특 허 법 원

제 1 부

판 결

사 건 2022허4079 등록무효(특)

원 고 주식회사 A

대표이사 B

소송대리인 법무법인 새록 담당변호사 전형호, 채우리, 황영민

특허법인 아주 담당변리사 박대진, 윤종화, 김종욱,

이용우, 류공일

변리사 김병진, 강형석

피 고 주식회사 C

대표이사 D

소송대리인 법무법인 민후

담당변호사 김경환, 양진영, 원준성, 최주선

변 론 종 결 2023. 4. 11.

판 결 선 고 2023. 6. 1.

주 문

1. 원고의 청구를 기각한다.

2. 소송비용은 원고가 부담한다.

청 구 취 지

특허심판원이 2022. 5. 25. 2022당336호에 관하여 한 심결을 취소한다.

이 유

1. 기초사실

가. 이 사건 특허발명

1) 발명의 명칭: 다중 안전 잠금 기능을 구비하는 금융 거래 중계 시스템 및 그의 처리 방법

2) 출원일/ 등록일/ 등록번호: 2014. 9. 18./ 2015. 8. 4./ 특허 제1543222호

3) 청구범위

【청구항 1】 금융 거래 중계 시스템에 있어서(이하 '**구성요소 1-1**'이라 한다):

통신망과(이하 '**구성요소 1-2**'라 한다);

상기 통신망에 연결되고, 지문 정보를 입력하는 지문 인식기를 구비하는 고객 단말기(이하 '**구성요소 1-3**'이라 한다) 및;

상기 고객 단말기가 상기 통신망을 통하여 접속되고, 상기 고객 단말기로부터 지문 정보, 전화번호 및 계좌 비밀번호를 전송받아서 회원으로 등록하고, 상기 고객 단말기가 온라인 은행 거래 및 전자 상거래 중 어느 하나를 수행하면, 상기 고객 단말기로부터 지문 정보만을 전송받아서 인증하여 온라인 은행 시스템 또는 전자 상거래시스

템으로 무인증 접속하여 금융 거래가 이루어지도록 중계 처리하는 개인 금융 거래 중계 서버를 포함하되(이하 '**구성요소 1-4**'라 한다);

상기 개인 금융 거래 중계 서버는;

상기 고객 단말기로부터 지문 정보를 받아서 기등록된 지문 정보와 일치하는지를 비교하는 지문 인식 처리부와; 상기 온라인 은행 시스템에 등록된 상기 고객 단말기의 계좌 비밀번호를 등록하는 계좌 비밀번호 처리부 및; 상기 고객 단말기의 전화번호를 이용하여 인증하는 전화번호 인증 처리부를 포함하는 다중 안전 잠금 모듈과 상기 지문 정보, 상기 계좌 비밀번호 및 상기 전화번호를 저장하는 데이터베이스를 구비하고(이하 '**구성요소 1-5**'라 한다);

상기 다중 안전 잠금 모듈은 미들웨어로 구비되며, 해킹 차단을 위한 방화벽 기능을 더 구비하는 것(이하 '**구성요소 1-6**'이라 한다)을 특징으로 하는 금융 거래 중계 시스템.

【청구항 4】 금융 거래 중계 시스템의 처리 방법에 있어서(이하 '**구성요소 4-1**'이라 한다);

상기 금융 거래 중계 시스템의 고객 단말기로부터 통신망을 통하여 상기 금융 거래 중계 시스템의 개인 금융 거래 중계 서버에 접속하는 단계와(이하 '**구성요소 4-2**'라 한다);

상기 고객 단말기의 지문 인식기를 통하여 지문 정보를 획득하고, 상기 통신망을 통하여 지문 정보를 상기 개인 금융 거래 중계 서버로 전송하여 상기 개인 금융 거래 중계 서버가 상기 고객 단말기에 대응하여 지문 정보를 데이터베이스에 등록하는 단계와(이하 '**구성요소 4-3**'이라 한다);

상기 개인 금융 거래 중계 서버가 상기 데이터베이스에 저장된 상기 고객 단말기의 전화번호를 이용하여 인증하고, 상기 개인 금융 거래 중계 서버가 상기 고객 단말기의 통장 계좌번호에 대한 비밀번호를 상기 데이터베이스에 등록하여 상기 고객 단말기의 지문 정보, 전화번호 및 계좌 비밀번호를 매칭시켜서 상기 개인 금융 거래중계 서버의 회원으로 등록하는 단계와(이하 '**구성요소 4-4**'라 한다);

상기 고객 단말기가 온라인 은행 거래 및 전자 상거래 중 어느 하나를 수행하기 위하여, 인증 절차를 처리하면, 상기 개인 금융 거래 중계 서버의 다중 안전 잠금 모듈 중 지문인식처리부가 상기 고객 단말기로부터 지문 정보만을 전송받아서 지문 인증을 처리하는 단계(이하 '**구성요소 4-5**'라 한다) 및;

전송된 지문 정보가 상기 개인 금융 거래 중계 서버의 데이터베이스에 저장된 지문 정보와 일치하면, 상기 개인 금융 거래 중계 서버가 무인증으로 온라인 은행 시스템 또는 전자 상거래 시스템에 접속하여 금융 거래를 중계하는 단계(이하 '**구성요소 4-6**'이라 한다)를 포함하는 것을 특징으로 하는 금융 거래 중계 시스템의 처리 방법.

【청구항 2, 3, 5, 6】 (삭제).

4) 발명의 개요

㉮ 기술분야 및 배경기술

【0001】 본 발명은 금융 거래 중계 시스템에 관한 것으로, 좀 더 구체적으로 지문 인식, 전화번호 인증 및 계좌 비밀번호 인증을 이용한 다중 안전 잠금 기능을 구비하는 온라인 금융 거래 중계 시스템 및 그의 처리 방법에 관한 것이다.

【0003】 현재, 모바일 기기는 신용카드를 대신하여 은행 업무, 전자 상거래 등의 금융 거래를 수행할 수 있도록 은행에서 발급되는 칩을 이용한다. 이를 위해 모바일 기기는 칩을 내장하여 전용 단말기가 설치된 편의점 및 매장에서 비용 결제에 이용하고 있으나, 결제 가능한 비용에 제한이 있고, 전용 단말기가 없는 곳에서는 결제를 수행할 수 없다. 또한, 모바일

기기에 내장된 칩으로는 계좌 이체나, 일반 상거래 시, 비용 결제를 즉각 처리하기 어려운 측면이 있다.

【0004】 일반적으로, 개인이 은행과의 전자 금융 거래에서 개인 신상 정보 또는 비밀번호 등의 누설과 도용으로 발생할 수 있는 개인 피해를 방지하기 위하여 공인인증서와 비밀번호 등으로 개인의 금융 거래를 보호하고 있으나, 이는 은행의 보안 기술만을 의존하고 있기 때문에, 개인 실수로 인한 개인 피해 발생을 은행이 방지하거나 보호하지 못하고 있는 실정이다.

【0006】 본 발명의 목적은 지문 인식을 이용한 다중 안전 잠금 기능을 구비하는 금융 거래 시스템 및 그의 처리 방법을 제공하는 것이다.

【0007】 본 발명의 다른 목적은 고객의 편의성을 제공하기 위한 지문 인식을 이용한 다중 안전 잠금 기능을 구비하는 금융 거래 시스템 및 그의 처리 방법을 제공하는 것이다.

【0008】 본 발명의 또 다른 목적은 지문 인식, 전화번호 인증 및 계좌번호 인증을 이용한 다중 안전 잠금 기능을 구비하는 금융 거래 시스템 및 그의 처리 방법을 제공하는 것이다.

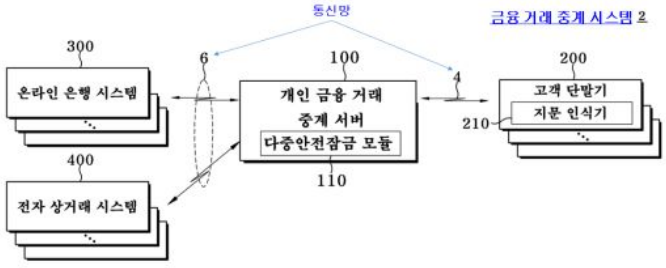
㈏ 발명의 주요 내용

【0024】 도 1 및 도 2를 참조하면, 본 발명의 금융 거래 중계 시스템(2)은 지문 인식을 포함하는 다중 안전 잠금 기능을 이용하여 은행 거래, 전자 상거래를 무인증 접속 방식으로 중계 처리한다.

【0025】 이를 위해 본 발명의 금융 거래 중계 시스템(2)은 개인 금융 거래 중계 서버(100)에 지문 인식, 계좌 비밀번호 인증 및 전화번호 인증을 통하여 회원으로 등록하고, 고객 단말기(200)와 온라인 은행 시스템(300) 및 전자 상거래 시스템(400)들 간에 금융 거래 시, 지문 인증으로 무인증 접속이 이루어지도록 처리한다.

【0026】 본 발명의 금융 거래 중계 시스템(2)은 통신망(4, 6)과 고객 단말기(200)와 온라인 은행 시스템(300)과 전자 상거래 시스템(400) 및 개인 금융 거래 중계 서버(100)를 포함한다.

[도 1] 본 발명에 따른 금융 거래 중계 시스템의 네트워크 구성



【0027】 통신망(4, 6)은 예컨대, 유무선 통신망, 이동 통신망 등으로 구비되어, 고객 단말기(200)와 온라인 은행 시스템(300) 및 개인 금융 거래 중계 서버(100)들 그리고 고객 단말기(200)와 전자 상거래 시스템(400) 및 개인 금융거래 중계 서버(100)들 간에 데이터 통신이 이루어지도록 연결되는 단일 또는 복합의 통신망으로 구비된다.

【0028】 고객 단말기(200)는 예를 들어, 스마트폰, 태블릿 컴퓨터, 노트북 등과 같은 휴대용 컴퓨터나 퍼스널 컴퓨터 등으로 구비되고, 통신망(4)을 통하여 개인 금융 거래 중계 서버(100)에 접속한다.

【0029】 고객 단말기(200)는 지문 정보를 획득하는 지문 인식기(210)를 구비한다. 고객 단말기(200)는 지문 인식기(210)로부터 획득된 지문 정보를 통신망(4)을 통해 개인 금융 거래 중계 서버(100)로 제공한다.

【0031】 온라인 은행 시스템(300)은 제휴 은행에 구비되어, 온라인으로 처리되는 은행 업무 예를 들어, 입출금, 이체 등의 금융 거래를 처리한다. 온라인 은행 시스템(300)은 금융 거래 시, 개인 금융 거래 중계 서버(100)를 통해 고객 단말기(200)가 무인증으로 접속된다.

【0032】 전자 상거래 시스템(400)은 예를 들어, 백화점, 할인점 등의 온라인 쇼핑몰 시스템, 항공, 철도 등의 여객 운송 예약 시스템, 콘도, 호텔 등의 숙박 예약 시스템, 영화, 연극, 음악회 등의 문화 공연 예약 시스템, 레저 예약시스템 등으로 구비되어, 개인 금융 거래 중계 서버(100)를 통하여 전자 상거래 이용 시, 고객 단말기(200)가 무인증으로 접속된다.

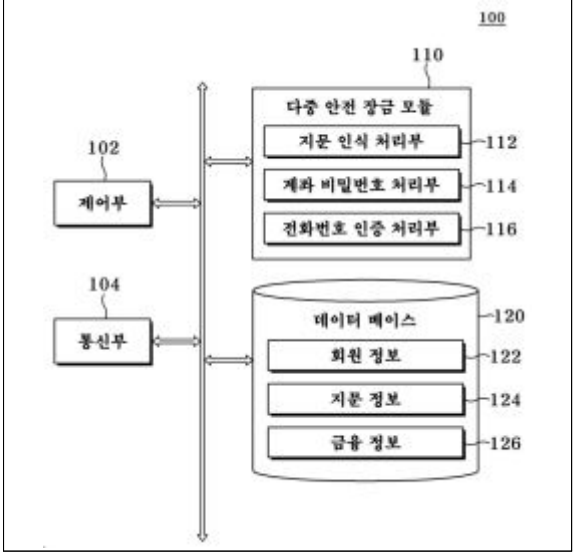
【0033】 개인 금융 거래 중계 서버(100)는 고객 단말기(200)가 회원 가입 시, 다중 안전 잠금 모듈(110)을 통해 회원으로 등록하고, 온라인 은행 시스템(300) 및 전자 상거래 시스템(400)과의 금융 거래 시, 고객 단말기(200)로부터 지문 정보를 받아서 인증 처리하고, 온라인 은행 시스템(300) 및 전자 상거래 시스템(400)으로 금융 거래 및 전자 상거래 시, 지문 인증을 통해 무인증 접속으로 금융 거래가 이루어지도록 처리한다. 【0034】 구체적으로, 개인 금융 거래 중계 서버(100)는 도 2에 도시된 바와 같이, 제어부(102)와 통신부(104)와 다중 안전 잠금 모듈(110) 및 데이터베이스(120)를 포함한다.

【0035】 제어부(102)는 개인 금융 거래 중계 서버(100)의 제반 동작을 제어 및 처리한다.

【0036】 통신부(104)는 통신망(4, 6)을 통해 고객 단말기(200)와 온라인 은행 시스템(300) 및 전자 상거래 시스템(400)들을 연결하여, 무인증 접속으로 금융 거래 및 전자 상거래가 이루어지도록 고객 단말기(200)와 개인 금융 거래 중계 서버(100)를 연결한다.

【0037】 다중 안전 잠금 모듈(110)은 예컨대, 미들웨어로 구비되며, 고객 단말기(200)의 개인 인증 기능과 해킹 차단을 위한 방화벽 기능을 구비한다. 이 실시예에서 다중 안전 잠금 모듈(110)은 고객 단말기(200)로부터 지문 정보를 받아서 데이터베이스(120)에 기등록된 지문 정보와 일치하는지를 비교하는 지문 인식 처리부(112)와 온라인 은행 시스템(300)에 등록된 고객 단말기(200)의 계좌 비밀번호를 등록하는 계좌 비밀번호 처리부(114) 및 고객 단말기(200)의 전화번호를 이용하여 인증하는 전화번호 인증 처리부(116)를 포함한다.

[도 2] 개인 금융 거래 중계 서버의 구성



【0038】 데이터베이스(120)는 제어부(102)의 제어를 받아서 다중 안전 잠금 모듈(110)의 처리 과정에 따른 다양한 정보들을 저장한다.

【0039】 구체적으로 데이터베이스(120)는 회원 정보(122)와 지문 정보(124) 및 금융 정보(126)를 저장한다. 회원 정보(122)는 고객 단말기(200)들 각각이 개인 금융 거래 중계 서버(100)의 회원으로 등록할 때, 입력된 정보 즉, 고객 단말기(200)들의 사용자 정보 예를 들어, 이름, 아이디(ID), 비밀번호, 전화번호, 이메일 주소 등을 포함한다. 회원 정보(122)는 지문 정보(124)와 금융 정보(126)들과 상호 매칭 된다.

【0040】 지문 정보(124)는 고객 단말기(200)의 사용자가 개인 금융 거래 중계 서버(100)의 회원으로 등록 시, 고객 단말기(200)의 지문 인식기(210)로부터 획득된 지문 정보를 전송받아서 저장한다. 그리고 금융 정보(126)는 고객 단말기(200)의 온라인 은행 시스템(300)에 등록된 통장 계좌의 비밀번호를 저장한다.

【0041】 그리고 도 3은 본 발명에 따른 금융 거래 중계 시스템의 다중 안전 잠금 기능을 이용하여 무인증 금융 거래를 중계 처리하는 수순을 도시한 흐름도이다.

【0042】 도 3을 참조하면, 본 발명의 금융 거래 중계 시스템(2)은 단계 S150에서 고객 단말기(200)가 통신망(4)을 통하여 개인 금융 거래 중계 서버(100)에 접속하고, 단계 S152에서 회원으로 가입한다. 이때, 고객 단말기(200)는 성명, 아이디, 비밀번호, 전화번호, 이메일 주

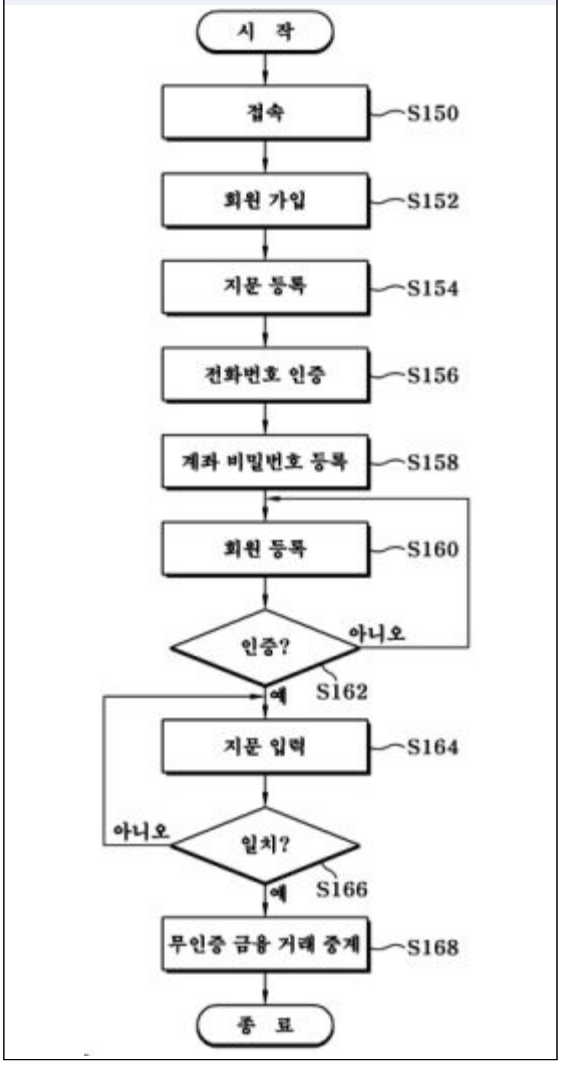
소 등의 회원 정보를 입력한다.

【0043】 단계 S154에서 고객 단말기(200)는 지문 인식기(210)를 통하여 지문 정보를 획득하고, 통신망(4)을 통하여 지문 정보를 개인 금융 거래 중계 서버(100)로 전송하면, 개인 금융 거래 중계 서버(100)는 고객 단말기(200)에 대응하여 지문 정보를 등록한다. 이 때, 개인 금융 거래 중계 서버(100)는 데이터베이스(120)에 지문 정보(124)를 저장한다.

【0044】 단계 S156에서 개인 금융 거래 중계 서버(100)는 전화번호를 이용하여 고객 단말기(200)를 인증한다. 단계 S158에서 개인 금융 거래 중계 서버(100)는 고객 단말기(200)의 통장 계좌번호에 대한 비밀번호를 등록한다. 등록된 계좌 비밀번호는 데이터베이스(120)의 금융 정보(126)에 저장된다.

【0045】 단계 S160에서 개인 금융 거래 중계 서버(100)는 지문 인증, 전화번호 인증 및 계좌 비밀번호 등록을 매칭시켜서 고객 단말기(200)를 회원으로 등록한다.

[도 3] 본 발명에 따른 금융 거래 중계 시스템의 다중 안전 잠금 기능을 이용하여 무인증 금융 거래를 중계 처리하는 수순



【0046】 단계 S162에서 고객 단말기(200)가 온라인 은행 거래 및 전자 상거래를 수행하기 위하여, 인증 절차를 처리하면, 단계 S164에서 개인 금융 거래 중계 서버(100)는 고객 단말기(200)로부터 지문 정보를 입력받아서 지문 인증을 처리한다.

【0047】 단계 S166에서 입력된 지문 정보가 데이터베이스(120)에 저장된 지문 정보(124)와 일치하면, 단계 S168에서 개인 금융 거래 중계 서버(100)는 무인증으로 온라인 은행 시스템(300) 또는 전자 상거래 시스템(400)에 접속하여 금융 거래를 중계한다.

㈐ 발명의 효과

【0017】 상술한 바와 같이, 본 발명의 금융 거래 중계 시스템은 고객 단말기의 지문 정보,

전화번호 및 계좌 비밀번호를 매칭시켜서 회원으로 등록하고, 고객 단말기가 온라인 은행 거래 및 전자 상거래 중 어느 하나를 수행하면, 고객 단말기로부터 지문 정보를 받아서 인증 처리함으로써, 온라인 은행 시스템 및 전자 상거래 시스템을 무인증 접속으로 금융 거래가 가능하다.

나. 선행발명들

1) 선행발명 1(갑 제4호증)

2006. 6. 9. 공개특허공보 제2006-0061996호로 공개된 '실시간 지문 인식을 통한 사용자 인증 방법 및 그 시스템'에 관한 것으로, 주요 내용은 다음과 같다.

㉮ 기술분야 및 배경기술

【0002】 본 발명은 실시간 지문 인식을 통한 사용자 인증 방법 및 그 시스템에 관한 것이다. 더욱 상세하게는, 전자 상거래 등의 결제 및 기타 무선 서비스 접속에 있어서 사용자의 지문을 실시간으로 인식하는 인증 방식을 사용함으로써 해킹의 염려를 원천적으로 막을 수 있는 보안성이 높은 인증 방법 및 시스템에 관한 것이다.

【0005】 최근에는 사용자 인증 방법으로서, 지문을 이용한 인증 방법이 사용되고 있다. 이 방법은 사용자 PC에서 인증용 지문 데이터를 네트워크로 전송하여 서버에 저장되어 있는 지문 데이터와 비교하여 인증하는 방식으로, 지문 데이터는 통상 암호화시켜 전송한다. 이 경우 지문 데이터가 네트워크로 전송하는 도중 해킹에 의해 노출되는 것을 방지하기 위해 해싱 함수(Hashing Function)라는 암호화 방식을 사용하여 해킹한 지문 자체는 사용이 불가능하게 구성하여 보안성을 강화하고 있다.

【0006】 여기서 해싱 함수(Hashing Function)란, 순 방향 계산은 쉬우나 역방향 계산은 매우 어렵다는 특징을 이용하여 한번 사용된 패스워드를 재사용할 수 없도록 하는 방식으로서, 패스워드가 서버로 전송되는 도중에 네트워크에서 노출되어도 이를 이용한 거짓 인증의 위험을 없앨 수 있는 방식이다.

【0007】 그러나, 이러한 방식 또한 지문을 암호화하는 단계가 아니라 인증 과정에 있어서의 암호화이기 때문에 원천적으로 해킹을 피할 수 있는 기술은 아니며, 인증 과정에 시간이 많이 소요된다는 단점이 있다.

【0008】 따라서, 해킹의 염려를 원천적으로 막을 수 있고, 사용자에게는 사용 방법이 간단하고 편리한 사용자 인증 방법이 요구된다.

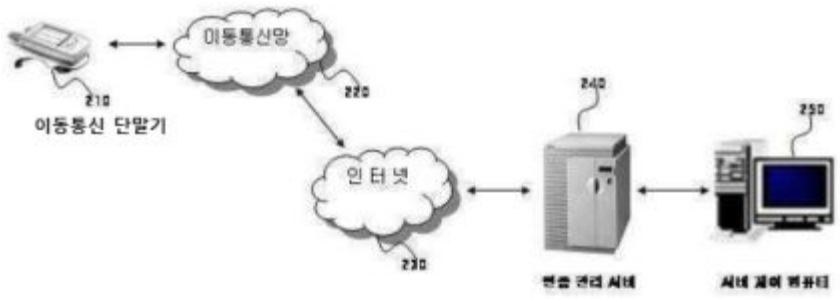
【0009】 특히, 이동통신 단말기에 장착되는 카메라의 화소수가 수십만 또는 수백만 화소 이상으로 향상되어 해상도 높은 촬영 이미지를 얻을 수 있어서 이러한 이동통신 단말기에 무선 통신망을 이용한 데이터 송신 기술을 적용하는 경우 먼 거리에서도 사물을 직접 대면하는 것과 같은 효과를 얻을 수 있으므로, 이동통신 단말기를 통해 실시간으로 전송되는 사용자 지문 정보를 이용할 경우 사용자의 간편함과 보안성을 모두 갖춘 인증 방법을 제공할 수 있을 것으로 기대된다.

【0010】 상기한 문제점을 해결하기 위해 본 발명은, 전자 상거래 등의 결제 및 기타 무선 서비스 접속에 있어 사용자의 지문을 실시간으로 인식하는 인증 방식을 사용함으로써 해킹의 염려를 원천적으로 막을 수 있고 보안 인증 방법을 제공함에 그 목적이 있다.

㈏ **발명의 구성 및 작용**

【0030】 본 발명의 바람직한 실시예에 따른 실시간 지문 인식을 통한 사용자 인증 서비스 시스템은 이동통신 단말기(210), 이동통신망(220), 인터넷(230), 인증 관리 서버(240), 서버 제어 컴퓨터(250)를 포함한다.

[도 2A] 본 발명의 바람직한 실시예에 따른 실시간 지문 인식을 통한 사용자 인증 서비스 시스템을 간략하게 나타낸 블록도



【0031】 이동통신 단말기(210)는 이동통신망(220)을 경유하여 상대방과 무선 통신으로 전화 통화를 수행할 뿐만 아니라 구비된 정보 검색 기능을 이용하여 무선으로 인터넷(230)에 접속하여 원하는 정보를 검색하고 데이터를 송수신할 수 있는 단말기이다. 이를 위해 이동통신 단말기(210)는 (중략) SK 텔레콤사의 'NATE' 등과 같은 인터넷 접속용 브라우저를 이용하여 이동통신망(220)을 경유하여 인증 관리 서버(240)로 접속한다.

【0016】 본 발명의 바람직한 실시예에 따른 실시간 지문 인식을 통한 사용자 인증 기능을 구비한 이동통신 단말기(100)의 내부 구성은 키 입력부(102), 디스플레이부(104), 프로그램 저장부(106), 모드 상태 저장부(108), 카메라부(110), 마이크로프로세서(112), 디지털 신호 처리부(114), 베이스밴드 변환부(116), RF 신호 처리부(118), 안테나(120), 스피커(122), 마이크로폰(124) 등을 포함한다.

[도 1] 본 발명의 바람직한 실시예에 따른 실시간 지문 인식을 통한 사용자 인증 기능을 구비한 이동통신 단말기의 내부 구성

【0017】 키 입력부(102)는 전화번호 등의 숫자를 입력하기 위한 숫자 키를 비롯하여 문자 입력을 위한 버튼과 메뉴 선택 버튼을 구비하고 있으며, 간편하게 무선 인터넷에 접속할 수 있도록 하는 특수키를 구비하고 있다. 또한, 본 발명의 실시예에 따라 이동통신 단말기에 구비된 카메라부(110)를 사용하여 실시간으로 지문 영상 데이터를 인증 관리 서버로 전송함으로써 보안 인증을 받을 수 있도록, 지문 부위를 촬영하기 위한 특수키를 구비하고 있다.

【0020】 프로그램 저장부(106)에는 본 발명의 바람직한 실시예에 따른 실시간 지문 인식을 통한 실시간 사용자 인증 프로그램이 탑재되어 있다. 실시간 지문 인식을 통한 실시간 사용자 인증 프로그램은 이동통신 단말기의 카메라부(110)를 통해 촬영된 사용자의 지문 부위에 관한 실시간 이미지 데이터를 사용자의 인증을 필요로 하는 업체 측의 인증 관리 서버(240)로 전송하거나, 인증 관리 서버(240)로부터 제공되는 메뉴 화면에 따라 이동통신 단말기를 제어하여 사용자 인증을 받을 수 있도록 짜인 프로그램으로서, 운영체제(OS)에 따라 여러 가지로 구현할 수 있는데, 'C' 프로그램 언어나 객체 지향형의 'C++', 'JAVA' 프로그램 언어로 구현할 수 있다.

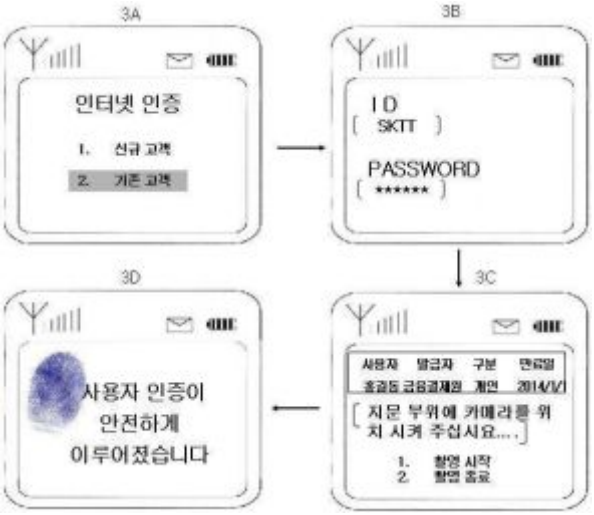
【0032】 이동통신망(220)은 무선 접속망, 이동통신 교환국, 망간 연동 장치 및 게이트웨이를 포함하고 있으며, 이동통신 단말기(210) 간의 통화 관리 및 이동통신 단말기(210)를 이용한 인터넷(230) 접속을 관리한다.

【0036】 인터넷(230)은 이동통신 단말기(210)가 이동통신 교환국을 거쳐 인증 관리 서버(240)에 접속하여서 데이터를 송수신하고 사용자 인증을 받을 수 있도록 접속 경로를 제공하는 통신망이다.

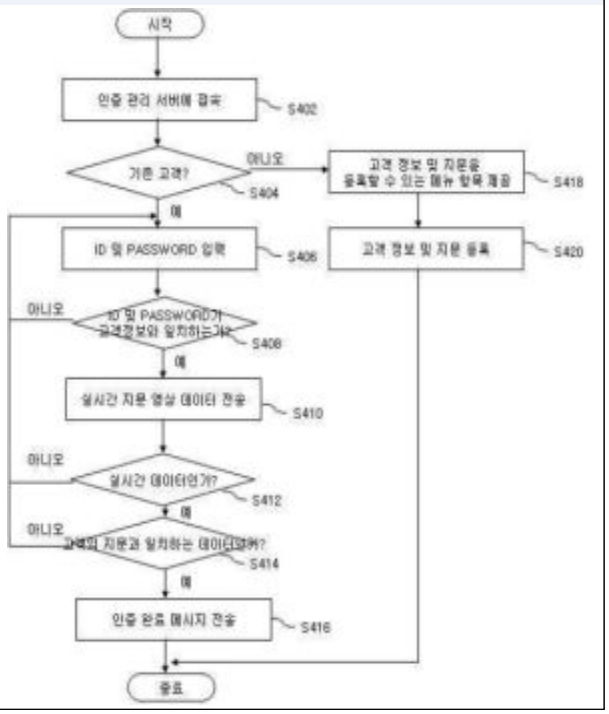
【0037】 인증 관리 서버(240)는 가입자가 자신의 지문을 등록할 수 있도록 하는 한편, 가입자가 인터넷 뱅킹이나 전자 상거래 등을 이용하기 위해 사용자 인증 요청을 하는 경우, 가입자의 이동통신 단말기에 부착되어 있는 카메라부를 통해 전송되는 실시간 지문 데이터와 미리 등록된 가입자의 지문 데이터를 비교하는 방식을 통해 사용자 인증 기능을 수행한다.

【0039】 위와 같은 시스템을 통해 가입자는 인증 관리 서버(240)에 자신의 지문을 등록한 후, 인터넷 뱅킹이나 전자 상거래 등을 이용하고자 할 시에 이동통신 단말기(100)에 부착되어 있는 카메라부(110)를 이용해 자신의 지문 데이터를 실시간으로 서버로 전송하며, 인증 관리 서버(240)는 서버 내의 데이터베이스(243)에 저장되어 있는 가입자의 지문 데이터와 실시간으로 전송되는 가입자의 지문 이미지 데이터를 비교하여 사용자 인증 여부를 판단하게 된다.

[도 3] 사용자의 이동통신 단말기에 제공되는 인터페이스 화면의 예시도

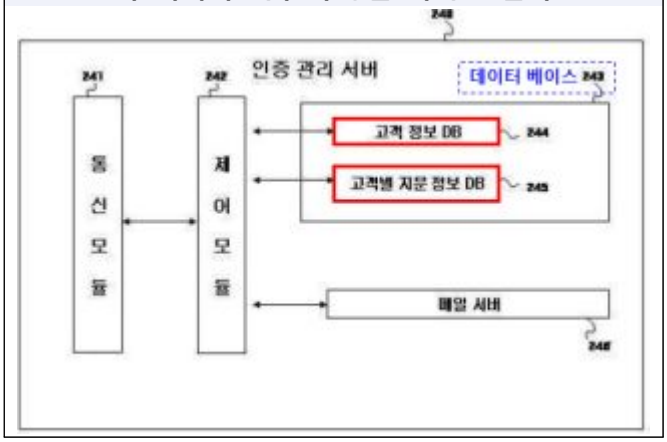


[도 4] 이동통신 단말기에 구비된 카메라부를 이용하여 실시간 지문 인식 방법에 의해 사용자 인증을 받는 과정



【0041】 도 2B에서 도시된 바와 같이, 본 발명의 바람직한 실시예에 따른 인증 관리 서버(240)는 통신 모듈(241), 제어 모듈(242), 데이터베이스(243) 및 메일 서버(246) 등을 포함할 수 있다.

[도 2B] 본 발명의 바람직한 실시예에 따른 인증 관리 서버의 내부 구성을 나타낸 블록도



【0042】 본 발명의 바람직한 실시예에 따른 통신 모듈(241)은 통신망을 통해 접속한 이동통신 단말기(210) 등과 필요한 정보를 송수신할 수 있게 한다. 즉, 인증 관리 서버(240)는 통신 모듈(241)을 통해 사용자 인증을 위한 서비스 가입자의 실시간 지문 이미지 데이터 등을 수신한다.

【0043】 본 발명의 바람직한 실시예에 따른 제어 모듈(242)은 이동통신 단말기 이용자에게 실시간 지문 인식을 통한 사용자 인증 서비스를 제공하기 위해 통신 모듈(241), 데이터베이스(243) 및 메일 서버(246) 등의 동작 및 이들 간의 통신을 제어한다. 상세하게는, 이동통신 단말기(210)의 접속 요청 신호를 전송받으면 데이터베이스(243)에서 고객 정보를 조회하여 인증 진행 여부를 결정하고, 신규 고객으로부터 접속 요청 신호를 전송받은 경우에는 가입 절차에 관한 메뉴 화면 및 인증 관리를 위한 지문 등록 절차를 안내한다.

【0044】 본 발명의 바람직한 실시예에 따른 데이터베이스(243)는 실시간 지문 인식을 통한 사용자 인증 서비스에 필요한 고객 정보, 고객별 지문 정보, 제품 구매 내역 정보, 인증 갱신 정보, 결제 정보를 저장하며, 제어모듈(242)의 제어에 의해 이동통신 단말기(210)나 전자상거래 업체 또는 인터넷 뱅킹 업체 등에 사용자인증을 위한 정보 등을 제공한다. 데이터베이스(243)는 내부 구성요소로서 고객 정보 데이터베이스(244), 고객별 지문 정보 데이터베이스(245) 등을 포함할 수 있다.

【0045】 본 발명의 바람직한 실시예에 따른 데이터베이스(243)는 실시간 지문 인식을 통한 사용자 인증 서비스를 이용하는 회원과 관련된 고객 정보를 가지고 있다. 여기서, 고객 정보는 회원의 성명, 회원 아이디, 비밀번호, 주민등록번호, 주소지, 전화번호, 전자메일 주소 등의 개인 정보뿐만 아니라 회원의 은행 계좌번호, 신용카드번호 등의 신용 정보 등을 포함할 수 있다. 고객 정보 데이터베이스(244)는 제어 모듈(242)의 제어에 의해 실시간 지문 인

식을 통한 사용자 인증 서비스를 받고자 하는 자가 신규 회원으로 가입하는 경우 새로운 고객 정보를 생성하며, 실시간 지문 인식을 통한 사용자 인증 서비스를 받고자 하는 자가 고객 정보를 변경하는 경우 고객 정보를 갱신하여, 가장 최근의 고객 정보를 가지고 있게 된다.

【0046】 또한, 본 발명의 바람직한 실시예에 따른 데이터베이스(243)는 실시간 지문 인식을 통한 사용자 인증 서비스를 이용하는 회원이 인증 관리 서버(240)로 전송한 지문 이미지 데이터를 가지고 있다. 여기서 지문 이미지 데이터는 서비스 회원으로부터 인터넷 뱅킹 또는 전자 상거래 등을 위한 사용자 인증 요청이 있는 경우 사용자 인증을 위한 기준이 되며, 제어 모듈(242)의 제어에 의해 사용자의 이동통신 단말기로부터 전송되는 실시간 지문 이미지 데이터가 고객별 지문 정보 데이터베이스(245)에 저장되어 있는 지문 이미지 데이터와 일치하는지 여부의 방식으로 사용자 인증 과정이 수행된다.

【0050】 인증 관리 서버(240)에 접속한 사용자는 인증 관리 서버(240)에서 제공하는 [0050] 사용자 인증에 관한 메뉴 화면에 따라 '신규 고객'인 경우와 '기존 고객'인 경우로 나누어서 절차를 진행하게 된다.

【0051】 '신규 고객' 항목은 사용자가 최초로 서비스에 가입하거나 기존 서비스 가입자인 경우라 하더라도 종전 지문에 갈음하는 새로운 지문으로 전자 상거래 등을 위한 사용자 인증을 받고자 할 때 선택하는 항목이다. 사용자는 '신규 고객' 항목을 선택하여 회원 정보에 관한 데이터 및 인증을 위한 지문 데이터 등을 등록한다.

【0052】 인증 관리 서버(240)는 이렇게 등록된 회원 정보에 관한 데이터 및 인증을 위한 지문 데이터를 데이터베이스(243)에 저장하고, 제어 모듈(242)의 제어에 의해 사용자 인증을 필요로 하는 다른 웹사이트로 전송할 수도 있다. 이러한 인증 관리 서버(240)를 포함하는 웹사이트를 통해 등록된 회원 정보에 관한 데이터 및 인증을 위한 지문 데이터는 모든 웹사이트들 각각에 대해 사용할 수 있기 때문에 모든 웹사이트들 각각에 대해 회원 정보 및 지문 등록을 각각 해야만 하는 번거로움과 불편을 제거할 수 있다.

【0053】 '기존 고객' 항목은 인터넷 뱅킹 또는 전자 상거래 등을 사용하고자 하는 인터넷 인증 서비스 회원이 실시간 지문 인식을 통한 사용자 인증을 받고자 하는 경우에 선택하는 항목이다.

【0054】 사용자가 '기존 고객' 항목을 선택하는 입력 신호를 발생시키는 경우 인증 관리 서

버(240)의 제어 모듈(242)은 도 3B에서 보이는 바와 같이 사용자의 ID와 PASSWORD를 확인하는 메뉴 항목을 발생시키도록 제어하고, 사용자의 ID 및 PASSWORD가 일치하는 경우에는 도 3C에서 보이는 바와 같이 고객별 지문 정보 데이터베이스(245)에 저장되어 있는 고객 지문과 대조하기 위해, 사용자의 이동통신 단말기(100)에 부착된 카메라부(110)를 통해 사용자의 지문 영상 데이터를 실시간으로 전송할 수 있도록 하는 메뉴 항목을 발생시키도록 제어한다. 여기서, 사용자의 ID와 PASSWORD를 확인하는 단계는 사용자가 인터넷 인증 서비스 회원인지 여부 및 데이터베이스(243)에 미리 저장되어 있는 지문 데이터를 추출하기 위해 사용되는 것이며, 실제적인 인증은 데이터베이스(243)에서 추출한 고객에 관한 지문 데이터와 사용자의 이동통신 단말기(100)로부터 실시간으로 전송되는 지문 영상 데이터를 비교 판단함으로써 이루어진다.

【0056】 사용자 인증 과정이 성공적으로 수행된 경우에는 도 3D와 같은 인증 확인 메시지가 사용자의 이동통신 단말기(100)에 전송되고, 사용자는 안전하게 인터넷 뱅킹, 전자 상거래 등과 같은 서비스를 이용할 수 있게 된다.

2) 선행발명 2(갑 제5호증)

2010. 11. 5. 등록특허공보 제992573호로 공고된 '휴대단말기를 이용한 인증 방법 및 시스템'에 관한 것으로, 주요 내용은 다음과 같다.

㉮ 기술분야

【0001】 본 발명은 휴대단말기를 이용한 인증 방법 및 시스템에 대한 것으로, 더욱 상세하게는 휴대단말기, 서비스 서버 및 인증 시스템을 연계하여 인증을 수행함으로써 ㅓ 타인에 의한 인증을 차단하는 휴대단말기를 이용한 인증 방법 및 시스템에 관한 것이다.

㉯ 발명의 내용 및 도면

【0027】 도 1을 참조하면, 본 발명에 따른 인증 방법은, 사용자 단말기(50)가 서비스 서버(300)에 접속하여 인증을 수행할 때, 예를 들어 로그인을 수행할 때, 서비스 서버(300)는 사용자 단말기(50)로 식별자가 포함되는 인증 인터페이스를 제공한다.

【0032】 사용자 단말기(50)의 모니터에 식별자(60)를 포함하는 인증 인터페이스가 표시된 후, 사용자는 휴대단말기(100)를 이용하여 식별자(60)를 촬상하고, 촬상된 식별자(60)를 인증 시스템(200)에 전송하거나 또는 촬상된 식별자(60)에 대해 이미지 프로세싱을 수행하여 숫자열,

문자열, 색상 값, 바코드 값 및 기타 인증 시스템(200)과 약정된 식별자 정보를 추출한다.

【0034】 다음으로, 휴대단말기(100)는 식별자 정보를 인증 시스템(200)에 제공한다.

【0035】 인증 시스템(200)은 휴대단말기(100)와 무선 네트워크로 접속되어 식별자 정보를 획득하거나 또는 휴대단말기(100)에 통신 서비스를 제공하는 이동통신사 서버(미도시)를 통해 유선 네트워크를 이용하여 식별자 정보를 획득할 수 있다.

【0037】 인증 시스템(200)은 서비스 서버(300)가 사용자 단말기(50)로 제공한 식별자로부터 식별자 정보를 생성하고, 이를 휴대단말기(100)가 제공한 식별자 정보를 비교하여 식별자 정보의 정당성을 판단한다. 이후, 식별자 정보가 정당하다고 판단되면, 인증 시스템(200)은 휴대단말기(100)로 인증 정보를 요청하며, 휴대단말기(100)는 인증 시스템(200)으로 인증 정보를 제공하여 최종 인증 과정을 수행하게 된다. 여기서, 인증 정보는,

【0038】 - 아이디/ 패스워드,

【0039】 - 사용자와 약정된 인증번호,

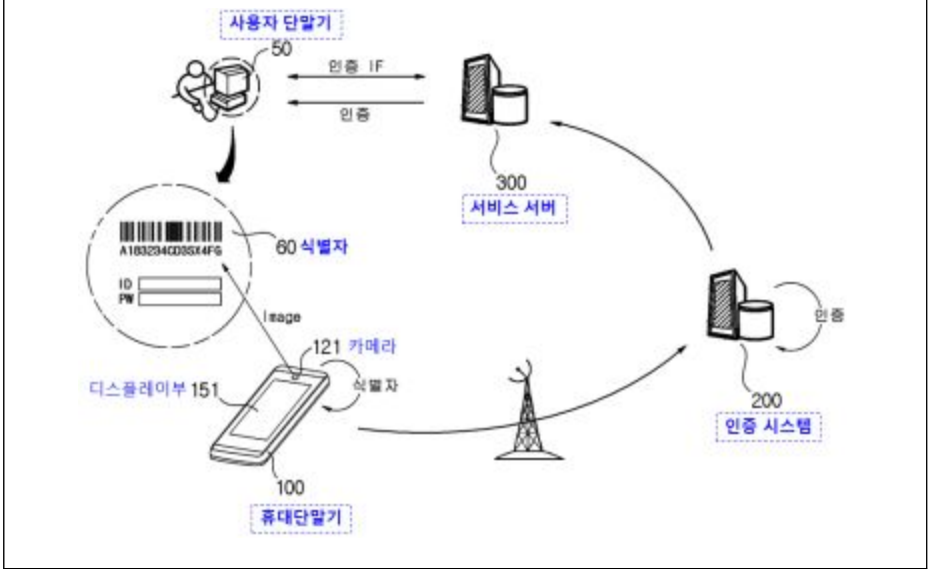
【0040】 - 홍체 정보, 지문 및 음성과 같은 생체정보,

【0041】 - 인증 시스템(200)이 휴대단말기(100)로 발급하는 임시 승인번호 중 어느 하나일 수 있다. 인증 시스템(200)이 사용자와 약정된 인증번호를 구비하는 경우, 사용자는 사용자 단말기(50) 또는 휴대단말기(100)를 통해 인증 시스템(200)에 자신의 인증번호를 미리 등록해둘 필요가 있으며, 임시 승인번호는 휴대단말기(100)의 식별자 정보가 정당할 때, 해당 휴대단말기(100)로 발급되는 1회성 승인번호일 수 있다.

【0045】 인증 시스템(200)은 휴대단말기(100)가 전송한 식별자 정보와 서비스 서버(300)에서 제공되는 식별자에 대한 식별자 정보가 일치하면, 휴대단말기(100)로부터 인증 정보를 획득하고, 인증 정보도 일치할 때, 서비스 서버(300)로 인증 결과(인증 성공 또는 인증 실패)를 통보한다. 서비스 서버(300)는 인증 결과에 따라 식별자가 발급된 사용자 단말기(50)를 인증하여 로그인 가능한 것으로 판단한다.

【0046】 이때, 인증 정보는, 휴대단말기(100)의 폰 번호, MAC 어드레스, USIM 또는 SIM 카드 정보 및 사용자 설정된 인증 번호 중 하나 또는 둘 이상일 수 있다. 여기서, MAC 어드레스는 유무선 통신을 수행하는 휴대단말기의 통신 모듈에 부여되는 고유 번호로서, 동일한 것이 존재하지 않으므로, 휴대단말기(100)를 확인하는데 매우 정확하고 유효하다.

[도 1]



3) 선행발명 3(갑 제6호증)

2012. 11. 19. 등록특허공보 제1202671호로 공고된 '사용자가 가입자 단말에서 단말 장치에 원격으로 접속할 수 있게 하기 위한 원격 접속 시스템 및 방법'에 관한 것으로, 주요 내용은 다음과 같다.

㉮ **기술분야**

【0001】 본 발명은 일반적으로 다른 네트워크 장치를 통하여 한 네트워크 장치에 저장된 데이터를 원격으로 관리하는 것에 관한 것으로, 구체적으로 사용자가 예를 들어 이동 전화와 같은 가입자 단말에서 개인용 컴퓨터와 같은 단말 장치에 원격으로 접속할 수 있게 하기 위한 원격 제어 시스템 및 방법에 관한 것이다.

㉯ **발명의 내용 및 도면**

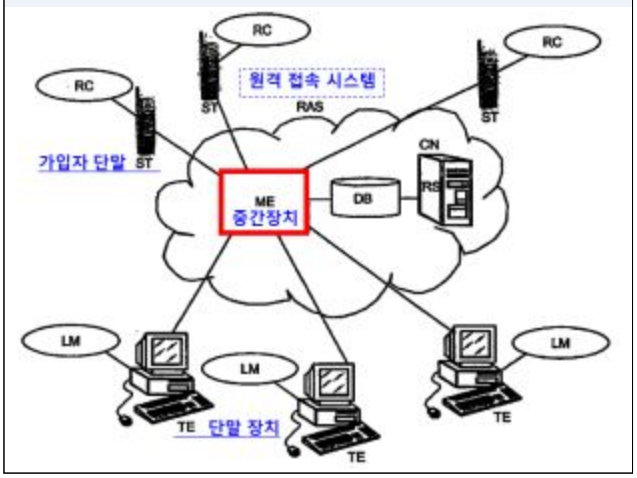
【0022】 도 1은 소위 이동 사무실 서비스, 즉 사용자가 그(그녀) 소유의 가입자 단말(ST)을 통하여 그(그녀) 소유의 단말 장치(TE)에 원격으로 접속할 수 있도록 하는 서비스를 제공하는 원격 접속 시스템(RAS)의 블록도를 나타낸다.

【0026】 본 발명의 바람직한 실시예에 따르면, 원격 접속 시스템은 서비스 센터에서 서버 상에서 동작하고, Radius 서버와 통신하는, 이하에서 중간 장치(Mediator; ME)로 불리는 중

간 장치 소프트웨어 어플리케이션 및 Radius 서버와 중간 장치 모두에 의해 접속 가능하고 이동 통신 네트워크에 연결되고 Radius 서버에 의해 인증된 가입자 단말 상의 정보를 포함하는 인증 데이터베이스(DB)를 포함한다.

【0028】 바람직하게, 중간 장치는 자바 언어로 구현되고 JADE(자바 에이전트 개발 프레임워크; 본 출원의 출원일에 주소 http://jade.tilab.com에서 인터넷을 통하여 접속 가능한 관련 문서)로 알려진 피어 투 피어(peer-to-peer) 에이전트 기반 어플리케이션을 위한 개방 소스 플랫폼을 사용하여 개발된 소프트웨어 어플리케이션이다. Jade는 FIPA(Foundation for Intelligent Physical Agents) 표준에 따르는 미들웨어 및 디버깅(debugging) 및 배포 단계를 지원하는 일련의 그래픽 툴들을 통하여 멀티 에이전트 시스템의 구현을 간단하게 한다.

[도 1]



【0029】 중간 장치는 중간 장치와 원격 제어기 및 중간 장치와 로컬 관리자 사이의 인증 및 비밀성 제한을 위하여 예를 들면, 보안 세션 레이어(SSL) 프로토콜을 사용하여 원격 제어기 및 로컬 관리자와 통신할 수 있다.

【0073】 또한 본 발명은 네트워크 어드레스 전송 시스템 및(또는) 동적 IP 어드레스 할당 뒤에 위치하거나 방화벽에 의해 보호되는 경우에도 사용자 단말 장치에 원격 접속할 수 있게 한다. 실제로, 중간 장치가 단말 장치와 가입자 단말 사이의 모든 통신을 중재하기 때문에, 단말 장치와 가입자 단말은 직접 연결될 필요가 없고, 통신이 도달해야만 하는 것은 단말 장치 및 가입자 단말이 아닌 단지 중간 장치이다.

【0074】 게다가 단말 장치 및 가입자 단말은 입력 연결(방화벽 및 NAT의 적절한 설정을 요구하는)을 처리할 필요가 없고 오직 중간 장치와의 연결을 시작하기만 하면 된다.

4) 선행발명 4(을 제3호증)

2003. 1. 23. 공개특허공보 제2003-0006901호로 공개된 '지문 인증에 의한 전자상거래 결제 시스템 및 방법'에 관한 것으로, 주요 내용은 다음과 같다.

㉮ **기술분야 및 배경기술**

【0002】 본 발명은 지문 인증에 의한 전자 상거래 결제 시스템 및 방법에 관한 것으로서, 보다 구체적으로는 인터넷 상에서 이루어지는 전자 상거래의 결제에 있어서 거래자의 지문 인증 과정을 추가시킴으로써 금융 정보의 유출로 인한 선의의 피해자의 발생을 방지하여 건전한 전자 상거래 질서를 확립하는데 기여하고자 하는 시스템 및 방법에 관한 것이다.

【0005】 현실적으로 전자 상거래의 대금 지급 방법으로 광범위하게 활용되고 있는 방법으로는 계좌 이체에 의한 직불 방법, 신용카드에 의한 후불 방법 및 캐시 카드나 IC카드를 활용한 전자결제 등이다. 이러한 방법들의 이용에 있어서 공통적으로 요구되는 것은 계좌번호나 카드번호 및 비밀번호의 전송인데, 이러한 금융 정보들이 아무런 조치 없이 인터넷 상에서 전송되는 것은 타인에 의한 도용의 위험이 내포되어 있어, 인터넷 거래자가 전자 상거래를 적극적으로 활용하는 것을 꺼리는 하나의 요인이 되어 건전한 전자 상거래의 발전을 저해할 수 있다.

【0008】 이러한 방법은 공통적으로 계좌번호나 신용카드번호 및 비밀번호 같은 금융 정보의 외부 유출을 막기 위한 방안으로서, 일단 타인에 의해 도용된 금융 정보의 무단 이용으로 인한 선의의 피해자의 양산 및 이로 인한 전자 상거래의 위축을 막기 위한 방안에 대한 논의는 활발하지 못한 실정이다.

【0006】 인터넷을 통한 전자 상거래의 발전을 위해서는 금융 정보의 보안을 유지하기 위한 방안이 제시되어야 하고, 현재 이에 대한 연구가 활발하게 진행되고 있다.

【0007】 그러나, 금융 정보에 대한 보안유지를 위한 방안으로서 제시되고 있는 것들의 대부분은 암호화 인증서 또는 인증키를 활용한 데이터의 암호화 또는 부호화나 전자서명 또는 네트워크의 전용선 또는 가상 전용선(VPN : Virtual Private Network)이다.

【0008】 이러한 방법은 공통적으로 계좌번호나 신용카드번호 및 비밀번호 같은 금융 정보의 외부 유출을 막기 위한 방안으로서, 일단 타인에 의해 도용된 금융 정보의 무단이용으로 인한 선의의 피해자의 양산 및 이로 인한 전자 상거래의 위축을 막기 위한 방안에 대한 논의는 활발하지 못한 실정이다.

【0009】 본 발명은 전자 상거래의 결제방식에 지문에 의한 본인 인증 과정을 추가시킴으로써 금융 정보의 도용으로 인한 거래자의 피해를 막고자 하는 취지에서 안출된 것이다.

【0011】 아울러, 본 발명은 전자 상거래의 결제방식에 지문에 의한 본인 인증 과정을 추가

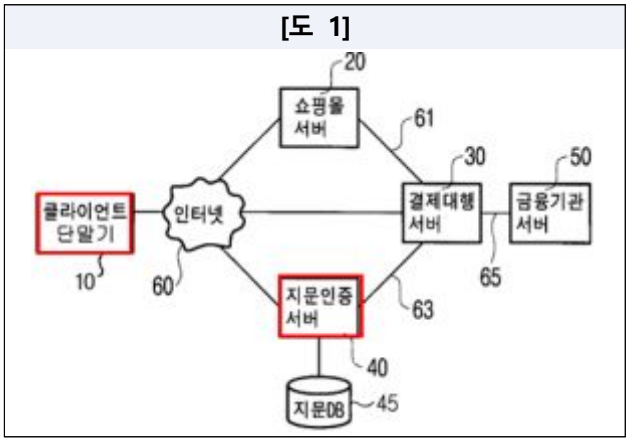
시키기 위해 기존의 전자 상거래 시스템과는 독립된 지문 인증 서버를 구축함으로써, 기존의 전자 상거래 시스템에 대한 호환이 보다 용이하도록 한 지문 인증에 의한 전자 상거래 결제 시스템 및 방법을 제공하는 데 다른 목적이 있는 것이다.

【0012】 또한, 본 발명의 목적은 전자 상거래의 결제방식에 지문에 의한 본인 인증 과정을 추가시키기 위해 기존의 전자 상거래 시스템과는 독립된 지문 인증 서버를 구축함으로써, 전자 상거래 시스템의 오동작시 이에 대한 문제 해결이 보다 신속하게 이루어질 수 있도록 한 지문 인증에 의한 전자 상거래 결제 시스템 및 방법을 제공하는 것이다.

㈐ 발명의 내용 및 도면

【0029】 도 1에서 보는 바와 같이, 인터넷을 이용하여 상품이나 서비스를 구매하는 거래자의 시스템을 의미하는 클라이언트 단말기(10)와 클라이언트 단말기(10)에게 각종 상품이나 서비스에 대한 정보와 광고를 제공하면서, 상품이나 서비스를 판매하는 쇼핑몰 서버(20), 쇼핑몰 서버(20)에서 이루어지는 거래에 대한 결제를 대행하는 결제 대행 서버(30) 및 지문에 의하여 거래자의 본인 인증을 하기 위한 지문 인증 서버(40)는 인터넷 상에서 연결되어 있고, 쇼핑몰 서버(20)와 결제 대행 서버(30), 결제 대행 서버(30)와 지문 인증 서버(40) 간에는 전용선(61, 63)으로 연결되어 있다.

[도 1]



【0030】 결제 대행 서버(30)와 금융기관 서버(50) 간에는 현재 금융결제원과 각종 은행 또는 신용카드 회사를 연결시켜 놓은 금융 공동 전산망이나 신용카드 회사 네트워크에 의하여 연결된다.

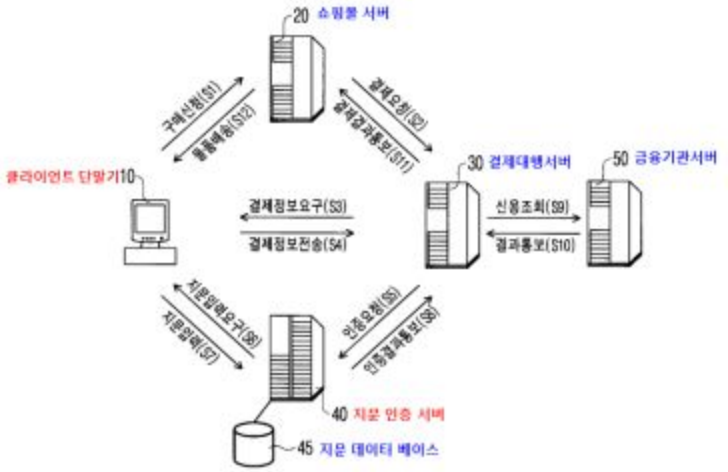
【0031】 거래자의 컴퓨터 시스템인 클라이언트 단말기(10)는 웹 서버에 접속하여 웹 페이지를 디스플레이하기 위하여 웹 브라우저를 구비하고 있어야 하고, 지문 인증 서버(40)에 의해 지문 인증을 받기 위해서는, 필수적으로 지문 입력기를 포함하는 지문 입력 모듈을 구비하고 있어야 한다.

【0033】 지문 인증 서버(40)는 사전에 거래자의 지문을 등록받아 이를 지문 데이터베이스(45)에 거래자를 특정할 수 있는 아이디(ID : Identification) 등과 함께 저장하여 두고, 결제

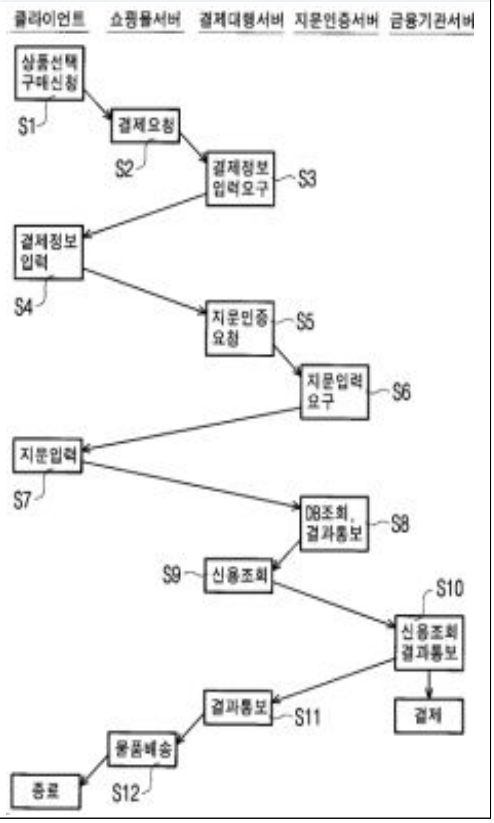
과정에서 거래자의 지문을 입력받아 저장되어 있는 지문데이터와 일치여부를 판단함으로써 본인인증을 하는 서버이다.

【0035】 전제되어야 할 것은 지문 인증 서버(40)의 지문 데이터베이스(45)에는 거래자의 지문데이터와 ID가 등록되어 있어야 한다는 것이다. 지문 등록 방법으로는 여러 가지 방법이 있을 수 있으나, 거래자가 쇼핑몰 서버(20)에 회원 등록 시 온라인 또는 오프라인으로 지문을 등록하는 방법을 생각할 수 있을 것이다.

[도 2]



[도 3]



【0036】 클라이언트 단말기(10)는 인터넷(60)을 통하여 쇼핑몰 서버(20)에 접속하여 쇼핑몰 서버(20)에서 제공하는 다양한 상품이나 서비스에 관한 정보를 토대로 원하는 품목을 선택하여 구매 신청을 한다(S1)(도 3 참조). 쇼핑몰 서버(20)에 접속하여 쇼핑을 하는 과정에서 등록회원에 관한 인증 과정을 거칠 수 있는데, 지문 인증 서버(40)를 이용하여 지문에 의한 인증을 하는 것도 가능하다. 클라이언트 단말기(10)의 구매 신청 시 품목, 수량, 대금 총액 등의 거래정보를 쇼핑몰 서버(20)에 전송한다. 거래자에 관한 정보는 등록된 정보를 활용할

수 있다.

【0039】 위와 같은 시스템을 통해 가입자는 인증 관리 서버(240)에 자신의 지문을 등록한 후, 인터넷 뱅킹이나 전자 상거래 등을 이용하고자 할 시에 이동통신 단말기(100)에 부착되어 있는 카메라부(110)를 이용해 자신의 지문 데이터를 실시간으로 서버로 전송하며, 인증 관리 서버(240)는 서버 내의 데이터베이스(243)에 저장되어 있는 가입자의 지문 데이터와 실시간으로 전송되는 가입자의 지문 이미지 데이터를 비교하여 사용자 인증 여부를 판단하게 된다.

【0045】 본 발명의 바람직한 실시예에 따른 데이터베이스(243)는 실시간 지문 인식을 통한 사용자 인증 서비스를 이용하는 회원과 관련된 고객 정보를 가지고 있다. 여기서, 고객 정보는 회원의 성명, 회원 아이디, 비밀번호, 주민등록번호, 주소지, 전화번호, 전자메일 주소 등의 개인 정보뿐만 아니라 회원의 은행 계좌번호, 신용카드번호 등의 신용 정보 등을 포함할 수 있다. 고객 정보 데이터베이스(244)는 제어 모듈(242)의 제어에 의해 실시간 지문 인식을 통한 사용자 인증 서비스를 받고자 하는 자가 신규 회원으로 가입하는 경우 새로운 고객 정보를 생성하며, 실시간 지문 인식을 통한 사용자 인증 서비스를 받고자 하는 자가 고객 정보를 변경하는 경우 고객 정보를 갱신하여, 가장 최근의 고객 정보를 가지고 있게 된다.

【0046】 또한, 본 발명의 바람직한 실시예에 따른 데이터베이스(243)는 실시간 지문 인식을 통한 사용자 인증 서비스를 이용하는 회원이 인증 관리 서버(240)로 전송한 지문 이미지 데이터를 가지고 있다. 여기서 지문 이미지 데이터는 서비스 회원으로부터 인터넷 뱅킹 또는 전자 상거래 등을 위한 사용자 인증 요청이 있는 경우 사용자 인증을 위한 기준이 되며, 제어 모듈(242)의 제어에 의해 사용자의 이동통신 단말기로부터 전송되는 실시간 지문 이미지 데이터가 고객별 지문 정보 데이터베이스(245)에 저장되어 있는 지문 이미지 데이터와 일치하는지 여부의 방식으로 사용자 인증 과정이 수행된다.

【0047】 본 발명의 바람직한 실시예에 따른 메일 서버(246)는 이동통신 단말기(210)나 전자 상거래 업체 또는 인터넷 뱅킹 업체 등에 전자메일 및(또는) 단문 메시지 서비스(Short Message Service)를 제공한다. 즉, 회원 확인 정보, 인증 확인 정보, 인증에 관한 갱신 안내 정보 등은 전자메일 형태 및(또는) 단문 메시지 형태로 이동통신 단말기(210) 등에 전송할 수 있다.

【0054】 사용자가 '기존 고객' 항목을 선택하는 입력 신호를 발생시키는 경우 인증 관리 서버(240)의 제어 모듈(242)은 도 3B에서 보이는 바와 같이 사용자의 ID와 PASSWORD를 확인하는 메뉴 항목을 발생시키도록 제어하고, 사용자의 ID 및 PASSWORD가 일치하는 경우에는 도 3C에서 보이는 바와 같이 고객별 지문 정보 데이터베이스(245)에 저장되어 있는 고객 지문과 대조하기 위해, 사용자의 이동통신 단말기(100)에 부착된 카메라부(110)를 통해 사용자의 지문 영상 데이터를 실시간으로 전송할 수 있도록 하는 메뉴 항목을 발생시키도록 제어한다. 여기서, 사용자의 ID와 PASSWORD를 확인하는 단계는 사용자가 인터넷 인증 서비스 회원인지 여부 및 데이터베이스(243)에 미리 저장되어 있는 지문 데이터를 추출하기 위해 사용되는 것이며, 실제적인 인증은 데이터베이스(243)에서 추출한 고객에 관한 지문 데이터와 사용자의 이동통신 단말기(100)로부터 실시간으로 전송되는 지문 영상 데이터를 비교 판단함으로써 이루어진다.

【0055】 이 경우, 진료 관리 서버(240)의 제어 모듈(242)은 사용자로부터 전송되는 지문 영상 데이터가 실시간 전송되는 데이터인지 판단하는 단계와 실시간 데이터인 경우에는 데이터베이스(243)에서 추출한 고객 지문과 일치하는 데이터인지를 판단하는 단계를 거쳐서 사용자 인증 과정을 수행하므로 네트워크상에서의 해킹 염려를 원천적으로 막을 수 있다. 즉, 이동통신 단말기(100)에 저장된 이미지를 이용하여 사용자 인증을 하는 방식이 아닌, 수신되는 데이터가 실시간 영상 데이터인 경우에만 인증 과정이 수행되는 방식을 채택함으로써 지문 이미지 데이터가 서버로 전송되는 도중에 네트워크에서 노출되어도 이를 이용한 거짓 인증의 위험을 방지할 수 있어서, 전자 상거래 등을 이용하는 사용자의 보안성을 높일 수 있다.

【0056】 사용자 인증 과정이 성공적으로 수행된 경우에는 도 3D와 같은 인증 확인 메시지가 사용자의 이동통신 단말기(100)에 전송되고, 사용자는 안전하게 인터넷 뱅킹, 전자 상거래 등과 같은 서비스를 이용할 수 있게 된다.

다. 이 사건 심결의 경위

1) 피고는 2022. 2. 8. 원고를 상대로 특허심판원에, 이 사건 제1항 발명은 해당 기술분야에서 통상의 지식을 가진 사람(이하 '통상의 기술자'라 한다)이 선행발명 1 내지 3에 의해, 이 사건 제4항 발명은 선행발명 1, 2에 의해 쉽게 발명할 수 있으므로,

진보성이 부정된다고 주장하면서 특허무효심판을 청구하였다(2022당336호).

2) 원고는 심판청구 계속 중인 2022. 3. 18. 이 사건 제1항 발명의 청구범위를 정정하는 내용의 정정청구를 하였다.

3) 특허심판원은 2022. 5. 25. 원고의 정정청구는 부적법하고, 정정청구 전의 이 사건 제1항 발명[1]은 선행발명 1 내지 3에 의해, 이 사건 제4항 발명은 선행발명 1, 2에 의해 진보성이 부정된다는 이유로 피고의 심판청구를 인용하는 심결을 하였다(이하 '이 사건 심결'이라 한다).

【인정근거】 다툼 없는 사실, 갑 제1 내지 6호증, 을 제3호증의 각 기재, 변론 전체의 취지

2. 당사자들의 주장

가. 원고

다음과 같은 이유로 이 사건 제1, 4항 발명은 진보성이 부정되지 않는다. 이와 달리 판단한 이 사건 심결은 위법하여 취소되어야 한다.

1) 이 사건 특허발명은 다중 안전 잠금 기능을 구비하고, 단 1회의 절차만으로 해당 시스템에 무인증 접속되게 하는 금융 거래 중계 서버를 개시하고 있다. 반면 선행발명들에는 이와 같은 기술사상이 나타나 있지 않다. 따라서 이 사건 특허발명과 선행발명 1 내지 4는 그 기술분야 및 과제해결의 원리, 작용효과가 상이하다.

2) 이 사건 제1항 발명의 구성요소 1, 4 내지 6은 선행발명들로부터 쉽게 도출할 수 없다.

3) 이 사건 제4항 발명은 선행발명 1, 2, 4로부터 쉽게 도출할 수 없다.

---

1) 앞서 1. 가. 항에 기재된 이 사건 특허발명과 동일하다.

나. 피고

다음과 같은 이유로 이 사건 제1, 4항 발명은 진보성이 부정된다. 이와 같이 판단한 이 사건 심결은 적법하다.

1) 이 사건 제1항 발명과 선행발명들은 모두 인증에 관한 것으로 기술분야가 동일하고, 인증 처리만을 위한 인증 서버를 별도로 두고 있다는 점에서 구성도 동일하다.

2) 이 사건 제1항 발명과 선행발명 1, 2, 4는 다양한 고객 정보가 인증 서버에 등록된다는 점, 고객 지문 정보에 기반을 둔 인증이 인증 서버에서 완료되면 고객 단말기가 서비스 서버로 무인증 접속된다는 점에서 동일하다.

3) 이 사건 제1항 발명에 개시된 '미들웨어 및 방화벽' 구성은 주지관용기술에 해당할 뿐만 아니라 선행발명 3에 개시된 '인증 기능을 하는 중각 장치가 미들웨어로 구현되어 있고 방화벽으로 보호'되는 구성과 동일하다.

4) 따라서 이 사건 제1항 발명은 선행발명 1에 선행발명 2, 3, 4를 결합하여 쉽게 도출할 수 있다.

5) 이 사건 제4항 발명은 이 사건 제1항 발명의 방법 발명으로서 그 내용이 실질적으로 동일하므로, 선행발명 1에 선행발명 2, 3, 4를 결합하여 쉽게 도출할 수 있다.

3. 이 사건 심결의 위법 여부[2)]

가. 이 사건 제1항 발명의 진보성 부정 여부

1) 기술분야 대비

가) 이 사건 제1항 발명은 고객 단말기와 온라인 은행 시스템 및 전자 상거래 시스템들 사이를 중계하는 시스템으로서, 공인인증서 등 은행에서 제공되는 종래의 보

2) 원고는 이 사건 심결 중 정정청구가 부적법하다고 보아 인정되지 않은 부분에 대해서는 다투지 않으므로, 이하 정정 청구 전의 이 사건 특허발명을 대상으로 등록무효사유가 존재하는지를 판단한다.

안 기술만으로는 사용자의 실수로 인한 보안 사고를 방지할 수 없다는 종래 기술의 문제점을 해결하고 사용자의 편의를 높이기 위하여, 고객 단말기와 온라인 은행 시스템(또는 전자 상거래 시스템) 사이에서 거래를 중계하는 개인 금융 거래 중계 서버를 구축하고, 해당 서버에 사용자의 지문, 전화번호 및 계좌번호를 등록하고, 지문 정보를 이용하여 인증 업무를 처리하는 다중 안전 잠금 모듈을 구비하고 있다(갑 제2호증 식별번호 [0001] 내지 [0004], [0006] 내지 [0011], 청구항 1 참조).

나) 선행발명 1은 실시간 지문 인식을 통한 사용자 인증 방법 및 그 시스템에 관한 것으로서, 인증 데이터가 전송 과정에서 노출될 위험이 있다는 종래 기술의 문제점을 해결하고 보안성을 높이기 위하여, 사용자 단말로부터 실시간으로 채취되어 전송되는 사용자의 지문을 인증 관리 서버에 저장된 지문과 대조하여 인증하는 방식을 채택하고 있다(갑 제4호증 식별번호 [0002] 내지 [0010], [0029], 도2 참조).

다) 선행발명 2는, 서비스 서버에서 인증을 함께 처리하는 경우 서비스 서버가 해킹되면 서비스 서버에 저장된 인증 정보가 노출될 수 있다는 종래 기술의 문제점을 해결하기 위하여, 서비스 서버와 인증 서버를 분리하고, 사용자 단말기에서 서비스 서버로 서비스 요청이 들어오면, 서비스 서버는 인증 서버로부터 식별자 정보를 받아 사용자 단말기를 통해 사용자에게 보여준 다음, 사용자가 휴대폰 단말기를 이용하여 사용자 단말기에 표시된 식별자를 촬영하여 인증 서버로 전송하면, 인증 서버가 식별자의 동일 여부를 판단한 후 동일한 경우 사용자 단말기로 지문 등의 인증 정보를 요청하여 인증을 수행하는 구성을 채택하고 있다(갑 제5호증 식별번호 [0001] 내지 [0011], [0013], [0027] 내지 [0041] 참조).

라) 선행발명 3은 단말 장치와 가입자 단말 사이의 통신의 비밀 및 보안성을 보

장하는 것 등에 그 목적이 있고, 이를 위하여 단말 장치와 가입자 단말 사이에서 사용자가 가입자 단말을 통하여 단말 장치에 원격으로 접속할 수 있도록 중계하는 구성(원격 접속 시스템)을 채택하고 있다(갑 제6호증 식별번호 [0011] 참조).

마) 선행발명 4는 전자 상거래 과정에서 금융 정보 도용으로 인한 사용자의 피해를 방지하는 것에 그 목적이 있고, 이를 위하여 전자 상거래 시스템과 독립된 지문 인증 시스템을 구축하고 결제 시 사용자로부터 지문 정보를 입력받아 지문 인증 시스템에서 인증을 수행하는 구성을 채택하고 있다(을 제3호증 식별번호 [0002], [0003] 참조).

바) 이 사건 제1항 발명과 선행발명 1, 2, 4는 금융 거래, 전자 상거래 등 서비스를 제공하는 시스템으로부터 분리된 별도의 인증 관리 서버에서 사전에 입력, 저장된 지문 정보와 인증 시 입력된 지문 정보를 대조하여 인증을 수행한다는 점에서 기술분야가 공통된다.

사) 선행발명 3은 지문 인증에 관한 것은 아니지만, 네트워크 시스템의 보안을 강화한다는 점에서 이 사건 특허발명과 목적이 공통되고, 서비스를 제공하는 서버로부터 분리된 인증 서버[원격 접속 시스템]에서 고객 단말기[가입자 단말]와 온라인 거래 시스템 등[단말 장치]을 중계한다는 점에서 이 사건 특허발명과 기술분야가 동일하다.

2) 구성 대비

이 사건 제1항 발명의 구성요소와 선행발명 1의 구성요소를 대비하면 다음 표 기재와 같다.

구성요소	이 사건 제1항 발명	선행발명 1(갑 제4호증)
1-1	금융 거래 중계 시스템에 있어서:	사용자 인증 서비스 시스템에 있어서,

구성 요소	이 사건 제1항 발명	선행발명 1(갑 제4호증)
1-2	통신망과;	이동통신망(220) 또는 인터넷(230)(식별번호 [0030])
1-3	상기 통신망에 연결되고, 지문 정보를 입력하는 지문 인식기를 구비하는 고객 단말기 및;	이동통신 단말기에 구비된 카메라부(110)를 사용하여 실시간으로 지문 영상 데이터를 인증 관리 서버로 전송(식별번호 [0017])
1-4	상기 고객 단말기가 상기 통신망을 통하여 접속되고, 상기 고객 단말기로부터 지문 정보, 전화번호 및 계좌 비밀번호를 전송받아서 회원으로 등록하고, 상기 고객 단말기가 온라인 은행 거래 및 전자 상거래 중 어느 하나를 수행하면, 상기 고객 단말기로부터 지문 정보만을 전송받아서 인증하여 온라인 은행 시스템 또는 전자 상거래 시스템으로 무인증 접속하여 금융 거래가 이루어지도록 중계 처리하는 개인 금융 거래 중계 서버를 포함하되;	사용자가 본 발명의 실시예에 따른 인터넷 인증 서비스를 이용하여 사용자 인증을 받고자 하는 경우, 이동 통신 단말기(210)의 무선 인터넷 메뉴의 '인터넷 인증' 항목을 지정하여 인증 관리 서버(240)에 접속한다(식별번호 [0049]). 인증 관리 서버(240)에 접속한 사용자는 인증 관리 서버(240)에서 제공하는 사용자 인증에 관한 메뉴 화면에 따라 절차를 진행하게 된다. 사용자는 '신규 고객' 항목을 선택하여 회원 정보에 관한 데이터 및 인증을 위한 지문 데이터 등을 등록한다(식별번호 [0050], [0051]). '기존 고객' 항목은 인터넷 뱅킹 또는 전자 상거래 등을 사용하고자 하는 인터넷 인증 서비스 회원이 실시간 지문 인식을 통한 사용자 인증을 받고자 하는 경우에 선택하는 항목이다(식별번호 [0053]). 사용자가 '기존 고객' 항목을 선택하는 입력 신호를 발생시키는 경우 인증 관리 서버(240)의 제어 모듈(242)은 사용자의 ID와

구성 요소	이 사건 제1항 발명	선행발명 1(갑 제4호증)
		PASSWORD를 확인하는 메뉴 항목을 발생시키도록 제어하고, 사용자의 ID 및 PASSWORD가 일치하는 경우에는 고객별 지문 정보 데이터베이스(245)에 저장되어 있는 고객 지문과 대조하기 위해, 사용자의 이동통신 단말기(100)에 부착된 카메라부(110)를 통해 사용자의 지문 영상 데이터를 실시간으로 전송할 수 있도록 하는 메뉴 항목을 발생시키도록 제어한다. 여기서, 사용자의 ID와 PASSWORD를 확인하는 단계는 사용자가 인터넷 인증 서비스 회원인지 여부 및 데이터베이스(243)에 미리 저장되어 있는 지문 데이터를 추출하기 위해 사용되는 것이며, 실제적인 인증은 데이터베이스(243)에서 추출한 고객에 관한 지문 데이터와 사용자의 이동통신 단말기(100)로부터 실시간으로 전송되는 지문 영상 데이터를 비교 판단함으로써 이루어진다(식별번호 [0053], [0054]).
1-5	상기 개인 금융 거래 중계 서버는; 상기 고객 단말기로부터 지문 정보를 받아서 기등록된 지문 정보와 일치하는지를 비교하는 지문 인식 처리부와 상기 온라인 은행 시스템에 등록된 상기 고객 단말기의 계좌 비밀번호를 등록하는 계좌 비밀번호 처리부 및 상기 고객 단말기의 전화번호를 이용하여 인	인증 관리 서버(240)는 가입자가 자신의 지문을 등록할 수 있도록 하는 한편, 가입자가 인터넷 뱅킹이나 전자 상거래 등을 이용하기 위해 사용자 인증 요청을 하는 경우, 가입자의 이동통신 단말기에 부착되어 있는 카메라부를 통해 전송되는 실시간 지문 데이터와 미리 등록된 가입자의 지문 데이터를 비교하

구성요소	이 사건 제1항 발명	선행발명 1(갑 제4호증)
	증하는 전화번호 인증 처리부를 포함하는 다중 안전 잠금 모듈과 상기 지문 정보, 상기 계좌 비밀번호 및 상기 전화번호를 저장하는 데이터베이스를 구비하고,	는 방식을 통해 사용자 인증 기능을 수행한다(식별번호 [0037]). 본 발명의 바람직한 실시예에 따른 데이터베이스(243)는 실시간 지문 인식을 통한 사용자 인증 서비스를 이용하는 회원과 관련된 고객 정보를 가지고 있다. 여기서, 고객 정보는 회원의 성명, 회원 아이디, 비밀번호, 주민등록번호, 주소지, 전화번호, 전자메일 주소 등의 개인 정보뿐만 아니라 회원의 은행 계좌번호, 신용카드번호 등의 신용 정보 등을 포함할 수 있다. 또한, 본 발명의 바람직한 실시예에 따른 데이터베이스(243)는 실시간 지문 인식을 통한 사용자 인증 서비스를 이용하는 회원이 인증 관리 서버(240)로 전송한 지문 이미지 데이터를 가지고 있다(식별번호 [0045], [0046]).
1-6	상기 다중 안전 잠금 모듈은 미들웨어로 구비되며, 해킹 차단을 위한 방화벽 기능을 더 구비하는 것을 특징으로 하는 금융 거래 중계 시스템.	(대응구성 없음)

3) 공통점 및 차이점

가) 구성요소 1-1

이 사건 제1항 발명의 구성요소 1-1은 '금융 거래 중계 시스템'으로서 그 서비스 대상이 금융 거래에 한정되나, 선행발명 1의 대응 구성요소는 '사용자 인증 서비스 시스템'으로서 그 서비스 대상이 금융 거래에 한정되지 않고 사용자 인증이 요구되는

모든 서비스 시스템에 해당된다는 점에서 차이가 있다(이하 '**차이점 1**'이라 한다).

나) 구성요소 1-2, 1-3

이 사건 제1항 발명 구성요소 1-2와 선행발명 1의 대응 구성요소는 모두 '통신망'이라는 점에서 동일하다. 이 사건 제1항 발명의 구성요소 1-3과 선행발명 1의 대응 구성요소는 모두 '통신망[이동통신망 또는 인터넷]에 연결되고 지문 인식기[실시간으로 지문 영상 데이터를 채취하는 카메라부]를 구비한 단말기'라는 점에서 동일하다(이에 관하여는 당사자 사이에 다툼이 없다).

다) 구성요소 1-4

이 사건 제1항 발명 구성요소 1-4와 선행발명 1의 대응 구성요소는 모두 고객 단말기[이동통신 단말기]가 통신망[이동통신망 또는 인터넷]을 통하여 접속되고, 고객 단말기[이동통신 단말기]를 통해 회원 정보 및 지문 정보[지문 데이터]를 전송받아서 데이터베이스에 등록하며, 고객 단말기[이동통신 단말기]를 이용하여 온라인 은행 거래나 전자 상거래를 수행하려는 사용자로부터 고객 단말기[이동통신 단말기]를 통해 지문[지문 데이터]를 전송받아 사용자 인증을 한다는 점에서 동일하다.

반면 이 사건 제1항 발명의 구성요소 1-4는 고객 등록 시 계좌 비밀번호를 입력받지만, 선행발명 1의 대응 구성요소에는 계좌 비밀번호의 입력 여부가 명시되어 있지 않다는 점에서 차이가 있다(이하 '**차이점 2**'라 한다). 이 사건 제1항 발명의 구성요소 1-4는 온라인 은행 거래나 전자 상거래 수행 시 고객 단말기로부터 지문 정보만을 전송받아 인증을 수행하지만, 선행발명 1의 대응 구성요소는 먼저 사용자의 아이디와 패스워드(Password)를 입력 받고, 저장된 정보와 일치하는 경우 사용자의 지문 정보를 추가로 전송받아 인증한다는 점에서 차이가 있다(이하 '**차이점 3**'이라 한다). 이 사건

제1항 발명의 구성요소 1-4는 개인 금융 거래 중계 서버가 온라인 은행 시스템 또는 전자 상거래 시스템에 접속하여 금융 거래를 중계하지만, 선행발명 1의 대응 구성요소에는 인증 관리 서버의 금융 거래 중계 여부가 명시되어 있지 않다는 점에서도 차이가 있다(이하 '**차이점 4**'라 한다).

라) 구성요소 1-5

이 사건 제1항 발명의 구성요소 1-5와 선행발명 1의 대응 구성요소는 고객 단말기[이동통신 단말기]로부터 지문 정보를 입력받아서 데이터베이스에 이미 등록되어 있는 지문 정보와 비교한다는 점에서 동일하다.

그러나 이 사건 제1항 발명의 구성요소 1-5는 고객 단말기의 계좌 비밀번호를 등록하는 계좌 비밀번호 처리부를 구비하나 선행발명 1의 대응 구성요소에는 계좌 비밀번호 등록에 관하여 명시되어 있지 않고(이하 '**차이점 5**'라 한다), 이 사건 제1항 발명의 구성요소 1-5는 고객 단말기의 전화번호를 이용하여 인증하는 전화번호 인증 처리부를 구비하나, 선행발명 1의 대응 구성요소에는 전화번호를 이용한 인증에 관하여 명시되어 있지 않다는 점에서 차이가 있다(이하 '**차이점 6**'이라 한다). 나아가 이 사건 제1항 발명의 구성요소 1-5는 지문 인식 처리부, 계좌 비밀번호 처리부, 전화번호 인증 처리부로 구성되는 다중 안전 잠금 모듈을 구비하고 있으나, 선행발명 1의 대응 구성요소에는 이러한 구성이 명시되어 있지 않다는 점에서 차이가 있다(이하 '**차이점 7**'이라 한다).

마) 구성요소 1-6

이 사건 제1항 발명의 구성요소 1-6은 '다중 안전 잠금 모듈이 미들웨어로 구비되며, 방화벽 기능을 더 구비'하는 것이지만, 선행발명 1의 대응 구성요소에는 이러

한 구성이 명시되어 있지 않다는 점에서 차이가 있다(이하 '**차이점 8**'이라 한다).

4) 차이점들에 관한 분석

가) 차이점 1, 4

다음과 같은 이유로 차이점 1, 4는 통상의 기술자가 선행발명 1로부터 쉽게 극복할 수 있다.

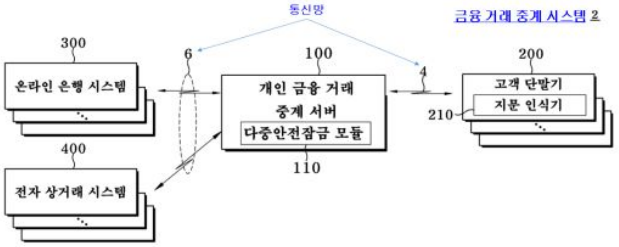
(1) 이 사건 특허발명 명세서의 다음과 같은 기재에 의하면, 이 사건 제1항 발명의 '금융 거래 중계 시스템'은 고객 단말기로부터 입력된 사용자의 지문 정보와 금융 거래 중계 시스템에 등록된 지문 정보를 대조하여 사용자 인증을 수행함으로써 별도의 추가 인증 없이 고객 단말기가 온라인 은행 거래 또는 전자 상거래 시스템에 접속되도록 기능한다는 점을 알 수 있다.

이 사건 특허발명(갑 제2호증)

【0009】 본 발명의 금융 거래 중계 시스템은 지문 인식을 포함하는 다중 안전 잠금 기능을 이용하여 금융 거래를 중계하도록 처리하는데 그 한 특징이 있다. 이와 같은 금융 거래 중계 시스템은 고객단말기가 온라인 은행 거래 및 전자 상거래 중 어느 하나를 수행하면, 고객 단말기로부터 지문 정보를 받아서 인증 처리함으로써, 온라인 은행 시스템 및 전자 상거래 시스템을 무인증 접속으로 금융 거래가 가능하다.

【0031】 온라인 은행 시스템(300)은 제휴 은행에 구비되어, 온라인으로 처리되는 은행 업무 예를 들어, 입출금, 이체 등의 금융 거래를 처리한다. 온라인 은행 시스템(300)은 금융 거래 시, 개인 금융 거래 중계 서버(100)를 통해 고객 단말기(200)가 무인증으로 접속된다.

[도 1] 본 발명에 따른 금융 거래 중계 시스템의 네트워크 구성



(2) 선행발명 1 명세서의 다음과 같은 기재에 의하면, 선행발명 1의 '사용자 인증 서비스 시스템'은 이동통신 단말기로부터 입력된 지문 데이터를 데이터베이스에 저장된 지문 데이터와 비교하는 방식으로 사용자 인증을 수행한다는 점을 알 수 있다. 비록 선행발명 1의 명세서에는 위 인증 이후 인터넷 뱅킹 등을 위하여 추가 인증이 필요하지 않다는 내용이 명시되어 있지는 않다. 그러나 "인증 관리 서버(240)는 이렇게 등록된 회원 정보에 관한 데이터 및 인증을 위한 지문 데이터를 데이터베이스(243)에 저장하고, 제어 모듈(242)의 제어에 의해 사용자 인증을 필요로 하는 다른 웹사이트로 전송할 수도 있다. 이러한 인증 관리 서버(240)를 포함하는 웹사이트를 통해 등록된 회원 정보에 관한 데이터 및 인증을 위한 지문 데이터는 모든 웹사이트들 각각에 대해 사용할 수 있기 때문에 모든 웹사이트들 각각에 대해 회원 정보 및 지문 등록을 각각 해야만 하는 번거로움과 불편을 제거할 수 있다.", "사용자 인증 과정이 성공적으로 수행된 경우에는 도 3D와 같은 인증 확인 메시지가 사용자의 이동통신 단말기(100)에 전송되고, 사용자는 안전하게 인터넷 뱅킹, 전자 상거래 등과 같은 서비스를 이용할 수 있게 된다."라는 기재에 비추어(갑 제4호증 식별번호 [0052], [0056] 참조), 선행발명 1의 경우에도 지문 인증 서버에서 인터넷 뱅킹 또는 전자 상거래 시스템에 등록되는 지문 정보를 일괄 관리할 수 있다는 점, 일단 지문 인증이 완료되면 각각의 웹사이트에 추가 인증 없이도 사용자가 인터넷 뱅킹 또는 전자 상거래 시스템에 접속되도록 기능할 수 있다는 점을 알 수 있다. 따라서 선행발명 1의 인증 관리 서버의 경우에도 일단 지문 데이터를 이용한 인증이 완료되면, 별도의 추가 인증 없이 인터넷 뱅킹, 전자 상거래 시스템에 접속할 수 있다는 점에서 이 사건 특허발명의 '금융 거래 중계 시스템'과 실질적으로 동일하다(설령 실질적으로 동일하지 않더라도, 적어도 선행발명 1에는 지문 인증이 완료되면 별도 추가 인증 없이 사용자 단말기를 인터넷 뱅킹, 전자 상거래 시스템에 접속시키는 구성이 암시되어 있다고 볼 수 있

다).

선행발명 1(갑 제5호증)
【0037】 인증 관리 서버(240)는 가입자가 자신의 지문을 등록할 수 있도록 하는 한편, 가입자가 인터넷 뱅킹이나 전자 상거래 등을 이용하기 위해 사용자 인증 요청을 하는 경우, 가입자의 이동통신 단말기에 부착되어 있는 카메라부를 통해 전송되는 실시간 지문 데이터와 미리 등록된 가입자의 지문 데이터를 비교하는 방식을 통해 사용자 인증 기능을 수행한다. 【0039】 위와 같은 시스템을 통해 가입자는 인증 관리 서버(240)에 자신의 지문을 등록한 후, 인터넷 뱅킹이나 전자 상거래 등을 이용하고자 할 시에 이동통신 단말기(100)에 부착되어 있는 카메라부(110)를 이용해 자신의 지문 데이터를 실시간으로 서버로 전송하며, 인증 관리 서버(240)는 서버 내의 데이터베이스(243)에 저장되어 있는 가입자의 지문 데이터와 실시간으로 전송되는 가입자의 지문 이미지 데이터를 비교하여 사용자 인증 여부를 판단하게 된다. 【0052】 인증 관리 서버(240)는 이렇게 등록된 회원 정보에 관한 데이터 및 인증을 위한 지문 데이터를 데이터베이스(243)에 저장하고, 제어 모듈(242)의 제어에 의해 사용자 인증을 필요로 하는 다른 웹사이트로 전송할 수도 있다. 이러한 인증 관리 서버(240)를 포함하는 웹사이트를 통해 등록된 회원 정보에 관한 데이터 및 인증을 위한 지문 데이터는 모든 웹사이트들 각각에 대해 사용할 수 있기 때문에 모든 웹사이트들 각각에 대해 회원 정보 및 지문 등록을 각각 해야만 하는 번거로움과 불편을 제거할 수 있다. 【0056】 사용자 인증 과정이 성공적으로 수행된 경우에는 도 3D와 같은 인증 확인 메시지가 사용자의 이동통신 단말기(100)에 전송되고, 사용자는 안전하게 인터넷 뱅킹, 전자 상거래 등과 같은 서비스를 이용할 수 있게 된다.

(3) 선행발명 1에는 지문을 이용하여 인증 처리를 수행하는 인증 관리 서버를 전자 상거래 업체 또는 인터넷 뱅킹 거래에 적용할 수 있다는 점이 암시되어 있다(갑 제4호증 식별번호 [0046] 참조).

(4) 나아가 통상의 기술자가 선행발명 1의 인증 관리 서버 구성을 금융 거래에 적용하는 데에 특별한 기술적 어려움이 있다고 볼 수도 없다.

나) 차이점 2, 5

다음과 같은 이유로 차이점 2, 5는 통상의 기술자가 선행발명 1로부터 또는 선행발명 1에 주지관용기술을 결합하여 쉽게 극복할 수 있다.

(1) 아래에서 보는 바와 같이 이 사건 제1항 발명의 명세서에는 '고객 단말기로부터 지문 정보, 전화번호 및 계좌 비밀번호를 매칭시켜서 회원으로 등록하고, 지문 정보를 이용하여 인증 업무를 처리한다.'는 내용만이 기재되어 있을 뿐, 인증 수단으로서의 '계좌 비밀번호' 자체가 가지는 독자적인 기술적 의의가 나타나 있지 않다. 따라서 계좌 비밀번호는 개인 금융 거래 중계 서버에 등록(저장)되는 고객 정보의 일종일 뿐 그 자체로 기술적 의의를 갖는다고 보기 어렵다.

이 사건 특허발명(갑 제2호증)
【0017】 상술한 바와 같이, 본 발명의 금융 거래 중계 시스템은 고객 단말기의 지문 정보, 전화번호 및 계좌 비밀번호를 매칭시켜서 회원으로 등록하고, 고객 단말기가 온라인 은행 거래 및 전자 상거래 중 어느 하나를 수행하면, 고객 단말기로부터 지문 정보를 받아서 인증 처리함으로써, 온라인 은행 시스템 및 전자 상거래 시스템을 무인증 접속으로 금융 거래가 가능하다. 【0018】 또 본 발명의 금융 거래 중계 시스템은 한 번의 회원 가입으로 고객 단말기의 지문 정보, 전화번호 및 계좌 비밀번호를 등록함으로써, 금융 거래에 따른 안전 잠금 기능을 제공할 수 있으며, 번거롭게 공인인증서를 발급하는 불편함을 해소시킬 수 있어서 금융 거래에 대한 새로운 변화의 경제적인 편리성을 제공할 수 있다. 【0025】 이를 위해 본 발명의 금융 거래 중계 시스템(2)은 개인 금융 거래 중계 서버(100)에 지문 인식, 계좌 비밀번호 인증 및 전화번호 인증을 통하여 회원으로 등록하고, 고객 단말기(200)와 온라인 은행 시스템(300) 및 전자 상거래 시스템(400)들 간에 금융 거래 시, 지문 인증으로 무인증 접속이 이루어지도록 처리한다.

(2) 다음과 같이 선행발명 1의 명세서에는 다양한 고객 정보가 열거되어 있고, 고객 정보로 회원의 은행 계좌번호, 신용카드번호 등의 신용 정보 등을 포함할 수 있다는 내용이 기재되어 있다.

선행발명 1(갑 제5호증)
【0017】 본 발명의 바람직한 실시예에 따른 데이터베이스(243)는 실시간 지문 인식을 통한 사용자 인증 서비스를 이용하는 회원과 관련된 고객 정보를 가지고 있다. 여기서, 고객 정보는 회원의 성명, 회원 아이디, 비밀번호, 주민등록번호, 주소지, 전화번호, 전자메일 주소 등의 개인 정보뿐만 아니라 회원의 은행 계좌번호, 신용카드번호 등의 신용 정보 등을 포함할 수 있다.

(3) 선행발명 4 명세서의 다음과 같은 기재에 의하면, 은행 계좌번호나 신용카드번호 또는 비밀번호를 이용하여 본인 인증을 처리하는 것은 주지관용기술에 해당한다고 보는 것이 타당하다.

선행발명 4(을 제3호증)
【0005】 현실적으로 전자 상거래의 대금 지급 방법으로 광범위하게 활용되고 있는 방법으로는 계좌 이체에 의한 직불 방법, 신용카드에 의한 후불 방법 및 캐시 카드나 IC카드를 활용한 전자결제 등이다. 이러한 방법들의 이용에 있어서 공통적으로 요구되는 것은 계좌번호나 카드번호 및 비밀번호의 전송인데, 이러한 금융 정보들이 아무런 조치 없이 인터넷 상에서 전송되는 것은 타인에 의한 도용의 위험이 내포되어 있어, 인터넷 거래자가 전자 상거래를 적극적으로 활용하는 것을 꺼리는 하나의 요인이 되어 건전한 전자 상거래의 발전을 저해할 수 있다. 【0008】 이러한 방법은 공통적으로 계좌번호나 신용카드번호 및 비밀번호 같은 금융 정보의 외부 유출을 막기 위한 방안으로서, 일단 타인에 의해 도용된 금융 정보의 무단 이용으로 인한 선의의 피해자의 양산 및 이로 인한 전자 상거래의 위축을 막기 위한 방안에 대한 논의는 활발하지 못한 실정이다.

(4) 통상의 기술자는 필요에 따라 선행발명 1에 개시된 등록 정보의 일부를 계좌 비밀번호로 변경할 수 있고 그러한 변경에 어떠한 기술적 어려움이 있다고 볼 수 없다.

다) 차이점 3

다음과 같은 이유로 차이점 3은 통상의 기술자가 선행발명 1 또는 선행발명 1, 2 또는 선행발명 1, 4로부터 쉽게 극복할 수 있다.

(1) 선행발명 1에서 아이디와 패스워드는 사용자가 인터넷 인증 서비스 회원인지 여부를 확인하고 데이터베이스에 미리 저장되어 있는 지문 데이터를 추출하기 위해 사용되는 것에 불과하고, 실질적인 인증은 사용자의 이동통신 단말기로부터 전송된 지문 데이터와 인증 관리 서버의 데이터베이스에서 추출한 고객에 관한 지문 데이터를 비교함으로써 이루어진다(갑 제4호증 식별번호 [0054] 참조).

(2) 선행발명 2 명세서 및 선행발명 4 명세서의 다음과 같은 기재에 의하면, 선행발명 2 및 선행발명 4에는 '지문 정보만을 이용하여 인증을 수행'하는 기술적 사상이 개시되어 있음을 알 수 있다.

선행발명 2(갑 제5호증)
【0035】 인증 시스템(200)은 휴대단말기(100)와 무선 네트워크로 접속되어 식별자 정보를 획득하거나 또는 휴대단말기(100)에 통신 서비스를 제공하는 이동통신사 서버(미도시)를 통해 유선 네트워크를 이용하여 식별자 정보를 획득할 수 있다. 【0037】 인증 시스템(200)은 서비스 서버(300)가 사용자 단말기(50)로 제공한 식별자로부터 식별자 정보를 생성하고, 이를 휴대단말기(100)가 제공한 식별자 정보를 비교하여 식별자 정보의 정당성을 판단한다. 이후, 식별자 정보가 정당하다고 판단되면, 인증 시스템(200)은 휴대단말기(100)로 인증 정보를 요청하며, 휴대단말기(100)는 인증 시스템(200)으로 인증 정보를 제공하여 최종 인증 과정을 수행하게 된다. 여기서, 인증 정보는, 【0038】 - 아이디/ 패스워드, 【0039】 - 사용자와 약정된 인증번호, 【0040】 - 홍체 정보, **지문** 및 음성**과 같은 생체정보**, 【0041】 - 인증 시스템(200)이 휴대단말기(100)로 발급하는 임시 승인번호 **중 어느 하나**일 수 있다.

선행발명 4(을 제3호증)
【0002】 본 발명은 지문 인증에 의한 전자 상거래 결제 시스템 및 방법에 관한 것으로서, 보다 구체적으로는 인터넷 상에서 이루어지는 전자 상거래의 결제에 있어서 거래자의 지문 인증 과정을 추가시킴으로써 금융 정보의 유출로 인한 선의의 피해자의 발생을 방지하여 건전한 전자 상거래 질서를 확립하는데 기여하고자 하는 시스템 및 방법에 관한 것이다. 【0009】 본 발명은 전자 상거래의 결제방식에 지문에 의한 본인 인증 과정을 추가시킴으로써 금융 정보의 도용으로 인한 거래자의 피해를 막고자 하는 취지에서 안출된 것이다. 【0011】 아울러, 본 발명은 전자 상거래의 결제방식에 지문에 의한 본인 인증 과정을 추가시키기 위해 기존의 전자 상거래 시스템과는 독립된 지문 인증 서버를 구축함으로써, 기존의 전자 상거래 시스템에 대한 호환이 보다 용이하도록 한 지문 인증에 의한 전자 상거래 결제 시스템 및 방법을 제공하는 데 다른 목적이 있는 것이다. 【0033】 지문 인증 서버(40)는 사전에 거래자의 지문을 등록받아 이를 지문 데이터베이스(45)에 거래자를 특정할 수 있는 아이디(ID : Identification) 등과 함께 저장하여 두고, 결제 과정에서 거래자의 지문을 입력받아 저장되어 있는 지문데이터와 일치여부를 판단함으로써 본인인증을 하는 서버이다. 【0035】 전제되어야 할 것은 지문 인증 서버(40)의 지문 데이터베이스(45)에는 거래자의 지문데이터와 ID가 등록되어 있어야 한다는 것이다. 지문 등록 방법으로는 여러 가지 방법이 있을 수 있으나, 거래자가 쇼핑몰 서버(20)에 회원 등록 시 온라인 또는 오프라인으로 지문을 등록하는 방법을 생각할 수 있을 것이다.

(3) 선행발명 1에서 아이디와 패스워드 입력 부분을 삭제하고, 선행발명 2 또는 선행발명 4에 개시된 것과 같이 지문 정보만으로 인증을 수행하는 것으로 변경하는 데에 어떠한 기술적 어려움이 있다고 볼 수 없다.

(4) 입력 정보 및 인증 절차를 간소화하는 것은 인증 기술분야에서 일반적으로 요구되는 사항이므로, 통상의 기술자에게는 아이디와 패스워드 입력 부분을 삭제할 만한 동기가 있다.

라) 차이점 6

다음과 같은 이유로 차이점 5는 통상의 기술자가 선행발명 1 또는 선행발명 1, 2로부터 쉽게 극복할 수 있다.

(1) 선행발명 1의 명세서에는 '사용자가 회원으로 가입할 때 전화번호 등의 정보를 인증 관리 서버의 데이터베이스에 등록하여 저장한다'는 내용이 기재되어 있다(갑 제4호증 식별번호 [0016], [0017], [0044], [0045] 참조). 선행발명 2의 명세서에는 '인증 시스템으로 전송된 휴대 단말기의 전화번호를 이용하여 인증을 처리한다'는 내용이 기재되어 있다(갑 제5호증 식별번호 [0037], [0045], [0046] 참조). 따라서 통상의 기술자로서는 이러한 구성에 착안하여, 이 사건 제1항 발명에서와 같이 고객 등록 시 전화번호를 이용하여 인증하고 데이터베이스에 등록하는 구성을 쉽게 도출할 수 있다.

(2) 고객 등록 시 휴대 단말기의 전화번호를 인증 수단으로 하는 것은 통상의 기술자가 필요에 따라 설계변경하거나 부가할 수 있는 구성에 불과하고, 그러한 변경에 어떠한 기술적 어려움이 있다고 볼 수 없다.

마) 차이점 7

다음과 같은 이유로 차이점 7은 통상의 기술자가 선행발명 1 또는 선행발명 1, 2로부터 쉽게 극복할 수 있다.

(1) 이 사건 특허발명 명세서에는 "개인 금융 거래 중계 서버(100)는 고객 단말기(200)가 회원 가입 시, 다중 안전 잠금 모듈(110)을 통해 회원으로 등록하고, 온라인 은행 시스템(300) 및 전자 상거래 시스템(400)과의 금융 거래 시, 고객 단말기(200)로부터 지문 정보를 받아서 인증 처리하고, 온라인 은행 시스템(300) 및 전자 상거래 시스템(400)으로 금융 거래 및 전자 상거래 시, 지문 인증을 통해 무인증 접속으로 금융 거래가 이루어지도록 처리한다.", "다중 안전 잠금 모듈(110)은 예컨대, 미들웨어로 구비되며, 고객 단말기(200)의 개인 인증 기능과

해킹 차단을 위한 방화벽 기능을 구비한다. 이 실시예에서 다중 안전 잠금 모듈(110)은 고객 단말기(200)로부터 지문 정보를 받아서 데이터베이스(120)에 기등록된 지문 정보와 일치하는지를 비교하는 지문 인식 처리부(112)와 온라인 은행 시스템(300)에 등록된 고객 단말기(200)의 계좌 비밀번호를 등록하는 계좌 비밀번호 처리부(114) 및 고객 단말기(200)의 전화번호를 이용하여 인증하는 전화번호 인증 처리부(116)를 포함한다."라고 기재되어 있다(갑 제2호증 식별번호 [0033], [0037] 참조). 위 기재에 의하면, 이 사건 제1항 발명 중 '다중 안전 잠금 모듈'은 회원 가입 시에는 지문 정보 및 계좌 비밀번호를 등록하고 고객 단말기의 전화번호를 인증하는 기능을 하고, 회원 가입 후에는 지문 정보만을 이용하여 인증을 수행하는 기능을 한다는 점을 알 수 있다.

(2) 통상의 기술자가 선행발명 1 또는 선행발명 1, 2 또는 선행발명 1, 4로부터 계좌 비밀번호를 등록하는 구성을, 선행발명 1 또는 선행발명 1, 2로부터 회원 등록 시 전화번호를 이용하여 인증하는 구성을 쉽게 도출할 수 있다는 점은 앞서 본 바와 같다. 나아가 선행발명 1에 계좌 비밀번호 등록, 전화번호 인증 구성을 추가하려면, 등록·인증 과정을 처리하는 계좌 비밀번호 처리부, 전화번호 인증 처리부를 구성해야 한다는 점은 통상의 기술자에게 자명하다.

(3) 원고는 선행발명 1에 '계좌 비밀번호 처리부'를 추가하기 위해서는 미들웨어 구성을 변경해야 하고, '계좌 비밀번호 처리부'의 작용효과가 현저하므로, 통상의 기술자가 '계좌 비밀번호 처리부' 구성을 쉽게 도출할 수 없다는 취지로 주장한다. 그러나 미들웨어 구성의 변경은 통상의 기술자가 그 필요에 따라 쉽게 변경할 수 있는 사항에 불과하다. 나아가 이 사건 특허발명의 명세서에는 계좌 비밀번호를 등록하는 구성 또는 계좌 비밀번호 처리부 구성이 갖는 고유의 효과가 기재되어 있지 아니하므로,

'계좌 비밀번호 처리부' 구성이 현저한 효과를 갖는다고 볼 수도 없다. 원고의 이 부분 주장은 이유 없다.

바) 차이점 8

다음과 같은 이유로 차이점 8은 통상의 기술자가 선행발명 1 또는 선행발명 1, 3으로부터 쉽게 극복할 수 있다.

(1) 갑 제7, 8호증의 각 기재에 의하면, 서버 또는 클라이언트 컴퓨터에 데이터의 송신과 수신을 용이하게 하는 미들웨어[3]를 설치하는 것, 불법 접근 또는 데이터의 불법 유출을 방지하는 등 보안을 강화하기 위하여 방화벽을 설치하는 것은 분산 컴퓨팅[4] 분야에서 기술상식 또는 주지관용기술에 해당한다는 점을 알 수 있다.

(2) 선행발명 3 명세서의 다음과 같은 기재에 의하면, 선행발명 3에는 미들웨어로 구현되고 방화벽이 구비된 중간 장치(가입자 단말이 단말 장치에 원격 접속하는 것을 매개하는 장치)가 개시되어 있음을 알 수 있다.

선행발명 3(갑 제6호증)
【0022】 도 1은 소위 이동 사무실 서비스, 즉 사용자가 그(그녀) 소유의 가입자 단말(ST)을 통하여 그(그녀) 소유의 단말 장치(TE)에 원격으로 접속할 수 있도록 하는 서비스를 제공하는 원격 접속 시스템(RAS)의 블록도를 나타낸다. 【0026】 본 발명의 바람직한 실시예에 따르면, 원격 접속 시스템은 서비스 센터에서 서버 상에서 동작하고, Radius 서버와 통신하는, 이하에서 중간 장치(Mediator; ME)로 불리는 중간 장치 소프트웨어 어플리케이션; 및 Radius 서버와 중간 장치 모두에 의해 접속 가능하고 이동 통신 네트워크에 연결되고 Radius 서버에 의해 인증된 가입자 단말 상의 정보를 포함하는 인증 데이터베이스(DB)를 포함한다.

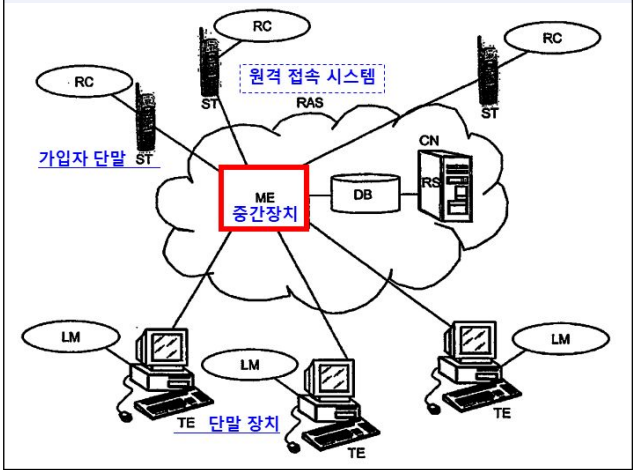
3) 통신망으로 연결된 여러 컴퓨터 사이에서 서로 데이터를 쉽게 주고받을 수 있도록 매개 역할을 하는 소프트웨어를 의미한다.

4) 분산 컴퓨팅(Distributed Computing): 네트워크로 연결된 여러 컴퓨터 또는 서버와 클라이언트를 이용하여 컴퓨팅 작업을 처리하는 것을 의미한다.

선행발명 3(갑 제6호증)

【0028】 바람직하게, 중간 장치는 자바 언어로 구현되고 JADE(자바 에이전트 개발 프레임워크; 본 출원의 출원일에 주소 http://jade.tilab.com에서 인터넷을 통하여 접속 가능한 관련 문서)로 알려진 피어 투 피어(peer-to-peer) 에이전트 기반 어플리케이션을 위한 개방 소스 플랫폼을 사용하여 개발된 소프트웨어 어플리케이션이다. Jade는 FIPA(Foundation for Intelligent Physical Agents) 표준에 따르는 미들웨어 및 디버깅(debugging) 및 배포 단계를 지원하는 일련의 그래픽 툴들을 통하여 멀티 에이전트 시스템의 구현을 간단하게 한다.

[도 1]



【0073】 또한 본 발명은 네트워크 어드레스 전송 시스템 및(또는) 동적 IP 어드레스 할당 뒤에 위치하거나 방화벽에 의해 보호되는 경우에도 사용자 단말 장치에 원격 접속할 수 있게 한다. 실제로, 중간 장치가 단말 장치와 가입자 단말 사이의 모든 통신을 중재하기 때문에, 단말 장치와 가입자 단말은 직접 연결될 필요가 없고, 통신이 도달해야만 하는 것은 단말 장치 및 가입자 단말이 아닌 단지 중간 장치이다.

(3) 이 사건 제1항 발명에 개시된 개인 금융 거래 중개 서버 및 선행발명 1에 개시된 인증 관리 서버는 모두 통신망[인터넷망]으로 연결된 고객 단말기[이동통신 단말기]와 데이터를 송수신한다. 따라서 통상의 기술자로서는 데이터의 원활한 송수신과 보안을 강화하기 위하여 선행발명 1의 인증 관리 서버를 미들웨어로 구현하거나 방화벽 기능을 추가할 동기가 있다. 나아가 서버를 미들웨어로 구현하는 것이나 방화벽 기능을 추가하는 것은 통상의 기술자가 선행발명 3 또는 주지관용기술을 참작하여 필요에 따라 설계변경하거나 부가할 수 있는 구성에 불과하다.

(4) 원고는, 선행발명 3에서 '미들웨어' 구성만을 발췌하여 선행발명 1과 결합하는 것은 선행발명 1, 3 각각의 전체적인 기술구성 내에서 각 구성이 가지고 있는 기

술적 의의 및 유기적 결합관계를 해치는 것이 되어 통상의 기술자가 쉽게 생각해내기 어렵다는 취지로 주장한다. 그러나 미들웨어는 '통신망으로 연결된 여러 컴퓨터 사이에서 서로 데이터를 쉽게 주고받을 수 있도록 매개 역할을 하는 소프트웨어'로서 네트워크 시스템에서 그 필요에 따라 일반적으로 채택되는 구성에 불과하므로, 선행발명 3의 나머지 구성들과 분리될 수 없을 정도로 유기적으로 결합하고 있다고 볼 수는 없다. 이와 다른 전제에 선 원고의 이 부분 주장은 이유 없다.

(5) 원고는 선행발명 1과 선행발명 3의 출원 및 등록 시점이 다르므로, 위 각 발명에 적용되어야 하는 미들웨어의 구체적인 내용이 서로 달라 선행발명 3의 미들웨어를 선행발명 1에 적용할 수 없다는 취지로 주장한다. 그러나 앞서 본 바와 같이 미들웨어는 '통신망으로 연결된 여러 컴퓨터 사이를 매개하는 역할을 하는 소프트웨어'를 칭하는 일반적 용어로서, 그 구체적인 내용은 제품별로 일부 차이가 있다. 선행발명 3의 미들웨어 구성을 선행발명 1에 결합한다는 것은, 선행발명 3에 적용된 소프트웨어 제품을 선행발명 1에 적용하여야 한다는 의미가 아니라 '미들웨어'로 분류되고 기능하는 소프트웨어(통신망으로 연결된 여러 컴퓨터 사이를 매개하는 역할을 하는 소프트웨어)를 결합해야 한다는 의미이다. 나아가 미들웨어의 구체적인 제품 선택은 통상의 기술자가 필요에 따라 쉽게 변경할 수 있는 사항에 불과하다. 원고의 이 부분 주장 역시 이유 없다.

5) 작용효과에 관한 검토

이 사건 제1항 발명은 고객 단말기로부터 전송 받은 지문 정보만으로 인증을 처리한 후 추가적인 인증 없이 금융 거래가 이루어지도록 하는 작용효과가 있다. 그러나 이러한 효과는 앞서 본 선행발명 1의 '미리 등록된 가입자의 지문 데이터와 비교하여

사용자 인증을 수행하는 것', '가입자가 회원 등록 시 전화번호 등의 개인 정보를 등록하는 것', 선행발명 2의 '휴대 단말기가 전화번호 등을 인증 정보로 활용하는 것', 선행발명 3의 '중간 장치가 미들웨어 및 방화벽을 구비하는 것'을 결합한 구성에 의하여 쉽게 달성된다는 점에서, 위 각 구성의 결합으로부터 예측되는 결과를 넘는 현저한 효과라고 보기 어렵다.

6) 원고의 나머지 주장에 관한 판단

가) 원고는, 아이디와 패스워드를 입력하는 1단계, 실시간으로 촬영된 지문 영상 데이터를 전송하는 2단계, 실시간으로 촬영된 지문 영상 데이터와 보관된 지문 데이터를 비교하는 3단계의 절차를 거쳐야 하는 선행발명 1과는 달리, 이 사건 제1항 발명은 사용자가 고객 단말기의 온라인 은행 거래 또는 전자 상거래 중 어느 하나를 선택하는 단 1회의 절차만으로 해당 시스템에 무인증 접속되게 한다는 점에서 목적의 특이성이 있다고 주장한다. 그러나 ① 이 사건 제1항 발명의 경우에도 고객 단말기를 통하여 입력된 지문 정보를 개인 금융 거래 중계 서버로 전송하는 단계, 입력된 지문 정보와 저장된 지문 정보를 대조하기 위하여 데이터베이스에 저장된 지문 정보를 조회하는 단계를 거쳐야 한다는 점, ② 선행발명 1에 개시된 '아이디와 패스워드'는 기존에 등록된 지문 데이터를 조회하기 위한 수단에 불과하므로(갑 제4호증 식별번호 [0054] 참조) '아이디와 패스워드를 입력하는 단계'는 필요에 따라 쉽게 삭제할 수 있는 점(아이디와 패스워드 없이 입력된 지문 데이터만을 기준으로 지문 데이터베이스를 조회하여 대조하는 방법도 얼마든지 가능하다)에 비추어 보면, 원고가 주장하는 '지문 입력만으로 해당 시스템에 접속되게 한다'는 목적 및 효과는 선행발명 1에 의하여서도 쉽게 예측할 수 있다고 판단된다. 원고의 이 부분 주장은 이유 없다.

나) 원고는 이 사건 제1항 발명의 금융 거래 중계 서버는 단순히 인증을 하거나 온라인 시스템 등에 접속만 하게 하는 것이 아니라 결제 등 금융 거래를 실행하는 것이므로, 선행발명 1 내지 4와 차이가 있다고 주장한다. 이 사건 특허발명의 명세서에 "온라인 은행 시스템(300)은 제휴 은행에 구비되어, 온라인으로 처리되는 은행 업무 예를 들어, 입출금, 이체 등의 금융 거래를 처리한다. 온라인 은행 시스템(300)은 금융 거래 시, 개인 금융 거래 중계 서버(100)를 통해 고객 단말기(200)가 무인증으로 접속된다.", "단계 S162에서 고객 단말기(200)가 온라인 은행 거래 및 전자 상거래를 수행하기 위하여, 인증 절차를 처리하면, 단계 S164에서 개인 금융 거래 중계 서버(100)는 고객 단말기(200)로부터 지문 정보를 입력받아서 지문 인증을 처리한다."라고 기재된 사실은 인정된다(식별번호 [0031], [0046] 참조). 그러나 위 기재만으로는 금융 거래 중계 서버가 실제 금융 거래를 실행하는 것이라고 인정하기에 부족하고, 달리 이를 인정할 만한 증거가 없다. 오히려 중간에서 이어 준다는 "중계"의 사전적 의미와 "고객 단말기로부터 지문 정보를 전송 받아서 인증하여 온라인 은행 시스템 또는 전자 상거래 시스템으로 무인증 접속하여 금융 거래가 이루어지도록 중계 처리하는 개인 금융 거래 중계 서버"라는 이 사건 특허발명의 명세서 기재(갑 제2호증 식별번호 [0010] 참조)를 고려하면, 금융 거래 중계 서버는 고객 단말기를 온라인 은행 시스템 또는 전자 상거래 시스템에 접속하게 함으로써 고객 단말기와 위 온라인 은행 시스템 등을 서로 이어 주는 역할만을 한다고 보는 것이 타당하다. 이와 다른 전제에 선 원고의 이 부분 주장은 이유 없다.

다) 원고는, 이 사건 제1항 발명의 구성요소 1-6에 개시된 미들웨어 및 방화벽 구성 자체가 주지관용기술에 해당한다 하더라도, 이러한 구성을 금융거래 중개 시스템에 적용시킨 것은 주지관용기술에 해당하지 않는다고 주장한다. 이 사건 특허발명의

명세서에는 "다른 실시예에 있어서, 상기 다중 안전 잠금 모듈은; 해킹 차단을 위한 방화벽 기능을 더 구비한다.", "다중 안전 잠금 모듈(110)은 예컨대, 미들웨어로 구비되며, 고객 단말기(200)의 개인 인증 기능과 해킹 차단을 위한 방화벽 기능을 구비한다."라고 기재되어 있을 뿐(갑 제2호증 식별번호 [0012], [0037] 참조) '미들웨어 및 방화벽' 구성을 금융 거래 중개 시스템에 적용했을 때 나타나는 특별한 기술적 의의 또는 이질적인 효과가 기재되어 있지 않고, 달리 이를 인정할 만한 증거가 없다. 따라서 이 사건 제1항 발명에 개시된 미들웨어 및 방화벽 구성은 분산 컴퓨팅 분야에서 일반적으로 사용되는 주지관용기술을 적용한 것에 불과하다고 보는 것이 타당하다. 원고의 이 부분 주장은 이유 없다.

7) 검토 결과의 정리

이 사건 제1항 발명은 선행발명 1 또는 선행발명 1과 선행발명 2, 3, 4의 결합에 의하여 진보성이 부정된다.

나. 이 사건 제4항 발명의 진보성 부정 여부

1) 구성 대비

이 사건 제4항 발명의 구성요소와 선행발명 1의 구성요소를 대비하면 다음 표 기재와 같다.

구성요소	이 사건 제4항 발명	선행발명 1(갑 제4호증)
4-1	금융 거래 중계 시스템의 처리 방법에 있어서;	인터넷 인증 서비스가 제공되는 과정에 있어서,
4-2	상기 금융 거래 중계 시스템의 고객 단말기로부터 통신망을 통하여 상기 금융 거래 중	사용자가 본 발명의 실시예에 따른 인터넷 인증 서비스를 이용하여 사용자 인증을 받고

구성 요소	이 사건 제4항 발명	선행발명 1(갑 제4호증)
	계 시스템의 개인 금융 거래 중계 서버에 접속하는 단계와;	자 하는 경우, 이동 통신 단말기(210)의 무선 인터넷 메뉴의 '인터넷 인증' 항목을 지정하여 인증 관리 서버(240)에 접속한다(식별번호 [0049]).
4-3	상기 고객 단말기의 지문 인식기를 통하여 지문 정보를 획득하고, 상기 통신망을 통하여 지문 정보를 상기 개인 금융 거래 중계 서버로 전송하여 상기 개인 금융 거래 중계 서버가 상기 고객 단말기에 대응하여 지문 정보를 데이터베이스에 등록하는 단계와;	인증 관리 서버(240)에 접속한 사용자는 인증 관리 서버(240)에서 제공하는 사용자 인증에 관한 메뉴 화면에 따라 절차를 진행하게 되고, … 사용자는 '신규 고객' 항목을 선택하여 회원 정보에 관한 데이터 및 인증을 위한 지문 데이터 등을 등록한다. 인증 관리 서버(240)는 이렇게 등록된 회원 정보에 관한 데이터 및 인증을 위한 지문 데이터를 데이터베이스(243)에 저장(식별번호 [0050] ~ [0052]). 본 발명의 바람직한 실시예에 따른 데이터베이스(243)는 실시간 지문 인식을 통한 사용자 인증 서비스를 이용하는 회원과 관련된 고객 정보를 가지고 있다. 여기서, 고객 정보는 회원의 성명, 회원 아이디, 비밀번호, 주민등록번호, 주소지, 전화번호, 전자메일 주소 등의 개인 정보뿐만 아니라 회원의 은행 계좌번호, 신용카드번호 등의 신용 정보 등을 포함할 수 있다. 또한, 본 발명의 바람직한 실시예에 따른 데이터베이스(243)는 실시간 지문 인식을 통한 사용자 인증 서비스를 이용하는 회원이 인증 관리 서버(240)
4-4	상기 개인 금융 거래 중계 서버가 상기 데이터베이스에 저장된 상기 고객 단말기의 전화번호를 이용하여 인증하고, 상기 개인 금융 거래 중계 서버가 상기 고객 단말기의 통장 계좌번호에 대한 비밀번호를 상기 데이터베이스에 등록하여 상기 고객 단말기의 지문 정보, 전화번호 및 계좌 비밀번호를 매칭시켜서 상기 개인 금융 거래중계 서버의 회원으로 등록하는 단계와;	

구성 요소	이 사건 제4항 발명	선행발명 1(갑 제4호증)
		로 전송한 지문 이미지 데이터를 가지고 있다(식별번호 [0045], [0046]).
4-5	상기 고객 단말기가 온라인 은행 거래 및 전자 상거래 중 어느 하나를 수행하기 위하여, 인증 절차를 처리하면, 상기 개인 금융 거래 중계 서버의 다중 안전 잠금 모듈 중 지문인식처리부가 상기 고객 단말기로부터 지문 정보만을 전송받아서 지문 인증을 처리하는 단계 및;	사용자가 기존의 인터넷 인증 서비스 가입 회원인 경우에는 인증 관리 서버(240)가 제공하는 메뉴 화면에 따라 ID 및 PASSWORD를 입력하고(S406), 인증 관리 서버(240)는 입력된 ID 및 PASSWORD가 데이터베이스(243)에 저장되어 있는 고객 정보와 일치하는지 여부를 판단한다(S408). 사용자가 입력한 ID 및 PASSWORD가 데이터베이스(243)에 저장되어 있는 고객 정보와 일치하는 경우, 인증 관리 서버(240)의 제어모듈(242)은 사용자의 이동통신 단말기(100)에 부착되어 있는 카메라부(110)를 통하여 사용자의 실시간 지문 영상 데이터를 전송 할 수 있도록 하는 메뉴 항목을 제공하고 통신 모듈(241)을 제어한다(식별번호 [0061], [0062]).
4-6	전송된 지문 정보가 상기 개인 금융 거래 중계 서버의 데이터베이스에 저장된 지문 정보와 일치하면, 상기 개인 금융 거래 중계 서버가 무인증으로 온라인 은행 시스템 또는 전자 상거래 시스템에 접속하여 금융 거래를 중계하는 단계를 포함하는 것을 특징으로 하는 금융 거래 중계 시스템의 처리 방법.	인증 관리 서버(240)가 수신한 데이터가 실시간 생성되는 데이터인 것으로 판단되는 경우에, 인증 관리 서버(240)의 제어 모듈(242)은 데이터베이스(243)에 저장되어 있는 사용자의 지문 데이터를 추출하여 수신한 데이터와 일치하는지 여부를 판단한다(S414). 판단 결과, 사용자로부터 수신한 실시간 지문 데이터가 데이터베이스(243)에

구성 요소	이 사건 제4항 발명	선행발명 1(갑 제4호증)
		저장되어 있는 사용자의 지문 데이터와 일치하는 것으로 판단되는 경우에는, 사용자의 이동통신 단말기(210)에 인증 완료 메시지를 전송(S416)(식별번호 [0064])

2) 판단

가) 이 사건 제4항 발명은 물건의 발명인 이 사건 제1항 발명을 방법 발명으로 구성한 것으로서 이 사건 제1항 발명의 내용과 실질적으로 동일하다[이 사건 제1항 발명에는 '상기 고객 단말기의 지문 정보, 전화번호 및 계좌 비밀번호를 매칭'하는 구성(구성요소 4-4)이 명시되어 있지 않다. 그러나 이 사건 제1항 발명에는 '상기 고객 단말기로부터 지문 정보, 전화번호 및 계좌 비밀번호를 전송받아서 회원으로 등록'하는 구성이 개시되어 있고, '지문 정보, 전화번호 및 계좌 비밀번호를 전송받아 회원으로 등록'한다는 것이 결국 '위 정보들을 서로 매칭시켜 등록한다'는 의미임은 통상의 기술자에게 자명하다. 따라서 이 사건 제1항 발명의 '상기 고객 단말기로부터 지문 정보, 전화번호 및 계좌 비밀번호를 전송받아서 회원으로 등록'하는 구성과 이 사건 제4항 발명의 '고객 단말기의 지문 정보, 전화번호 및 계좌 비밀번호를 매칭'하는 구성은 실질적으로 동일하다].

나) 따라서 이 사건 제1항 발명의 진보성 판단 부분에서 본 바와 같은 이유로 이 사건 제4항 발명은 선행발명 1 또는 선행발명 1에 선행발명 2, 3, 4를 결합하여 쉽게 도출할 수 있다. 따라서 이 사건 제4항 발명은 선행발명 1 또는 선행발명 1과 선행발명 2, 3, 4의 결합에 의하여 진보성이 부정된다.

다. 소결론

이상에서 살펴본 바와 같이 이 사건 제1, 4항 발명은 모두 진보성이 부정되므로, 그 특허가 무효로 되어야 한다. 이 사건 심결은 이와 결론이 같아 적법하다.

4. 결론

이 사건 심결의 취소를 구하는 원고의 청구는 이유 없으므로 기각한다.

재판장 판사 문주형

판사 권보원

판사 한지윤