(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0100549
(43) 공개일자 2012년09월12일

(51) 국제특허분류(Int. Cl.)
G06Q 20/40 (2012.01)
(21) 출원번호 10-2011-0019528
(22) 출원일자 2011년03월04일
심사청구일자 2011년03월04일

(71) 출원인
주식회사 인센트릭
경기도 성남시 분당구 황새울로200번길 28, 508호 (수내동, 오너스타워)
(72) 발명자
허태열
경기도 부천시 원미구 부천로36번길 53, 3층 (심곡동)
(74) 대리인
특허법인지명

전체 청구항 수 : 총 8 항

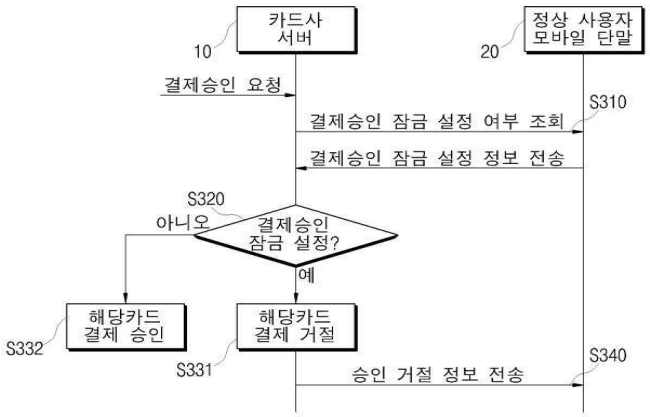
(54) 발명의 명칭 **금융 결제 보안 서비스 방법**

(57) 요 약

본 발명은 금융 결제 보안 서비스 방법에 관한 것으로서, 본 발명의 일면에 따른 금융 결제 보안 서비스 방법은, 해당 결제 수단으로 결제 승인이 요청되면, 실시간으로 상기 사용자의 모바일 단말로 결제 승인 잠금 설정 여부를 조회하는 단계와, 조회 결과, 결제 승인 잠금 설정이 되어 있는 경우, 상기 해당 결제 수단의 결제 승인을 거절하는 단계를 포함하여 구성된다.

본 발명에 따르면, 스마트 폰 등과 같은 모바일 단말에 설치되는 금융 결제 보안을 위한 어플리케이션을 이용하여 제3자가 무단으로 카드 결제, 또는 온라인 계좌 이체 등의 금융 결제를 원천적으로 차단할 수 있는 보안 서비스를 제공함으로써 금융 결제 시 발생할 수 있는 피해와 사고를 미연에 방지할 수 있다.

대 표 도 - 도3



특허청구의 범위

청구항 1

결제 수단 사용자의 결제 요청에 대하여 전반적인 처리를 수행하는 결제 서버가 수행하는 금융 결제 보안 서비스 방법으로서,

해당 결제 수단으로 결제 승인이 요청되면, 실시간으로 상기 사용자의 모바일 단말로 결제 승인 잠금 설정 여부를 조회하는 단계; 및

조회 결과, 결제 승인 잠금 설정이 되어 있는 경우, 상기 해당 결제 수단의 결제 승인을 거절하는 단계

를 포함하는 결제 서버가 수행하는 금융 결제 보안 서비스 방법.

청구항 2

제1항에 있어서,

상기 해당 결제 수단의 결제 승인이 거절된 경우, 상기 해당 결제 수단의 정상 사용자에게 승인 거절 완료 정보를 전송하는 단계

를 더 포함하는 결제 서버가 수행하는 금융 결제 보안 서비스 방법.

청구항 3

결제 수단 사용자의 결제 요청에 대하여 전반적인 처리를 수행하는 결제 서버가 수행하는 금융 결제 보안 서비스 방법으로서,

모바일 단말 내의 보안 어플리케이션에서 특정 결제 수단의 결제 승인 설정이 되면, 상기 모바일 단말로부터 해당 결제 수단의 결제 승인 정보를 전송 받아 저장하는 단계;

해당 결제 수단으로 결제가 요청되면, 해당 결제 수단의 결제 요청을 받은 시각이 해당 결제 수단의 결제가 승인되는 기 정의된 시간 범위 내인지 여부를 판단하는 단계; 및

판단 결과, 해당 결제 수단의 결제 요청을 받은 시각이 상기 기 정의된 시간 범위 내인 경우에는 상기 해당 결제 수단의 결제를 승인하는 단계

를 포함하는 결제 서버가 수행하는 금융 결제 보안 서비스 방법.

청구항 4

제3항에 있어서,

판단 결과, 해당 결제 수단의 결제 요청을 받은 시각이 상기 기 정의된 시간 범위 밖인 경우에는 상기 결제 수단의 결제 승인을 거절하는 단계; 및

결제 승인이 거절된 경우, 상기 해당 결제 수단의 정상 사용자에게 승인 거절 완료 정보를 전송하는 단계

를 더 포함하는 결제 서버가 수행하는 금융 결제 보안 서비스 방법.

청구항 5

결제 수단 사용자의 결제 요청에 대하여 전반적인 처리를 수행하는 결제 서버가 수행하는 금융 결제 보안 서비스 방법으로서,

모바일 단말 내의 보안 어플리케이션에서 해당 결제 수단의 결제 승인 잠금 설정이 되면, 상기 모바일 단말로부터 해당 결제 수단의 결제 승인 잠금 정보를 전송 받아 저장하는 단계;

해당 결제 수단으로 결제가 요청되면, 상기 결제 수단에 대하여 결제 승인 잠금 정보가 저장되어 있는지 여부를 조회하는 단계; 및

조회 결과, 상기 결제 잠금 정보가 있는 경우 상기 결제 수단의 결제 승인을 거절하는 단계

를 포함하는 결제 서버가 수행하는 금융 결제 보안 서비스 방법.

청구항 6

결제 수단 사용자의 결제 요청에 대하여 전반적인 처리를 수행하는 결제 서버와, 사용자 정보를 도용하여 서버에 접근하는 제3자에 대해 제공 서비스를 차단하는 보안 서버를 포함하는 금융 결제 보안 서비스 시스템에서 상기 보안 서버가 수행하는 방법으로서,

상기 결제 서버에 해당 결제 수단으로 결제 승인이 요청되면, 상기 결제 서버로부터 결제 승인 잠금 설정 정보를 요청 받는 단계;

상기 사용자의 모바일 단말로 결제 승인 잠금 설정 여부를 조회하는 단계; 및

조회된 결제 승인 잠금 설정 정보를 상기 결제 서버로 전송하는 단계

를 포함하는 보안 서버가 수행하는 금융 결제 보안 서비스 방법.

청구항 7

결제 수단 사용자의 결제 요청에 대하여 전반적인 처리를 수행하는 결제 서버와, 사용자 정보를 도용하여 서버에 접근하는 제3자에 대해 제공 서비스를 차단하는 보안 서버를 포함하는 금융 결제 보안 서비스 시스템에서 상기 보안 서버가 수행하는 방법으로서,

모바일 단말 내의 보안 어플리케이션에서 특정 결제 수단의 결제 승인 설정이 되면, 상기 모바일 단말로부터 상기 결제 수단의 결제 승인 정보를 전송 받아 이를 상기 결제 서버로 전송하는 단계

를 포함하는 보안 서버가 수행하는 금융 결제 보안 서비스 방법.

청구항 8

결제 수단 사용자의 결제 요청에 대하여 전반적인 처리를 수행하는 결제 서버와, 사용자 정보를 도용하여 서버에 접근하는 제3자에 대해 제공 서비스를 차단하는 보안 서버를 포함하는 금융 결제 보안 서비스 시스템에서 상기 보안 서버가 수행하는 방법으로서,

모바일 단말 내의 보안 어플리케이션에서 해당 결제 수단의 결제 승인 잠금 설정이 되면, 상기 모바일 단말로부터 해당 결제 수단의 결제 승인 잠금 정보를 전송 받아 저장하는 단계;

해당 결제 수단으로 결제가 요청되면, 상기 결제 서버로부터 결제 승인 잠금 설정 정보를 요청 받는 단계; 및

저장된 상기 결제 승인 잠금 정보를 상기 결제 서버로 전송하는 단계

를 포함하는 보안 서버가 수행하는 금융 결제 보안 서비스 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 금융 결제 보안 서비스 방법에 관한 것으로서, 보다 상세하게는 사용자 단말을 이용하여 카드 결제, 온라인 계좌 이체 등의 금융 결제 시, 1차적인 보안 서비스를 제공할 수 있는 금융 결제 보안 서비스 방법에 관한 것이다.

배 경 기 술

[0002] 카드 및/또는 IC(Integrated Circuit)카드 및/또는 소정의 무선 단말기에 탑재 또는 이탈착되는 IC칩을 포함하는 매체(Media)에 소정의 결제수단을 구비하고, 온/오프라인 상의 금융 결제 시, 상기 매체에 구비된 결제수단을 이용하여 결제 처리하는 전자결제 시스템이 보편화되었다.

[0003] 상기 전자결제 시스템은 적어도 하나 이상의 유효한 결제수단을 구비한 사용자 소유 매체(예컨대, MS카드, IC카드, IC칩 등)와, 상기 매체를 인식하고 상기 매체로부터 유효한 결제수단 정보를 독출하여 기 정의된 결제 처리 절차를 수행하는 가맹점 결제단말과, 상기 결제수단에 대한 결제 처리를 승인하는 결제서버 및 상기 결제단말과

결제서버를 연결하는 결제 네트워크를 포함하여 이루어진다.

[0004] 최근 들어, 카드 서버에 등록된 카드 정보 및 은행 서버에 등록된 계좌 이체 비밀 번호 등을 도용하여 제3자가 무단으로 금융 결제를 하는 등의 해킹 행위가 심각한 사회 문제로 대두되고 있다.

[0005] 따라서, 이러한 문제점을 해소하기 위하여 온/오프라인으로 금융 결제 시, 본인 인증 등의 추가적인 보안 서비스가 제공될 필요가 있다.

발명의 내용

해결하려는 과제

[0006] 본 발명은 상술한 종래 기술의 문제점을 해결하기 위하여, 사용자 단말을 이용하여, 등록된 카드 및 은행 계좌의 결재 기능 잠금 설정을 통하여 카드 결제, 온라인 계좌 이체 등의 온/오프라인 금융 결제 시, 1차적인 보안 서비스를 제공할 수 있는 금융 결제 보안 서비스 방법을 제공하는 것을 목적으로 한다.

[0007] 본 발명의 목적은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0008] 전술한 목적을 달성하기 위한 본 발명의 일면에 따른 금융 결제 보안 서비스 방법은, 보안 어플리케이션이 설치된 모바일 단말과, 결제 수단 사용자의 결제 요청에 대하여 전반적인 처리를 수행하는 결제 서버로 구성된 금융 결제 보안 서비스 시스템에서 상기 결제 서버에서 수행된다.

[0009] 구체적으로 사용자에 의해 해당 결제 수단으로 결제 승인이 요청되면, 결제서버는 실시간으로 상기 사용자의 모바일 단말로 결제 승인 잠금 설정 여부를 조회하고 조회 결과, 결제 승인 잠금 설정이 되어 있는 경우, 상기 해당 결제 수단의 결제 승인을 거절한다. 그리고 해당 결제 수단의 결제 승인이 거절되면, 해당 결제 수단의 정상 사용자에게 승인 거절 정보를 전송한다.

발명의 효과

[0010] 이상 상술한 바와 같이 본 발명에 따르면, 스마트 폰 등과 같은 모바일 단말에 설치되는 금융 결제 보안을 위한 어플리케이션을 이용하여 제3자가 무단으로 카드 결제, 또는 온라인 계좌 이체 등의 금융 결제를 원천적으로 차단할 수 있는 보안 서비스를 제공함으로써 금융 결제 시 발생할 수 있는 피해와 사고를 미연에 방지할 수 있다.

도면의 간단한 설명

[0011] 도 1은 본 발명의 일 실시예에 따른 금융 결제 보안 서비스 방법이 수행되는 금융 결제 보안 서비스 시스템의 구성을 도시한 구성도이다.

도 2는 본 발명의 일 실시예에 따라 모바일 단말에 설치된 금융 결제 보안을 위한 어플리케이션이 실행되는 예를 도시한 예시도이다.

도 3은 본 발명의 일 실시예에 따라 금융 결제 서버가 수행하는 금융 결제 보안 서비스 방법의 제1 형태를 도시한 도면이다.

도 4는 본 발명의 일 실시예에 따라 금융 결제 서버가 수행하는 금융 결제 보안 서비스 방법의 제2 형태를 도시한 도면이다.

도 5는 본 발명의 일 실시예에 따라 금융 결제 서버가 수행하는 금융 결제 보안 서비스 방법의 제3 형태를 도시한 도면이다.

도 6은 본 발명의 다른 실시예에 따른 금융 결제 보안 서비스 방법이 수행되는 금융 결제 보안 서비스 시스템의 구성을 도시한 구성도이다.

도 7은 본 발명의 다른 실시예에 따라 보안 서버가 수행하는 금융 결제의 제1 형태를 도시한 도면이다.

도 8은 본 발명의 다른 실시예에 따라 보안 서버가 수행하는 금융 결제 보안 서비스 방법의 제2 형태를 도시한 도면이다.

도 9는 본 발명의 다른 실시예에 따라 보안 서버가 수행하는 금융 결제 보안 서비스 방법의 제3 형태를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0012] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하며, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 한편, 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다.

[0013] 이하, 본 발명의 바람직한 실시예를 첨부된 도면들을 참조하여 상세히 설명한다. 우선 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[0014] 도 1을 참조하여 본 발명의 일 실시예에 따른 금융 결제 보안 서비스 방법이 수행되는 금융 결제 보안 서비스 시스템을 설명한다. 도 1은 본 발명의 일 실시예에 따른 금융 결제 보안 서비스 방법이 수행되는 금융 결제 보안 서비스 시스템의 구성을 도시한 구성도이다.

[0015] 도 1을 참조하면, 본 발명의 일 실시예에 따라 금융 결제 보안 서비스 방법이 수행되는 금융 결제 보안 서비스 시스템은, 금융 결제 서버(10)와, 정상 사용자 모바일 단말(20)을 포함하여 구성된다.

[0016] 사용자 모바일 단말(20)에는 금융 결제 보안 기능을 수행하는 어플리케이션이 설치되는데, 이하 상기 어플리케이션이 제공하는 금융 결제 보안 서비스의 일 예를 도 2를 참조하여 구체적으로 설명한다. 도 2는 본 발명의 일 실시예에 따라 모바일 단말에 설치된 금융 결제 보안을 위한 어플리케이션이 실행되는 예를 도시한 예시도이다.

[0017] 상기 어플리케이션을 이용하여 금융 결제 보안 서비스를 이용하기 위해서는 본 서비스를 이용하고자 하는 결제 수단(예를 들어, 일반적인 신용 카드와 같은 결제 수단으로서 직불카드 및 계좌 이체와 같은 기타 다양한 지불 매체적인 의미)를 등록하는 과정이 필요하다. 등록의 대상이 되는 결제 수단은 카드사, 은행 등과 같이 카테고리 별로 분류되고, 카드사 카테고리는 신용 카드 및 체크카드 등으로 하위 카테고리로 분류되고, 대표적인 신용 카드, 체크카드는 기 설정되어 있을 수 있으며, 사용자가 직접 해당 결제 수단을 추가할 수도 있다.

[0018] 도 2에 도시된 실시예를 들어 설명하면, 결제 수단 중 신용 카드에 대하여 본 서비스를 제공 받고자 하는 경우에는, 해당 카드사의 서버(10)에 본 발명에 따른 서비스 등록 신청이 선행되어야 한다.

[0019] 이후, 사용자 모바일 단말(20)에서 보안 어플리케이션이 실행된 상태에서, 사용자는 자신이 소지하고 있는 카드에 대하여 추가 버튼을 터치하여 등록과정을 개시하는데, 사용자가 등록 버튼을 터치하여 카드사 회사(10)의 서버에 서비스 등록 신청 시 입력했던 아이디, 비밀번호 등을 입력하면, 금융 결제 서버(10)로 아이디, 비밀번호 및 모바일 단말의 식별자(예컨대, 전화번호)가 전송된다.

[0020] 이를 수신한 금융 결제 서버(10)에서는 아이디 및 비밀번호로 사용자 인증을 수행하고, 정당 사용자임을 확인하면 모바일 단말 번호를 해당 아이디와 연계하여 저장하고 해당 신용 카드에 대하여 금융 결제 보안 서비스를 활성화한다. 정상 등록이 된 상태에서 사용자는 모바일 단말의 보안 어플리케이션을 이용하여 해당 신용 카드 대한 결제 승인 여부를 결정하는 온(On) 또는 오프(Off) 버튼을 선택할 수 있는데, 온(On)은 해당 신용 카드에 대하여 결제를 승인하는 것이고, 오프(Off)는 해당 신용 카드에 대하여 결제를 승인하지 않는 것이다.

[0021] 이후, 해당 카드의 정당 사용자 또는 제3자가 카드 결제 시, 금융 결제 서버(10)는 서비스 등록 신청 시 저장된 모바일 단말 번호를 이용하여 모바일 단말(20)에 설정된 금융 결제 승인 여부를 확인하고, 이에 따라 해당 카드에 의한 결제 승인 여부를 결정한다.

[0022] 예컨대, 사용자가 모바일 단말(20)에서 오프(Off) 버튼을 선택하여 해당 카드에 대하여 금융 결제 잠금 설정을 한 경우, 금융 결제 서버(10)는 이를 확인하여 해당 카드에 의한 결제를 승인하지 않고, 사용자 단말(20)에는 “잠금 상태 입니다. 스마트 폰 OFF를 해제하시고, 다시 결제해주시기 바랍니다.” 와 같은 메시지가 출력되도록 한다.

[0023] 여기서, 사용자의 모바일 단말(20)은 사용자 소유의 모바일 단말 및 사용자가 사전에 지정하여 이용하는 모바일 단말을 포함하며, 각 금융 결제 서버(10)에 등록된다.

[0024] 한편, 본 발명의 일 실시예 따른 금융 결제 보안 서비스는 해당 카드사 및 은행의 서버(10)가 제공할 수 있는데, 이하 금융 결제 서버(10)가 수행하는 로그인 잠금 설정을 통한 온라인 계정 도용 방지 방법을 도 3 내지 도 5를 참조하여 설명한다. 도 3은 본 발명의 일 실시예에 따라 금융 결제 서버가 수행하는 금융 결제 보안 서비스 방법의 제1 형태를 도시한 도면이고, 도 4는 본 발명의 일 실시예에 따라 금융 결제 서버가 수행하는 금융 결제 보안 서비스 방법의 제2 형태를 도시한 도면이고, 도 5는 본 발명의 일 실시예에 따라 금융 결제 서버가 수행하는 금융 결제 보안 서비스 방법의 제3 형태를 도시한 도면이다.

[0025] 도 3은 금융 결제 서버(10)가 수행하는 금융 결제 보안 서비스 방법의 제1 형태를 도시한 것으로서, 본 명세서에서 금융 결제 서버(10)는 신용카드 또는 체크 카드 등에 의한 결제 요청에 대하여 전반적인 처리를 수행하는 카드사 서버, 온라인 계좌 이체 등에 대한 전반적인 처리를 수행하는 은행 서버, 증권 거래 업무에 대한 전반적인 처리를 수행하는 증권사 서버 등을 포함하는 개념으로 사용된다.

[0026] 이하, 이해를 돕기 위해 카드 결제 시 금융 결제 서버(10)가 제공하는 보안 서비스 방법을 예를 들어 설명하도록 한다. 본 발명에 따른 보안 서비스 방법은 아래에서 설명되는 카드 결제뿐 만 아니라, 계좌 이체, 증권 거래 업무 등 기타 다양한 금융 결제에도 적용될 수 있음은 물론이다.

[0027] 사용자가 카드 결제를 통해 카드사 서버(10)로 결제 승인 요청을 하면, 결제 승인 요청을 받은 카드사 서버(10)는 해당 카드의 정상 사용자의 모바일 단말(20)로 결제 승인 잠금 여부를 조회한다(S310).

[0028] 해당 카드의 정상 사용자는 카드사 서버의 데이터베이스에 아이디, 패스워드, 주민등록번호, 전화번호, 이메일 주소, 메신저 주소 등의 사용자 정보를 등록한 자로서 카드사 서버(10)는 해당 카드에 의한 결제 승인 요청을 접수하면, 데이터베이스를 검색하여 해당 카드의 정상 사용자의 등록된 정보를 획득할 수 있고, 등록된 정보에 포함된 모바일 단말(20)로 이동통신망, 무선 인터넷 망과 같은 무선 통신망을 통해 결제 승인 잠금 여부를 실시간으로 조회할 수 있다.

[0029] 해당 카드의 정상 사용자는 모바일 단말(20)에 설치된 보안 어플리케이션에 의해 해당 카드의 결제 승인 잠금 설정 여부를 선택할 수 있는데, 사용자에 의해 설정된 결제 승인 잠금 여부에 관한 정보는 카드사 서버(10)에 의해 실시간으로 조회되어, 모바일 단말(20)에서 카드사 서버(20)로 전송되고, 카드사 서버(20)는 전송된 결제 승인 잠금 정보에 따라 카드 결제를 승인할 것인지 여부를 결정한다(S320).

[0030] 예를 들어, 조회된 결과 해당 카드의 결제 승인 잠금 설정이 되어 있는 경우에는 카드사 서버(10)는 해당 카드에 의한 결제를 승인하지 않고 (S331), 해당 카드의 결제 승인 잠금 설정이 해제된 경우라면 해당 카드에 의한 결제를 승인한다 (S333).

[0031] 만약, 카드사 서버(10)가 해당 카드의 결제 승인을 거절한 경우라면, 해당 카드의 정상 사용자의 모바일 단말(20)로 이동 통신망과 무선 인터넷 망을 통해 승인 거절 정보를 전송한다(S340). 이때, 카드사 서버(20)는 정상 사용자에게 카드 분실 신고 안내 등의 사고처리 과정을 수행할 수도 있다.

[0032] 사고처리 과정에서 카드 분실 신고 안내는 카드사 서버(10)의 데이터베이스에 등록된 사용자 정보에 포함된 정상 사용자의 모바일 단말, 이메일, 메신저 등으로 통보될 수 있다.

[0033] 도 4는 카드사 서버가 수행하는 금융 결제 보안 서비스 방법의 제2 형태를 도시한 것으로서, 해당 카드의 정상 사용자가 모바일 단말(20)에 설치된 어플리케이션에서 등록된 해당 카드에 대하여 결제 승인 설정을 하면, 특정 카드에 의한 결제를 승인하는 결제 승인 정보가 모바일 단말(20)에서 카드사 서버(10)로 전송되고, 전송된 해당 카드의 결제 승인 정보는 카드사 서버(10)의 데이터베이스에 저장되거나, 또는 캐쉬 메모리에 임시 저장된다 (S410).

[0034] 여기서, 결제 승인 정보에는 모바일 단말(20)에서 결제 승인 설정이 된 이후, 또는 카드사 서버(10)가 해당 카드의 결제 승인 정보를 전송 받은 이후부터 기 정의된 시간(예를 들어, 30초, 1분 등) 동안에만 해당 카드의 결제가 승인된다는 정보가 포함되는 것이 바람직하다.

[0035] 상기 두 가지 방법 중, 모바일 단말(20)에서 결제 승인 설정이 된 이후 기 정의된 시간 동안에만 해당 카드의 결제를 승인하는 방식을 사용하기 위해서는 모바일 단말(20)에서 결제 승인 설정이 된 시각의 시간 정보까지 카드사 서버(10)로 전송되는 것이 바람직하다.

[0036] 이후, 사용자가 해당 카드를 이용하여 결제를 하는 경우, 해당 카드에 의한 결제 요청을 받은 카드사 서버(10)는 해당 카드의 결제 요청을 받은 시각이 해당 카드의 결제가 승인되는 기 정의된 시간 범위 내인지 여부를 판단하고(S420), 판단 결과, 해당 카드의 결제 요청을 받은 시각이 기 정의된 시간 범위 내에 있으면 해당 카드의 결제를 승인하고(S431), 그렇지 않은 경우에는 해당 카드의 결제 승인을 거절한다(S433).

[0037] 해당 카드의 결제 승인이 거절된 경우(S433), 카드사 서버(10)는 해당 카드의 정상 사용자에게 승인 거절 정보를 전송한다(S440).

[0038] 예를 들어, 모바일 단말(20)에서 특정 카드에 대하여 11시 5분에 결제 승인 설정이 되었다면, 11시 5분에 결제 승인 설정이 되었다는 시간 정보와 함께, 해당 카드의 결제 승인 설정 정보가 카드사 서버(10)로 전송되고, 이 정보는 카드사 서버(10)의 데이터베이스 등에 저장된다.

[0039] 이후, 11시 5분 20초에 사용자가 해당 카드를 이용하여 결제를 요청하면, 카드사 서버(10)는 해당 카드에 의한 결제를 승인하고, 만약 결제 요청을 받은 시각이 11시 5분 40초인 경우라면 해당 카드의 결제 승인을 거절하고(결제 승인이 허용되는 기 정의된 시간이 30초인 경우), 승인 거절 정보를 해당 카드의 정상 사용자에게 전송한다.

[0040] 도 5는 카드사 서버(10)가 수행하는 금융 결제 보안 서비스 방법의 제3 형태를 도시한 것으로서, 해당 카드의 정상 사용자가 모바일 단말(20)에 설치된 어플리케이션에서 등록된 해당 카드에 대하여 결제 승인 잠금 설정(off 설정)을 하면, 해당 카드에 의한 결제 승인이 거절된다는 결제 승인 잠금 정보가 모바일 단말(20)에서 카드사 서버(10)로 전송되고, 전송된 해당 카드의 결제 승인 잠금 정보는 카드사 서버(10)의 데이터베이스에 저장되거나, 또는 캐쉬 메모리에 임시 저장된다(S510).

[0041] 이후, 해당 카드를 이용하여 정상 사용자 또는 제3자가 결제를 요청하면, 결제 요청을 받은 카드사 서버(10)는 해당 카드에 의한 결제 승인을 거절하고(S520), 해당 카드의 정상 사용자의 모바일 단말(20)로 이동 통신망과 무선 인터넷 망을 통해 승인 거절 완료 정보를 전송한다(S530). 이때, 카드사 서버(20)는 정상 사용자에게 카드 분실 신고 안내 등의 사고처리 과정을 수행할 수는 앞에서 설명한 것과 마찬가지이다.

[0042] 그리고 해당 계정의 정상 사용자가 모바일 단말(20)에 설치된 어플리케이션에서 해당 카드에 대하여 결제 승인 잠금 설정을 해제하면, 해당 카드에 의한 결제가 승인된다는 결제 승인 정보가 모바일 단말(20)에서 카드사 서버(10)로 전송되고, 전송된 결제 승인 정보는 카드사 서버(10)의 데이터베이스 또는 캐쉬 메모리 등에 저장된다(S540).

[0043] 이후, 해당 카드를 이용하여 정상 사용자 또는 제3자가 결제를 요청하면, 결제 요청을 받은 카드사 서버(10)는 해당 카드에 결제를 승인한다(S550).

[0044] 도 6을 참조하여 본 발명의 다른 실시예에 따른 금융 결제 보안 서비스 방법이 수행되는 금융 결제 보안 서비스 시스템을 설명한다. 도 6은 본 발명의 다른 실시예에 따른 금융 결제 보안 서비스 방법이 수행되는 금융 결제 보안 서비스 시스템의 구성을 도시한 구성도이다.

[0045] 도 6을 참조하면, 본 발명의 다른 실시예에 따라 금융 결제 보안 서비스 시스템은, 카드사 서버(10), 정상 사용자 모바일 단말(20), 보안 서버(30)를 포함하여 구성된다.

[0046] 상기의 본 발명의 다른 실시예 따른 금융 결제 보안 서비스는 카드사 서버(10)와, 보안 서버(30)가 연동하여 제공할 수 있는데, 이하 카드사 서버(10)와 보안 서버(30)가 수행하는 금융 결제 보안 서비스 방법을 도 7 내지 도 9를 참조하여 설명한다. 도 7은 본 발명의 다른 실시예에 따라 보안 서버가 수행하는 금융 결제의 제1 형태를 도시한 도면이고, 도 8은 본 발명의 다른 실시예에 따라 보안 서버가 수행하는 금융 결제 보안 서비스 방법의 제2 형태를 도시한 도면이고, 도 9는 본 발명의 다른 실시예에 따라 보안 서버가 수행하는 금융 결제 보안 서비스 방법의 제3 형태를 도시한 도면이다.

[0047] 도 7은 보안 서버가 카드사 서버와 연동하여 수행하는 금융 결제 보안 서비스 방법의 제1 형태를 도시한 것으로서, 사용자가 카드 결제를 통해 카드사 서버(10)로 결제 승인 요청을 하면, 결제 요청을 받은 카드사 서버(10)는 보안 서버(30)로 해당 카드의 결제 승인 잠금 설정 정보를 요청하고, 보안 서버(40)는 해당 카드의 정상 사용자 모바일 단말(20)로 결제 승인 잠금 여부를 조회한다(S710).

[0048] 해당 카드의 정상 사용자는 카드사 서버(10)의 데이터베이스에 아이디, 패스워드, 주민등록번호, 전화번호, 이메일 주소, 메신저 주소 등의 사용자 정보를 등록한 자로서, 보안 서버(30)는 카드사 서버(20)와 연동하여 사용자 정보를 공유할 수 있다. 해당 카드로 결제 요청이 접수되면, 카드사 서버(10)는 데이터베이스를 검색하여 해

당 계정의 정상 사용자의 등록된 정보를 획득할 수 있고, 해당 카드의 결제 승인 잠금 설정 정보를 보안 서버(30)에 요청하면서 상기 등록된 정보를 함께 전송한다.

[0049] 보안 서버(30)는 등록된 정보에 포함된 모바일 단말(20)로 이동통신망, 무선 인터넷 망과 같은 무선 통신망을 통해 결제 승인 잠금 여부를 실시간으로 조회할 수 있다.

[0050] 해당 카드의 정상 사용자는 모바일 단말(20)에 설치된 어플리케이션에 의해 해당 카드의 결제 승인 잠금 설정 여부를 선택할 수 있는데, 사용자에 의해 설정된 결제 승인 잠금 여부에 관한 정보는 조회되어, 모바일 단말(20)에서 보안 서버(30)로 전송되고, 보안 서버(30)는 전송된 결제 승인 잠금 여부에 관한 정보를 카드사 서버(10)에 다시 전송한다(S720).

[0051] 카드사 서버(10)는 전송된 결제 승인 잠금 여부에 관한 정보에 따라 결제 요청된 해당 카드의 결제를 승인할 것인지 여부를 결정한다.

[0052] 예를 들어, 조회된 결과 해당 카드의 결제 승인 잠금 설정이 되어 있는 경우에는 카드사 서버(10)는 해당 카드에 의한 결제를 거절하고, 결제 승인 잠금 설정이 해제된 경우라면 해당 카드의 결제를 승인한다.

[0053] 만약, 카드사 서버(10)가 해당 카드의 결제를 거절한 경우라면, 해당 카드의 정상 사용자의 모바일 단말(20)로 이동 통신망과 무선 인터넷 망을 통해 결제 승인 거절 정보를 전송한다(S340). 이때, 카드사 서버(10)는 정상 사용자에게 카드 분실 신고 안내 등의 사고처리 과정을 수행할 수도 있다.

[0054] 사고처리 과정에서 분실 신고 안내는 카드사 서버(10)의 데이터베이스에 등록된 사용자 정보에 포함된 정상 사용자의 모바일 단말, 이메일, 메신저 등으로 통보될 수 있다.

[0055] 도 8은 보안 서버가 카드사 서버와 연동하여 수행하는 금융 결제 보안 서비스 방법의 제2 형태를 도시한 것으로서, 해당 카드의 정상 사용자가 모바일 단말(20)에 설치된 어플리케이션에서 해당 카드에 대하여 결제 승인 설정을 하면, 해당 카드에 의한 결제를 승인하는 정보가 모바일 단말(20)에서 보안 서버(30)로 전송되고, 전송된 결제 승인 정보는 보안 서버(30)를 거쳐 카드사 서버(10)로 전송된다(S810).

[0056] 여기서, 결제 승인 정보에는 모바일 단말(20)에서 결제 승인 설정이 된 이후, 또는 카드사 서버(10)가 해당 카드의 결제 승인 정보를 전송 받은 이후부터 기 정의된 시간(예를 들어, 30초, 1분 등) 동안에만 해당 카드의 결제가 승인된다는 정보가 포함되는 것이 바람직하다.

[0057] 상기 두 가지 방법 중, 모바일 단말(20)에서 결제 승인 설정이 된 이후 기 정의된 시간 동안에만 해당 카드의 결제를 승인하는 방식을 사용하기 위해서는 모바일 단말(20)에서 결제 승인 설정이 된 시각의 시간 정보까지 카드사 서버(10)로 전송되는 것이 바람직하다.

[0058] 이후, 사용자가 해당 카드를 이용하여 결제를 하는 경우, 결제 요청을 받은 카드사 서버(10)는 해당 카드의 결제 요청을 받은 시각이 해당 카드의 결제가 승인되는 기 정의된 시간 범위 내인지 여부를 판단하고, 판단 결과, 해당 카드의 결제 요청을 받은 시각이 기 정의된 시간 범위 내에 있으면 해당 카드의 결제를 승인하고, 그렇지 않은 경우에는 해당 카드의 결제 승인을 거절하고, 승인 거절 정보를 해당 카드의 정상 사용자에게 전송한다.

[0059] 예를 들어, 모바일 단말(20)에서 해당 카드에 대하여 11시 5분에 결제 승인이 설정되었다면, 11시 5분에 결제 승인 설정이 되었다는 시간 정보와 함께, 해당 카드의 결제 승인 정보가 보안 서버(30)로 전송되고, 이 정보는 보안 서버(30)를 거쳐 카드사 서버(10)로 전송된다.

[0060] 이후, 11시 5분 20초에 사용자가 해당 카드로 결제를 요청하면, 카드사 서버(10)는 해당 카드의 결제를 승인하고, 만약 사용자로부터 결제 요청을 받은 시각이 11시 5분 40초인 경우라면 해당 카드의 결제를 거절한다(로그인이 허용되는 기 정의된 시간이 30초인 경우).

[0061] 도 9는 보안 서버가 카드사 서버와 연동하여 수행하는 금융 결제 보안 서비스 방법의 제3 형태를 도시한 것으로서, 해당 카드의 정상 사용자가 모바일 단말(20)에 설치된 어플리케이션에서 해당 카드에 대하여 결제 승인 잠금 설정을 하면, 결제 승인 잠금 정보가 모바일 단말(20)에서 보안 서버(30)로 전송되고, 전송된 해당 카드의 결제 승인 잠금 정보는 보안 서버(30)의 데이터베이스에 저장된다(S910).

[0062] 이후, 사용자가 해당 카드로 결제를 요청하면, 결제 요청을 받은 카드사 서버(10)는 보안 서버(30)로 해당 카드의 결제 승인 잠금 설정 정보를 요청하고, 보안 서버(30)는 카드사 서버(10)로 해당 카드의 결제 승인 잠금 정보를 전송한다(S920).

[0063] 결제 승인 잠금 정보를 전송 받은 카드사 서버(10)는 해당 카드의 결제 승인을 거절하고, 해당 카드의 정상 사용자의 모바일 단말(20)로 이동 통신망과 무선 인터넷 망을 통해 거절 완료 정보를 전송한다. 이때, 카드사 서버(10)는 정상 사용자에게 분실 신고 안내를 통보하는 등의 사고처리 과정을 수행할 수는 앞에서 설명한 것과 마찬가지이다.

[0064] 그리고 해당 카드의 정상 사용자가 모바일 단말(20)에 설치된 어플리케이션에서 해당 카드에 대하여 결제 승인 잠금 설정을 해제하면, 해당 카드에 대한 결제 승인 정보가 모바일 단말(20)에서 보안 서버(40)로 전송되고, 전송된 해당 카드의 결제 승인 정보는 보안 서버(30)의 데이터베이스에 저장된다(S930).

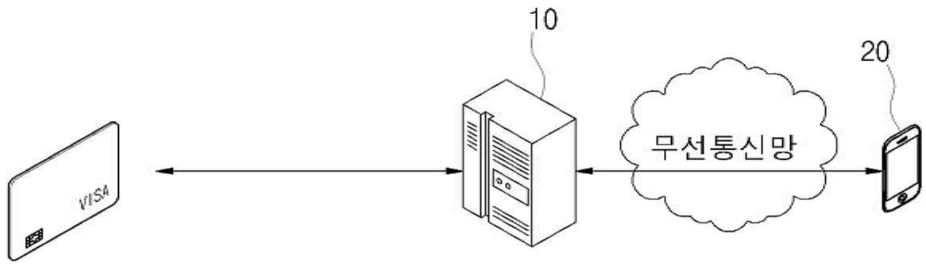
[0065] 이후, 사용자가 해당 카드로 결제를 요청하면, 결제 요청을 받은 카드사 서버(10)는 보안 서버(30)로 해당 카드의 결제 승인 잠금 설정 정보를 요청하고, 보안 서버(30)는 카드사 서버(10)로 해당 카드의 결제 승인 정보를 전송한다(S940).

[0066] 그리고 해당 카드의 결제 승인 정보를 전송 받은 카드사 서버(10)는 해당 카드의 결제를 승인한다.

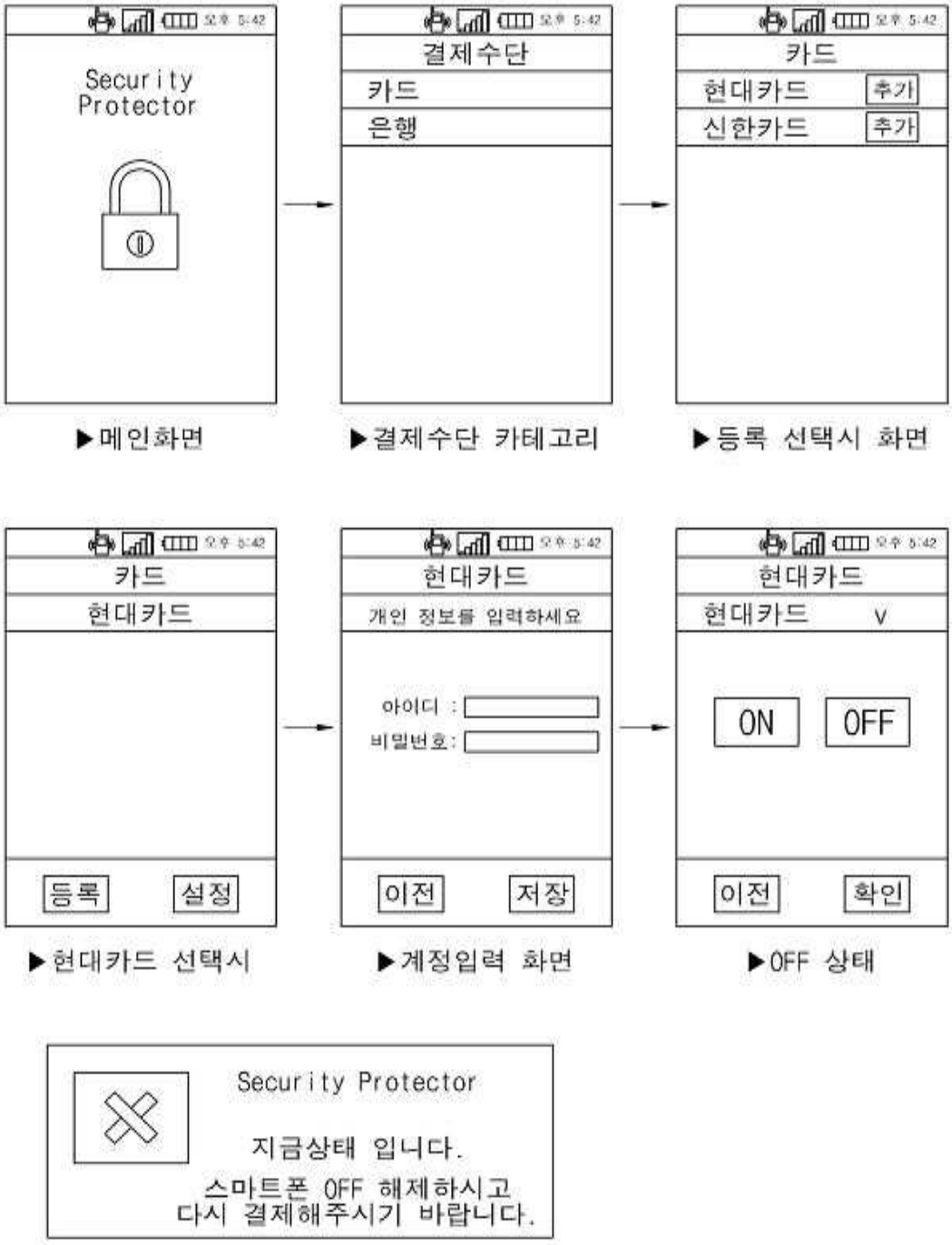
[0067] 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 본 발명의 보호범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구의 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

도면

도면1

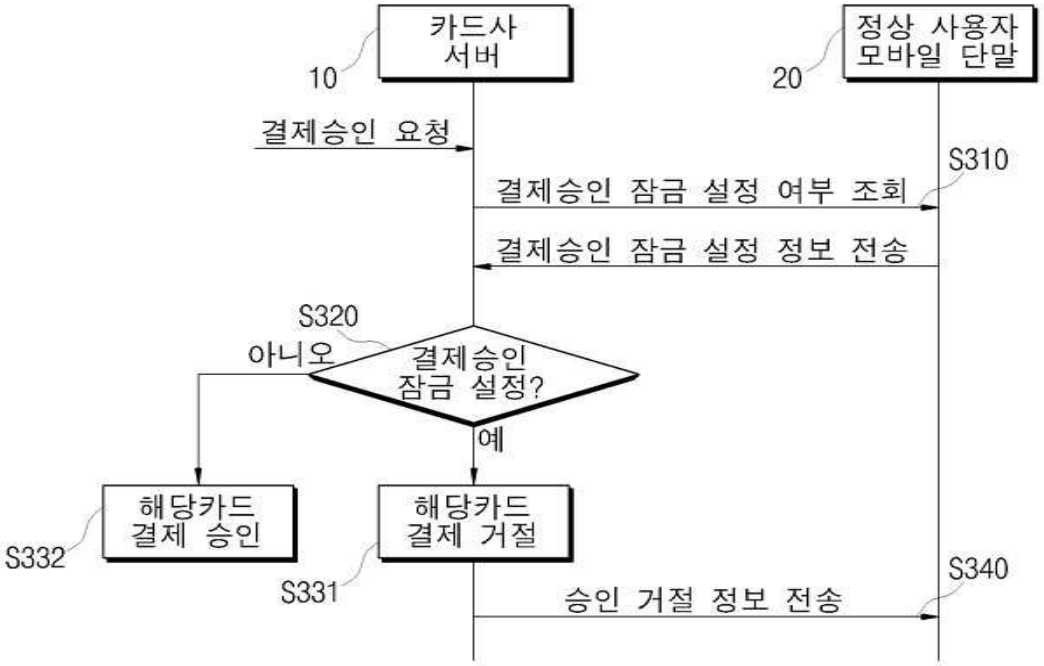


도면2

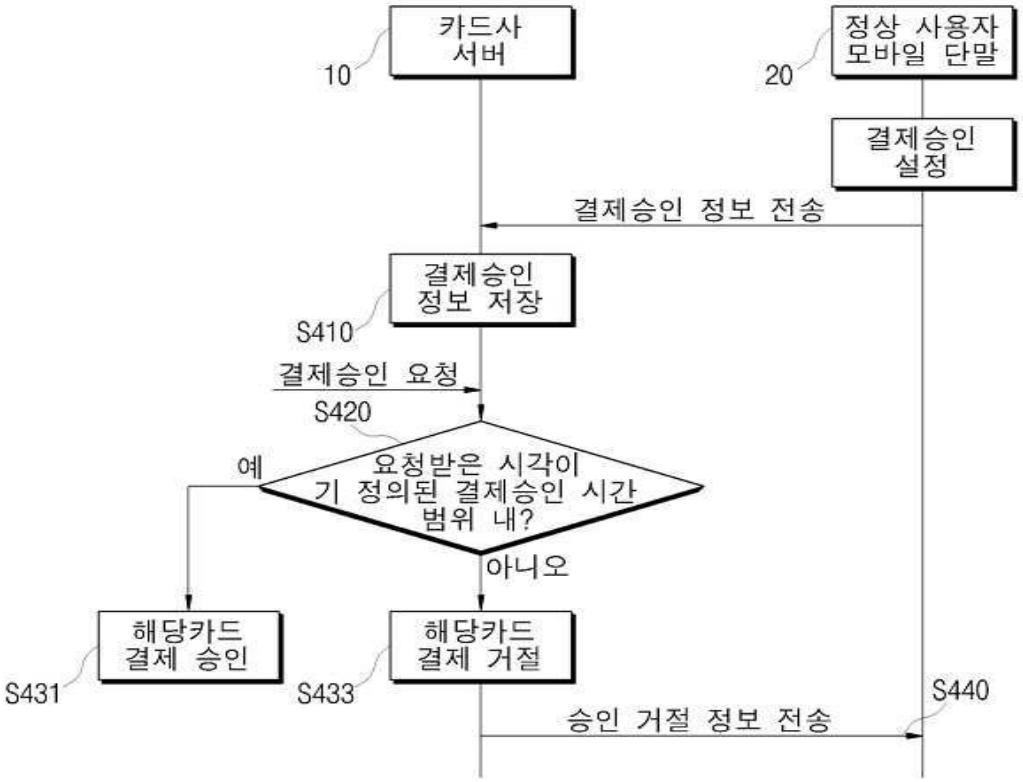

Security Protector
결제수단
카드
은행
카드
현대카드
추가
신한카드
추가
▶메인화면
▶결제수단 카테고리
▶등록 선택시 화면
카드
현대카드
등록
설정
▶현대카드 선택시
현대카드
개인 정보를 입력하세요
아이디 :
비밀번호:
이전
저장
▶계정입력 화면
현대카드
현대카드 v
ON
OFF
이전
확인
▶OFF 상태

Security Protector
지금상태 입니다.
스마트폰 OFF 해제하시고
다시 결제해주시기 바랍니다.

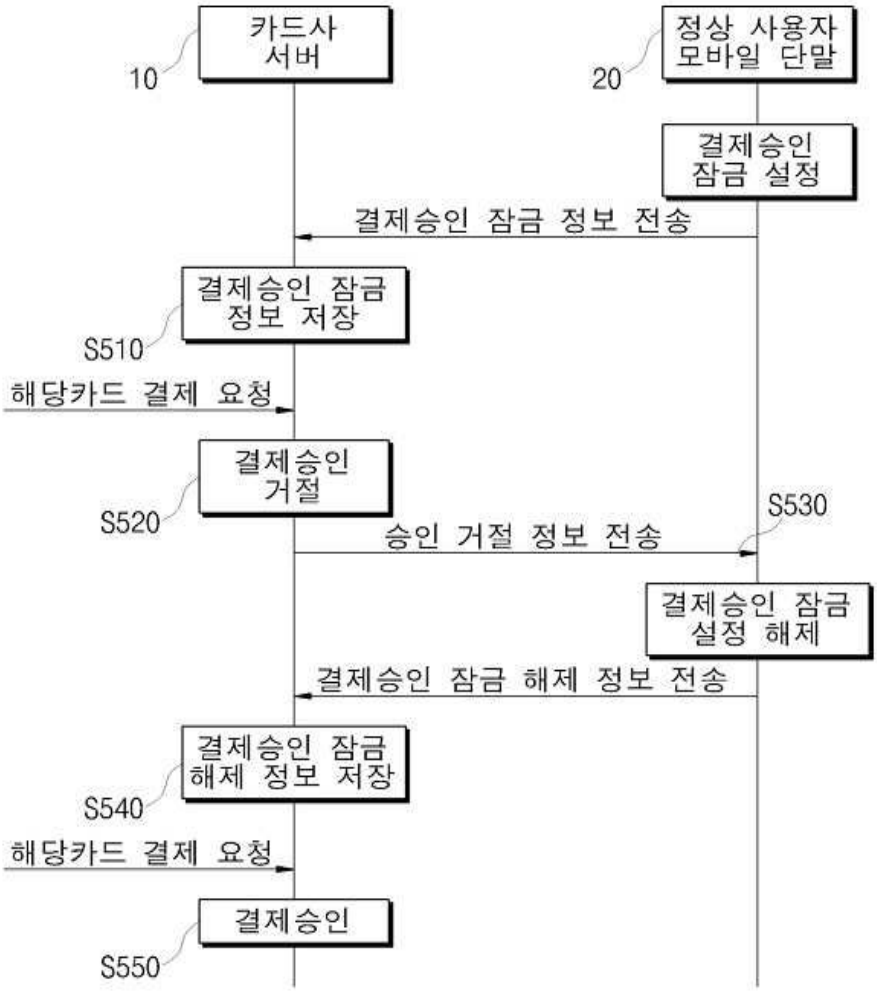
도면3


카드사
서버
10
정상 사용자
모바일 단말
20
결제승인 요청
S310
결제승인 잠금 설정 여부 조회
결제승인 잠금 설정 정보 전송
S320
아니오
결제승인
잠금 설정?
예
해당카드
결제 승인
S332
해당카드
결제 거절
S331
S340
승인 거절 정보 전송

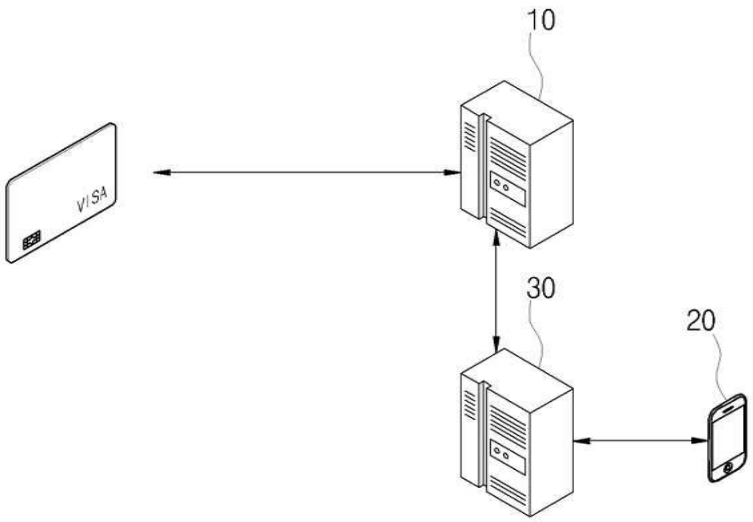
도면4


카드사
서버
10
정상 사용자
모바일 단말
20
결제승인
설정
결제승인 정보 전송
결제승인
정보 저장
S410
결제승인 요청
S420
예
요청받은 시각이
기 정의된 결제승인 시간
범위 내?
아니오
해당카드
결제 승인
S431
해당카드
결제 거절
S433
S440
승인 거절 정보 전송

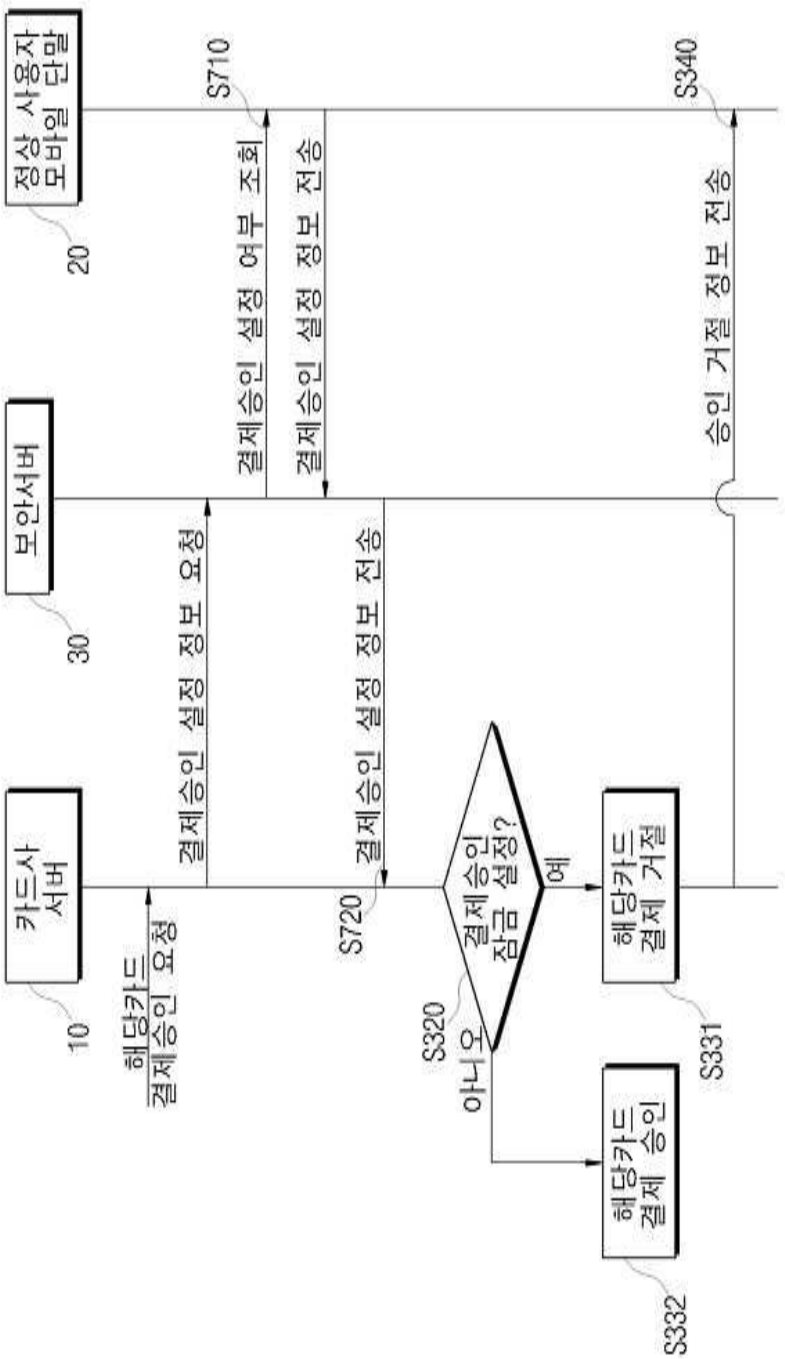
도면5


카드사 서버
10
정상 사용자 모바일 단말
20
결제승인 잠금 설정
결제승인 잠금 정보 전송
결제승인 잠금 정보 저장
S510
해당카드 결제 요청
결제승인 거절
S520
S530
승인 거절 정보 전송
결제승인 잠금 설정 해제
결제승인 잠금 해제 정보 전송
결제승인 잠금 해제 정보 저장
S540
해당카드 결제 요청
결제승인
S550

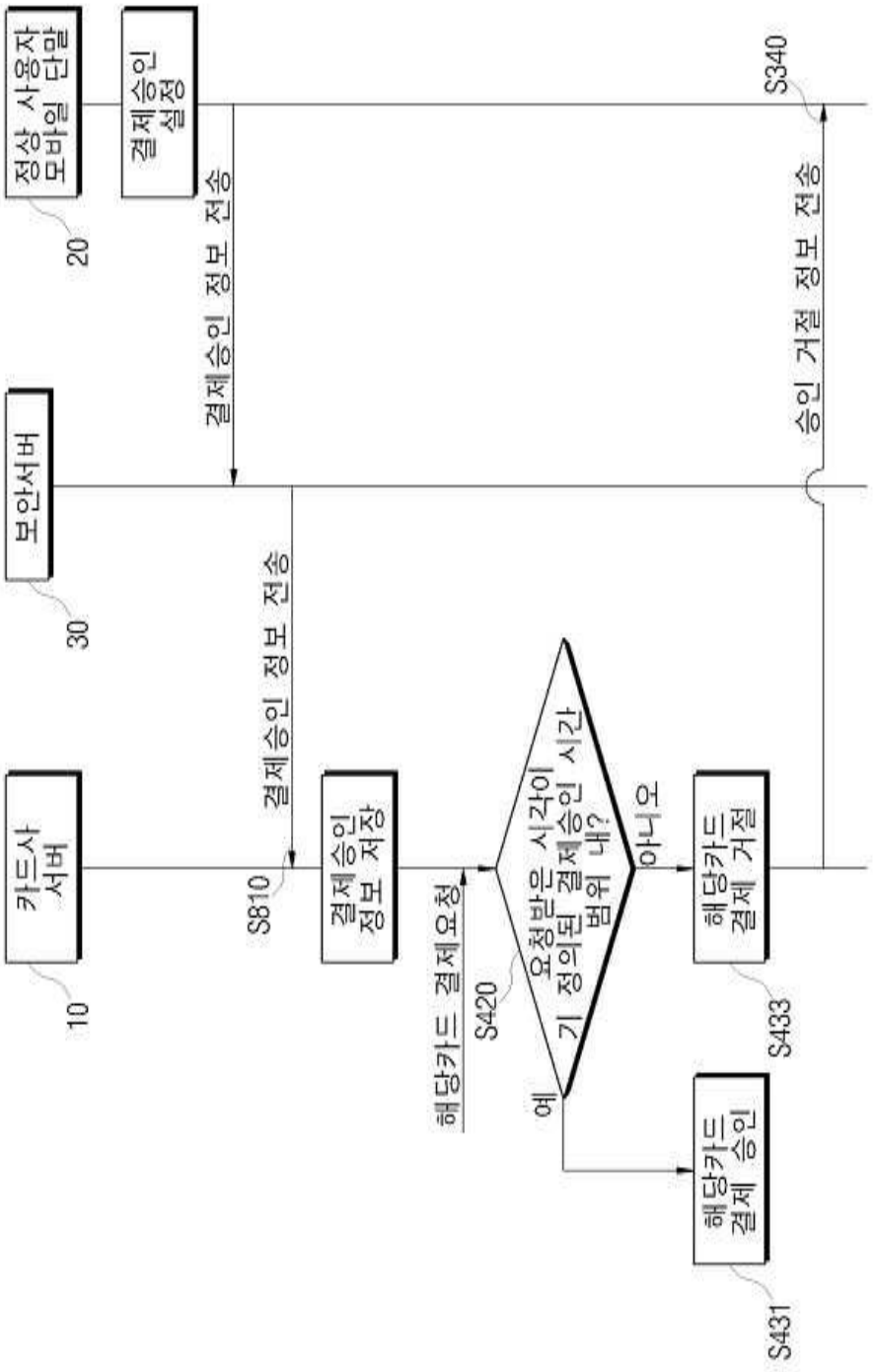
도면6


10
VISA
30
20

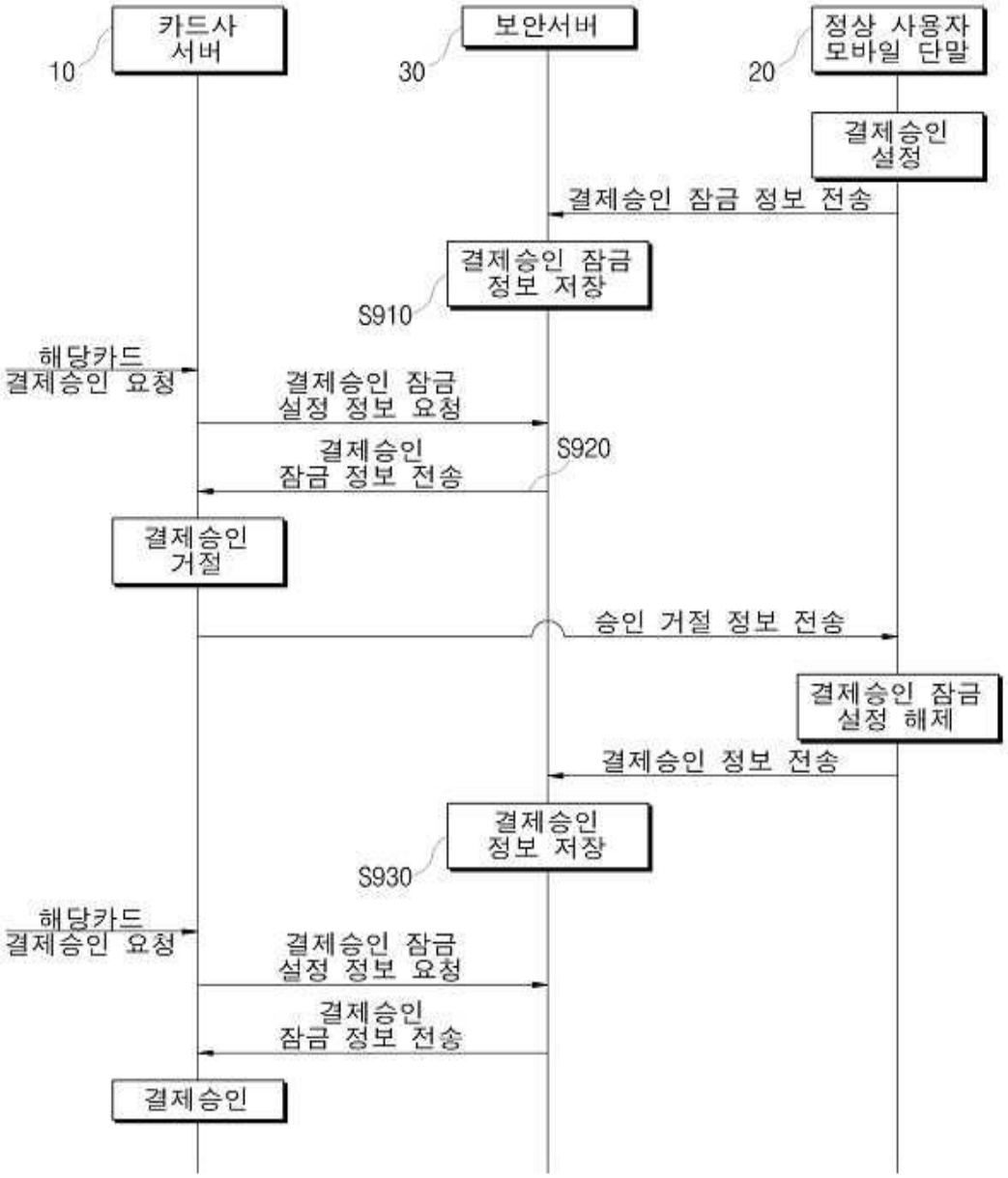
도면7


정상 사용자 모바일 단말
20
보안서버
30
카드사 서버
10
S710
결제승인 설정 여부 조회
결제승인 설정 정보 전송
S340
승인 거절 정보 전송
결제승인 설정 정보 요청
해당카드 결제승인 요청
결제승인 설정 정보 전송
S720
결제승인 잠금 설정?
S320
예
아니오
해당카드 결제 거절
S331
해당카드 결제 승인
S332

도면8


정상 사용자 모바일 단말
20
결제승인 설정
결제승인 정보 전송
S340
승인 거절 정보 전송
보안서버
30
결제승인 정보 전송
S810
카드사 서버
10
결제승인 정보 저장
해당카드 결제요청
S420
요청받은 시각이 기 정의된 결제승인 시간 범위 내?
예
아니오
해당카드 결제 승인
S431
해당카드 결제 거절
S433

도면9


카드사 서버
10
보안서버
30
정상 사용자 모바일 단말
20
결제승인 설정
결제승인 잠금 정보 전송
결제승인 잠금 정보 저장
S910
해당카드 결제승인 요청
결제승인 잠금 설정 정보 요청
결제승인 잠금 정보 전송
S920
결제승인 거절
승인 거절 정보 전송
결제승인 잠금 설정 해제
결제승인 정보 전송
결제승인 정보 저장
S930
해당카드 결제승인 요청
결제승인 잠금 설정 정보 요청
결제승인 잠금 정보 전송
결제승인