



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0138891
(43) 공개일자 2016년12월06일

(51) 국제특허분류(Int. Cl.)
G06Q 20/38 (2012.01) G06Q 20/32 (2012.01)
(52) CPC특허분류
G06Q 20/38215 (2013.01)
G06Q 20/3221 (2013.01)
(21) 출원번호 10-2016-0031364
(22) 출원일자 2016년03월16일
심사청구일자 2016년03월16일
(30) 우선권주장
1020150073158 2015년05월26일 대한민국(KR)

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
성순화
대전광역시 유성구 은구비남로 34, 새미래아파트
812-802 (노은동, 열매마을8단지)
(74) 대리인
김원준

전체 청구항 수 : 총 9 항

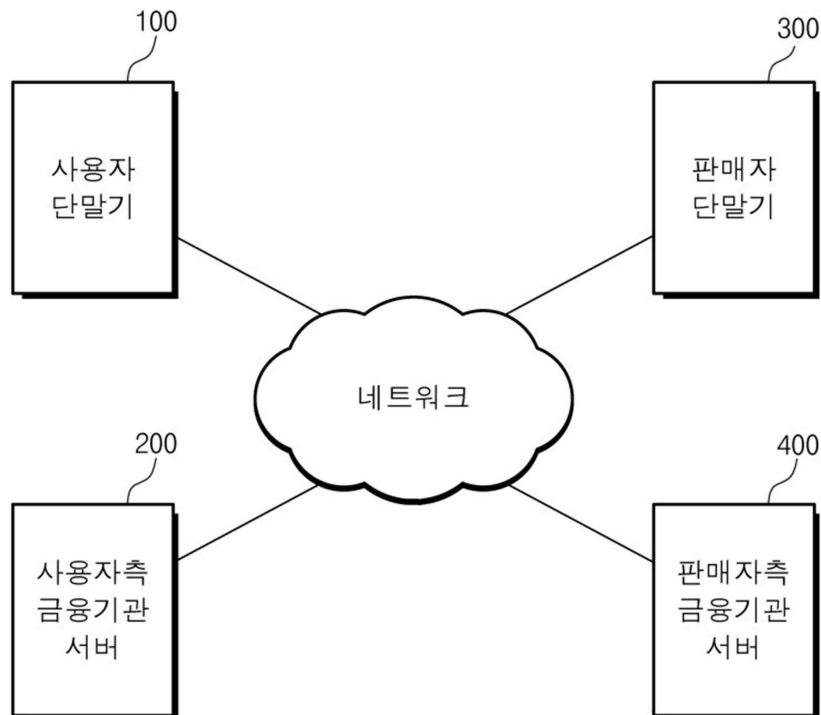
(54) 발명의 명칭 웹을 기반으로 하는 모바일 결제 방법

(57) 요약

본 발명은 사용자가 주도적으로 거래를 인증하며 거래에 관여하는 다수의 주체들이 인증 절차에 개입하는 것에 의해 인증 시 사용자의 정보 유출 가능성을 낮출 수 있으며, 결제를 위한 추가적인 단말기를 필요로 하지 않아 보다 간편화된 웹을 기반으로 하는 모바일 결제 방법에 관한 것으로, 보다 상세하게는 (A) 사용자로부터 온라인

(뒷면에 계속)

대표도 - 도2



또는 오프라인 상점에서 선택된 상품 또는 서비스에 대한 대금 결제를 위해 신용카드 결제 또는 계좌 이체가 선택되는 단계; (B) 상기 (A) 단계의 주문정보에 대해 판매자가 판매자측 금융기관 서버에 인증하는 단계; (C) 상기 (B) 단계의 인증이 성공하면 상기 (A) 단계의 주문정보에 대해 사용자와 사용자측 금융기관 서버가 상호 인증하는 단계; (D) 상기 (C) 단계의 상호 인증이 성공하면, 사용자측 금융기관 서버가 판매자측 금융기관 서버에 상기 주문에 대한 결제를 통보하는 단계; 및 (E) 결제를 통보받은 판매자측 금융기관 서버가 판매자에게 결제 승인 메시지를 전달하여 결제가 완료되는 단계;를 포함하는 것을 특징으로 하는 모바일 결제 방법에 관한 것이다.

(52) CPC특허분류

G06Q 20/3227 (2013.01)

G06Q 20/3829 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 2014-0603-02

부처명 미래창조과학부

연구관리전문기관 한국연구재단

연구사업명 2015년여성과학기술인R&D경력복귀지원사업

연구과제명 사용자 중심 결제 시스템을 위한 보안 서비스

기 여 율 1/1

주관기관 한국여성과학기술인지원센터

연구기간 2015.03.01 ~ 2015.12.31

명세서

청구범위

청구항 1

- (A) 사용자로부터 온라인 또는 오프라인 상점에서 선택된 상품 또는 서비스에 대한 대금 결제를 위해 신용카드 결제 또는 계좌 이체가 선택되는 단계;
- (B) 상기 (A) 단계에 선택된 주문정보에 대해 판매자가 판매자측 금융기관 서버에 인증하는 단계;
- (C) 상기 (B) 단계의 인증이 성공하면 상기 (A) 단계의 주문정보에 대해 사용자와 사용자측 금융기관 서버가 상호 인증하는 단계;
- (D) 상기 (C) 단계의 상호 인증이 성공하면, 사용자측 금융기관 서버가 판매자측 금융기관 서버에 상기 주문에 대한 결제를 통보하는 단계; 및
- (E) 결제를 통보받은 판매자측 금융기관 서버가 판매자에게 결제 승인 메시지를 전달하여 결제가 완료되는 단계;
- 를 포함하는 것을 특징으로 하는 웹을 기반으로 하는 모바일 결제 방법.

청구항 2

제 1 항에 있어서,

상기 (B) 단계의 인증은 암호화된 판매자의 계좌 정보를 포함한 판매자 정보와 상기 주문에 대한 정보가 포함된 인증서를 판매자의 비밀키로 서명하는 것에 의한 거래 인증을 포함하는 것을 특징으로 하는 웹을 기반으로 하는 모바일 결제 방법.

청구항 3

제 1 항에 있어서,

상기 (C) 단계의 상기 주문정보에 대한 사용자와 사용자측 금융기관 서버의 상호 인증은,

암호화된 사용자의 계좌정보를 포함한 사용자 정보와 상기 주문에 대한 정보가 포함된 인증서를 사용자의 비밀키로 서명하는 것에 의한 거래 인증을 포함하는 것을 특징으로 하는 웹을 기반으로 하는 모바일 결제 방법.

청구항 4

제 1 항에 있어서,

상기 (C) 단계와 (D) 단계의 사이에,

사용자에 대해 판매자측 금융기관 서버가 판매자 정보 및 주문정보를 사용하여 상기 거래를 인증하는 단계를 추가로 포함하는 것을 특징으로 하는 웹을 기반으로 하는 모바일 결제 방법.

청구항 5

제 1 항에 있어서,

상기 (D) 단계 이후, (E) 단계와 별도로 사용자측 금융기관 서버가 사용자에게 결제 완료를 통보하는 단계를 추가로 포함하는 것을 특징으로 하는 웹을 기반으로 하는 모바일 결제 방법.

청구항 6

제 1 항 내지 제 5 항 중 어느 한 항에 있어서,

상기 (C) 단계의 주문정보에 대한 사용자와 사용자측 금융기관 서버의 상호 인증은,

데이터베이스 및 프로세서를 포함하며 단말기 및 서버와 통신하는 컴퓨팅 장치에 의해 이루어지며,

(a) 사용자의 단말기로부터 수신받은 사용자의 아이디 및 비밀번호와 상기 사용자의 거래에 관하여 사전에 등록된 고유 정보를 이용하여 상기 사용자 단말기로부터 수신된 사용자 정보의 진정성을 검사하는 단계;

(b) 상기 사용자 정보가 진정한 것으로 확인되면, ① 상기 사용자측 금융기관 서버로 상기 사용자 정보를 처리하여 얻은 제 1 정보를 송신하고, ② 상기 사용자측 금융기관 서버로부터 상기 제 1 정보를 처리하여 생성된 제 2 정보를 수신받은 후, ③ 상기 제 2 정보를 기초로 상기 사용자측 금융기관 서버 인증을 결정하는, 사용자에게 대한 서버 인증 단계; 및

(c) 상기 서버에 대한 인증이 성공하면, ① 상기 사용자를 인증하기 위해 상기 제 2 정보를 처리하여 얻은 제 3 정보를 상기 서버로 송신하고, ② 상기 제 3 정보를 기초로 상기 사용자 인증을 결정하는, 서버에 대한 사용자 인증 단계;

를 포함하여 이루어지는 것을 특징으로 하는 웹을 기반으로 하는 모바일 결제 시스템.

청구항 7

제 6 항에 있어서,

상기 사용자 정보의 진정성을 검사하는 단계는,

상기 데이터베이스로부터, 상기 사용자의 아이디에 해쉬 함수를 적용하여 얻은 제 1 해쉬 데이터 및 상기 제 1 해쉬 데이터와 상기 사용자의 비밀번호를 XOR 연산한 제 2 해쉬 데이터를 불러오는 단계;

상기 제 2 해쉬 데이터와 상기 사용자 단말기로부터 수신된 비밀번호를 XOR 연산하여 제 1 검사 데이터를 생성하는 단계; 및

상기 제 1 검사 데이터와 상기 제 1 해쉬 데이터를 비교하여, 상기 제 1 검사 데이터와 상기 제 1 해쉬 데이터가 일치하면 상기 사용자 정보가 진정한 것으로 결정하는 단계;

를 포함하는 것을 특징으로 하는 웹을 기반으로 하는 모바일 결제 시스템.

청구항 8

제 7 항에 있어서,

상기 사용자에게 대한 서버 인증 단계는,

① 상기 제 1 검사 데이터와 제 1 논스(nonce) 데이터를 XOR 연산하여 제 1 암호화 데이터를 생성하는 소단계 및 제 1 정보로서 상기 사용자의 아이디와 상기 제 1 암호화 데이터를 상기 사용자측 금융기관 서버로 송신하는 소단계로 이루어지는 제 1 정보 송신 단계;

② 상기 사용자의 아이디에 해쉬 함수를 적용하여 제 3 해쉬 데이터를 생성하는 소단계, 상기 제 1 암호화 데이터와 상기 제 3 해쉬 데이터를 XOR 연산하여 제 2 암호화 데이터를 생성하는 소단계, 상기 제 3 해쉬 데이터와 상기 제 1 논스 데이터를 XOR 연산하여 제 3 암호화 데이터를 생성하는 소단계, 상기 제 1 암호화 데이터와 상기 제 3 암호화 데이터 및 제 1 세션키를 연결(concatenation)한 데이터에 해쉬 함수를 적용하여 제 4 암호화 데이터를 생성하는 소단계,에 의해 상기 사용자측 금융기관 서버가 생성한 상기 제 3 암호화 데이터 및 상기 제 4 암호화 데이터를 제 2 정보로서 상기 사용자측 금융기관 서버로부터 수신하는 소단계로 이루어지는 제 2 정보 수신 단계;

③ 상기 제 3 암호화 데이터와 상기 제 1 검사 데이터를 XOR 연산하여 제 5 암호화 데이터를 생성하는 소단계, 상기 제 1 암호화 데이터와 상기 제 3 암호화 데이터 및 제 2 세션키를 연결한 데이터에 해쉬 함수를 적용하여 제 6 암호화 데이터를 생성하는 소단계, 및 상기 제 4 암호화 데이터와 상기 제 6 암호화 데이터를 비교하여 두 데이터가 일치하면 상기 서버에 대한 인증이 성공한 것으로 결정하는 소단계로 이루어지는 서버 인증 결정 단계;

를 포함하는 것을 특징으로 하는 웹을 기반으로 하는 모바일 결제 시스템.

청구항 9

제 8 항에 있어서,

상기 서버에 대한 사용자 인증 단계는,

① 상기 제 1 검사 데이터와 상기 제 5 암호화 데이터 및 상기 제 1 논스 데이터를 연결한 데이터에 해쉬 함수를 적용하여 제 7 암호화 데이터를 생성하는 소단계와 상기 제 3 정보로서 상기 제 7 암호화 데이터를 상기 서버로 송신하는 소단계로 이루어지는 제 3 정보 송신 단계;

② 상기 서버가 상기 제 7 암호화 데이터를 수신하고, 상기 서버가 상기 제 3 해쉬 데이터와 상기 제 2 암호화 데이터 및 제 2 논스 데이터를 연결한 데이터에 해쉬 함수를 적용하여 제 8 암호화 데이터를 생성하고, 상기 제 7 암호화 데이터와 상기 제 8 암호화 데이터가 일치하는 것으로 판별되면 상기 사용자에게 대한 인증이 성공한 것으로 결정하는 소단계로 이루어지는 사용자 인증 결정 단계;

를 포함하는 것을 특징으로 하는 웹을 기반으로 하는 모바일 결제 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 사용자가 주도적으로 거래를 인증하며 거래에 관여하는 다수의 주체들이 인증 절차에 개입하는 것에 의해 인증 시 사용자의 정보 유출 가능성을 낮출 수 있으며 결제를 위한 추가적인 단말기를 필요로 하지 않아 보다 간편화된 웹을 기반으로 하는 모바일 결제 방법에 관한 것이다.

배경 기술

[0002] 최근 전자상거래, 특히 이동 전자상거래에서 사용자 인증이 중요한 이슈로 떠오르고 있다. 스마트폰과 같은 이동 단말기에서 애플리케이션을 통해 상품 또는 서비스를 거래하거나 오프라인 상점에서 상품 또는 서비스를 거래 시, 고객인 사용자가 이동 단말기로 결제를 시도하는 경우 사용자는 본인이 결제 서비스를 이용할 권한이 있는 진정한 자임을 인증한다. 그러나, 기존의 인증 절차는 사용자 정보 유출의 가능성이 있어 보안에 취약하다는 단점을 가지며, 인증 시 사용자가 단순히 아이디 및 패스워드와 같은 정보만을 서버로 제공할 뿐 인증 절차 전반에 있어서 사용자측에서 적극적으로 개입하지는 못하고 있다.

[0003] 현재 모바일 결제 방법은 주로 두 가지 형식으로 나누어 볼 수 있다. 첫 번째는 이동 전화, 스마트 카드 혹은 신용 카드를 기반으로 할 수 있는 계좌 기반 결제 방법이며, 두 번째는 고객이 자동판매기 혹은 이동 장치가 있는 소매점에서 물건을 구입할 수 있는 이동 POS(Post of Sale) 결제 방법이다. POS는 판매 시점 관리 단말기로써 개인용 컴퓨터에 카드 결제 장치를 달아 판매 시점의 상품명이나 가격 등의 데이터를 저장하는 단말기로, 종합적인 매출 관리를 해야 하는 대형 마트는 물론 소형 가맹점에서도 많이 사용하고 있다. 이러한 POS 시스템은 결제 시 고객 카드 정보 유출 경로로 이용되는 경우가 많아 그 해결 방안이 필요한 시점이다. 따라서 첫 번째, 두 번째 모바일 결제 시스템 모두에서 안전한 웹 거래를 위한 사용자 인증과 이동 금융 거래의 사용자 신뢰를 증가시킬 수 있는 기술이 요구된다.

[0004] SET(Secure Electric Transaction)는 인터넷 상의 신용 카드 거래를 보호하기 위해 설계된 공개된 암호 및 보안 설명서이다. SET을 사용하면, 사용자(구매자)에게 전자지갑(디지털 인증서)이 주어지며, 구매자와 상인, 그리고 구매자의 거래은행 간에는 기밀을 보장하는 방식으로 디지털 인증서와 전자서명의 조합을 사용함으로써 거래

가 이루어지고, 또한 인증된다. 도 1을 참조하여 SET 거래 흐름을 살펴보면 다음과 같다.

- [0005] 1. 사용자는 상인 웹 사이트에 접근하여 원하는 상품을 선택한다.
- [0006] 2. 시스템은 결제 방법을 묻고 사용자는 SET를 사용한 신용 카드를 통한 결제를 선택한다.
- [0007] 3. 사용자는 전자지갑(Digital Wallet)의 그가 소유하고 있는 신용 카드 중 하나를 선택하여 SET를 사용한 전자 거래를 진행한다.
- [0008] 4. 사용자 결제 항목을 얻은 후, 상인은 상인 인증과 결제를 위한 상인 은행과 연락한다.
- [0009] 5. 상인 은행은 사용자 은행과 연락하여 결제 승인을 요청한다.
- [0010] 6. 사용자 은행은 신용 카드 정보를 확인하여 상인 은행에 결제를 승인한다.
- [0011] 7. 사용자 은행으로부터 결제를 승인받으면 상인 은행은 상인에게 거래를 승인한다.
- [0012] 8. 상인은 거래를 완료한후 주문이 진행된 것을 사용자에게 확인시킨다.
- [0013] SET 프로토콜은 현 신용 카드 기반 결제 방법을 진화시켰고 등록과 인증에 의한 거래자의 신원 인증 뿐만 아니라 정보 전송을 위한 향상된 보안을 제공한다. 그러나 도 1의 화살표 방향에서 확인할 수 있듯이 종래의 SET에서는 인증의 흐름이 사용자에서 상인의 단방향으로 진행되어 사용자의 신용 및 인출 카드의 모든 항목이 상인 측을 통해야만 한다. 이는 데이터가 복사되고 인증없이 고객 계좌가 나중에 사용될 수 있는 여지를 남겨 사용자 정보 위험을 가중시킨다. 또한 사용자는 인증의 대상이 될 뿐이어서 인증 절차 전반에 사용자측에서 적극적으로 개입할 여지가 없었다.

발명의 내용

해결하려는 과제

- [0014] 본 발명은 상기와 같은 종래기술의 문제점을 해결하기 위한 것으로 일측에 의한 일방적인 절차 진행을 지양하고 거래에 관여하는 다수의 주체들이 인증 절차에 개입할 수 있는 거래 인증 방법을 이용한 모바일 결제 방법을 제공하는 것을 목적으로 한다.
- [0015] 또한 본 발명은 사용자 주체의 결제 거래에 의해 인증 과정에서의 사용자의 정보 유출 가능성을 낮출 수 있는 거래 인증 방법을 이용한 모바일 결제 방법을 제공하는 것을 다른 목적으로 한다.

과제의 해결 수단

- [0016] 전술한 목적을 달성하기 위한 본 발명은 (A) 사용자로부터 온라인 또는 오프라인 상점에서 선택된 상품 또는 서비스에 대한 대금 결제를 위해 신용카드 결제 또는 계좌 이체가 선택되는 단계; (B) 상기 (A) 단계의 주문정보에 대해 판매자가 판매자측 금융기관 서버에 인증하는 단계; (C) 상기 (B) 단계의 인증이 성공하면 상기 (A) 단계의 주문정보에 대해 사용자와 사용자측 금융기관 서버가 상호 인증하는 단계; (D) 상기 (C) 단계의 상호 인증이 성공하면, 사용자측 금융기관 서버가 판매자측 금융기관 서버에 상기 주문에 대한 결제를 통보하는 단계; 및 (E) 결제를 통보받은 판매자측 금융기관 서버가 판매자에게 결제 승인 메시지를 전달하여 결제가 완료되는 단계;를 포함하는 것을 특징으로 하는 웹을 기반으로 하는 모바일 결제 방법에 관한 것이다.

발명의 효과

- [0017] 이상과 같이 본 발명의 모바일 결제 방법에 의하면 일측에 의해 일방적으로 절차가 진행되는 것이 아니라 거래에 관여하는 다수의 주체들이 인증 절차에 개입하여 해당 거래에 대해 상호 검증을 하기 때문에 가장 공격에 대해 보다 안전한 결제가 가능하다.
- [0018] 그리고 본 발명의 모바일 결제 방법에서는 사용자의 결제 계좌 정보가 판매자를 통하지 않기 때문에 데이터가 복사되어 유출될 가능성을 크게 낮출 수 있으며, 추후 부정하게 사용될 위험 없이 안전하게 결제할 수 있다.

[0019] 또한 본 발명의 모바일 결제 방법에 의하면 결제를 위한 추가적인 단말기를 필요로 하지 않아 보다 간편화된 결제가 가능하다.

도면의 간단한 설명

[0020] 도 1은 SET 방법에 의한 결제 흐름을 보여주는 도면.

도 2는 본 발명의 일 실시예에 따른 거래 인증 방법을 통해 모바일 결제가 실시되는 시스템의 개략적인 도면.

도 3은 본 발명의 일 실시예에 따라 사용자와 사용자측 금융기관 간에 수행되는 인증 절차를 설명하기 위한 예시적인 흐름도.

발명을 실시하기 위한 구체적인 내용

[0021] 이하 첨부된 도면을 참조하여 본 발명을 보다 상세히 설명한다. 그러나 첨부된 도면은 본 발명의 기술적 사상의 내용과 범위를 쉽게 설명하기 위한 예시일 뿐, 이에 의해 본 발명의 기술적 범위가 한정되거나 변경되는 것은 아니다. 이러한 예시에 기초하여 본 발명의 기술적 사상의 범위 안에서 다양한 변형과 변경이 가능함은 당업자에게는 당연할 것이다.

[0022] 도 2는 본 발명의 일 실시예에 따른 거래 인증 방법을 통해 이동 결제가 실시되는 시스템의 개략적인 도면이다. 도 2에 도시된 바와 같이, 사용자가 판매자로부터 상품 또는 서비스를 구매하는 경우 사용자, 사용자측 금융기관, 판매자, 판매자측 금융기관의 개체들은 사용자 단말기(100), 사용자측 금융기관 서버(200), 판매자 단말기(300) 및 판매자측 금융기관 서버(400)를 통해 네트워크로 연결되어 결제를 진행하게 된다. 사용자 단말기 또는 판매자 단말기는 휴대폰, PC, 노트북 등 그 종류를 막론하고 네트워크의 연결과 입력이 가능한 것은 무엇이든 무방하다.

[0023] 본 발명에서의 웹을 기반으로 하는 모바일 결제 방법은 (A) 사용자로부터 온라인 또는 오프라인 상점에서 선택된 상품 또는 서비스에 대한 대금 결제를 위해 신용카드 결제 또는 계좌 이체가 선택되는 단계; (B) 상기 (A) 단계의 주문정보에 대해 판매자가 판매자측 금융기관 서버에 인증하는 단계; (C) 상기 (B) 단계의 인증이 성공하면 상기 (A) 단계의 주문정보에 대해 사용자와 사용자측 금융기관 서버가 상호 인증하는 단계; (D) 상기 (C) 단계의 상호 인증이 성공하면, 사용자측 금융기관 서버가 판매자측 금융기관 서버에 상기 주문에 대한 결제를 통보하는 단계; 및 (E) 결제를 통보받은 판매자측 금융기관 서버가 판매자에게 결제 승인 메시지를 전달하여 결제가 완료되는 단계;를 포함하여 이루어진다.

[0024] 사용자는 판매자로부터 상품 또는 서비스를 구매하는 경우 사용자는 사용자 단말기를 통해 이동 결제 서비스를 이용할 수 있다. 이를 위하여 사용자는 판매자가 개설한 온라인 또는 오프라인 상점에서 상품 또는 서비스를 선택하고, 대금 결제를 위해 신용카드 결제 또는 계좌 이체를 이용할 수 있다. 이 대금 결제는 사용자가 본인의 사용자 단말기(100)를 통해 실시할 수 있다.

[0025] 판매자는 사용자가 (A) 단계에서 선택한 주문정보에 대해 판매자측 금융기관 서버에 인증한다. 온라인에서 선택한 주문에 대해서는 판매자의 웹사이트에서 선택될 수 있으며, 오프라인 상점의 경우, 판매자가 판매자 웹사이트에 수동으로 또는 바코드 인식기 등을 통해 입력할 수 있다.

[0026] 상기 주문정보는 세금과 배송비를 포함한 총 금액, 주문의 타임스탬프와 같은 정보를 포함할 수 있다.

[0027] 이때, 판매자의 판매자측 금융기관 서버에 대한 인증은 암호화된 판매자의 계좌정보를 포함한 판매자 정보와 상기 주문에 대한 정보가 포함된 인증서를 판매자의 비밀키로 서명하는 것에 의한 거래 인증으로 이루어질 수 있다. 판매자의 계좌정보는 상기 대금이 지불되어 입금될 계좌의 정보를 의미한다. 이와 같은 판매자의 비밀키에 의한 서명에 의해 사용자의 요구 시 사용자에게 대한 상호 인증 결제 거래를 지원한다.

[0028] 상기 주문정보에 대해 판매자와 판매자측 금융기관 서버의 인증이 실패하면, 모바일 결제는 더 이상 진행되지 않고 종료된다. 판매자의 인증이 성공하면, 상기 주문정보에 대해 사용자와 사용자측 금융기관 서버가 상호 인증을 수행한다. 상기 주문정보에 대한 사용자와 사용자측 금융기관 서버의 상호 인증은, 암호화된 사용자의 계좌정보를 포함한 사용자 정보와 상기 주문에 대한 정보가 포함된 인증서를 사용자의 비밀키로 서명하는 것에 의한 거래 인증에 의해 이루어질 수 있다. 이때 사용자의 계좌정보라 함은 결제를 위해 선택한 신용카드 정보 또

는 이체될 은행 계좌의 정보를 의미한다.

- [0029] 상기와 같이 본 발명은 사용자의 계좌정보가 판매자를 통하지 않고 사용자측 금융기관 서버와 사용자 간에 이루어지기 때문에 판매자를 통한 정보의 유출 우려가 없다. 또한 단순히 아이디와 패스워드에 의해 인증이 이루어지는 경우 사용자 아이디와 패스워드를 가장한 사용자 공격이 용이한 것에 비해 사용자의 아이디, 비밀번호와 함께 주문정보를 비밀키로 서명하도록 한 본 발명의 경우 사용자 가장 공격 시 사용자의 비밀키로 확인이 가능하다.
- [0030] 상기 (C) 단계와 (D) 단계의 사이에는, 사용자에게 대해 판매자측 금융기관 서버가 판매자 정보 및 주문정보를 사용하여 상기 거래를 인증하는 단계를 추가로 포함할 수 있다. 상기 단계에 의하면 종래의 모바일 결제가 판매자를 통하여 사용자의 거래가 인증되었던 것에 비해 사용자 주도로 판매자와 거래를 인증할 수 있어보다 안전한 거래가 가능하다.
- [0031] 이와 같이 사용자, 사용자측 금융기관 서버, 판매자, 판매자측 금융기관 서버 간의 상호 인증이 성공적으로 완료되면, 사용자측 금융기관 서버는 판매자측 금융기관 서버에 상기 주문에 대한 결제를 통보하게 되며 결제를 통보받은 판매자측 금융기관 서버는 판매자에게 결제 승인 메시지를 전달하여 결제가 완료되게 된다.
- [0032] 이때, 상기 (D) 단계 이후, (E) 단계와 별도로 사용자측 금융기관 서버는 사용자에게 결제 완료통보를 통보하는 단계를 추가로 포함할 수 있다. 결제 완료의 통보 시에는 판매자 정보와 함께 주문정보를 함께 제공할 수 있다. 또한, 신용카드 결제인 경우에는 해당 월 사용액의 누계나 해당 청구기간의 사용액의 누계와 같은 추가적인 정보를 제공할 수 있으며, 은행 계좌 이체를 통한 결제인 경우에는 해당 월 결제액의 누계나 계좌 잔고와 같은 추가적인 정보를 제공할 수 있다. 이 경우, 이러한 단계의 추가에 의해 사용자는 거래의 종료 후 다시 그의 은행 웹사이트나 신용카드 웹사이트에 로그인하여 잔고를 확인해야 할 필요가 없게 된다.
- [0033] 상기 인증을 위해서는 별도의 거래 인증 서버가 도입될 수 있다. 거래 인증 서버는 전자거래를 위한 사용자, 사용자측 금융기관, 판매자, 판매자측 금융기관의 객체들을 인증하기 위하여 최소의 계산과 최소의 인증 횟수로 사용자 단말기, 판매자 단말기, 사용자측 금융기관 서버 및 판매자측 금융기관 서버와 데이터를 주고 받으면서 인증을 수행하도록 한다. 상기 거래 인증 서버는 통신부, 저장부 및 처리부를 포함하는 컴퓨팅 장치이다. 상기 통신부는 인증에 개입하는 주체들과 데이터를 주고 받는 통신 모듈이다. 상기 저장부는 인증에 필요한 기본 정보를 데이터베이스로 구축하여 저장하는 저장 장치이다. 일 예로, 대용량의 데이터를 저장하는 HDD 또는 SSD 일 수 있으나, 이에 제한되지는 않는다. 상기 처리부는 데이터를 처리하여 인증 절차를 수행하는 프로세서로서, CPU, 컨트롤러 등을 포함하나 이에 제한되지는 않는다. 상기 거래 인증 서버는 제3의 인증기관(TTA)으로부터 인증 관리를 받는다.
- [0034] 도 3은 본 발명의 일 실시예에 따라 사용자와 사용자측 금융기관 간에 수행되는 인증 절차를 설명하기 위한 예시적인 흐름도이다.
- [0035] 도 3을 참조하면, 상기 (C)단계의 주문정보에 대한 사용자와 사용자측 금융기관 서버의 상호 인증은 데이터베이스 및 프로세서를 포함하며 단말기 및 서버와 통신하는 컴퓨팅 장치(거래 인증 서버)에 의해 이루어지며, (a) 사용자의 단말기로부터 수신받은 사용자의 아이디 및 비밀번호(S110)와 상기 사용자의 거래에 관하여 사전에 등록된 고유 정보를 이용하여 상기 사용자 단말기로부터 수신된 사용자 정보의 진정성을 검사하는 단계(S120); (b) 상기 사용자 정보가 진정한 것으로 확인되면, ① 상기 사용자측 금융기관 서버로 상기 사용자 정보를 처리하여 얻은 제 1 정보를 송신하고(S130), ② 상기 사용자측 금융기관 서버로부터 상기 제 1 정보를 처리하여 생성된 제 2 정보를 수신받은 후(S140), ③ 상기 제 2 정보를 기초로 상기 사용자측 금융기관 서버 인증을 결정하는(S150), 사용자에게 대한 서버 인증 단계; 및 (c) 상기 서버에 대한 인증이 성공하면, ① 상기 사용자를 인증하기 위해 상기 제 2 정보를 처리하여 얻은 제 3 정보를 상기 서버로 송신하고(S160), ② 상기 제 3 정보를 기초로 상기 사용자 인증을 결정하는(S170), 서버에 대한 사용자 인증 단계;를 포함하여 이루어질 수 있다.
- [0036] 위 인증 절차를 수행하기 위해, 상기 거래 인증 서버는 사용자에게 관한 고유 정보를 사전에 데이터베이스로 구축할 수 있다.
- [0037] 구체적으로, 상기 거래 인증 서버는 사전에 사용자의 아이디 ID_c 및 비밀번호 Pw_c를 입력받고, 아이디 ID_c와 타임스탬프 TSP와 상기 서버의 프라이빗 키 Pri_s를 기초로 해쉬 함수를 적용하여 Vc = H(ID_c, TSP, Pri_s)와 같이

제 1 해쉬 데이터 V_c 를 생성할 수 있다.

- [0038] 그리고, 상기 거래 인증 서버는 제 1 해쉬 데이터와 사용자의 비밀번호 Pw_c 를 XOR 연산하여 $A_c = V_c \text{ XOR } Pw_c$ 와 같이 제 2 해쉬 데이터 A_c 를 생성할 수 있다.
- [0039] 그리고 나서, 상기 거래 인증 서버는 사용자의 고유 정보로 아이디 ID_c , 제 1 해쉬 데이터 V_c , 제 2 해쉬 데이터 A_c , 및 해쉬 함수 $H(.)$ 를 저장할 수 있다. 저장된 고유 정보는 해당 사용자로부터 인증 요청이 있을 때마다 데이터 베이스로부터 독출되어 사용될 수 있다.
- [0040] 본 발명의 일 실시예에 따르면, 상기 사전에 등록된 고유 정보와 비밀번호 Pw_c 를 이용하여 사용자 단말기로부터 수신된 사용자 정보의 진정성을 검사하는 단계(S120)는, 데이터베이스로부터 제 1 해쉬 데이터 V_c 및 제 2 해쉬 데이터 A_c 를 불러오는 단계를 포함할 수 있다.
- [0041] 그리고 나서, 상기 단계(S120)는 제 2 해쉬 데이터 A_c 와 사용자 단말기로부터 수신된 비밀번호 Pw_c 를 XOR 연산하여 $B_c = A_c \text{ XOR } Pw_c$ 와 같이 제 1 검사 데이터 B_c 를 생성하는 단계를 포함할 수 있다.
- [0042] 그리고 나서, 상기 단계(S120)는 상기 제 1 검사 데이터 B_c 와 상기 제 1 해쉬 데이터 V_c 를 비교하여, 두 데이터가 일치하면(즉, $B_c = V_c$), 사용자 단말기로부터 수신된 사용자 정보가 진정한 것으로 결정하는 단계를 포함할 수 있다. 만약 두 데이터가 불일치하면 인증 절차는 종료된다.
- [0043] 이와 같이 사용자 정보의 진정성을 검사하여 해당 정보가 진정한 것으로 확인되면, 상기 거래 인증 서버는 사용자측 금융기관 서버로 사용자 정보를 처리하여 얻은 제 1 정보를 송신할 수 있다.
- [0044] 본 발명의 일 실시예에 따르면, 제 1 정보를 송신하는 단계(S130)는, 제 1 검사 데이터 B_c 와 제 1 논스(nonce) 데이터 N_c 를 XOR 연산하여 $C_1 = B_c \text{ XOR } N_c$ 와 같이 제 1 암호화 데이터 C_c 를 생성하는 단계를 포함할 수 있다. 여기서, 제 1 논스 데이터 N_c 는 사용자측 정보 송신을 위해 사용되는 임시 데이터이다.
- [0045] 그리고 나서, 상기 단계(S130)는 사용자의 아이디 ID_c 와 제 1 암호화 데이터 C_1 을 금융기관 서버로 송신하는 단계를 포함할 수 있다.
- [0046] 금융기관 서버로 사용자의 아이디 ID_c 와 제 1 암호화 데이터 C_1 을 포함하는 제 1 정보가 송신되면, 사용자와 그 금융기관 간의 상호 인증을 위한 본격적인 절차가 실시된다.
- [0047] 구체적으로, 금융기관 서버는 사용자의 아이디 ID_c 와 타임스탬프 TSP와 프라이빗 키 Pri_s 를 기초로 해쉬 함수를 적용하여 $B_s = H(ID_c, TSP, Pri_s)$ 와 같이 제 3 해쉬 데이터 B_s 를 생성할 수 있다.
- [0048] 그리고 나서, 금융기관 서버는 제 1 암호화 데이터 C_1 과 제 3 해쉬 데이터 B_s 를 XOR 연산하여 $C_2 = C_1 \text{ XOR } B_s$ 와 같이 제 2 암호화 데이터 C_2 를 생성할 수 있다.
- [0049] 그리고 나서, 금융기관 서버는 제 3 해쉬 데이터 B_s 와 제 1 논스 데이터 N_c 를 XOR 연산하여 $C_3 = B_s \text{ XOR } N_c$ 와 같이 제 3 암호화 데이터 C_3 를 생성할 수 있다.
- [0050] 그리고 나서, 금융기관 서버는 제 1 암호화 데이터 C_1 과 제 3 암호화 데이터 C_3 와 제 1 세션키 Sk_1 을 연결(concatenation, $\parallel$)한 데이터에 해쉬 함수를 적용하여 $C_4 = H(C_1 \parallel C_3 \parallel Sk_1)$ 와 같이 제 4 암호화 데이터 C_4 를 생성할 수 있다. 여기서, 제 1 세션키 Sk_1 은 제 3 해쉬 데이터 B_s 와 제 2 암호화 데이터 C_2 와 제 2 논스 데이터 N_s 를 연결한 데이터에 해쉬 함수를 적용하여 $Sk_1 = H(B_s \parallel C_2 \parallel N_s)$ 와 같이 생성한 것이며, 제 2 논스 데이터 N_s 는 금융기관 서버 측 정보 송신을 위해 사용되는 임시 데이터이다.
- [0051] 그리고 나서, 금융기관 서버는 금융기관 서버의 인증 절차를 위해 제 3 암호화 데이터 C_3 및 제 4 암호화 데이터 C_4 를 포함하는 제 2 정보를 거래 인증 서버로 송신할 수 있다(S140).

- [0052] 금융기관 서버로부터 제 3 암호화 데이터 C_3 및 제 4 암호화 데이터 C_4 를 포함하는 제 2 정보를 수신하면, 거래 인증 서버는 제 2 정보를 기초로 금융기관 서버를 인증할 수 있다(S150).
- [0053] 본 발명의 일 실시예에 따르면, 제 2 정보를 기초로 금융기관 서버를 인증하는 단계(S150)는, 제 3 암호화 데이터 C_3 와 제 1 검사 데이터 B_c 를 XOR 연산하여 $C_5 = C_3 \text{ XOR } B_c$ 와 같이 제 5 암호화 데이터 C_5 를 생성하는 단계를 포함할 수 있다.
- [0054] 그리고, 상기 단계(S150)는 제 1 암호화 데이터 C_1 과 제 3 암호화 데이터 C_3 및 제 2 세션키 Sk_2 를 연결한 데이터에 해쉬 함수를 적용하여 $C_6 = H(C_1 \parallel C_3 \parallel Sk_2)$ 와 같이 제 6 암호화 데이터 C_6 를 생성하는 단계를 포함할 수 있다. 여기서, 제 2 세션키 Sk_2 는 제 1 검사 데이터 B_c 와 제 5 암호화 데이터 C_5 및 제 1 논스 데이터 N_c 를 연결한 데이터에 해쉬 함수를 적용하여 $Sk_2 = H(B_c \parallel C_5 \parallel N_c)$ 와 같이 생성한 것이다.
- [0055] 그리고 나서, 상기 단계(S150)는 제 4 암호화 데이터 C_4 와 제 6 암호화 데이터 C_6 를 비교하여, 두 데이터가 일치하면($C_6 = C_4$), 금융기관 서버에 대한 인증이 성공한 것으로 결정하는 단계를 포함할 수 있다. 만약 두 데이터가 불일치하면, 금융기관 서버에 대한 인증이 실패하여 인증 절차는 종료된다.
- [0056] 금융기관 서버에 대한 인증이 성공하면, 거래 인증 서버는 사용자에게 대한 인증 절차를 위해 제 2 정보를 처리하여 얻은 제 3 정보를 금융기관 서버로 송신할 수 있다(S160).
- [0057] 본 발명의 일 실시예에 따르면, 제 3 정보를 금융기관 서버로 송신하는 단계(S160)는, 제 1 검사 데이터 B_c 와 제 5 암호화 데이터 C_5 및 제 1 논스 데이터 N_c 를 연결한 데이터에 해쉬 함수를 적용하여 $C_7 = H(B_c \parallel C_5 \parallel N_c)$ 와 같이 제 7 암호화 데이터 C_7 를 생성하는 단계를 포함할 수 있다.
- [0058] 그리고 나서, 상기 단계(S160)는 제 7 암호화 데이터 C_7 를 포함하는 제 3 정보를 금융기관 서버로 송신하는 단계를 포함할 수 있다.
- [0059] 금융기관 서버가 거래 인증 서버로부터 제 7 암호화 데이터 C_7 를 포함하는 제 3 정보를 수신하면, 금융기관 서버는 제 3 정보를 기초로 사용자 인증 절차를 수행할 수 있다(S170).
- [0060] 본 발명의 일 실시예에 따르면, 제 3 정보를 기초로 사용자 인증 절차를 수행하는 단계(S170)는, 금융기관 서버가 제 3 해쉬 데이터 B_s 와 제 2 암호화 데이터 C_2 및 제 2 논스 데이터 N_s 를 연결한 데이터에 해쉬 함수를 적용하여 $C_8 = H(B_s \parallel C_2 \parallel N_s)$ 와 같이 제 8 암호화 데이터 C_8 를 생성하는 단계를 포함할 수 있다.
- [0061] 그리고 나서, 상기 단계(S170)는 제 7 암호화 데이터 C_7 과 제 8 암호화 데이터 C_8 를 비교하여, 두 데이터가 일치하는 것으로 판별되면($C_8 = C_7$), 금융기관 서버는 사용자 인증이 성공한 것으로 결정하는 단계를 포함할 수 있다.
- [0062] 사용자에게 대한 인증 절차가 완료되면, 금융기관 서버는 거래 인증 서버로 인증 결과를 보고할 수 있다(S180).
- [0063] 이와 같은 본 발명의 상호 인증 방법에 의하면, 사용자측 금융기관 서버가 사용자를 인증하기 위해 사용자의 N_c 와 서버의 세션키인 Sk_1 을 사용하며, 사용자가 사용자측 금융기관 서버를 인증하기 위해 서버의 N_s 와 사용자의 세션키인 Sk_2 를 사용하여 안전한 거래를 완성한다. 따라서 서버의 세션키를 가장하여 서버를 공격한다고 하더라도 사용자의 세션키가 없으면 상호 인증이 이루어지지 않기 때문에 가장 서버를 가장한 공격이 이루어진다고 하더라도 가장 공격의 목적을 이룰 수 없다.
- [0064] 또한 본 발명은 서버와 사용자의 논스 생성과 타임스탬프로 공격자가 재전송 공격을 할 수 없도록 지원한다.
- [0065] 판매자와 판매자측 금융기관 간의 인증 절차 역시 전술한 사용자와 사용자측 금융기관 간의 상호 인증 절차와 동일하게 수행될 수 있으나, 실시예에 따라 판매자와 그 금융기관 간의 인증 절차는 그보다 더 간단하게 수행될 수도 있다.
- [0066] 본 발명의 실시예에 따른 거래 인증 방법은 컴퓨터에서 실행되기 위한 프로그램으로 제작되어 컴퓨터가 읽을 수

있는 기록매체에 저장될 수 있다. 상기 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 저장장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있다. 또한, 상기 거래 인증 방법은 컴퓨터와 결합되어 실행시키기 위하여 매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.

부호의 설명

100: 사용자 단말기

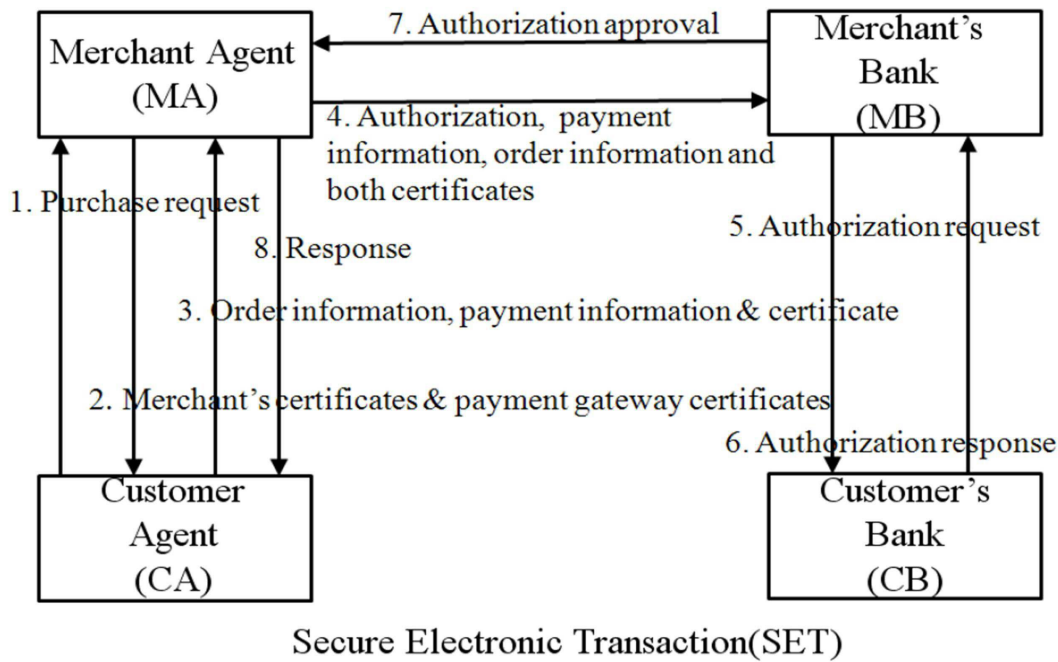
200: 사용자측 금융기관 서버

300: 판매자 단말기

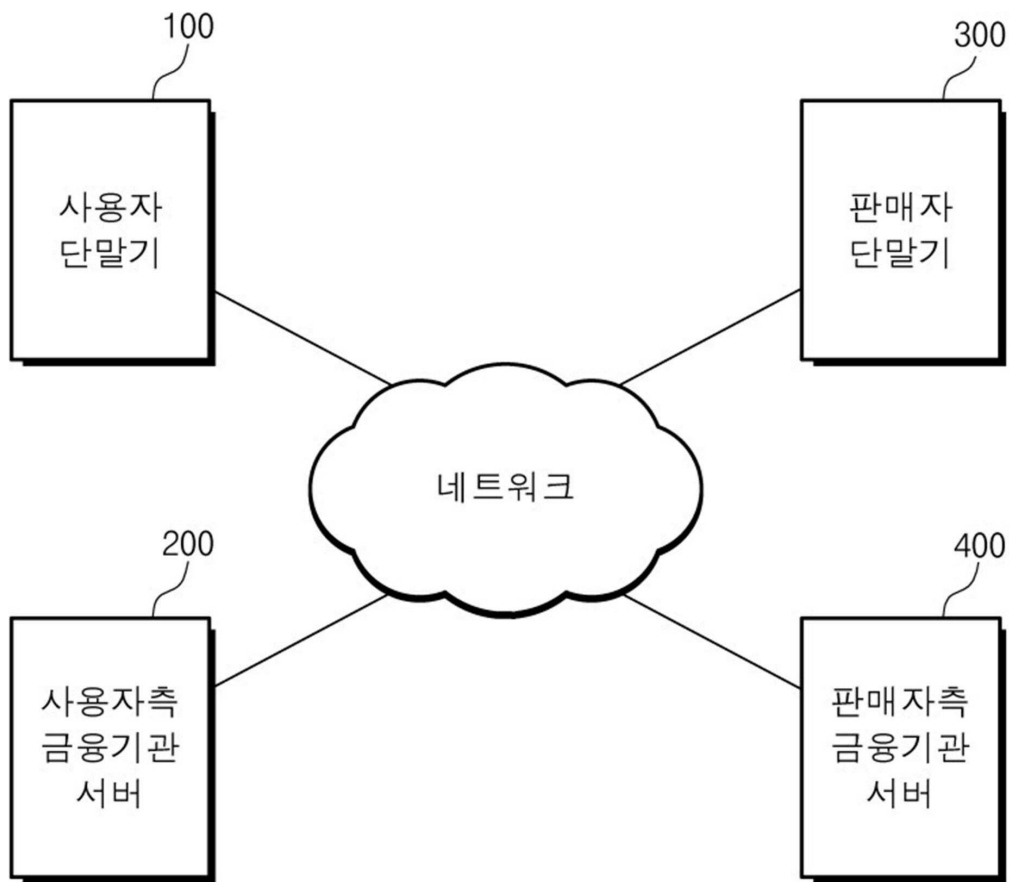
400: 판매자측 금융기관 서버

도면

도면1



도면2



도면3

