라는 해쉬함수에 의해 만들어진 결과값(해쉬함수값이라고 함)에 이벤트 인덱스 정보의 끝 두자리가 부가된 값이 되는 것이다.

[0041] 위와 같이 OTP가 생성 표시되면 단말기 사용자는 PC(200)를 통해 고객 단말기를 통해 얻어진 OTP 정보와 자신의 고객식별정보(예:주민등록번호 혹은 자신의 ID)를 쇼핑몰 서버(300)로 전송하여 준다. 이러한 정보들은 카드 결제 시스템(400)으로 전송되어 카드결제 처리를 위한 정보로 이용된다.

[0042] 한편 OTP 갱신요구와 같은 새로운 이벤트가 발생하면 이벤트 인덱스 갱신모듈(150)은 "0000"으로 갱신된 이벤트 인덱스 정보를 "0001"로 갱신한다. 이벤트 발생에 따라 이벤트 인덱스 정보가 갱신되면 OTP 생성모듈(160)은 이후 갱신된 이벤트 인덱스 정보와 저장된 시드키 정보를 해쉬함수 인자로 설정한후 일방향 해쉬함수에 의거하여 다시 해쉬 함수값을 계산한다. 그리고 그 값 끝자리에 갱신된 이벤트 인덱스 정보를 부가하여 새로운 OTP를 생성하여 유저 인터페이스 모듈(140)을 통해 표시 출력한다.

[0043] 만약 사용자로부터 OTPGA 종료 요청이 있으면 이벤트 인덱스 갱신모듈(150)은 현재의 이벤트 인덱스 정보를 SEED 저장부(130)에 저장하고 본 발명의 실시예에 따른 OTPGA를 종료한다. 마지막으로 갱신된 이벤트 인덱스 정보의 저장에 의해서, 추후 이벤트 발생시에는 그 저장된 차순위 값이 새로운 이벤트 인덱스 값으로 갱신된다.

[0044] 이하 상술한 OTPGA에 의해 생성된 OTP 정보를 이용하여 카드 결제 수행하는 카드 결제 시스템(400)에 대해 설명

하기로 한다.

[0045] 도 3은 본 발명의 일실시예에 따른 카드 결제 시스템(400)의 일부 구성도를 도시한 것이다.

[0046] 도 3을 참조하면, 고객정보 저장모듈(420)은 카드 발급 고객의 카드정보(카드번호, CVC, 유효기간, 카드명 등)와 시드키 정보를 고객정보 DB(470)에 저장한다. 즉, 고객정보 DB(470)에는 고객명, 고객식별정보, 카드정보, 시드키 정보 등이 저장된다.

[0047] 시드키 생성모듈(430)은 온라인을 통한 OTP 발급 요청 혹은 관리자 컴퓨터를 통한 OTP 발급요청이 있으면 입력 혹은 고객정보 DB(470)에 저장된 카드정보(금융거래정보)에 기초하여 OTP 생성을 위한 시드키를 생성한다. 생성된 시드키는 시드키 발급을 요청한 카드 소유자의 단말기로 전송됨은 물론 고객정보 저장모듈(420)에 의해 고객정보 DB(470)에 저장 관리된다.

[0048] 어플리케이션 전송모듈(440)은 상기 생성된 시드키와 OTP 생성 어플리케이션 데이터를 고객 단말기측으로 전송한다. 이때의 고객 단말기란 카드 소유자가 지정한 휴대용 단말기를 의미하는 것으로 가정하기로 한다. 참고적으로 OTP 생성 어플리케이션 데이터는 시스템 내부 메모리에 저장되거나 어플리케이션 전송모듈(440)내에 저장된다. 경우에 따라 어플리케이션 전송모듈(440)은 시드키만을 지정된 고객 단말기측으로 전송할 수도 있을 것이다.

[0049] 한편 OTP 인증모듈(450)은 고객 단말기에서 생성된 OTP와 고객식별정보를 네트워크를 통해 전송받아 전송받은 OTP를 인증한다. 이러한 OTP 인증모듈(450)은 고객 단말기측으로부터 전송된 OTP에 부가되어 있는 이벤트 인덱스 정보를 생성하기 위한 이벤트 인덱스 정보 생성모듈을 포함한다. 보다 구체적으로, 이벤트 인덱스 정보 생성모듈은 이벤트 인덱스 정보의 고속 서치와 OTP의 고속 인증을 위해서, 인증 요청된 OTP에 부가된 이벤트 인덱스 정보를 끝자리로 가지는 이벤트 인덱스 정보들을 생성하는 것이 바람직하다. 예를 들어 인증 요청된 OTP에 부가된 이벤트 인덱스 정보가 십단위 정보로서 "67"이라면 그 인덱스 정보를 가지는 이벤트 인덱스 정보, 즉 "3967", "4067", "4167",..과 같은 이벤트 인덱스 정보를 생성하여 주는 역할을 담당한다.

[0050] 더 나아가 OTP 인증모듈(450)은 시드키 생성모듈(430)에서 생성된 시드정보와 상기 이벤트 인덱스 정보 생성모듈에서 생성된 이벤트 인덱스 정보를 해시함수 인자로 설정하여 해쉬함수값을 계산하기 위한 해쉬함수 계산모듈과, 계산된 해쉬함수값과 네트워크를 통해 전송된 OTP에 포함된 해쉬함수값을 비교하기 위한 OTP 비교모듈을 더 포함한다. 상기 OTP 비교모듈은 OTP의 인증결과에 따라 상기 이벤트 인덱스 정보의 생성을 이벤트 인덱스 정보 생성모듈에 요청하거나 그 인증 결과를 금융결제 처리모듈인 카드결제 처리모듈(460)로 전송하여 준다.

[0051] 카드결제 처리모듈(460)은 OTP 인증결과에 따라 카드 소유자로부터 전송받은 고객식별정보를 가지는 고객에 대해 카드결제 승인처리하여 그 결과를 쇼핑몰 서버(300)로 전송하여 준다.

[0052] 이상에서 설명한 고객정보 저장모듈(420), 시드키 생성모듈(430), 어플리케이션 전송모듈(440), OTP 인증모듈(450), 카드결제 처리모듈(460)은 카드 결제 시스템(400)의 운영체제(410) 상에서 구동 가능한 하나의 어플리케이션으로 구현 가능하며 넓게 OTP 인증 및 카드 처리부로 명명될 수도 있다.

[0053] 이하 상술한 구성을 가지는 카드 결제 시스템(400)의 동작을 도 4를 참조하여 설명하기로 한다.

[0054] 도 4는 본 발명의 일실시예에 따른 OTP를 이용한 카드결제 처리 흐름도를 도시한 것이다.

[0055] 도 4를 참조하면, 우선 시드키 생성모듈(430)은 카드 소유자로부터 시드키 발급요청이 있으면 해당 카드 소유자에게 발급된 카드번호, CVC 정보, 카드명, 유효기간 정보에 기초하여 OTP 생성을 위한 시드키를 생성(S1)한다. 생성된 시드키는 어플리케이션 전송모듈(440)에 전달됨으로서, 어플리케이션 전송모듈(440)은 전달받은 시드키가 포함된 OTP 생성 어플리케이션 데이터를 시드키 발급 요청한 카드 소유자의 고객 단말기로 전송(S2)하여 준다.

[0056] 이와 같이 OTP 생성 어플리케이션 데이터를 고객 단말기에 전송받은 카드 소유자는 이후 카드결제 필요시마다 상기 어플리케이션을 실행하여 하나의 OTP를 생성한다. 고객 단말기에서 OTP가 생성되는 과정은 도 2의 동작설명에서 상세히 언급하였으므로 이에 대한 부연 설명은 생략하기로 한다.

[0057] 고객 단말기에 설치된 어플리케이션을 실행시켜 하나의 OTP가 생성되면, 카드 소유자는 생성된 OTP를 자신의 고객식별정보와 함께 쇼핑몰 서버(300)의 카드결제 사이트를 통해 입력한다. 이러한 입력정보는 최종적으로 카드결제 시스템(400)으로 전송될 것이다.

[0058] OTP와 고객식별정보를 전송받은 카드 결제 시스템(400)내의 OTP 인증모듈(450)은 전송받은 OTP가 정상적인 카드

소유자에 의해 생성된 것인가를 인증한다. 보다 구체적으로 OTP 인증모듈(450)을 구성하는 이벤트 인덱스 정보 생성모듈은 우선적으로 인증 요청된 OTP에 부가된 이벤트 인덱스(EI) 정보를 끝자리로 가지는 이벤트 인덱스 정보를 생성(S3)한다. 생성되어야 하는 이벤트 인덱스 정보는 설정된 최대치를 초과할 경우 다시 초기화된다.

[0059] 이벤트 인덱스 정보가 생성되었으면, 해쉬함수 계산모듈은 카드 결제 요청한 사용자의 시드키 정보와 새로이 생성된 이벤트 인덱스 정보를 해쉬함수 인자로 설정하여 해쉬함수값((fx))을 계산(S4)한다.

[0060] 해쉬함수값(f(x)) 계산이 완료되면 OTP 비교모듈은 계산된 해쉬 함수값과 전송된 OTP에 포함된 해쉬함수값과 비교(S5)한다. 비교결과 해쉬함수값이 다르면, OTP 비교모듈은 이벤트 인덱스 정보의 생성을 요청함으로서, 이벤트 인덱스 정보 생성모듈은 다시 OTP에 부가된 이벤트 인덱스(EI) 정보를 가지는 이벤트 인덱스(EI) 정보를 생성한다. 즉, OTP 인증모듈(224)에서는 새로이 생성된 이벤트 인덱스 정보를 이용하여 계산된 해쉬 함수값이 인증 요청된 일회용 비밀번호(OTP)에 포함된 해쉬 함수값과 동일할때 까지 이벤트 인덱스 정보를 생성하되, 인증 요청된 OTP에 부가된 이벤트 인덱스(EI) 정보를 끝자리로 가지는 이벤트 인덱스 정보들을 생성함에 특징이 있는 것이다.

[0061] 상술한 이벤트 인덱스 정보의 생성과 해쉬함수값의 비교 인증을 구체적인 수치로 예시하면, 우선 카드 결제 요청한 사용자에 대해 미리 저장되어 있는 이벤트 인덱스 정보가 "3940"이라 하고, 전송된 OTP에 부가된 이벤트 인덱스 정보가 "46"이라 하면, OTP 인증모듈(450)은 "3946", "4046", "4146",..과 같이 이벤트 인덱스 정보를 순차적으로 생성해 가면서 생성된 값을 이용하여 계산된 해쉬함수값을 OTP에 포함된 해쉬함수값과 비교하는 것이다.

[0062] 이와 같은 해쉬 함수값의 비교과정에서 동일한 것으로 판명(S6)되면, OTP 비교모듈은 그 비교 결과를 금융결제 처리모듈에 해당하는 카드결제 처리모듈(460)로 전달하는 한편, 마지막으로 생성된 이벤트 인덱스 정보의 저장을 고객정보 저장모듈(420)로 요청(S7)한다.

[0063] 이에 카드결제 처리모듈(460)은 전송받은 고객식별정보를 가지는 고객이 소지한 카드에 대해 일반적인 카드결제 승인 절차를 밟고 그 결과를 쇼핑몰 서버(300)로 전송하여 준다.

[0064] 이에 따라 카드 결제 요청한 카드 소유자는 카드번호, CVC 정보와 같은 구체적인 카드정보를 전송하지 않고서도 OTP와 자신의 식별정보 전송만으로 신용카드(체크카드) 거래를 온라인상에서 실현할 수 있다.

[0065] 따라서 본 발명은 온라인상에서 카드정보의 유출을 사전에 막을 수 있는 효과를 얻을 수 있게 되는 것이다.

[0066] 한편 본 발명의 또 다른 실시예로서 OTP 생성 어플리케이션의 복제 여부 판단모듈을 구비하여 OTP 생성 어플리케이션(OTPGA)의 복제여부를 판단할 수 있다.

[0067] 즉, OTP 생성 어플리케이션 복제 판단모듈은 고객이 입력한 OTP에 포함된 해쉬함수값과 일치하는 해쉬함수값을 얻는데 이용된 이벤트 인덱스 정보를 고객정보 DB(470)에 저장되어 있는 이벤트 인덱스 정보와 비교한다. 만약 입력 전송된 OTP에 포함된 해쉬함수값과 일치하는 해쉬함수값을 얻는데 이용된 이벤트 인덱스 정보가 기 저장되어 있는 사용자별 이벤트 인덱스 정보보다 작은 값을 가질 경우에는, 어느 하나의 OTP가 불법 복제된 OTP 생성 어플리케이션에 의해 생성된 것을 의미하므로 그 판단결과를 OTP 인증모듈(450)로 건네 준다. 이에 OTP 인증모듈(450)은 그 사실을 금융결제 처리모듈인 카드결제 처리모듈(460) 혹은 관리자 단말기로 출력하여 주거나 SMS를 이용하여 고객 단말기로 복제사실이 통보될 수 있도록 조치한다.

[0068] 따라서 본 발명은 OTP 생성 프로그램이 불법 복제되어 이중 사용되는 것을 검출할 수 있는 효과도 가지게 되는 것이다.

[0069] 더 나아가 본 발명의 실시예에서는 카드의 비밀번호를 입력하지 않는 것으로 하였으나, 비밀번호의 입력을 추가로 요구하여 보안상의 취약점을 보완하도록 시스템을 구성할 수도 있을 것이다. 즉, 카드 결제 시스템(400)내의 OTP 인증모듈(450)은 사용자에게 발급받은 카드의 비밀번호 입력을 요구하고, 그 비밀번호가 카드 발급과정에서 사용자로부터 제공된 비밀번호와 일치할 경우에만 사용자 인증이 정상적으로 완료된 것으로 간주할 수 있다.

[0070] 이상의 실시예에서는 금융거래 시스템의 하나로서 카드 결제 시스템을 예시하여 본 발명의 실시예를 설명하였으나, 별 다른 변형 없이 계좌이체와 조회 업무를 수행하는 금융거래 시스템에서도 본 발명을 적용할 수 있다. 즉, 금융거래 고객의 계좌정보에 기초하여 시드키를 생성하고, 이러한 시드키를 기반으로 OTP를 생성하여 고객 식별정보와 함께 금융거래 시스템으로 전송하면, 해당 금융거래 시스템에서는 OTP를 인증하고 그 결과에 따라 계좌간 이체를 수행하거나, 계좌 조회 서비스를 제공한다. 이에 따라 계좌정보와 같은 금융거래정보가 온라인상

에서 노출될 수 있는 위험을 사전에 예방할 수 있다.

발명의 효과

[0071] 이상에서 설명한 바와 같이 본 발명은 카드번호, CVC 정보, 유효기간과 같은 구체적인 카드정보 혹은 계좌정보와 같은 금융거래정보를 온라인상에서 전송하지 않으므로 해킹 등에 의해 금융거래정보가 유실될 수 있는 문제를 원천적으로 제거할 수 있는 효과가 있으며,

[0072] 더 나아가 OTP 전송만으로 금융거래가 이루어질 수 있음은 물론, 여러 가지의 금융거래정보를 입력할 필요가 없기 때문에 그만큼 사용자의 편의성을 도모하여 줄 수 있는 장점이 있다.

[0073] 한편 본 발명은 도면에 도시된 실시예들을 참고로 설명되었으나 이는 예시적인 것에 불과하며, 당해 기술분야에 통상의 지식을 지닌자라면 이로부터 다양한 변형 및 균등한 타실시예가 가능하다는 점을 이해할 것이다. 예를 들면, 본 발명의 실시예에서는 발명의 이해를 돕기 위해 카드(금융) 결제 시스템내에 시드키 생성모듈과, 어플리케이션 전송모듈이 포함되는 것으로 하였으나, 시드키 생성모듈과 어플리케이션 전송모듈을 별도의 서비스 서버에 포함시켜 그 서버와 카드(금융) 결제 시스템이 서로 연동되도록 하여 본 발명의 목적을 달성될 수 있도록 구현할 수도 있을 것이다. 즉, 시드키 생성과 전송은 서비스 서버에서 수행하고, 카드(금융)결제 시스템은 그 생성된 시드키를 전송받아 고객별로 저장한후 그 시드키를 이용하여 생성된 OTP를 인증한 후에 카드결제 승인처리하는 시스템으로 제작할 수 있는 것이다. 따라서 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위에 의해서만 정해져야 할 것이다.

도면의 간단한 설명

[0001] 도 1은 본 발명의 일실시예에 따른 금융거래 시스템의 하나인 카드 결제 시스템의 전체 시스템 구성 예시도.

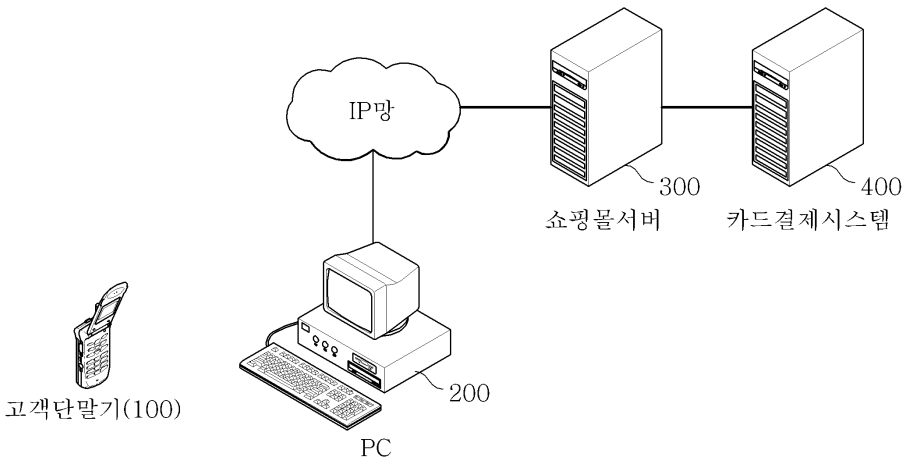
[0002] 도 2는 본 발명의 실시예에 따라 휴대용 고객 단말기에 설치되는 OTP 생성 어플리케이션(120)의 프로그램 모듈 구성 예시도.

[0003] 도 3은 본 발명의 일실시예에 따른 카드 결제 시스템(400)의 일부 구성도.

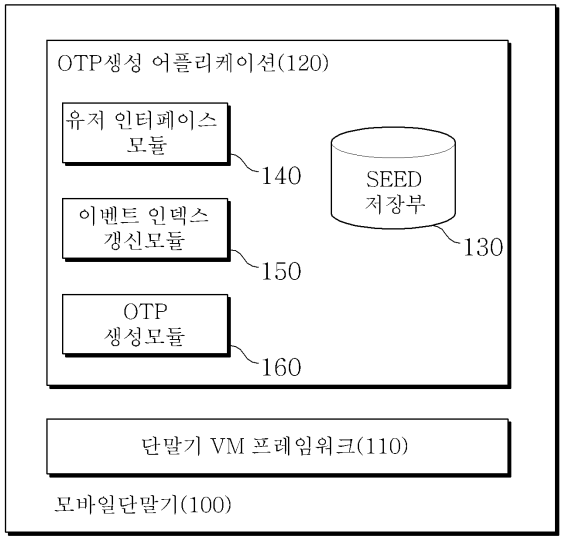
[0004] 도 4는 본 발명의 일실시예에 따른 OTP를 이용한 카드결제 처리 흐름도.

도면

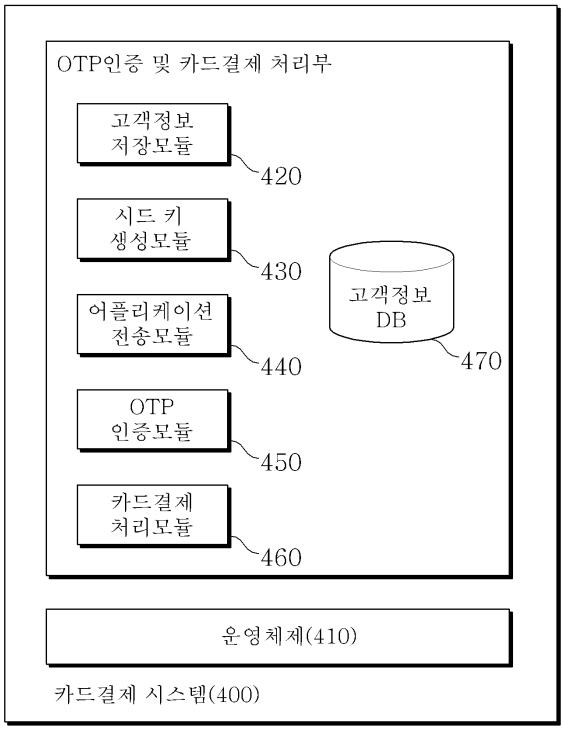
도면1



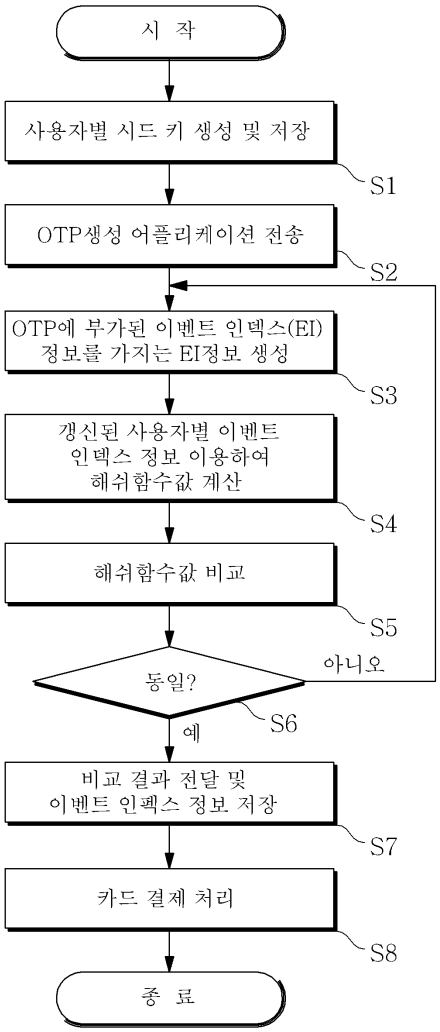
도면2


OTP생성 어플리케이션(120)
유저 인터페이스 모듈
140
이벤트 인덱스 갱신모듈
150
OTP 생성모듈
160
SEED 저장부
130
단말기 VM 프레임워크(110)
모바일단말기(100)

도면3


OTP인증 및 카드결제 처리부
고객정보 저장모듈
420
시드 키 생성모듈
430
어플리케이션 전송모듈
440
OTP 인증모듈
450
카드결제 처리모듈
460
고객정보 DB
470
운영체제(410)
카드결제 시스템(400)

도면4


시 작
사용자별 시드 키 생성 및 저장
S1
OTP생성 어플리케이션 전송
S2
OTP에 부가된 이벤트 인덱스(EI) 정보를 가지는 EI정보 생성
S3
갱신된 사용자별 이벤트 인덱스 정보 이용하여 해쉬함수값 계산
S4
해쉬함수값 비교
S5
동일?
아니오
S6
예
비교 결과 전달 및 이벤트 인덱스 정보 저장
S7
카드 결제 처리
S8
종 료