(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0022425
(43) 공개일자 2009년03월04일

(51) Int. Cl.
G06F 21/20 (2006.01) *G06F 17/00* (2006.01)
G06F 15/00 (2006.01)
(21) 출원번호 10-2007-0087766
(22) 출원일자 2007년08월30일
심사청구일자 2007년08월30일

(71) 출원인
씨티아이에스(주)
서울 영등포구 문래동3가 82-8 태양빌딩 5층
(72) 발명자
이병윤
경기 고양시 일산동구 중산동 중산마을 1007-301
(74) 대리인
유병옥

전체 청구항 수 : 총 6 항

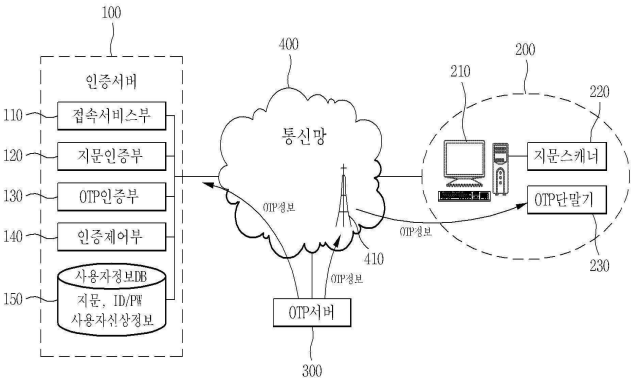
(54) 다중인증 접속 시스템 및 그 방법

(57) 요 약

본 발명은 아이디/패스워드(ID/PW)에 의한 1차 인증 후 지문, 일회용 패스워드(OTP: One Time Password)를 이용한 2차 또는 3차의 다중인증을 수행하여 서버시스템에 대한 접속을 인증하도록 하는 다중인증 접속 시스템 및 그 방법에 관한 것으로서,

상술한 다중인증 접속 시스템은, 통신망을 통해 접속을 요청하는 사용자에 대한 아이디와 패스워드에 의한 1차 인증을 수행한 후 지문 또는 일회용패스워드(OTP: One Time Password) 정보 중 적어도 하나 이상의 다중인증정보를 이용하는 다중인증을 수행하여 사용자의 접속을 인증하는 인증서버와; 상기 통신망을 통해 상기 인증서버로 접속하여 상기 1차 인증을 수행하고, 상기 1차 인증 이후 상기 인증서버가 요청하는 다중인증을 위한 다중인증정보를 상기 인증서버로 전송하여 접속이 인증되는 사용자장치부와; 상기 인증서버에 의한 일회용패스워드 인증 수행을 위하여 상기 1차 인증된 사용자에 대한 일회용패스워드를 생성하여 상기 인증서버 및 상기 사용자장치부로 전송하는 OTP서버;를 포함하여 구성되는 것을 특징으로 한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

통신망을 통해 접속을 요청하는 사용자에 대한 아이디와 패스워드에 의한 1차 인증을 수행한 후 지문 또는 일회용패스워드(OTP: One Time Password) 정보 중 적어도 하나 이상의 다중인증정보를 이용하는 다중인증을 수행하여 사용자의 접속을 인증하는 인증서버와;

상기 통신망을 통해 상기 인증서버로 접속하여 상기 1차 인증을 수행하고, 상기 1차 인증 이후 상기 인증서버가 요청하는 다중인증을 위한 다중인증 정보를 상기 인증서버로 전송하여 접속이 인증되는 사용자장치부와;

상기 인증서버에 의한 일회용패스워드 인증 수행을 위하여 상기 1차 인증된 사용자에 대한 일회용패스워드를 생성하여 상기 인증서버 및 상기 사용자장치부로 전송하는 OTP서버;를 포함하여 구성되는 것을 특징으로 하는 다중인증 접속 시스템.

청구항 2

청구항 1에 있어서, 상기 인증서버는,

상기 사용자에 대한 아이디와 패스워드에 의한 1차 인증을 수행하여 접속서비스를 제공하는 접속서비스부와;

상기 접속서비스부에서 1차 인증된 사용자에 대하여 다중인증으로서의 지문 인증을 수행하는 지문인증부와;

상기 접속서비스부에서 1차 인증된 사용자에 대하여 다중인증으로서의 일회용패스워드(OTP) 인증을 수행하는 OTP인증부와;

상기 사용자의 아이디와 패스워드, 신상정보, 지문정보를 포함하는 사용자정보를 저장하는 사용자정보DB;로 구성되는 것을 특징으로 하는 다중인증 접속 시스템.

청구항 3

청구항 2에 있어서, 상기 인증서버는,

상기 지문인증부와 상기 OTP인증부에 의한 다중인증의 순서를 설정하여 다중인증을 제어하는 인증제어부를 더 포함하여 구성되는 것을 특징으로 하는 다중인증 접속 시스템.

청구항 4

청구항 1에 있어서, 상기 사용자장치부는,

상기 통신망을 통해 상기 인증서버에 접속한 후 다중인증을 수행하여 인터넷 서비스를 제공받는 사용자단말기와;

상기 사용자의 지문을 스캔하여 상기 사용자단말기로 전송하는 지문스캐너와;

상기 OTP서버에서 생성된 일회용패스워드를 수신하는 OTP단말기;로 구성되는 것을 특징으로 하는 다중인증 접속 시스템.

청구항 5

통신망을 통해 인증서버에 접속하여 사용자정보와 지문정보와 아이디 및 패스워드를 정보를 등록하는 사용자정보등록과정과;

상기 통신망을 통해 접속되는 사용자에 대하여 인증서버가 아이디와 패스워드를 이용한 1차 인증을 수행하는 1차인증과정과;

상기 인증서버가 상기 1차인증과정에서 인증된 사용자에 대하여 지문정보 또는 일회용패스워드 정보 중 적어도 하나 이상의 인증정보를 이용한 다중인증을 수행하는 다중인증과정;을 포함하여 이루어지는 것을 특징으로 하는 다중인증 접속 방법.

청구항 6

청구항 5에 있어서, 상기 다중인증 과정은,

상기 1차 인증된 사용자의 지문정보를 이용하는 지문인증과정과;

상기 1차 인증된 사용자에 대한 일회용패스워드를 이용하는 OTP인증과정과;

상기 지문 인증 및 OTP인증을 모두 적용하는 복합인증과정 중 어느 하나인 것을 특징으로 하는 다중인증 접속 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 서버시스템의 접속 방법에 관한 것으로서, 아이디/패스워드(ID/PW)에 의한 1차 인증 후 지문, 일회용 패스워드(OTP: One Time Password)를 이용한 2차 또는 3차의 다중인증을 수행하여 서버시스템에 대한 접속을 인증하도록 하는 다중인증 접속 시스템 및 그 방법에 관한 것이다.

배 경 기 술

<2> 최근의 고속 인터넷의 급속한 발달로 인해 오프라인에서 제공되는 서비스를 온라인 상에서 제공할 수 있게 되었다. 이러한 온라인 서비스는 사용자들로 하여금 시간과 경비를 절약할 수 있도록 하는 점에서 사용자의 이용 또한 급속히 증가하고 있다. 이에 따라 오프라인 서비스 제공업자들은 오프라인 제공 서비스들에 대한 온라인 서비스를 제공하기 위하여 인터넷 상에서 서비스를 제공할 수 있도록 하는 서버시스템을 구축하여 인터넷 서비스를 제공하고 있다.

<3> 이러한 서버 시스템은 사용자들의 별도의 인증 없이 접속하여 서비스 항목을 검색할 수 있도록 구현되어 공개적인 자료들을 제공하는 경우도 있으나, 컨택센터 등과 같은 시스템에서는 고객관리정보, 고객의 개인 정보 등 고객 이외의 제3자에게 노출되어서는 안 되는 자료들을 저장하는 경우도 있다. 이러한 자료들은 유용을 목적으로 하는 자들에 의하여 내외부로부터의 침입이 빈번해지고 있으며, 많은 자료들이 유출에 노출되어 있는 상황이다.

<4> 이러한 자료의 유출을 방지하기 위하여 일반적인 서버시스템들은 접속되는 사용자에 대한 인증을 수행하여 인증된 사용자들만이 시스템에 접속하여 정보를 이용할 수 있도록 하는 보안정책을 적용하고 있다. 예를 들어 일반적인 서버시스템은 사용자별로 아이디(ID)와 패스워드(PW)를 부여한 후 접속을 요청하는 사용자로부터 아이디와 패스워드의 입력을 요청하여 해당 사용자에 대한 인증을 수행한다. 즉, 사용자는 단말기를 이용하여 아이디와 패스워드로 이루어지는 인증정보를 서버에 송신하고 서버측에서는 인증용으로 미리 등록하고 있는 정보와 비교하여 접속에 대한 인증을 수행하게 된다.

<5> 그러나 상술한 바와 같은 종래기술의 아이디와 패스워드를 이용하는 인증 방법은 제3자에게 아이디와 패스워드가 유출되어, 제3자가 취득한 타인의 아이디와 패스워드를 이용하여 서버시스템에 접속을 요청하게 되면 서버시스템은 제3자가 해당 아이디와 패스워드를 이용하는 정당한 사용자인지를 판별할 수 없으므로 보안면에서 매우 취약하게 되는 문제점을 가진다.

발명의 내용

해결 하고자하는 과제

<6> 따라서 본 발명은 상술한 종래기술의 문제점을 해결하기 위한 것으로서, 서버시스템 접속을 위한 아이디와 패스워드의 유출이 발생하는 경우에도 정당한 사용자인지를 판별할 수 있도록 하는 다중인증을 수행하여 부당한 사용자의 접속을 차단하는 것에 의해 서버시스템의 보안성을 향상시키면서, 사용자 개인 정보의 유출을 차단할 수 있도록 하는 다중인증 접속 시스템 및 그 방법을 제공하는 것을 그 목적으로 한다.

과제 해결수단

<7> 상술한 목적을 달성하기 위한 본 발명의 다중인증 접속 시스템은, 통신망을 통해 접속을 요청하는 사용자에 대한 아이디와 패스워드에 의한 1차 인증을 수행한 후 지문 또는 일회용패스워드(OTP: One Time Password) 정보 중 적어도 하나 이상의 다중인증정보를 이용하는 다중인증을 수행하여 사용자의 접속을 인증하는 인증서버와;

상기 통신망을 통해 상기 인증서버로 접속하여 상기 1차 인증을 수행하고, 상기 1차 인증 이후 상기 인증서버가 요청하는 다중인증을 위한 다중인증 정보를 상기 인증서버로 전송하여 접속이 인증되는 사용자장치부와; 상기 인증서버에 의한 일회용패스워드 인증 수행을 위하여 상기 1차 인증된 사용자에 대한 일회용패스워드를 생성하여 상기 인증서버 및 상기 사용자장치부로 전송하는 OTP서버;를 포함하여 구성되는 것을 특징으로 한다.

<8> 상기 인증서버는, 상기 사용자에 대한 아이디와 패스워드에 의한 1차 인증을 수행하여 접속서비스를 제공하는 접속서비스부와; 상기 접속서비스부에서 1차 인증된 사용자에 대하여 다중인증으로서의 지문 인증을 수행하는 지문인증부와; 상기 접속서비스부에서 1차 인증된 사용자에 대하여 다중인증으로서의 일회용패스워드(OTP) 인증을 수행하는 OTP인증부와; 상기 사용자의 아이디와 패스워드, 신상정보, 지문정보를 포함하는 사용자정보를 저장하는 사용자정보DB;로 구성되는 것을 특징으로 한다.

<9> 상기 인증서버는 또한 상기 지문인증부와 상기 OTP인증부에 의한 다중인증의 순서를 설정하여 다중인증을 제어하는 인증제어부를 더 포함하여 구성될 수 있다.

<10> 상기 사용자장치부는, 통신망을 통해 상기 인증서버에 접속한 후 다중인증을 수행하여 접속 서비스를 제공받는 사용자단말기와; 상기 사용자의 지문을 스캔하여 상기 사용자단말기로 전송하는 지문스캐너와; 상기 OTP서버에서 생성된 일회용패스워드를 수신하는 OTP단말기;로 구성되는 것을 특징으로 한다.

<11> 상술한 구성에서 상기 OTP단말기는 상기 OTP서버와 직접 통신을 위한 단말기 또는 무선이동통신단말기로 구현될 수 있다.

<12> 상술한 목적을 달성하기 위한 본 발명의 다중인증 접속 방법은, 통신망을 통해 인증서버에 접속하여 사용자정보와 지문정보와 아이디 및 패스워드를 정보를 등록하는 사용자정보등록과정과; 상기 통신망을 통해 접속되는 사용자에 대하여 인증서버가 아이디와 패스워드를 이용한 1차 인증을 수행하는 1차인증과정과; 상기 인증서버가 상기 1차인증과정에서 인증된 사용자에 대하여 지문정보 또는 일회용패스워드 정보 중 적어도 하나 이상의 인증정보를 이용한 다중인증을 수행하는 다중인증과정;을 포함하여 이루어지는 것을 특징으로 한다.

<13> 상기 다중인증 과정은, 상기 1차 인증된 사용자의 지문정보를 이용하는 지문인증과정과; 상기 1차 인증된 사용자에 대한 일회용패스워드를 이용하는 OTP인증과정과; 상기 지문 인증 및 OTP인증을 모두 적용하는 복합인증과정 중 어느 하나인 것을 특징으로 한다.

<14> 상술한 구성을 가지는 본 발명은 서버시스템에 접속하는 사용자에 대하여 아이디와 패스워드에 의한 1차 인증을 수행한 후 1차 인증된 사용자가 아이디와 패스워드의 정당한 소유자인지를 확인할 수 있도록 한다.

효 과

<15> 상술한 본발명은 서버시스템에 접속하는 사용자에 대하여 아이디와 패스워드에 의한 1차 인증 및 1차인증된 사용자가 아이디와 패스워드의 정당한 소유자인지를 확인하는 것에 의해 아이디와 패스워드가 제3자에게 노출되는 경우에도 서버시스템에 대한 제3자의 접속을 차단할 수 있도록 하여 서버시스템에 대한 접속 보안을 현저히 향상시킴은 물론 개인정보의 유출을 차단시키는 효과를 제공한다.

발명의 실시를 위한 구체적인 내용

<16> 이하, 본발명의 바람직한 일 실시예를 나타내는 첨부 도면을 참조하여 본 발명을 더욱 상세히 설명한다.

<17> 도 1은 본발명의 일 실시 예에 따르는 다중인증 접속 시스템의 구성도이고, 도 2는 도 1의 다중인증 시스템에 의한 다중인증 방법의 처리과정을 나타내는 순서도이며, 도 3은 도 2의 다중인증 중 지문인증을 위한 지문인증정보 전송 과정을 나타내는 서브루틴도이고, 도 4는 도 2의 다중인증 중 일회용패스워드(OTP) 인증을 위한 OTP정보 전송 과정을 나타내는 서브루틴도이다.

<18> 도 1에 도시된 바와 같이 본발명의 일 실시 예에 따르는 다중인증 접속 시스템은 접속된 사용자에 대한 아이디와 패스워드를 이용한 1차 인증을 수행한 후, 1차 인증된 사용자가 1차 인증에 이용한 아이디와 패스워드의 정당한 사용자인지를 확인하는 다중인증을 수행하여 사용자에 대한 서버접속을 승인하는 인증서버(100)와; 상기 인증서버(100)에 접속하여 사용자가 사용자의 지문정보, 아이디와 패스워드정보, 주소, 이름, 전화번호, 주민등록번호 등의 신상정보를 포함하는 사용자정보를 등록할 수 있도록 하고, 이 후 통신망(400)을 통해 상기 인증서버(100)에 접속하여 아이디와 패스워드에 의한 1차 인증을 수행한 후, 지문 또는 일회용패스워드(OTP) 중 적어도 하나 이상을 이용한 다중인증을 수행하여 상기 인증서버(100)에 의해 인증 관리되는 시스템에 접속하는 사용자장치부(200)와; 인증서버(100)로부터 1차 인증된 사용자 정보와 함께 1차 인증된 사용자에 대한 일회용패스워

드(OTP) 인증 요청을 수신하는 경우 1차 인증된 사용자에 대한 일회용패스워드(OTP)를 생성하여 인증서버(100) 및 사용자장치부(200)로 전송하는 OTP서버(300)가 통신망(400)을 통해 연결 구성된다.

<19> 상술한 구성에서 상기 통신망(400)은 인터넷 서비스를 제공할 수 있도록 하는 유선 통신망, 무선 통신망 및 이동통신망을 포함한다.

<20> 상기 인증서버(100)는 상술한 바와 같이 접속요청 사용자에게 사용자정보 등록 및 사용자정보 등록 이후의 아이디와 패스워드에 의한 1차인증을 수행할 수 있도록 하고, 1차 인증된 후에는 다중인증 정보의 요청을 수행할 수 있도록 하며, 접속된 사용자에게 인터넷 검색 서비스를 제공할 수 있도록 하고, 인터넷 서비스 제공을 위한 사용자 인터페이스를 제공하는 접속서비스부(110)와; 1차 인증된 사용자에 대한 지문인증을 수행하는 지문인증부(120)와; 1차 인증된 사용자에 대한 일회용패스워드(OTP) 인증을 수행하는 OTP인증부(130)와; 지문인증, OTP인증, 지문 및 OTP인증 등의 인증방법 및 인증 순서를 설정하는 인증제어부(140)와; 사용자의 아이디와 패스워드, 지문정보, 주소, 주민번호, 전화번호 등의 사용자 신상정보를 저장하는 사용자정보DB(150) 및 도면에는 미도시되어 있으나, 상기 통신망(400)과의 통신인터페이스를 제공하는 통신부를 포함하여 구성된다.

<21> 다음으로 상기 사용자장치부(200)는 통신망(400)을 통해 인증서버(100)에 접속하여 인증서버(100)의 접속서비스부(100)가 제공하는 서비스를 수신할 수 있도록 하는 인터넷검색엔진을 구비하는 사용자단말기(210)와; 사용자의 지문을 스캔하여 사용자단말기(210)로 전송하는 지문스캐너(220)와; OTP 서버(300)가 전송하는 일회용패스워드(OTP)를 수신하는 OTP단말기(230)로 구성된다. 상기 사용자단말기(210) 및 OTP 단말기(230)기 또한 통신망(400)을 통신을 수행할 수 있도록 하는 통신부를 구비한다.

<22> 상술한 구성에서 상기 사용자단말기(210)는 도 1에서는 개인용컴퓨터로 도시되어 있으나, 이에 한정되는 것은 아니며 유무선 인터넷 통신망을 통해 인증서버(100)에 접속될 수 있는 모든 단말기를 포함한다.

<23> 그리고 상기 OTP단말기(230)는 상기 사용자단말기(210)에 탑재되는 소프트웨어모듈로 구현되거나, 무선이동통신망을 통해 일회용패스워드(OTP) 정보를 수신하도록 독립적으로 구성될 수 있다. 이때 상기 OTP단말기(230)가 무선이동통신망을 통해 일회용패스워드(OTP)를 수신하도록 구성되는 경우 상기 OTP단말기(230)는 이동통신단말기의 형태로 구현될 수 있다.

<24> 다음으로, 상기 OTP서버(300)는 인증서버(100)로부터 1차 인증된 사용자의 정보를 수신하여 1차 인증된 사용자에 대한 일회용패스워드(OTP)를 실시간으로 생성한 후 생성된 일회용패스워드(OTP) 정보를 통신망(400)을 통해 인증서버(100) 및 사용자의 OTP단말기(230)로 전송하도록 구성된다. 이때 사용자의 OTP단말기(230)가 이동통신단말기인 경우 인증서버(100)는 일회용패스워드(OTP) 인증을 위한 일회용패스워드 생성을 OTP서버(300)로 요청하면서 사용자의 이동통신 단말기 번호를 함께 전송한다. OTP서버(300)는 일회용패스워드를 생성하여 인증서버(100)로 전송함과 동시에 사용자 이동통신단말기 번호를 이용하여 SMS 등의 메시지를 생성하여 사용자 OTP단말기(230)인 사용자의 이동통신단말기로 전송하게 된다. 이때 사용자 이동통신단말기로 전송되는 일회용패스워드 정보는 통신망(400)에 포함되는 이동통신망의 기지국(410)을 경유하여 사용자의 이동통신단말기로 전송된다.

<25> 상술한 구성을 가지는 본발명의 다중인증 접속 시스템은 통신망(400)을 통해 접속 요청하는 사용자에 대하여 아이디와 패스워드를 이용하여 1차 인증을 수행하고, 이 후 1차 인증된 사용자에 대하여 지문정보 또는 일회용패스워드 중 적어도 하나 이상의 정보를 이용하여 다중인증을 수행하는 것에 의해 1차 인증된 사용자가 해당 아이디와 패스워드에 대한 정당한 사용자인지를 판별하여 시스템의 접속 보안을 향상시킴은 물론 개인의 경우 아이디와 패스워드의 제3자의 노출에 의한 도용을 방지하게 된다.

<26> 도 2 내지 도 4는 상술한 바와 같은 다중인증 접속 시스템에 의한 다중인증 접속 방법의 처리과정을 나타내는 것으로서, 이하 도 2 내지 도 4를 참조하여 본 발명의 다중인증 접속 방법을 상세히 설명한다.

<27> 도 2에 도시된 바와 같이 본발명의 다중인증 접속 방법은, 사용자가 사용자단말기(210)를 이용하여 통신망(400)을 통해 인증서버(100)에 접속한 후 인증서버(100)의 접속서비스부(110)가 제공하는 인터페이스 화면을 통해 아이디와 패스워드를 등록하고, 자신의 지문을 지문스캐너(220)를 통해 스캔하여 등록하며, 이외에 주소, 전화번호, 주민등록 번호 등의 사용자 신상정보를 등록하는 사용자정보등록과정으로 시작된다(S10).

<28> 상술한 바와 같이 사용자정보등록이 수행된 후 사용자가 인증서버(100)에 접속을 원하는 경우 사용자는 사용자단말기(210)를 통해 인증서버(100)로 접속하여 인증서버(100)의 접속서비스부(210)가 제공하는 인터페이스 화면을 통해 아이디와 패스워드를 입력하여 인증서버(100)로 전송하는 것에 의해 1차 인증을 요청한다(S20).

<29> 인증서버(100)의 접속서비스부(110)는 사용자 단말기(210)로부터 전송된 아이디와 패스워드를 사용자정보

DB(150)에 저장된 아이디와 패스워드 정보와 비교하여 사용자에 대한 1차 인증을 수행하게 된다(S30).

<30> 이 후 인증서버(100)의 접속서비스부(100)는 사용자가 전송한 아이디와 패스워드를 사용자정보DB(150)에 저장된 아이디와 패스워드를 비교하여 일치되지 않는 경우에는 해당 인증 절차 과정에서의 1차 인증 실패 회수가 기 지정된 회수와 일치하는 지를 판단하여 일치하지 않는 경우에는 S20과정으로 복귀하여 사용자가 아이디와 패스워드를 이용한 재인증을 수행하도록 하고(S40), 기 지정된 회수와 일치하는 경우에는 인증실패를 알리는 에러 메시지를 출력하고 처리과정을 종료한다(S50).

<31> 이와 달리 사용자가 전송한 아이디와 패스워드를 사용자정보DB(150)에 저장된 아이디와 패스워드를 비교하여 일치되는 경우에는 인증서버(100)의 접속서비스부(110)는 사용자의 아이디 정보에 1차 인증 성공에 대한 표시(예, 인증 성공을 나타내는 토큰 등의 식별자 부여)를 수행하여 1차 인증을 승인하다. 그리고 인증제어부(140)에 의해 다중인증 수행신호를 수신하는 경우에는 접속제어부(110)는 지문정보 또는 일회용패스워드 정보(OTP 정보) 중 적어도 하나 이상을 이용하는 다중인증의 수행을 사용자단말기(210)로 전송하여 사용자가 다중인증을 수행하도록 한다. 사용자는 사용자단말기(210)에 출력되는 다중인증 요청 방식에 따라 지문인증 또는 OTP정보를 전송하여 다중인증의 수행하게 된다(S70).

<32> 도 3은 상술한 다중인증 중 지문인증을 위한 지문정보 전송과정을 나타내며, 도 4는 일회용패스워드(OTP) 정보를 이용한 일회용패스워드(OTP) 정보 전송 과정을 나타내는 것으로서 각각의 정보 전송 과정을 먼저 설명하면 다음과 같다.

<33> 먼저, 도 3을 참조하여 지문정보 전송 과정을 설명하면, 인증서버(100)의 접속서비스부(110)가 1차 인증 후 사용자 단말기(210)로 지문인증을 요청한다(S71).

<34> 사용자는 사용자단말기(210)에 부착된 지문스캐너(220)를 이용하여 자신이 등록한 지문을 스캔하게 되고, 지문스캐너(220)에서 스캔된 사용자의 지문정보는 사용자단말기(210)에 의해 인증서버(100)로 전송된다(S72).

<35> 다음으로, 도 4를 참조하여 일회용패스워드(OTP) 정보 전송 과정을 설명하면, 인증서버(100)의 접속서비스부(110)가 1차 인증 후 사용자 단말기(210)로는 일회용패스워드인증을 요청하고, OTP서버(300)로는 1차 인증된 사용자 정보를 전송하여 1차 인증된 사용자에 대한 일회용패스워드(OTP)의 생성 및 전송을 요청한다(S73). OTP서버(300)는 인증서버(100)가 전송한 1차 인증된 사용자 정보를 이용하여 1차 인증된 사용자에 대한 일회용패스워드(OTP)를 생성하여, 인증서버(100) 및 사용자의 OTP단말기(230)로 전송한다. 이 때 사용자의 OTP단말기(230)가 이동통신 단말기인 경우에는 생성된 일회용패스워드(OTP) 정보는 사용자의 이동통신단말기의 번호를 이용하여 문자메시지의 형태로 사용자에게 전송된다(S74). OTP서버(300)로부터 일회용패스워드를 전송받은 사용자는 접속서비스부(110)가 제공하여 사용자단말기(210)에 출력되는 인터페이스화면에 수신된 일회용패스워드 정보를 입력하여 인증서버(100)로 전송한다(S75).

<36> 다음으로, 상술한 바와 같은 도 3 또는 도 4의 처리과정에 의해 지문정보 또는 일회용패스워드(OTP) 정보가 인증서버(100)로 전송되면, 인증서버(100)는 도 2에서와 같이 다중인증을 수행하게 된다. 이때, 지문정보에 의한 다중인증인 경우 인증서버(100)는 지문인증부(120)를 이용하여 사용자정보DB(150)에 저장된 1차 인증된 사용자의 지문정보와 사용자 단말기(210)로부터 전송된 지문정보를 비교하여 다중인증을 수행한다. 그리고 일회용패스워드(OTP) 정보에 의한 인증인 경우에는 OTP인증부(130)를 이용하여 OTP서버(300)가 전송한 일회용패스워드(OTP) 정보와 사용자 단말기(210)로부터 전송된 일회용패스워드(OTP) 정보를 비교하여 인증을 수행한다(S70).

<37> 상술한 처리과정에 의해 1차 인증된 사용자에 대한 다중인증을 수행한 인증서버(100)는 다중인증이 실패한 경우에는 해당 다중인증과정 동한 다중인증 실패 회수가 기지정된 실패 회수와 일치하는 지를 판단한다(S80). 판단결과 다중인증 실패 회수가 기 지정된 회수를 일치하지 않는 경우(작은 경우)에는 S60 과정으로 이동하여 1차 인증된 사용자가 다중인증정보를 재전송하도록 하고 처리과정을 다시 수행한다. 이와 달리 다중인증 실패 회수가 기 지정된 회수를 일치하는 경우에는 다중인증 실패를 알리는 에러메시지를 출력한 후 처리과정을 종료한다(S90).

<38> 다음으로, S70 과정에의 수행에 의해 다중인증이 성공한 경우에는 1차 인증된 사용자의 아이디에 다중인증 성공을 표시하는 식별자를 부여하여 사용자가 상기 아이디를 이용하여 시스템에 접속한 후 서비스를 제공받을 수 있도록 한 후 인증 처리과정을 종료한다(S100).

<39> 상술한 본발명의 다중인증은 지문인증, 일회용패스워드 인증 및 지문인증과 일회용패스워드 인증 중 어느 하나의 방식을 통해 구현될 수 있다. 이러한 적용은 사용자에 적용되는 보안 등급에 따라 선택적으로 적용되며, 이는 인증서버(100)의 인증제어부(140)에 의해 그 적용방식이 결정되도록 구성될 수 있다. 그리고 상술한 다중인

증 방법 중 지문정보 및 일회용패스워드 정보를 동시에 이용하는 다중인증에서 지문인증과 일회용패스워드 인증의 순서는 선택적으로 또는 동시에 적용될 수 있다.

도면의 간단한 설명

<40> 도 1은 본발명의 일 실시 예에 따르는 다중인증 접속 시스템의 구성도,

<41> 도 2는 상기 도 2의 다중인증 시스템에 의한 다중인증 방법의 처리과정을 나타내는 순서도,

<42> 도 3은 도 2의 다중인증 중 지문인증을 위한 지문인증정보 전송 과정을 나타내는 서브루틴도,

<43> 도 4는 도 2의 다중인증 중 일회용패스워드(OTP) 인증을 위한 OTP 정보 전송 과정을 나타내는 서브루틴도이다.

<44> * 도면의 주요 부호에 대한 설명 *

<45> 100: 인증서버

<46> 110: 접속서비스부 120: 지문인증부

<47> 130: OTP인증부 140: 인증제어부

<48> 150: 사용자정보DB

<49> 200: 사용자장치부

<50> 210: 사용자단말기 220: 지문스캐너

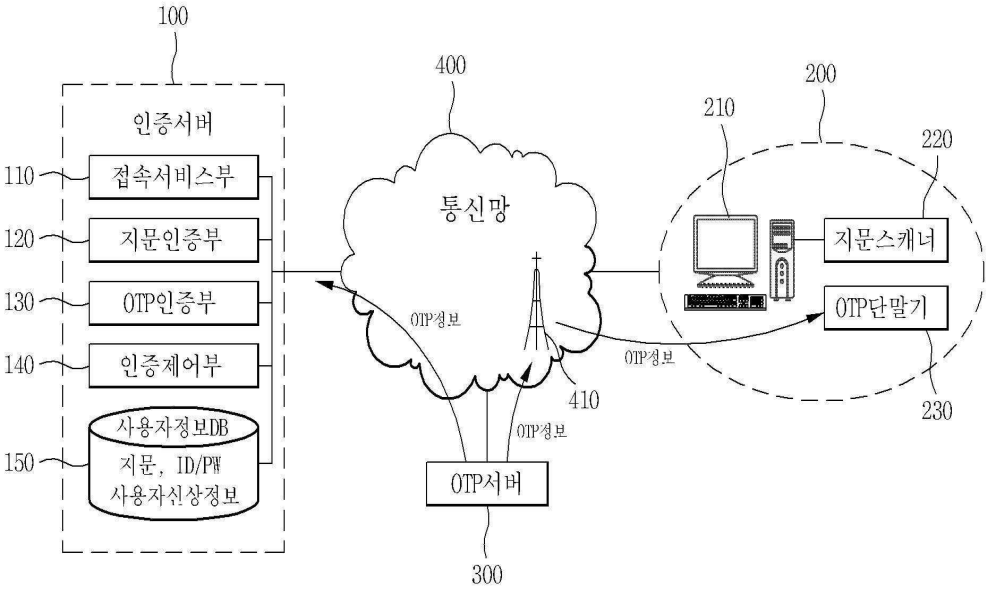
<51> 230: OTP단말기

<52> 300: OTP서버

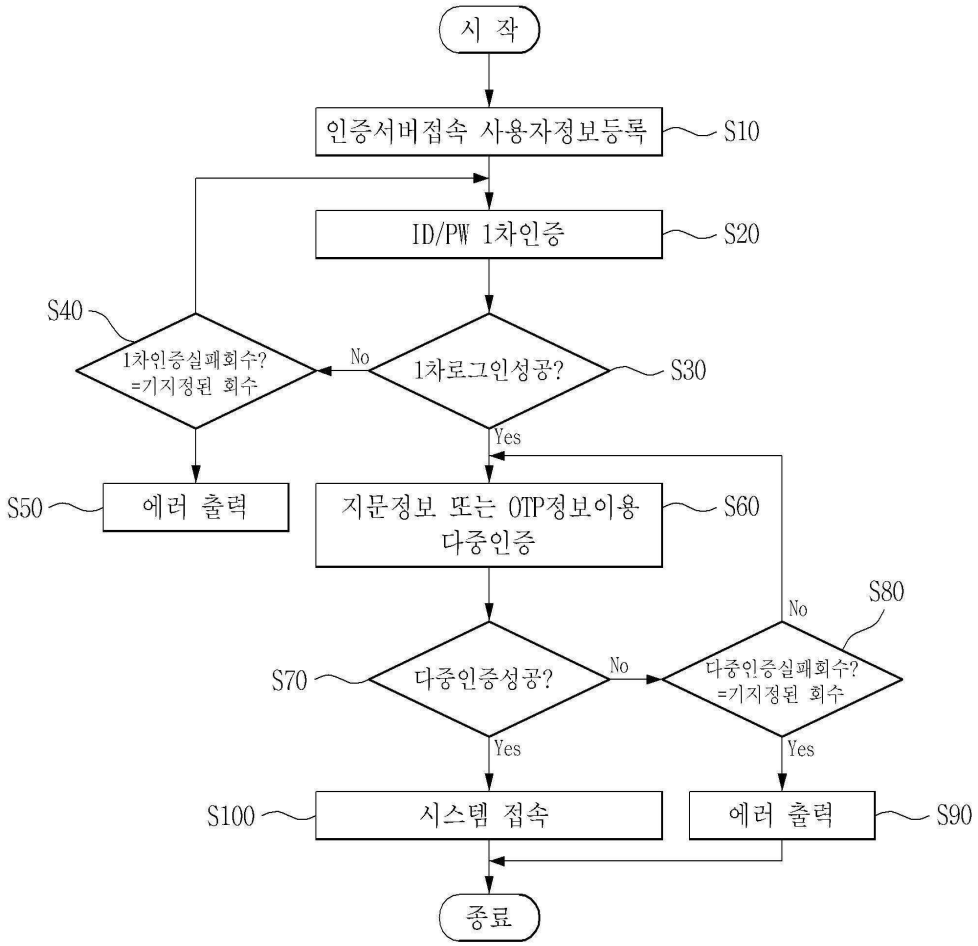
<53> 400: 통신망

도면

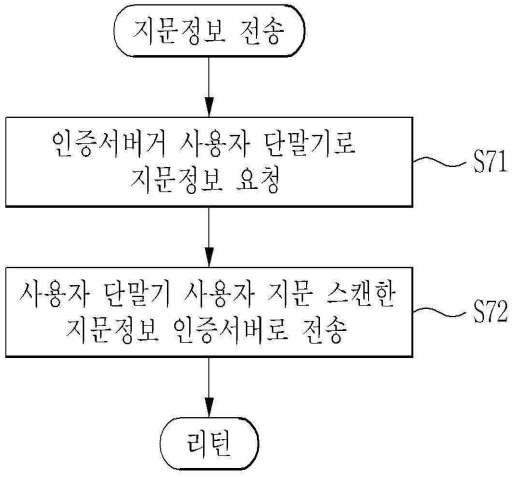
도면1



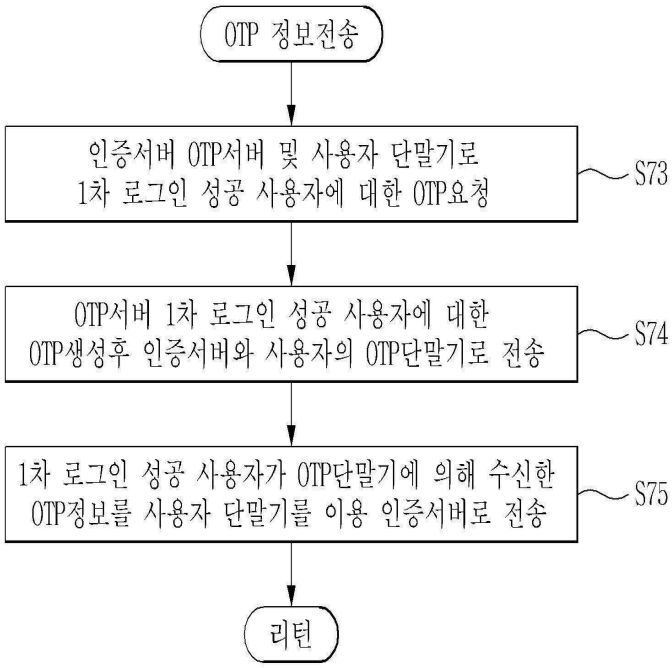
도면2


시 작
인증서버접속 사용자정보등록
S10
ID/PW 1차인증
S20
S40
1차인증실패회수?
=기지정된 회수
No
1차로그인성공?
S30
Yes
S50
에러 출력
지문정보 또는 OTP정보이용
다중인증
S60
S80
No
S70
다중인증성공?
No
다중인증실패회수?
=기지정된 회수
Yes
Yes
S100
시스템 접속
에러 출력
S90
종료

도면3


지문정보 전송
인증서버거 사용자 단말기로
지문정보 요청
S71
사용자 단말기 사용자 지문 스캔한
지문정보 인증서버로 전송
S72
리턴

도면4


OTP 정보전송
인증서버 OTP서버 및 사용자 단말기로
1차 로그인 성공 사용자에 대한 OTP요청
S73
OTP서버 1차 로그인 성공 사용자에 대한
OTP생성후 인증서버와 사용자의 OTP단말기로 전송
S74
1차 로그인 성공 사용자가 OTP단말기에 의해 수신한
OTP정보를 사용자 단말기를 이용 인증서버로 전송
S75
리턴