(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년06월04일
(11) 등록번호 10-1152610
(24) 등록일자 2012년05월29일

(51) 국제특허분류(Int. Cl.)
G06F 3/02 (2006.01) *G06F 21/00* (2006.01)
(21) 출원번호 10-2010-0015504
(22) 출원일자 2010년02월22일
심사청구일자 2010년02월22일
(65) 공개번호 10-2011-0096196
(43) 공개일자 2011년08월30일
(56) 선행기술조사문헌
KR100838488 B1
KR1020090036813 A
전체 청구항 수 : 총 3 항

(73) 특허권자
(주)이니시스
서울특별시 구로구 디지털로26길 61, 에이스하이-엔드타워2 12층 (구로동)
(72) 발명자
김태용
서울특별시 동작구 강남초등2길 15, 럭키그린하우스 402호 (상도1동)
(74) 대리인
백도현

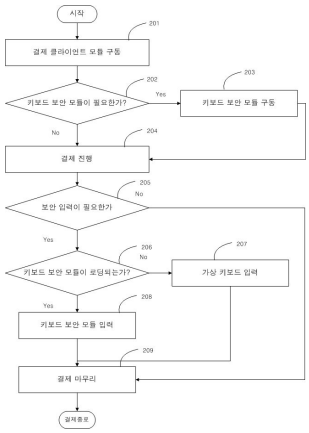
심사관 : 이정호

(54) 발명의 명칭 **가상 키보드 제공 방법**

(57) 요 약

본 발명은 화면에 전자상거래 결제 시 키보드를 출력하고, 이를 통해 글자를 입력하는 가상 키보드 제공 방법에 관한 것으로서, 숫자 및 문자의 배열을 임의로 변경하여 키로거 프로그램으로부터 입력 신호가 유출되는 것을 방지하기 위한 가상 키보드 제공 방법에 관한 것이다. 특히, 본 발명은 키보드 보안이 작동하지 않은 환경에서 선택적으로 가상 키보드를 제공하는 방법에 관한 것이다.

대 표 도 - 도2



특허청구의 범위

청구항 1

키보드 보안 모듈이 동작하지 않는 상황에서 수행되는 가상 키보드 클라이언트 모듈이 설치된 사용자 단말기와, 상기 사용자 단말기와 통신 가능하게 연결되어 있고 가상 키보드 관리 모듈이 설치된 서버를 포함하는 환경에서 수행되는, 상기 가상 키보드 클라이언트 모듈이 가상 키보드를 제공하는 방법에 있어서,

상기 가상 키보드 클라이언트 모듈이 가상 키보드 관리 모듈로부터 가상 키보드 조합 방식 정보와, 고유 세션키와, 시간 정보를 전송받는 단계와,

상기 가상 키보드 클라이언트 모듈이 상기 가상 키보드 조합 방식 정보에 따라 문자 또는 숫자의 배열을 가진 가상 키보드를 생성하여 상기 사용자 단말기의 화면에 표시하는 단계와,

상기 가상 키보드 클라이언트 모듈이 상기 표시된 가상 키보드를 통하여 입력값을 사용자로부터 입력 받는 단계와,

상기 가상 키보드 클라이언트 모듈이 상기 고유 세션키에 따른 암호화 알고리즘에 따라 상기 입력값과 상기 시간 정보를 조합하여 암호화 데이터를 생성하는 단계와,

상기 가상 키보드 클라이언트 모듈이 상기 암호화 데이터와 상기 고유 세션키를 상기 가상 키보드 관리 모듈로 전송하는 단계를 포함하는,

가상 키보드 제공 방법.

청구항 2

키보드 보안 모듈이 동작하지 않는 상황에서 수행되는 가상 키보드 클라이언트 모듈이 설치된 사용자 단말기와, 상기 사용자 단말기와 통신 가능하게 연결되어 있고 가상 키보드 관리 모듈이 설치된 서버를 포함하는 환경에서 수행되는, 상기 가상 키보드 관리 모듈이 가상 키보드를 제공하는 방법에 있어서,

상기 가상 키보드 관리 모듈이 상기 가상 키보드 클라이언트 모듈로 가상 키보드 조합 방식 정보 및 고유 세션키가 포함된 제1 시간 정보를 전송하는 단계와,

상기 가상 키보드 조합 방식 정보에 따라 생성된 가상 키보드를 통해 사용자로부터 입력받은 입력값과 제1 시간 정보를 조합하여 상기 고유 세션키에 따른 암호화 알고리즘에 따라서 상기 가상 키보드 클라이언트 모듈이 생성한 암호화 데이터를, 상기 가상 키보드 관리 모듈이 상기 가상 키보드 클라이언트 모듈로부터 전송 받는 단계와,

상기 가상 키보드 관리 모듈이 상기 가상 키보드 클라이언트 모듈로부터 상기 고유 세션키를 전송 받는 단계와,

상기 가상 키보드 관리 모듈이 제2 시간 정보를 생성하는 단계와,

상기 가상 키보드 관리 모듈이 상기 전송 받은 고유 세션키에 따른 복호화 알고리즘에 따라 암호화 데이터를 복호화하여 상기 입력값 및 상기 제1 시간 정보를 추출하는 단계와,

상기 가상 키보드 관리 모듈이 상기 추출된 제1 시간 정보와 상기 생성된 제2 시간 정보를 비교하여 유효성을 검증하는 단계를 포함하는,

가상 키보드 제공 방법.

청구항 3

청구항 1 또는 청구항 2에 있어서,

상기 가상 키보드 조합 방식 정보는 문자와 숫자의 배열을 랜덤하게 생성하는,

가상 키보드 제공 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 화면에 전자상거래 결제 시 키보드를 출력하고, 이를 통해 글자를 입력하는 가상 키보드 제공 방법에 관한 것으로서, 숫자 및 문자의 배열을 임의로 변경하여 키로거 프로그램으로부터 입력 신호가 유출되는 것을 방지하기 위한 가상 키보드 제공 방법에 관한 것이다. 특히, 본 발명은 키보드 보안이 작동하지 않은 환경에서 선택적으로 가상 키보드를 제공하는 방법에 관한 것이다.

배 경 기 술

[0002] 최근 컴퓨터 하드웨어와 네트워크 기반 기술의 발달로 인해 유무선 인터넷을 통한 개인과 단체/업체 사이의 각종 정보교환 및 정보공유가 활발히 이루어지고 있다. 이와 아울러 웹 브라우저의 활용도는 단순히 정보검색에 머물지 않고 온라인 쇼핑몰, 온라인 주식거래 및 인터넷 뱅킹을 포함하는 신용기반의 각종 서비스 영역까지 확장되고 있는 추세이다.

[0003] 다만, 이와 같은 기술 발달과 아울러, 개인과 단체 간에 이동되는 신용정보를 비롯한 개인정보를 유출하여 이익을 얻는 해커들도 급증하고 있다. 일반적으로 해커들은 개인정보 유출이라는 악의적인 목적을 달성하기 위해 여러가지 해킹툴을 이용하는데, 그 중에서도 사용자 컴퓨터의 키보드 눌림 신호를 가로채는 키로거(Key Logger) 프로그램이 보편적으로 이용되고 있다.

[0004] 이러한 키로거 프로그램은, 사용자 컴퓨터에 설치되어 CPU 및 메모리를 매우 낮게 점유하는 특성과, 윈도우 운영체제의 레지스트리에 그 설치 흔적을 남기지 않는 특성을 갖고 있는 바, 별도의 바이러스 백신 프로그램을 통해 정밀검사를 하지 않는 한 사용자는 키로거 프로그램의 실행 여부를 인지하기 어렵다는 문제가 있다.

[0005] 일반적으로 키로거 프로그램은, 해커에 의해 이메일 또는 다양한 배포수단을 통해 사용자 컴퓨터에 설치된다. 이후 키로거 프로그램에 감염된 사용자 컴퓨터가 웹브라우저를 통해 은행 서버에 접속하여 인터넷 뱅킹을 행하는 경우, 사용자는 웹브라우저 상에 표시되는 결제관련 입력창에 사용자의 비밀번호를 포함한 신용정보를 키보드를 통해 입력하게 된다. 여기에서 키보드의 눌림 신호에 의한 데이터는 키보드 드라이버를 거쳐 결제관련 입력창에 입력된 후 최종적으로 웹브라우저를 통해 서버로 전송된다. 이때, 키입력 데이터는 키보드 드라이버를 제어하는 키로거 프로그램에 의해 해커에게 유출된다. 키보드 눌림 신호는 운영체제 상에서 윈도우 이벤트를 발생시키고 그 눌림 신호는 윈도우 메시지 형태로 어플리케이션으로 전송되는데, 키로거 포로그램은 상기 윈도우 이벤트를 감지하여 해당 윈도우 메시지를 인터셉트함으로써 키보드를 통해 입력된 키입력 데이터를 빼내게 된다.

[0006] 이러한 키로거 프로그램의 폐해를 해소하기 위한 방법이 국내 등록특허 제10-0496462호(발명의 명칭: 키입력 도용 방지 방법)에 개시되어 있다. 상기 특허에는 종래와 같이 소정의 개인정보를 키보드를 통해서 입력받는 방식이 아닌, 사용자의 컴퓨터 화면에 디스플레이되는 가상의 키보드와 사용자가 마우스를 통해 상기 가상 키보드의 키를 클릭함으로써 입력받는 방식을 개시하고 있다. 즉, 개인정보 입력 자체가 키보드 및 키보드 드라이버를 거치지 않게 되므로 키로거 프로그램이 이를 가로챌 수 없게 되는 것이다.

[0007] 하지만, 상기 특허의 가상 키보드는 항상 동일한 키배열로 구성되어 있기 대문에 이 역시 해커들에 의한 공격 가능성이 상존하는 문제점이 있다.

[0008] 이를 해결하기 위해 국내 등록특허 제10-0745489호(발명의 명칭 : 키입력 해킹방지 방법)가 있다. 이는 보안이 필요한 웹 페이지 또는 이와 유사한 기능을 제공하는 응용프로그램 상에서 임의적으로 재배열되는 가상 키보드를 통해 사용자로부터 아이디 또는 패스워드 등의 데이터를 입력받아 이를 웹 페이지 또는 상기 응용프로그램으로 전송되게 함으로써, 키로거와 같은 해킹 프로그램에 의한 개인정보 유출을 방지할 수 있는 키입력 해킹방지 방법을 제공하고 있다.

[0009] 하지만, 상기 특허도 마우스 포인터 좌표를 감지하는 기술로부터 완전히 자유로울 수는 없는 문제가 있다.

발명의 내용

해결하려는 과제

[0010] 본 발명은 상기와 같은 문제점을 해결하기 위하여, 인터넷 브라우져와 OS를 구분하여 키보드 보안이 구동되지 않는 경우에만 가상 키보드가 사용되는 환경을 제공하고 있다.

[0011] 또한, 숫자 방식의 가상 키보드의 경우 자동으로 숫자가 섞이어 마우스 클릭 위치를 통한 입력값의 추정이 불가능 하도록 하는 가상 키보드를 제공하고자 한다.

[0012] 또한, 일반 입력 필드와 패스워드 입력 필드를 구분하여 패스워드 입력 필드에서만 가상 키보드가 자동으로 실행되도록 하여 사용자 편의를 높이는 가상 키보드를 제공하고자 한다.

과제의 해결 수단

[0014] 본 발명에 의한 가상 키보드 제공 방법은 상기의 목적을 위해 다음과 같은 과제 해결 수단을 제공하고 있다.

[0015] 키보드 보안 모듈이 동작하지 않는 상황에서 수행되는 가상 키보드 클라이언트 모듈이 설치된 사용자 단말기와, 상기 사용자 단말기와 통신 가능하게 연결되어 있고 가상 키보드 관리 모듈이 설치된 서버를 포함하는 환경에서 수행되는, 상기 가상 키보드 클라이언트 모듈이 가상 키보드를 제공하는 방법이고, 본 방법은 가상 키보드 관리 모듈로부터 가상 키보드 조합 방식 정보 및 고유 세션키가 포함된 시간 정보를 전송받는 단계와, 상기 가상 키보드 조합 방식 정보에 따라 문자 또는 숫자의 배열을 가진 가상 키보드를 생성하여 상기 사용자 단말기의 화면에 표시하는 단계와, 상기 표시된 가상 키보드를 통하여 값을 입력 받는 단계와, 상기 고유 세션키에 따른 암호화 알고리즘에 따라 상기 입력값과 상기 시간 정보를 조합하여 암호화 데이터를 생성하는 단계와, 상기 암호화 데이터와 상기 고유 세션키를 상기 가상 키보드 관리 모듈로 전송하는 단계를 포함한다.

[0017] 또한, 키보드 보안 모듈이 동작하지 않는 상황에서 수행되는 가상 키보드 클라이언트 모듈이 설치된 사용자 단말기와, 상기 사용자 단말기와 통신 가능하게 연결되어 있고 가상 키보드 관리 모듈이 설치된 서버를 포함하는 환경에서 수행되는, 상기 가상 키보드 관리 모듈이 가상 키보드를 제공하는 방법이고, 상기 가상 키보드 클라이언트 모듈로 가상 키보드 조합 방식 정보 및 고유 세션키가 포함된 제1 시간 정보를 전송하는 단계와, 상기 가상 키보드 클라이언트 모듈로부터 상기 가상 키보드 조합 방식 정보에 따라 생성된 가상 키보드를 통해 입력 받은 입력값과 제1 시간 정보를 조합하여, 상기 고유 세션키에 따른 암호화 알고리즘에 따라 생성된 암호화 데이터를 전송 받는 단계와, 상기 가상 키보드 클라이언트 모듈로부터 상기 고유 세션키를 전송 받는 단계와, 제2 시간 정보를 생성하는 단계와, 상기 전송 받은 고유 세션키에 따른 복호화 알고리즘에 따라 암호화 데이터를 복호화하여 입력값 및 상기 제1 시간 정보를 추출하는 단계와, 상기 추출된 제1 시간 정보와 제2 시간 정보를 비교하여 유효성을 검증하는 단계를 한다.

[0018] 그리고 상기 가상 키보드 조합 방식 정보는 문자와 숫자의 배열을 랜덤하게 생성하는 것이 바람직하다.

발명의 효과

[0019] 본 발명은 상기와 같은 문제점을 해결하기 위하여, 인터넷 브라우져와 OS를 구분하여 키보드 보안이 구동되지 않는 경우에만 가상 키보드가 사용되는 환경을 제공하고, 일반 입력 필드와 패스워드 입력 필드를 구분하여 패스워드 입력 필드에서만 가상 키보드가 자동으로 실행되도록 하여 사용자 편의를 높이는 효과가 있다.

[0020] 또한, 숫자 방식의 가상 키보드의 경우 자동으로 숫자가 섞이어 마우스 클릭 위치를 통한 입력값의 추정이 불가능 하도록 하여 보안성을 향상시키는 효과가 있다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 가상 키보드의 구성도.

도 2는 본 발명의 가상 키보드가 구현되는 상황의 흐름도.

도 3은 본 발명의 가상 키보드가 구현되는 상황의 흐름도.

도 4는 본 발명의 가상 키보드의 일 실시예.

도 5는 본 발명의 가상 키보드의 일 실시예.

발명을 실시하기 위한 구체적인 내용

[0023] 이하 첨부된 도면을 참조하여 본 발명에 대해 구체적으로 설명하기로 한다.

[0024] 도 1은 본 발명의 가상 키보드의 구성도이다. 본 발명은 사용자 단말기에 제공되는 결제 클라이언트 모듈(10)이 포함된다. 결제 클라이언트 모듈(10)은 일반적으로 키보드 보안 모듈(11)과 가상 키보드 클라이언트 모듈(12)을 포함한다. 본 발명은 키보드 보안 모듈(11)이 동작하지 않는 상황에 가상 키보드 클라이언트 모듈(12)을 수행하는 것이 핵심이다.

[0025] 서버(일반적으로 결제 서버일 것이나, 이에 본 권리범위가 제한되는 것은 아니다)(20)에는 암복호화 모듈(21)과 가상 키보드 관리 모듈(22)이 제공된다.

[0026] 도 2는 본 발명의 가상 키보드가 구현되는 상황의 흐름도이다. 결제 클라이언트 모듈이 구동되면(201), 현상황에서 키보드 보안 모듈이 필요한지를 판단한다(202). 키보드 보안 모듈이 필요하지 않으면 바로 결제가 진행되고(204), 키보드 보안 모듈이 필요한 경우에는 키보드 보안 모듈이 구동된 후 결제가 진행된다(203).

[0027] 이후 보안 입력이 필요한지 여부를 판단하게 되고(205), 필요하지 않은 경우에는 결제 마무리를 진행한다. 보안 입력이 필요한 경우에는 키보드 보안 모듈이 로딩되는지 여부를 판단한다(206). 필요한 경우에는 키보드 보안 모듈을 통해 입력을 진행하고(208), 필요하지 않은 경우에는 가상 키보드 통하여 입력을 진행한다(207).

[0028] 즉, 본 발명에 의한 가상 키보드는 키보드 보안 모듈이 로딩되지 않은 상황에서 작동하는 것을 핵심으로 한다.

[0029] 도 3은 본 발명의 가상 키보드가 구현되는 상황의 흐름도이다. 사용자 단말기에 제공되는 가상 키보드 클라이언트 모듈에서 가상 키보드를 요청한다(S301). 이를 요청받은 가상 키보드 관리 모듈은 가상 키보드 조합 방식 및 고유 세션키를 생성한다(S302).

[0030] 이후, 가상키보드 조합 방식 정보와, 제1 시간 정보, 고유 세션키를 가상 키보드 클라이언트 모듈로 전달한다(S303).

[0031] 여기에서 제1 시간 정보는 중요한 의미를 가지고 있다. 본 발명의 가상 키보드는 시간 제한을 통해 유효성을 검증하는 것을 주요 특징으로 한다. 즉, 제1 시간과, 후에 가상 키보드 클라이언트 모듈이 값을 전달하면서 제2 시간과 비교를 하여 그 유효성을 검증한다.

[0032] 그 유효성은 제2 시간 정보가 제1 시간 정보에 비해 미리 설정된 시간을 초과하지 않은 경우에 인정되는 것이 일반적이다.

[0033] 이를 전달 받은 가상 키보드 클라이언트 모듈은 가상 키보드를 생성하고 이를 표시한다(S304). 이후 사용자는 가상 키보드를 통해 값을 입력한다. 이후 입력값과 제1 시간 정보를 암호화한다(S305).

[0034] 이후, 암호화 데이터 및 고유 세션키를 가상 키보드 관리 모듈로 전송한다(S306). 가상 키보드 관리 모듈은 제2 시간 정보를 생성한다(S307). 제2 시간 정보는 현재의 시각을 의미한다.

[0035] 암호화 데이터를 전달받은 가상 키보드 관리 모듈은 고유 세션키에 따라 복호화를 한다(S308). 이후, 제1 시간 정보와 제2 시간 정보를 비교하여 그 입력값의 유효성을 검증한다(S309). 그리고 이를 가상 키보드 클라이언트 모듈로 결과를 전송한다(S310).

[0036] 사용자 단말기에 제공되는 가상 키보드 클라이언트 모듈이 수행하는 단계를 설명하면 다음과 같다.

[0037] 가상 키보드 관리 모듈로부터 가상 키보드 조합 방식 정보 및 고유 세션키가 포함된 시간 정보를 전송받는 단계와, 가상 키보드 조합 방식 정보에 따라 문자 또는 숫자의 배열을 가진 가상 키보드를 생성하여 사용자 단말기의 화면에 표시하는 단계와, 표시된 가상 키보드를 통하여 값을 입력 받는 단계와, 고유 세션키에 따른 암호화 알고리즘에 따라 입력값과 시간 정보를 조합하여 암호화 데이터를 생성하는 단계와, 암호화 데이터와

고유 세션키를 가상 키보드 관리 모듈로 전송하는 단계를 포함한다.

[0038] 서버에 제공되는 가상 키보드 관리 모듈이 수행하는 단계를 설명하면 다음과 같다.

[0039] 가상 키보드 클라이언트 모듈로 가상 키보드 조합 방식 정보 및 고유 세션키가 포함된 제1 시간 정보를 전송하는 단계와, 가상 키보드 클라이언트 모듈로부터 상기 가상 키보드 조합 방식 정보에 따라 생성된 가상 키보드를 통해 입력 받은 입력값과 제1 시간 정보를 조합하여, 고유 세션키에 따른 암호화 알고리즘에 따라 생성된 암호화 데이터를 전송 받는 단계와, 가상 키보드 클라이언트 모듈로부터 고유 세션키를 전송 받는 단계와, 제2 시간 정보를 생성하는 단계와, 전송 받은 고유 세션키에 따른 복호화 알고리즘에 따라 암호화 데이터를 복호화하여 입력값 및 제1 시간 정보를 추출하는 단계와, 추출된 제1 시간 정보와 제2 시간 정보를 비교하여 유효성을 검증하는 단계를 포함한다.

[0040] 가상 키보드 조합 방식 정보는 문자와 숫자의 배열을 랜덤하게 생성하는 것이 바람직하다.

[0041] 도 4 및 도 5는 본 발명의 가상 키보드의 일 실시 예이다. 본 발명의 가상 키보드는 주민 번호 뒷자리, 계좌 비밀번호와 같이 주요 정보가 입력되는 경우에만 구동된다. 숫자 타입의 경우 키패드 모양으로 구성되고, 전체 숫자 위치를 섞어서, 마우스 클릭 위치로 해킹하는 사항에 대하여서도 방지할 수 있다.

[0042] 또한, 숫자와 문자 타입의 혼합형도 가능하다. 인증서 패스워드, 로그인 패스원드와 같이 숫자와 문자를 같이 사용하는 패스워드의 경우 사용될 수 있다.

[0043] 본 발명에 의한 가상 키보드는 인터넷 브라우저와 OS를 구분하여 키보드 보안이 구동되지 않는 경우에만 가상 키보드가 사용되도록 하는 것이 특징이다. 또한, 숫자 방식의 가상 키보드의 경우 자동으로 숫자가 섞이어 마우스 클릭 위치를 통한 입력값의 추정이 불가능하다. 또한, 일반 입력 필드와 패스워드 입력 필드를 구분하여 패스워드 입력 필드에서만 가상 키보드가 자동으로 실행된다.

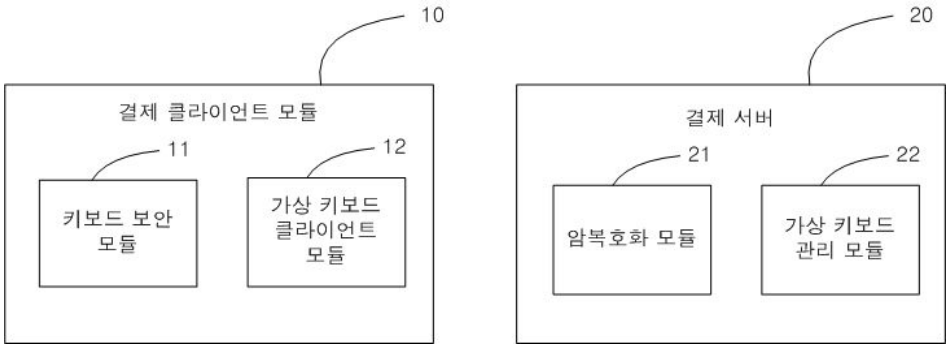
[0045] 본 발명은 상기와 같은 실시예에 의해 권리범위가 한정되는 것은 아니며, 본 발명의 기술적인 사상을 가지고 있다면 모두 본 발명의 권리범위에 해당된다고 볼 수 있으며, 본 발명은 특허청구범위에 의해 권리범위가 정해짐을 밝혀둔다.

부호의 설명

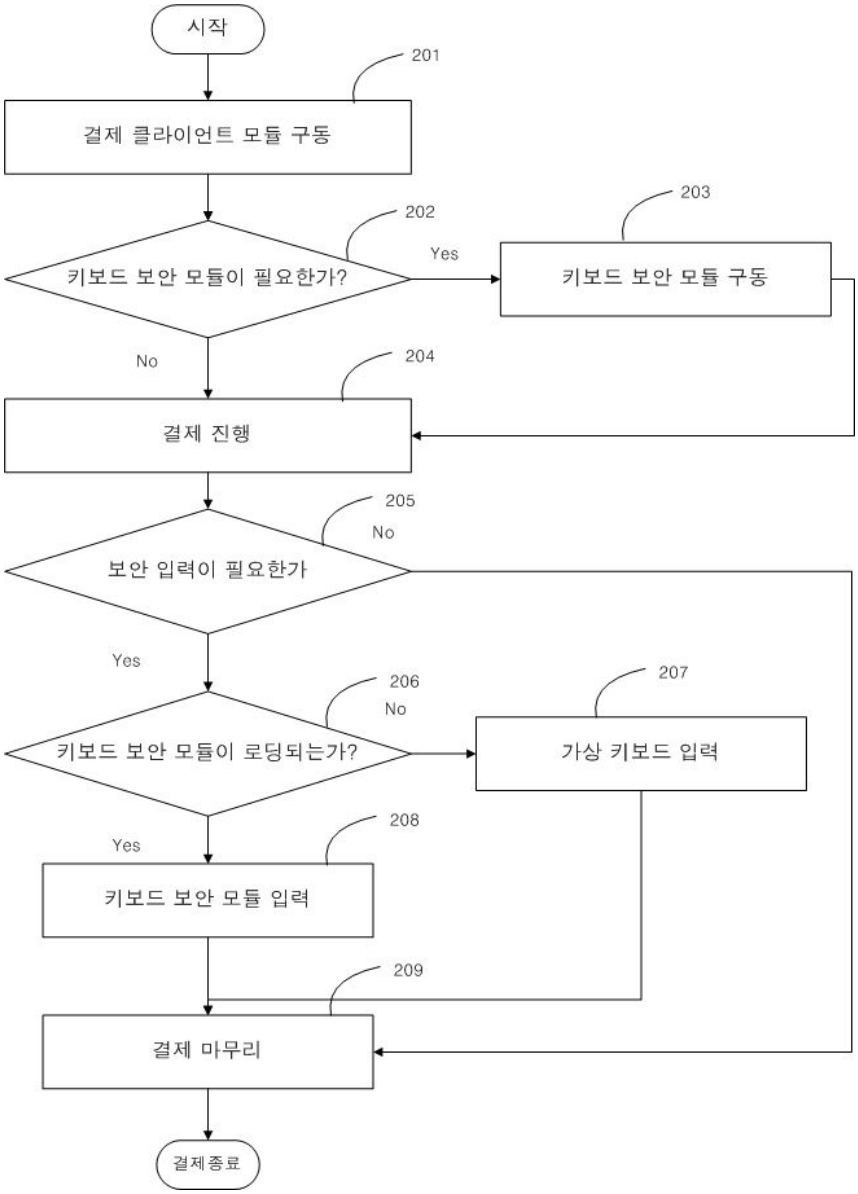
[0047]
10 : 결제 클라이언트 모듈
11 : 키보드 보안 모듈
12 : 가상 키보드 클라이언트 모듈
20 : 결제 서버
21 : 암복호화 모듈
22 : 가상 키보드 관리 모듈

도면

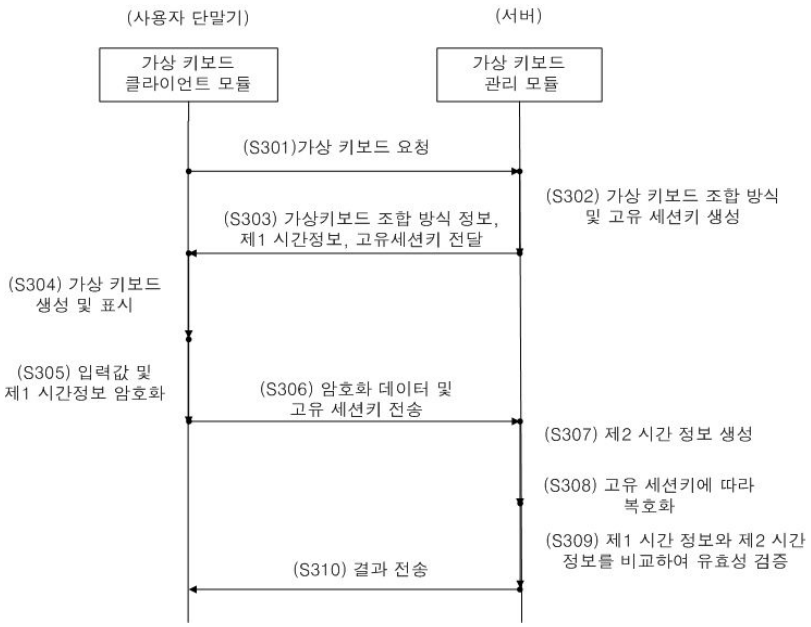
도면1



도면2


시작
201
결제 클라이언트 모듈 구동
202
키보드 보안 모듈이 필요한가?
Yes
203
키보드 보안 모듈 구동
No
204
결제 진행
205
No
보안 입력이 필요한가
Yes
206
No
207
키보드 보안 모듈이 로딩되는가?
가상 키보드 입력
Yes
208
키보드 보안 모듈 입력
209
결제 마무리
결제종료

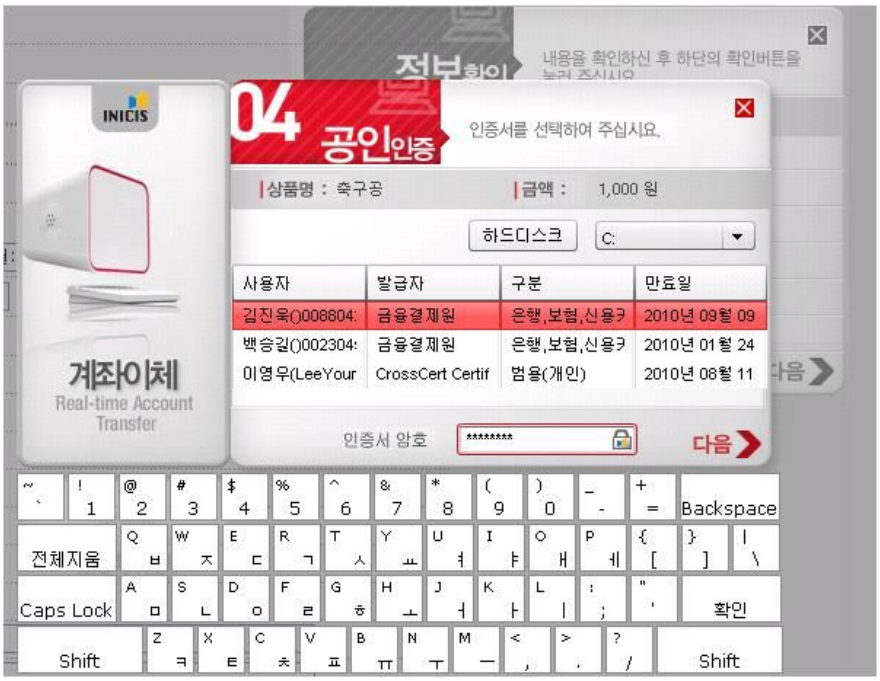
도면3


(사용자 단말기)
(서버)
가상 키보드 클라이언트 모듈
가상 키보드 관리 모듈
(S301)가상 키보드 요청
(S302) 가상 키보드 조합 방식 및 고유 세션키 생성
(S303) 가상키보드 조합 방식 정보, 제1 시간정보, 고유세션키 전달
(S304) 가상 키보드 생성 및 표시
(S305) 입력값 및 제1 시간정보 암호화
(S306) 암호화 데이터 및 고유 세션키 전송
(S307) 제2 시간 정보 생성
(S308) 고유 세션키에 따라 복호화
(S309) 제1 시간 정보와 제2 시간 정보를 비교하여 유효성 검증
(S310) 결과 전송

도면4


INICIS
계좌이체
Real-time Account Transfer
03 정보입력
고객님의 결제 계좌정보를 입력하여 주십시요.
상품명 : 축구공
금액 : 1,000 원
출금은행(증권사)
농협
예금주명
홍길동
주민(사업자)번호
780402
계좌번호
계좌비밀번호
스크린 키보드
3 9 0
6 5 2
8 7 4
1
전체지움
마우스로 입력하는 방식으로 키보드를 통해 입력하는 번호를 보호합니다.
이전
다음

도면5


INICIS
계좌이체
Real-time Account Transfer
04 공인인증
인증서를 선택하여 주십시요.
상품명 : 축구공
금액 : 1,000 원
하드디스크
C:
사용자
발급자
구분
만료일
김진욱()008804:
금융결제원
은행,보험,신용카
2010년 09월 09
백승길()002304:
금융결제원
은행,보험,신용카
2010년 01월 24
이영우(LeeYour
CrossCert Certif
범용(개인)
2010년 08월 11
인증서 암호
다음
전체지움
Caps Lock
확인
Shift
Backspace