



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0104667

(43) 공개일자 2015년09월16일

(51) 국제특허분류(Int. Cl.)

H04L 9/32 (2006.01)

(21) 출원번호 10-2014-0026041

(22) 출원일자 2014년03월05일

심사청구일자 2014년03월05일

(71) 출원인

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

이동훈

서울 종로구 사직로8길 34, 1404호 (내수동, 경희궁의아침3단지)

김현

서울 강북구 솔샘로 174, 114동 1302호 (미아동, SK북한산시티아파트)

(뒷면에 계속)

(74) 대리인

김홍석, 김동용

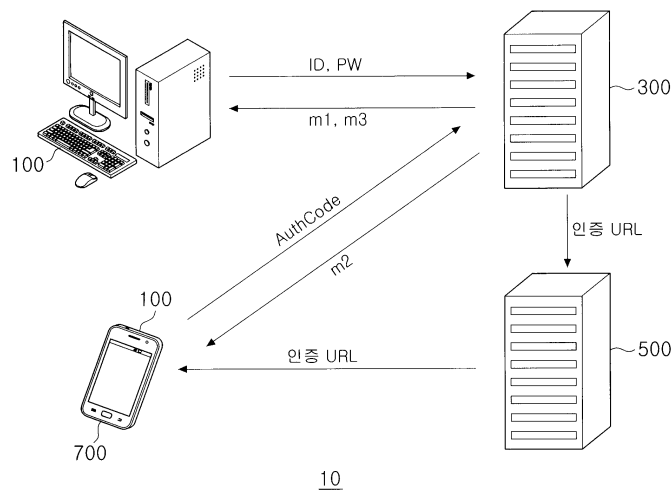
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 인증 방법

(57) 요약

제1 서버에서 사용자를 인증하는 방법이 개시된다. 상기 인증하는 방법은 상기 사용자의 제1 단말기로부터 상기 사용자의 아이디와 비밀번호를 수신하는 단계, 수신된 아이디 및 수신된 비밀번호를 이용하여 상기 사용자에 대한 제1 인증을 수행하는 단계, 상기 제1 서버의 URL(uniform resource locator)과 상기 사용자에 대한 인증 코드를 포함하는 인증 URL을 제2 서버로 송신하는 단계, 상기 사용자의 제2 단말기로부터 인증 코드를 수신하는 단계, 및 상기 인증 URL에 포함된 상기 인증 코드와 상기 제2 단말기로부터 수신된 인증 코드를 비교하여 상기 사용자에 대한 제2 인증을 수행하는 단계를 포함한다.

대표도 - 도1



(72) 발명자

이상혁

서울특별시 마포구 마포대로7길 22, 306동 1302호
(공덕동, 삼성래미안공덕3차아파트)

김종석

서울 광진구 동일로70길 30, 201호 (중곡동, 진양
아트빌)

명세서

청구범위

청구항 1

제1 서버에서 사용자를 인증하는 방법에 있어서,

상기 사용자의 제1 단말기로부터 상기 사용자의 아이디와 비밀번호를 수신하는 단계;

수신된 아이디 및 수신된 비밀번호를 이용하여 상기 사용자에 대한 제1 인증을 수행하는 단계;

상기 제1 서버의 URL(uniform resource locator)과 상기 사용자에 대한 인증 코드를 포함하는 인증 URL을 제2 서버로 송신하는 단계;

상기 사용자의 제2 단말기로부터 인증 코드를 수신하는 단계; 및

상기 인증 URL에 포함된 상기 인증 코드와 상기 제2 단말기로부터 수신된 인증 코드를 비교하여 상기 사용자에 대한 제2 인증을 수행하는 단계를 포함하는, 제1 서버에서 사용자를 인증하는 방법.

청구항 2

제1항에 있어서,

상기 제1 인증을 수행하는 단계는 상기 제1 인증의 결과 메시지를 상기 제1 단말기로 송신하는 단계를 더 포함하는, 제1 서버에서 사용자를 인증하는 방법.

청구항 3

제1항에 있어서,

상기 제2 인증을 수행하는 단계는 상기 제2 인증의 결과 메시지를 상기 제1 단말기와 상기 제2 단말기 중 적어도 하나의 단말기로 송신하는 단계를 더 포함하는, 제1 서버에서 사용자를 인증하는 방법.

청구항 4

제1항에 있어서,

상기 인증 URL에 포함된 상기 인증 코드는 상기 사용자의 아이디를 입력 값으로 하는 해쉬(hash) 함수의 결과 값으로부터 생성되는, 제1 서버에서 사용자를 인증하는 방법.

청구항 5

제1항에 있어서,

상기 제1 단말기는 PC(personal computer), 넷북(netbook), 노트북(notebook) 또는 태블릿 PC(tablet PC)이고,

상기 제2 단말기는 스마트폰(smart phone) 또는 모바일폰(mobile phone)이고,

상기 제2 서버는 SNS(social network service) 서버인, 제1 서버에서 사용자를 인증하는 방법.

청구항 6

제1항에 있어서,

상기 인증 코드를 수신하는 단계는,

상기 제2 단말기가 상기 제2 서버로부터 수신한 인증 URL에 포함된 상기 인증 코드를 상기 제2 단말기로부터 수신하는, 제1 서버에서 사용자를 인증하는 방법.

청구항 7

제1항에 있어서,

상기 제2 인증을 수행하는 단계는,

상기 제1 서버가 상기 인증 URL을 상기 제2 서버로 송신한 시간으로부터 미리 정해진 시간 안에 상기 제2 단말기로부터 상기 인증 코드가 수신된 경우, 상기 사용자를 인증하는, 제1 서버에서 사용자를 인증하는 방법.

청구항 8

제1항에 있어서,

상기 제1 서버에서 사용자를 인증하는 방법은,

상기 아이디와 상기 비밀번호를 수신하는 단계 이전에, 상기 제2 단말기를 식별하기 위한 제1 식별 정보와 상기 제2 서버를 식별하기 위한 제2 식별 정보를 등록하는 단계를 더 포함하는, 제1 서버에서 사용자를 인증하는 방법.

청구항 9

제8항에 있어서,

상기 등록하는 단계는,

상기 제1 식별 정보와 상기 제2 식별 정보를 상기 제1 단말기로부터 수신하는 단계;

상기 URL과 제2 인증 코드를 포함하는 제2 인증 URL을 상기 제2 서버로 송신하는 단계; 및

상기 제2 단말기로부터 상기 제2 인증 코드를 수신하는 단계를 포함하는, 제1 서버에서 사용자를 인증하는 방법.

청구항 10

제9항에 있어서,

상기 제2 인증 코드를 수신하는 단계는,

상기 제2 단말기가 상기 제2 서버로부터 수신한 제2 인증 URL에 포함된 상기 제2 인증 코드를 상기 제2 단말기로부터 수신하는, 제1 서버에서 사용자를 인증하는 방법.

청구항 11

제10항에 있어서,

상기 등록하는 단계는,

상기 제1 서버가 상기 제2 인증 URL을 상기 제2 서버로 송신한 시간으로부터 미리 정해진 시간 안에 상기 제2 단말기로부터 상기 제2 인증 코드가 수신된 경우, 상기 제1 식별 정보와 상기 제2 식별 정보를 DB(database)에 등록하는, 제1 서버에서 사용자를 인증하는 단계.

발명의 설명

기술 분야

[0001]

본 발명의 개념에 따른 실시 예는 인증 방법에 관한 것으로, 특히 사용자의 아이디와 비밀번호를 이용하여 제1 인증을 수행하고, 모바일 SNS 서버를 이용하여 제2 인증을 수행할 수 있는 인증 방법에 관한 것이다.

배경 기술

[0002]

인터넷을 이용하고 있는 사용자들은 인터넷 상에서 영화 예매, 쇼핑, 정보 검색, 메일, 인터넷 뱅킹 등과 같은 다양한 서비스들을 제공하고 있다. 이러한 서비스들을 제공하는 웹 서버 중 상당수는 비밀번호를 기반으로 하는 인증 방식, 즉 고정된 비밀번호만으로 사용자들에 대한 인증을 수행하기 때문에, 제3자에 의한 엿보기 공격(shoulder surfing), 추측 공격(guessing attack), 피싱/파밍(phishing/pharming) 공격 등에 취약한 문제점이 있다.

[0003] 상기와 같은 문제점을 해결하기 위해 투-팩터(two-factor) 인증 기법이 활용되고 있다. 상기 투-팩터 인증 기법은 비밀번호, PIN(personal Identification Number) 등과 같은 사용자가 알고 있는 것, OTP(One Time Password) 토큰, 모바일 OTP, SMS(Short Message Service) 인증 등과 같은 사용자가 소지한 것, 및 지문 등의 생체정보와 같은 사용자 그 자체 중에서 2 가지를 인증 과정에서 활용하는 기법이다.

[0004] 그러나, 상기 투-팩터 인증 기법들은 사용자 편의성이 낮거나 보안에 취약한 문제점이 존재한다. 예컨대, OTP 토큰을 이용한 인증 기법의 경우, 사용자가 금융 지점을 직접 방문해서 토큰을 구입해야 하고, 인증을 위해서는 OTP 토큰을 항상 소지하고 있어야 하는 불편함이 있다. 모바일 OTP를 이용한 인증 기법의 경우, 통합된 모바일 OTP 어플리케이션이 없기 때문에 제공하는 업체마다 서로 다른 어플리케이션을 사용해야 하는 불편함이 있다. SMS를 이용한 인증 기법의 경우, 인증 시마다 휴대 전화 번호, 통신사, 생년월일 등의 개인 정보의 입력을 요구하기 때문에, 키로깅(keylogging), 화면 캡처 등의 악성 코드에 의해서 개인 정보가 유출될 위험이 있다. 또한, OTP 토큰, 모바일 OTP, SMS를 이용하는 인증 방식은 사용자가 직접 웹 브라우저에 입력해야 하는 불편함이 있다.

[0005] 따라서, 사용자 편의성을 높일 수 있고, 보안에 강한 새로운 인증 기법이 필요하다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 대한민국 공개특허 제2013-0078842호
(특허문헌 0002) 대한민국 공개특허 제2009-0098766호

발명의 내용

해결하려는 과제

[0007] 본 발명이 이루고자 하는 기술적인 과제는 사용자의 제1 단말기로부터 수신된 아이디와 비밀번호를 이용하여 제1 인증을 수행하고, 상기 사용자의 제2 단말기로부터 수신한 인증 코드를 이용하여 제2 인증을 수행할 수 있는 인증 방법을 제공하는 것이다.

과제의 해결 수단

[0008] 본 발명의 실시 예에 따른 제1 서버에서 사용자를 인증하는 방법은, 상기 사용자의 제1 단말기로부터 상기 사용자의 아이디와 비밀번호를 수신하는 단계, 수신된 아이디 및 수신된 비밀번호를 이용하여 상기 사용자에게 대한 제1 인증을 수행하는 단계, 상기 제1 서버의 URL(uniform resource locator)과 상기 사용자에게 대한 인증 코드를 포함하는 인증 URL을 제2 서버로 송신하는 단계, 상기 사용자의 제2 단말기로부터 인증 코드를 수신하는 단계, 및 상기 인증 URL에 포함된 상기 인증 코드와 상기 제2 단말기로부터 수신된 인증 코드를 비교하여 상기 사용자에게 대한 제2 인증을 수행하는 단계를 포함한다.

[0009] 상기 제1 인증을 수행하는 단계는 상기 제1 인증의 결과 메시지를 상기 제1 단말기로 송신하는 단계를 더 포함할 수 있다.

[0010] 상기 제2 인증을 수행하는 단계는 상기 제2 인증의 결과 메시지를 상기 제1 단말기와 상기 제2 단말기 중 적어도 하나의 단말기로 송신하는 단계를 더 포함할 수 있다.

[0011] 또한, 상기 인증 URL에 포함된 상기 인증 코드는 상기 사용자의 아이디를 입력 값으로 하는 해쉬(hash) 함수의 결과 값으로부터 생성될 수 있다.

[0012] 상기 제1 단말기는 PC, 넷북, 노트북 또는 태블릿 PC로 구현될 수 있고, 상기 제2 단말기는 스마트폰(smart phone) 또는 모바일폰(mobile phone)으로 구현될 수 있고, 상기 제2 서버는 SNS(social network service) 서버로 구현될 수 있다.

[0013] 또한, 상기 인증 코드를 수신하는 단계는, 상기 제2 단말기가 상기 제2 서버로부터 수신한 인증 URL에 포함된 상기 인증 코드를 상기 제2 단말기로부터 수신할 수 있다.

- [0014] 또한, 상기 제2 인증을 수행하는 단계는, 상기 제1 서버가 상기 인증 URL을 상기 제2 서버로 송신한 시간으로부터 미리 정해진 시간 안에 상기 제2 단말기로부터 상기 인증 코드가 수신된 경우, 상기 사용자를 인증할 수 있다.
- [0015] 또한, 상기 제1 서버에서 사용자를 인증하는 방법은, 상기 아이디와 상기 비밀번호를 수신하는 단계 이전에, 상기 제2 단말기를 식별하기 위한 제1 식별 정보와 상기 제2 서버를 식별하기 위한 제2 식별 정보를 등록하는 단계를 더 포함할 수 있다.
- [0016] 또한, 상기 등록하는 단계는, 상기 제1 식별 정보와 상기 제2 식별 정보를 상기 제1 단말기로부터 수신하는 단계, 상기 URL과 제2 인증 코드를 포함하는 제2 인증 URL을 상기 제2 서버로 송신하는 단계, 및 상기 제2 단말기로부터 상기 제2 인증 코드를 수신하는 단계를 포함할 수 있다.
- [0017] 또한, 상기 제2 인증 코드를 수신하는 단계는, 상기 제2 단말기가 상기 제2 서버로부터 수신한 제2 인증 URL에 포함된 상기 제2 인증 코드를 상기 제2 단말기로부터 수신하는 단계일 수 있다.
- [0018] 또한, 상기 등록하는 단계는, 상기 제1 서버가 상기 제2 인증 URL을 상기 제2 서버로 송신한 시간으로부터 미리 정해진 시간 안에 상기 제2 단말기로부터 상기 제2 인증 코드가 수신된 경우, 상기 제1 식별 정보와 상기 제2 식별 정보를 DB(database)에 등록하는 단계일 수 있다.

발명의 효과

- [0019] 본 발명의 실시 예에 따른 인증 방법은 두 가지 인자(TWO-FACTOR)를 이용하여 인증 절차를 수행함으로써, 보안 위협으로부터 사용자를 보호할 수 있는 효과가 있다.
- [0020] 또한, 상기 인증 방법은 사용자가 소지하고 있는 스마트폰 등과 같은 핸드헬드 장치를 이용하여 인증 절차를 수행함으로써, 사용자의 편의성을 높일 수 있는 효과가 있다.
- [0021] 또한, 상기 인증 기법은 인증 결과를 사용자의 제1 단말기와 제2 단말기에 송신함으로써, 공격자의 재전송 공격, 추측 공격, 피싱/파밍 공격, 및 기기 장악 공격을 예방할 수 있으며, 인가되지 않은 사용자에 의한 인증 시도 시 실시간으로 계정 도용을 감지할 수 있는 효과가 있다.
- [0022] 또한, 상기 인증 기법의 제2 인증은 사용자의 제2 단말기를 통해 수행됨으로써, 상기 사용자의 제1 단말기, 예컨대 PC가 악성 코드에 감염되어 있어도 인증 코드가 유출되는 문제를 차단할 수 있는 효과가 있다.

도면의 간단한 설명

- [0023] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.
- 도 1은 본 발명의 일 실시 예에 따른 인증 시스템을 도시한다.
- 도 2는 도 1에 도시된 제1 서버의 기능 블록도이다.
- 도 3은 도 1에 도시된 인증 시스템의 등록 모드 동작을 설명하기 위한 흐름도이다.
- 도 4는 도 1에 도시된 인증 시스템의 인증 모드 동작을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0024] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.
- [0025] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.
- [0026] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명

될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

- [0027] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.
- [0028] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [0029] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [0030] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예를 상세히 설명한다.
- [0031] 도 1은 본 발명의 일 실시 예에 따른 인증 시스템을 도시한다.
- [0032] 도 1을 참조하면, 인증 시스템(10)은 사용자의 제1 단말기(100), 제1 서버(300), 제2 서버(500), 및 상기 사용자의 제2 단말기(700)를 포함한다.
- [0033] 제1 단말기(100)와 제1 서버(300), 제1 서버(300)와 제2 서버(500), 제2 서버(500)와 제2 단말기(700), 및 제2 단말기(700)와 제1 서버(300) 사이의 통신은 SSL(Secure Sockets Layer) 프로토콜을 이용하거나 별도의 암호화된 채널을 통하여 이루어질 수 있다.
- [0034] 제1 단말기(100)는 PC(personal computer), 태블릿 PC, 노트북(notebook), 넷-북(net-book), e-리더(e-reader), PDA(personal digital assistant), PMP(portable multimedia player), MP3 플레이어, 또는 MP4 플레이어와 같은 데이터 처리 장치로 구현될 수 있다.
- [0035] 제1 단말기(100)는 상기 사용자에게 대한 제1 인증을 위해 상기 사용자의 아이디(ID)와 비밀번호(PW)를 제1 서버(300)로 송신하고, 상기 제1 인증의 결과 메시지(m1)을 제1 서버(300)로부터 수신한다. 실시 예에 따라, 제1 단말기(100)는 상기 사용자에게 대한 제2 인증의 결과 메시지(m3)을 제1 서버(300)로부터 수신할 수도 있다.
- [0036] 제1 서버(300)는 제1 단말기(100)의 요청에 따라 소정의 콘텐츠 또는 서비스를 제1 단말기(100)를 통하여 상기 사용자에게 제공하는 웹 서버일 수 있다.
- [0037] 제1 서버(300)는 제1 단말기(100)로부터 수신한 아이디(ID)와 비밀번호(PW)를 이용하여 상기 사용자에게 대한 제1 인증을 수행하고, 상기 제1 인증의 결과 메시지(m1)를 제1 단말기(100)로 송신할 수 있다.
- [0038] 또한, 제1 서버(300)는 상기 사용자에게 대한 제2 인증을 수행하기 위하여,
- [0039] 상기 사용자에게 대한 인증 코드(AuthCode)와 제1 서버(300)의 URL(Uniform Resource Locator)을 포함하는 인증 URL을 제2 서버(500)로 송신할 수 있다.
- [0040] 또한, 제1 서버(300)는 제2 단말기(700)로부터 인증 코드(AuthCode)를 수신하고, 수신된 인증 코드(AuthCode)를 이용하여 상기 제2 인증을 수행하고, 상기 제2 인증의 결과 메시지(m2, m3)를 제1 단말기(100)와 제2 단말기(700) 중 적어도 하나의 단말기로 송신할 수 있다.
- [0041] 제2 서버(500)는 제2 단말기(700)를 통하여 상기 사용자에게 SNS(Social Network Service)를 제공하는 SNS 서버일 수 있다. 따라서, 제2 서버(500)는 제1 서버(300)로부터 수신한 상기 인증 URL을 제2 단말기(700)로 송신할 수 있다.

- [0042] 제2 단말기(700)는 모바일폰(mobile phone), 스마트폰(smart phone), 태블릿 PC, PMP, MP3 플레이어, 또는 MP4 플레이어와 같은 핸드헬드 장치(handheld device)로 구현될 수 있다.
- [0043] 제2 단말기(700)는 제2 서버(500)로부터 수신한 인증 URL에 포함되어 있는 인증 코드(AuthCode)를 제1 서버(300)로 송신하고, 상기 제2 인증의 결과 메시지인 제2 메시지(m2)를 제1 서버(300)로부터 수신할 수 있다. 상기 인증 URL은 상기 사용자가 제2 단말기(700)를 통하여 제2 서버(500)로부터 제공받는 SNS, 예컨대 모바일 메신저(mobile messenger) 서비스를 통하여 수신될 수 있다. 따라서, 상기 사용자는 상기 모바일 메신저 서비스를 이용하기 위하여 제2 단말기(700)에 설치된 모바일 어플리케이션(mobile application)의 대화창에 표시된 인증 URL을 클릭 또는 터치하는 동작만으로 인증 코드(AuthCode)를 제1 서버(300)로 송신할 수 있다.
- [0044] 또한, 제2 메시지(m2)는 제1 서버(300)로부터 제2 단말기(700)로 제공되거나, 제2 서버(500)를 통하여 제2 단말기(700)에 제공되거나, 또는 도시되지 않은 별도의 SMS(short message service) 서버를 통하여 제2 단말기(700)에 제공될 수도 있다.
- [0045] 도 2는 도 1에 도시된 제1 서버의 기능 블록도이다.
- [0046] 도 1과 도 2를 참조하면, 제1 서버(300)는 통신 모듈(310), 인증 URL 생성 모듈(330), 메모리(350), 및 제어 모듈(370)을 포함한다.
- [0047] 통신 모듈(310)은 제어 모듈(370)의 제어 하에 제1 단말기(100), 제2 서버(500) 또는 제2 단말기(700)와 통신할 수 있다.
- [0048] 인증 URL 생성 모듈(330)은 제어 모듈(370)의 제어 하에 인증 URL을 생성한다. 상기 인증 URL은 제1 서버(300)의 URL과 사용자를 인증하기 위한 인증 코드(AuthCode)를 포함한다. 인증 코드(AuthCode)는 상기 사용자의 ID, 상기 사용자의 세션에 대한 세션 아이디(session identification), 및 랜덤 함수의 결과 값인 임의의 랜덤 값 중 적어도 하나 이상을 입력으로 하여 생성된 해쉬(hash) 함수의 결과 값 자체이거나, 상기 해쉬 함수의 결과 값을 이용하여 생성된 값일 수 있다.
- [0049] 상기 URL과 상기 인증 코드(AuthCode)를 포함하는 인증 URL은 아래와 같은 형식으로 구현될 수 있다.
- [0050] `https://site.com/confirm?ac=AuthCode`
- [0051] 메모리(350)는 프로그램 메모리와 데이터 메모리를 포함할 수 있다. 상기 프로그램 메모리에는 제1 서버(300)의 동작을 제어하기 위한 프로그램들이 저장될 수 있다. 상기 데이터 메모리에는 상기 프로그램들을 수행하는 과정에서 발생하는 데이터들이 저장될 수 있다.
- [0052] 제어 모듈(370) 제1 서버(300)의 전반적인 동작을 제어한다. 즉, 제어 모듈(370)은 등록 모드와 인증 모드에 따라 통신 모듈(310), 인증 URL 생성 모듈(330), 및 메모리(180)의 동작을 제어할 수 있다.
- [0053] 등록 모드에서, 제어 모듈(370)은 통신 모듈(310)을 제어하여 제2 단말기(700)를 식별하기 위한 제1 식별 정보와 제2 서버(500)를 식별하기 위한 제2 식별 정보를 수신한다. 이때, 제어 모듈(370)은 통신 모듈(310)을 제어하여 상기 사용자의 아이디와 비밀번호를 추가적으로 수신할 수도 있다.
- [0054] 제2 단말기(700)가 스마트 폰 또는 모바일 폰 등으로 구현되는 경우, 상기 제1 식별 정보는 상기 스마트 폰 또는 상기 모바일 폰의 전화 번호일 수 있다. 실시 예에 따라, 상기 제1 식별 정보는 상기 사용자가 제2 서버(500)로부터 SNS를 제공받기 위해 사용하는 아이디일 수 있고, 상기 SNS를 제공받기 위해 사용하는 아이디는 상기 사용자의 이메일(e-mail) 계정일 수 있다.
- [0055] 또한, 제어 모듈(370)은 인증 URL 생성 모듈(330)을 제어하여 상기 사용자를 인증하기 위한 인증 URL을 생성하고, 생성된 인증 URL을 통신 모듈(310)을 통하여 제2 서버(500)로 송신한다. 즉, 제1 서버(300)는 제2 서버(500)를 통하여 상기 인증 URL을 제2 단말기(700)로 송신한다.
- [0056] 통신 모듈(310)을 통하여 제2 단말기(700)로부터 인증 코드(AuthCode)가 수신되면, 제어 모듈(370)은 제2 서버(500)로 송신된 인증 URL에 포함된 인증 코드와 제2 단말기(700)로부터 수신된 인증 코드를 비교하고, 상기 수신된 인증 URL에 포함된 인증 코드와 상기 수신된 인증 코드가 일치하는 경우, 상기 제1 식별 정보와 상기 제2 식별 정보를 DB에 등록 또는 저장할 수 있다. 추가적으로 수신된 상기 사용자의 아이디와 비밀번호 또한 제어 모듈(370)에 의해 상기 DB에 등록될 수 있다.
- [0057] 이때, 제어 모듈(370)은 상기 수신된 인증 코드가 상기 송신된 인증 URL을 송신한 시간으로부터 미리 정해진 시

간 내에 수신된 경우에만 상기 제1 식별 정보와 상기 제2 식별 정보를 상기 DB에 저장할 수 있다.

[0058] 상기와 같이 등록 모드는 상기 제1 식별 정보와 상기 제2 식별 정보를 DB에 등록하기 위해 수행된다.

[0059] 인증 모드에서, 제어 모듈(370)은 통신 모듈(310)을 통하여 수신된 사용자의 아이디와 비밀번호를 이용하여 상기 사용자에 대한 제1 인증을 수행한다. 제어 모듈(370)은 수신된 아이디 및 수신된 비밀번호를 DB에 저장된 아이디 및 비밀번호와 비교하고, 일치하는 경우 상기 사용자를 인증한다. 또한, 제어 모듈(370)은 통신 모듈(310)을 제어하여 상기 제1 인증의 결과 메시지인 제1 메시지(m1)를 제1 단말기(100)로 송신할 수 있다. 제1 메시지(m1)은 상기 제1 인증의 성공 여부에 관한 정보를 포함한다.

[0060] 상기 제1 인증이 성공한 경우, 제어 모듈(370)은 상기 사용자에 대한 제2 인증을 위해 인증 URL 생성 모듈(330)과 통신 모듈(310)을 제어한다. 즉, 인증 URL 생성 모듈(330)은 제어 모듈(370)의 제어에 따라, 인증 URL을 생성하고, 통신 모듈(310)은 제어 모듈(370)의 제어에 따라, 생성된 인증 URL을 제2 서버(500)로 송신한다.

[0061] 통신 모듈(310)을 통하여 인증 코드(AuthCode)가 수신된 경우, 제어 모듈(370)은 상기 사용자에 대한 제2 인증을 완료하고, 통신 모듈(310)을 제어하여 제1 단말기(100)와 제2 단말기(700) 중 적어도 하나의 단말기에 상기 제2 인증의 결과 메시지를 송신할 수 있다. 즉, 제2 메시지(m2)는 제2 단말기(700)로 송신될 수 있고, 제3 메시지(m3)는 제1 단말기(100)로 송신될 수 있다. 제2 메시지(m2)와 제3 메시지(m3)는 상기 제2 인증의 성공 여부에 관한 정보를 포함한다.

[0062] 실시 예에 따라, 제1 서버(300)는 상기 사용자의 아이디, 비밀번호, 제2 단말기(700)를 식별하기 위한 제1 식별 정보, 및 상기 사용자에 의하여 등록된 제2 서버를 식별하기 위한 제2 식별 정보를 저장하기 위한 DB(database)를 더 포함할 수도 있다. 상기 DB는 제어 모듈(370)에 의해 제어될 수 있다.

[0063] 도 2에 도시된 제1 서버(300)의 각각의 구성은 기능 및 논리적으로 분리될 수 있음으로 나타내는 것이며, 반드시 각각의 구성이 별도의 물리적 장치로 구분되거나 별도의 코드로 작성됨을 의미하는 것은 아님을 본 발명의 기술분야의 평균적 전문가가 용이하게 추론할 수 있을 것이다.

[0064] 또한, 본 명세서에서 모듈이라 함은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 모듈은 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것이 아니다.

[0065] 또한, 본 명세서에서 DB라 함은, 각각의 DB에 대응되는 정보를 저장하는 소프트웨어 및 하드웨어의 기능적 구조적 결합을 의미할 수 있다. DB는 적어도 하나의 테이블로 구현될 수도 있으며, 상기 DB에 저장된 정보를 검색, 저장, 및 관리하기 위한 별도의 DBMS(Database Management System)를 더 포함할 수도 있다. 또한, 링크드 리스트(linked-list), 트리(Tree), 관계형 DB의 형태 등 다양한 방식으로 구현될 수 있으며, 상기 DB에 대응되는 정보를 저장할 수 있는 모든 데이터 저장매체 및 데이터 구조를 포함한다.

[0066] 도 3은 도 1에 도시된 인증 시스템의 등록 모드 동작을 설명하기 위한 흐름도이다.

[0067] 도 1과 도 3을 참조하면, 제1 단말기(100)는 사용자의 아이디(ID), 비밀번호(PW), 제1 식별 정보(IF1), 및 제2 식별 정보(IF2)를 제1 서버(300)로 송신한다(S110).

[0068] 제1 서버(300)는 제2 서버(500)로 송신될 인증 URL을 생성(S120)하고, 생성된 인증 URL을 제2 서버(500)로 송신한다(S130). 상기 인증 URL은 제1 서버(300)의 URL과 인증 코드를 포함할 수 있다.

[0069] 제2 서버(500)는 수신된 인증 URL을 상기 사용자의 제2 단말기(700)로 송신한다(S140). 제2 단말기(700)는 수신된 인증 URL에 포함된 인증 코드(AuthCode)를 제1 서버(300)로 송신한다(S150).

[0070] 제1 서버(300)는 제2 서버(500)로 송신된 인증 URL에 포함된 인증 코드와 제2 단말기(700)로부터 송신된 인증 코드(AuthCode)가 동일할 경우, 제1 식별 정보(IF1)와 제2 식별 정보(IF2)를 DB에 등록한다(S160)

[0071] 도 4는 도 1에 도시된 인증 시스템의 인증 모드 동작을 설명하기 위한 흐름도이다.

[0072] 도 1과 도 4를 참조하면, 제1 단말기(100)는 사용자의 아이디(ID)와 비밀번호(PW)를 제1 서버(300)로 송신한다(S210). 제1 서버(300)는 수신된 아이디(ID) 및 비밀번호(PW)를 미리 저장된 아이디 및 비밀번호와 비교함으로써, 상기 사용자에 대한 제1 인증을 수행한다(S230). 제1 서버(300)는 상기 제1 인증의 수행 결과에 관한 정보를 포함하고 있는 제1 메시지(m1)를 제1 단말기(100)로 송신할 수 있다(S250). 구체적으로, 상기 제1 인증이 성

공적으로 수행된 경우, 즉 수신된 아이디(ID) 및 비밀번호(PW)가 상기 미리 저장된 아이디 및 비밀번호와 일치할 경우, 제1 메시지(m1)는 상기 제1 인증이 성공적으로 수행되었음을 알리는 메시지일 수 있고, 상기 제1 인증이 성공적으로 수행되지 않은 경우, 즉 수신된 아이디(ID) 및 비밀번호(PW)가 상기 미리 저장된 아이디 및 비밀번호와 일치하지 않는 경우, 제1 메시지(m1)는 상기 제1 인증이 성공적으로 수행되지 않았음을 알리는 메시지일 수 있다.

[0073] 상기 제1 인증이 성공적으로 수행된 경우, 제1 서버(300)는 제2 서버(500)로 송신될 인증 URL을 생성하고(S310), 생성된 인증 URL을 제2 서버(500)로 송신할 수 있다(S330). 제2 서버(500)는 수신된 인증 URL을 상기 사용자의 제2 단말기(700)로 송신한다(S350). 제2 단말기(700)는 수신된 인증 URL에 포함된 인증 코드(AuthCode)를 상기 제1 서버(300)로 송신한다(S370).

[0074] 제1 서버(300)는 제2 단말기(700)로부터 수신된 인증 코드(AuthCode)와 제2 서버로 전송된 인증 URL에 포함된 인증 코드를 비교함으로써, 상기 사용자에게 대한 제2 인증을 수행한다(S380). 제1 서버(300)는 상기 제2 인증의 수행 결과를 제1 단말기(100)와 제2 단말기(700) 중 적어도 하나의 단말기로 송신할 수 있다(S391 및 S393). 즉, 제2 메시지(m2)는 제2 단말기(700)로 송신될 수 있고(S391), 제3 메시지(m3)은 제1 단말기(100)로 송신될 수 있다(S393).

[0075] 또한, 제1 서버(300)는 상기 인증 URL을 제2 서버(500)로 송신한 시간으로부터 미리 정해진 시간 안에 상기 인증 코드(AuthCode)를 상기 제2 단말기(700)로부터 수신한 경우, 상기 사용자에게 대한 제2 인증을 수행할 수 있다.

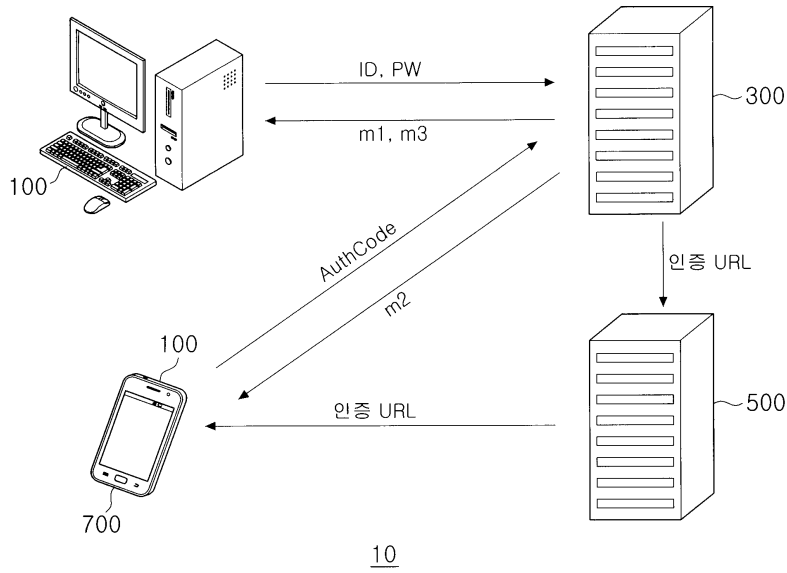
[0076] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

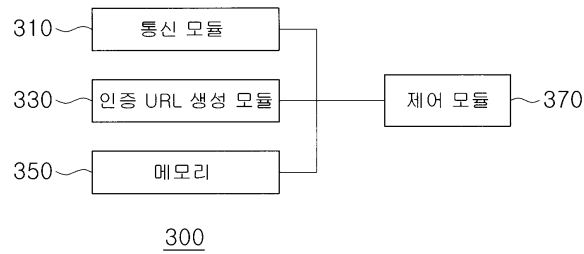
[0077] 10 : 인증 시스템 100 : 제1 단말기
300 : 제1 서버 310 : 통신 모듈
330 : 인증 URL 생성 모듈 350 : 메모리
370 : 제어 모듈 500 : 제2 서버
700 : 제2 단말기

도면

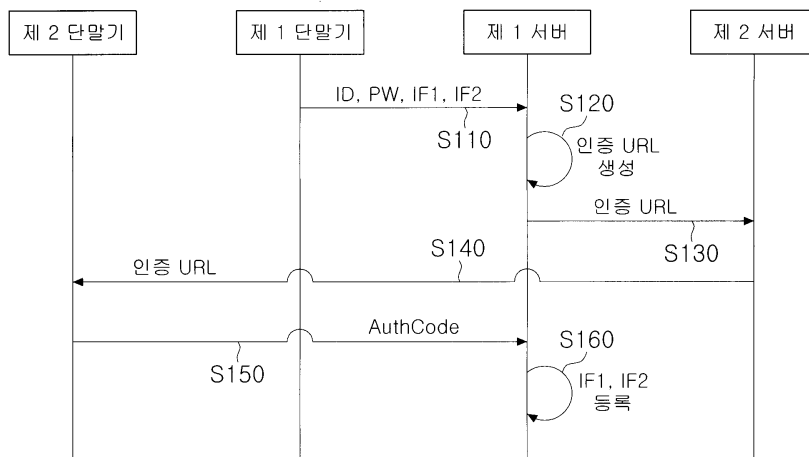
도면1



도면2



도면3



도면4

