(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0125654
(43) 공개일자 2018년11월26일

(51) 국제특허분류(Int. Cl.)
G06F 21/46 (2013.01) *G06F 21/31* (2013.01)
(52) CPC특허분류
G06F 21/46 (2013.01)
G06F 21/31 (2013.01)
(21) 출원번호 10-2017-0059887
(22) 출원일자 2017년05월15일
심사청구일자 2017년05월15일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
권신일
서울특별시 동대문구 무학로45길 37 309호 (용두동)
차성덕
서울특별시 성북구 동소문로34길 24, 106동 710호(돈암동, 삼성아파트)
(74) 대리인
김등용, 김홍석

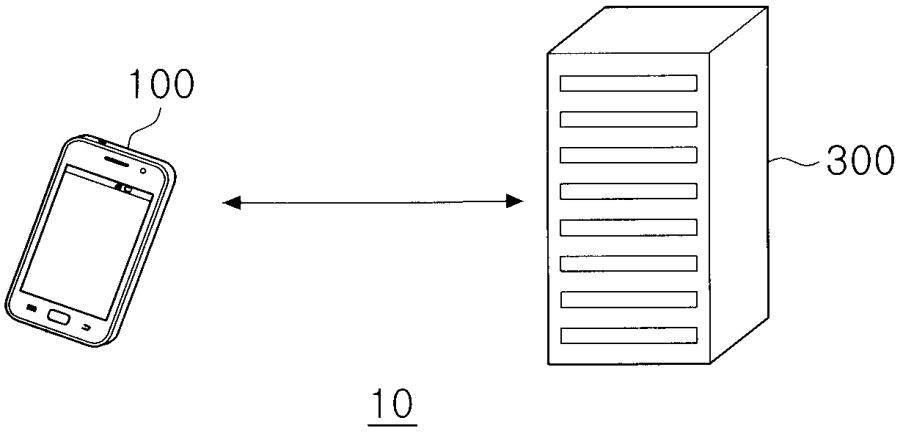
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **멀티미디어 데이터를 이용한 사용자 인증 방법**

(57) 요 약

사용자 인증 방법이 개시된다. 상기 사용자 인증 방법은 사용자 등록 단계와 사용자 인증 단계를 포함하고, 상기 사용자 등록 단계는 상기 서버가 단말로부터 아이디를 수신하는 단계, 상기 서버가 상기 아이디에 대응하는 패스워드 입력 요청 메시지를 상기 단말로 송신하는 단계, 및 상기 서버가 상기 단말로부터 적어도 하나의 멀티미디어 파일과 힌트를 수신하는 단계를 포함하고, 상기 적어도 하나의 멀티미디어 파일은 이미지 파일, 동영상 파일 또는 음성 파일인 것을 특징으로 한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 63/0428 (2013.01)
H04L 63/083 (2013.01)

명 세 서

청구범위

청구항 1

서버에 의해 수행되는 사용자 인증 방법에 있어서,

사용자 등록 단계와 사용자 인증 단계를 포함하고,

상기 사용자 등록 단계는,

상기 서버가 단말로부터 아이디를 수신하는 단계;

상기 서버가 상기 아이디에 대응하는 패스워드 입력 요청 메시지를 상기 단말로 송신하는 단계; 및

상기 서버가 상기 단말로부터 적어도 하나의 멀티미디어 파일과 힌트를 수신하는 단계를 포함하고,

상기 적어도 하나의 멀티미디어 파일은 이미지 파일, 동영상 파일 또는 음성 파일인,

사용자 인증 방법.

청구항 2

제1항에 있어서, 상기 사용자 인증 단계는,

상기 서버가 상기 단말로부터 상기 아이디를 수신하는 단계;

상기 서버가 상기 아이디에 대응하는 상기 힌트를 상기 단말로 송신하는 단계;

상기 서버가 상기 단말로부터 적어도 하나의 제2 멀티미디어 파일을 수신하는 단계; 및

상기 서버가 상기 적어도 하나의 제2 멀티미디어 파일과 상기 적어도 하나의 멀티미디어 파일의 동일성 여부에 기초하여 사용자 인증 여부를 결정하는 단계를 포함하는,

사용자 인증 방법.

청구항 3

서버에 의해 수행되는 사용자 인증 방법에 있어서,

사용자 등록 단계와 사용자 인증 단계를 포함하고,

상기 사용자 등록 단계는,

상기 서버가 단말로부터 아이디를 수신하는 단계;

상기 서버가 상기 아이디에 대응하는 패스워드 입력 요청 메시지를 상기 단말로 송신하는 단계; 및

상기 서버가 상기 단말로부터 암호화키를 이용하여 적어도 하나의 멀티미디어 파일을 암호화한 암호문과 힌트를 수신하는 단계를 포함하고,

상기 적어도 하나의 멀티미디어 파일은 이미지 파일, 동영상 파일 또는 음성 파일인,

사용자 인증 방법.

청구항 4

제3항에 있어서, 상기 사용자 인증 단계는,

상기 서버가 상기 단말로부터 상기 아이디를 수신하는 단계;

상기 서버가 상기 아이디에 대응하는 상기 힌트를 상기 단말로 송신하는 단계;

상기 서버가 상기 단말로부터 제2 암호문을 수신하는 단계; 및

상기 서버가 상기 암호문과 상기 제2 암호문을 이용하여 사용자 인증 여부를 결정하는 단계를 포함하는,

사용자 인증 방법.

청구항 5

제4항에 있어서,

상기 사용자 인증 여부를 결정하는 단계는, 상기 암호문과 상기 제2 암호문이 동일한 경우 사용자를 인증하는,

사용자 인증 방법.

청구항 6

제4항에 있어서,

상기 사용자 인증 여부를 결정하는 단계는, 상기 암호문의 복호화 결과와 상기 제2 암호문의 복호화 결과가 동일한 경우 사용자를 인증하는,

사용자 인증 방법.

청구항 7

사용자 등록 단계와 사용자 인증 단계를 포함하는 사용자 인증 방법에 있어서,

상기 사용자 등록 단계는,

서버가 단말로부터 아이디를 수신하는 단계;

상기 서버가 상기 아이디에 대응하는 패스워드 입력 요청 메시지를 상기 단말로 송신하는 단계;

상기 단말이 적어도 하나의 멀티미디어 파일을 암호화한 암호문과 힌트를 상기 서버로 송신하는 단계; 및

상기 단말이 상기 적어도 하나의 멀티미디어 파일을 클라우드 서버로 송신하는 단계를 포함하고,

상기 적어도 하나의 멀티미디어 파일은 이미지 파일, 동영상 파일 또는 음성 파일인,

사용자 인증 방법.

청구항 8

제7항에 있어서, 상기 사용자 인증 단계는,

상기 서버가 상기 단말로부터 상기 아이디를 수신하는 단계;

상기 서버가 상기 아이디에 대응하는 상기 힌트를 상기 단말로 송신하는 단계;

상기 단말이 상기 클라우드 서버로부터 적어도 하나의 제2 멀티미디어 파일을 수신하는 단계;

상기 단말이 상기 적어도 하나의 제2 멀티미디어 파일을 암호화한 제2 암호문을 상기 서버로 송신하는 단계;

상기 서버가 상기 암호문과 상기 제2 암호문을 이용하여 사용자 인증 여부를 결정하는 단계를 포함하는,

사용자 인증 방법.

청구항 9

제8항에 있어서,

상기 사용자 인증 여부를 결정하는 단계는, 상기 암호문과 상기 제2 암호문이 동일한 경우 사용자를 인증하는,

사용자 인증 방법.

청구항 10

제8항에 있어서,

상기 사용자 인증 여부를 결정하는 단계는, 상기 암호문의 복호화 결과와 상기 제2 암호문의 복호화 결과가 동일한 경우 사용자를 인증하는,

사용자 인증 방법.

발명의 설명

기 술 분 야

[0001] 본 발명의 개념에 따른 실시 예는 멀티미디어 데이터를 이용한 사용자 인증 방법에 관한 것으로, 특히 사용자에 의해 쉽게 기억되지만 제3자의 유추가 불가능한 멀티미디어 데이터 또는 멀티미디어 데이터의 암호화 결과인 암호문을 패스워드로 사용하는 멀티미디어 데이터를 이용한 사용자 인증 방법에 관한 것이다.

배 경 기 술

[0003] 서버 및 특정 기기에서 특정 사용자를 인증 및 확인하기 위하여 문자 기반 패스워드를 활용한 인증 시스템이 널리 사용되고 있다. 즉, 현재 대부분의 사용자 인증 시스템은 알파벳, 숫자 및 특수문자들을 조합한 문자 패스워드를 사용하고 있는 실정이다.

[0004] 그러나, 문자 패스워드는 기억하기 어렵고 사전 공격(dictionary attack)에 취약한 문제점이 있다. 이에 기억하기 쉽고 사전 공격에 안전한 사용자 인증 방법을 제안하고자 한다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 미합중국 등록특허 제9,270,452호

(특허문헌 0002) 대한민국 공개특허 제2004-0028158호

발명의 내용

해결하려는 과제

[0007] 본 발명이 이루고자 하는 기술적인 과제는 멀티미디어 데이터 또는 상기 멀티미디어 데이터의 암호화 결과인 암호문을 패스워드로 사용함으로써 사용자가 기억하기 쉽고 사전 공격에 안전한 사용자 인증 방법을 제공하는 것이다.

과제의 해결 수단

[0009] 본 발명의 일 실시 예에 의한 인증 방법은 서버에 의해 수행되고, 사용자 등록 단계와 사용자 인증 단계를 포함하고, 상기 사용자 등록 단계는 상기 서버가 단말로부터 아이디를 수신하는 단계, 상기 서버가 상기 아이디에 대응하는 패스워드 입력 요청 메시지를 상기 단말로 송신하는 단계, 및 상기 서버가 상기 단말로부터 적어도 하나의 멀티미디어 파일과 힌트를 수신하는 단계를 포함하고, 상기 적어도 하나의 멀티미디어 파일은 이미지 파일, 동영상 파일 또는 음성 파일인 것을 특징으로 한다.

[0010] 본 발명의 다른 실시 예에 의한 인증 방법은 서버에 의해 수행되고, 사용자 등록 단계와 사용자 인증 단계를 포함하고, 상기 사용자 등록 단계는 상기 서버가 단말로부터 아이디를 수신하는 단계, 상기 서버가 상기 아이디에 대응하는 패스워드 입력 요청 메시지를 상기 단말로 송신하는 단계, 및 상기 서버가 상기 단말로부터 암호화키를 이용하여 적어도 하나의 멀티미디어 파일을 암호화한 암호문과 힌트를 수신하는 단계를 포함하고, 상기 적어도 하나의 멀티미디어 파일은 이미지 파일, 동영상 파일 또는 음성 파일인 것을 특징으로 한다.

[0011] 본 발명의 또 다른 실시 예에 의한 인증 방법은 사용자 등록 단계와 사용자 인증 단계를 포함하고, 상기 사용자 등록 단계는 서버가 단말로부터 아이디를 수신하는 단계, 상기 서버가 상기 아이디에 대응하는 패스워드 입력 요청 메시지를 상기 단말로 송신하는 단계, 상기 단말이 적어도 하나의 멀티미디어 파일을 암호화한 암호문과 힌트를 상기 서버로 송신하는 단계, 및 상기 단말이 상기 적어도 하나의 멀티미디어 파일을 클라우드 서버로 송신하는 단계를 포함하고, 상기 적어도 하나의 멀티미디어 파일은 이미지 파일, 동영상 파일 또는 음성 파일인 것을 특징으로 한다.

발명의 효과

[0013] 본 발명에 의할 경우 다음과 같은 효과가 있다.

[0014] 첫째, 패스워드를 유추하기가 어렵다. 구체적으로, 문자 기반 패스워드는 임의의 문자열을 생성 및 시도하는 과정을 통해 패스워드를 유추할 수 있지만 이미지 데이터는 임의로 생성하여 유추하는 것이 불가능하다.

[0015] 둘째, 패스워드를 기억하기가 쉽다. 구체적으로, 기존의 문자 패스워드는 기억하기기 어려웠고, 이로 인하여 모든 사이트에 동일한 패스워드를 사용하는 일이 빈번하게 발생했다. 본 발명에서 제안하는 방식은 클라우드(cloud) 환경 또는 자신의 기기에 저장된 멀티미디어 데이터를 선택하여 업로드 하기만 하면 된다. 또한, 기억을 상기시키기 쉽게하기 위하여 서버에 패스워드 설정 시 힌트를 등록하는 방법도 고려할 수 있다. 유저는 힌트를 보고 자신의 패스워드를 상기시키고 해당 파일을 업로드하면 된다.

도면의 간단한 설명

[0017] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 의한 인증 시스템을 도시한다.

도 2는 도 1에 도시된 인증 시스템 상에서 수행되는 인증 방법 중 사용자 등록 단계의 일 예를 설명하기 위한 흐름도이다.

도 3은 도 1에 도시된 인증 시스템 상에서 수행되는 인증 방법 중 사용자 인증 단계의 일 예를 설명하기 위한 흐름도이다.

도 4는 본 발명에서 사용되는 패스워드를 설명하기 위한 멀티미디어 파일의 예시를 도시한다.

도 5는 본 발명의 다른 실시 예에 의한 인증 시스템을 도시한다.

도 6은 도 5에 도시된 인증 시스템 상에서 수행되는 인증 방법 중 사용자 등록 단계의 예를 설명하기 위한 흐름도이다.

도 7은 도 5에 도시된 인증 시스템 상에서 수행되는 인증 방법 중 사용자 인증 단계의 예를 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 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.

[0019] 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.

[0020] 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 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0021] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "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" 있다거나 "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.

[0022] 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.

[0023] 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 의미를 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.

[0024] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0026] 도 1은 본 발명의 일 실시 예에 의한 인증 시스템을 도시한다.

[0027] 도 1을 참조하면, 인증 시스템(10)은 단말(100)과 서버(300)를 포함한다.

[0028] 사용자는 단말(100)을 통하여 서버(300)가 제공하는 서비스를 제공받을 수 있다. 이때, 단말(100)과 서버(300)는 유무선 통신망을 통하여 서로 통신할 수 있다. 또한, 사용자가 서비스를 서버(300)로부터 제공받기 위하여는 사용자 등록 과정과을 거쳐 사용자를 서버(300)에 등록하고, 인증 과정을 통하여 인증을 완료하여야 한다.

[0030] 도 2는 도 1에 도시된 인증 시스템 상에서 수행되는 인증 방법 중 사용자 등록 단계의 일 예를 설명하기 위한 흐름도이다.

[0031] 도 1 내지 도 2를 참조하면, 단말(100)은 사용자 등록을 위해 등록 요청 메시지를 서버(300)로 송신할 수 있다(S110). 서버(300)는 상기 등록 요청 메시지에 응답하여 아이디 입력 요청 메시지를 단말(100)로 송신할 수 있다(S120).

[0032] 아이디 입력 요청 메시지를 수신한 단말(100)은 소정의 입력 장치를 통하여 사용자로부터 아이디를 입력받고, 상기 사용자로부터 입력받은 아이디를 서버(300)로 송신한다(S130).

[0033] 단말(100)로부터 아이디를 수신한 서버(300)는 수신된 아이디의 중복 여부를 판단할 수 있고(S140), 수신된 아이디가 서버(300)에 저장된 아이디와 중복되는 경우 아이디를 재입력 받기 위해 아이디 재입력 요청 메시지를 단말(100)로 송신할 수 있다(S150).

[0034] 상기 아이디 재입력 요청 메시지에 응답하여 단말(100)은 새로운 아이디를 서버(300)로 송신할 수 있다(S160). 단말(100)로부터 수신된 아이디가 중복되지 않는 경우 서버(300)는 아이디에 대응하는 패스워드 입력 요청 메시지를 단말(100)로 송신할 수 있다(S170).

[0035] 상기 패스워드 입력 요청 메시지를 수신한 단말(100)은 단말(100) 내에 저장된 멀티미디어 파일들(또는 멀티비디어 데이터) 중 소정의 입력 장치를 통하여 사용자에 의해 선택된 적어도 하나의 파일을 서버(300)로 송신할 수 있다(S180). 즉, 단말(100)에 의해 송신된 파일 자체가 패스워드가 될 수 있으며, 상기 멀티미디어 파일은 이미지 파일, 음성 파일 또는 동영상 파일을 포함할 수 있다. 실시 예에 따라, 단말(100)은 추가적으로 상기 패스워드를 유추할 수 있는 힌트를 서버(300)로 송신할 수도 있다.

[0036] 단말(100)로부터 패스워드를 수신한 서버(300)는 사용자에 대한 등록 과정을 완료하고, 이에 따라 등록 완료 메시지를 단말(100)로 송신할 수 있다(S190). 이때, 상기 사용자의 아이디, 패스워드 및 힌트는 서버(300) 내에 저장될 수 있다.

[0038] 도 3은 도 1에 도시된 인증 시스템 상에서 수행되는 인증 방법 중 사용자 인증 단계의 일 예를 설명하기 위한 흐름도이다.

[0039] 서버(300)로부터 소정의 서비스를 제공받기 위해서는 사용자 인증이 선행되어야 한다. 따라서, 단말(100)은 인증 요청 메시지를 서버(300)로 송신한다(S210).

[0040] 상기 인증 요청 메시지에 응답하여 서버(300)는 아이디 입력 요청 메시지를 단말(100)로 송신할 수 있고(S220), 단말(100)은 소정의 입력 장치를 통해 사용자로부터 수신한 아이디를 서버(300)로 송신할 수 있다(S230).

[0041] 단말(100)로부터 아이디를 수신한 서버(300)는 수신된 아이디의 패스워드를 유출할 수 있는 힌트를 단말(100)로 송신할 수 있다(S240). 상기 힌트는 상기 아이디와 상기 패스워드를 등록하는 과정에서 단말(100)로부터 수신되어 서버(300)에 미리 저장되어 있을 수 있다.

[0042] 사용자에 의해 선택된 패스워드(즉, 적어도 하나의 멀티미디어 파일)는 단말(100)에 의해 서버(300)로 송신된다(S250). 단말(100)로부터 수신된 패스워드가 서버(300)에 저장되어 있는 패스워드와 동일할 경우, 단말(100)의 사용자에 대한 인증은 완료된다. 인증이 완료된 경우, 즉 인증이 성공적으로 완료된 경우, 서버(300)는 인증 완료 메시지를 단말(100)로 송신할 수 있다(S260). 이에 따라 사용자는 서버(300)로부터 소정의 서비스를 제공받을 수 있다.

[0044] 도 4는 본 발명에서 사용되는 패스워드를 설명하기 위한 멀티미디어 파일의 예시를 도시한다.

[0045] 도 4에는 4 개의 이미지 파일들이 도시되어 있다. 상기 4 개의 이미지 파일들은 단말(100) 내에 저장되어 있을 수 있고, 사용자 등록 단계나 사용자 인증 단계에서 단말(100)에 구비되어 있는 디스플레이 장치를 통하여 디스플레이될 수 있다.

[0046] 단말(100) 내에 터치 스크린이 구비된 경우, 사용자는 디스플레이되는 복수의 이미지 파일들 중 적어도 하나를 선택함으로써, 사용자 등록 단계나 사용자 인증 단계에서 사용될 이미지 파일을 선택할 수 있다. 사용자가 좌측 상단에 있는 이미지를 사용자 등록 단계에서 패스워드로 선택하는 경우, 사용자는 "Again 2007"을 힌트로 설정할 수 있다. 상기 힌트는 대한민국 프로야구단인 한화 이글스가 마지막으로 우승했던 연도를 적은 것으로 단말(100)의 사용자는 힌트와 이미지 파일들의 연관성을 용이하게 알 수 있으나, 단말(100)의 사용자가 아닌 사람은 상기 힌트로부터 패스워드를 유추하기는 어렵다.

[0048] 도 5는 본 발명의 다른 실시 예에 의한 인증 시스템을 도시한다.

[0049] 인증 시스템(30)은 단말(100), 서버(300) 및 클라우드 서버(500)를 포함한다.

[0050] 도 1을 통해 설명한 인증 시스템(10)에 의할 경우, 패스워드 파일이 항상 단말(100) 내에 저장되어야만 하는 편의성 문제와 패스워드 분실, 패스워드 해킹 및 패스워드가 저장된 단말(100)의 분실이나 도난 등으로 인한 보안 문제가 발생할 수 있다.

[0051] 따라서, 인증 시스템(30)은 멀티미디어 파일을 저장하기 위한 새로운 주체인 클라우드 서버(500)를 도입하여 편의성 문제를 해결하고, 암호화키를 도입하여 해킹, 도난 또는 분실로 인한 보안 문제를 해결하고자 한다.

[0052] 즉, 패스워드를 포함하는 복수의 멀티미디어 파일들을 클라우드 서버(300)에 업로드함으로써 장소에 구애받지 않고 패스워드 파일에 접근할 수 있다. 또한, 패스워드, 즉 멀티미디어 파일을 암호화키로 암호화한 결과를 서버(300)로 송신함으로써 패스워드 유출로 인한 문제점을 해결할 수 있다.

[0054] 도 6은 도 5에 도시된 인증 시스템 상에서 수행되는 인증 방법 중 사용자 등록 단계의 예를 설명하기 위한 흐름도이다.

[0055] 단말(100)은 사용자 등록을 위해 등록 요청 메시지를 서버(300)로 송신할 수 있다(S310). 서버(300)는 상기 등록 요청 메시지에 응답하여 아이디 입력 요청 메시지를 단말(100)로 송신할 수 있다(S320).

[0056] 아이디 입력 요청 메시지를 수신한 단말(100)은 소정의 입력 장치를 통하여 사용자로부터 아이디를 입력받고, 사용자로부터 입력받은 아이디를 서버(300)로 송신한다(S330).

[0057] 실시 예에 따라, S330 단계 이후에 서버(300)에 의한 수신된 아이디의 중복 여부를 판단 단계, 수신된 아이디가 서버(300)에 저장된 아이디와 중복되는 경우 아이디를 재입력받기 위해 아이디 재입력 요청 메시지를 단말(100)로 송신하는 단계, 및 상기 아이디 재입력 요청 메시지에 응답하여 단말(100)이 새로운 아이디를 서버(300)로 송신하는 단계가 수행될 수도 있다.

[0058] 단말(100)로부터 중복되지 않은 아이디가 수신된 경우 서버(300)는 아이디에 대응하는 패스워드 입력 요청 메시지를 단말(100)로 송신할 수 있다(S340).

[0059] 상기 패스워드 입력 요청 메시지를 수신한 단말(100)은 멀티미디어 파일을 소정의 암호화키를 이용하여 암호화함으로써 암호문을 생성하고, 생성된 암호문과 상기 암호문에 대응하는 힌트를 서버(300)로 송신할 수 있다(S350). 상기 멀티미디어 파일은 단말(100) 내에 저장된 복수의 멀티미디어 파일들 중 소정의 입력 장치를 통하여 사용자에 의해 선택된 파일을 의미할 수 있고, 상기 암호문은 상기 멀티미디어 파일에 대한 메시지 인증 코드(message authentication code, MAC)를 의미할 수도 있다. 여기서, 상기 암호화키는 대칭키 암호 기법에서 사용되는 대칭키, 공개키 암호 기법에서 사용되는 개인키 또는 공개키를 의미할 수 있다. 상기 암호화키가 상기 대칭키일 경우 상기 대칭키는 소정의 키 공유 알고리즘을 통하여 단말(100)과 서버(300)에 의해 미리 공유될 수 있으며, 상기 암호화키가 상기 개인키(즉, 단말(100)의 개인키)일 경우 상기 개인키에 대응하는 공개키(즉, 단말(100)의 공개키)가 단말(100) 또는 별도의 키 생성 서버에 의해 생성되어 공개되거나 서버(300)로 송신됨으로써 서버(300)에 미리 저장되어 있을 수 있으며, 상기 암호화키가 상기 공개키(즉, 서버(300)의 공개키)일 경우 상기 공개키에 대응하는 개인키(즉, 서버(300)의 개인키)가 서버(300)에 미리 저장되어 있을 수 있다. 또한, 실시 예에 따라 상기 암호문을 복호화하지 않고 상기 암호문 자체가 패스워드로 사용될 수 있으며, 이 경우 서버(300)에는 상기 암호문을 복호화하기 위한 대칭키 또는 공개키가 저장되어 있지 않을 수도 있다.

[0060] 또한, 단말(100)은 상기 멀티미디어 파일을 포함하는 적어도 하나의 멀티미디어 파일을 클라우드 서버(500)로 송신할 수 있다(S360). 상기 적어도 하나의 멀티미디어 파일을 클라우드 서버(500)에 저장함으로써, 상기 멀티미디어 파일이 단말(100)에 저장되어 있지 않은 상태에서 후술될 사용자 인증 과정이 수행될 수 있다.

[0061] 상기 암호문과 상기 힌트를 수신한 서버(300)는 상기 사용자에 대한 등록을 완료하고 등록 완료 메시지를 단말(100)로 송신할 수 있다(S370).

[0063] 도 7은 도 5에 도시된 인증 시스템 상에서 수행되는 인증 방법 중 사용자 인증 단계의 예를 설명하기 위한 흐름도이다.

[0064] 서버(300)로부터 소정의 서비스를 제공받기 위해서는 사용자 인증이 선행되어야 한다. 따라서, 단말(100)은 인증 요청 메시지를 서버(300)로 송신한다(S410).

[0065] 상기 인증 요청 메시지에 응답하여 서버(300)는 아이디 입력 요청 메시지를 단말(100)로 송신할 수 있고(S420), 단말(100)은 소정의 입력 장치를 통해 사용자로부터 수신한 아이디를 서버(300)로 송신할 수 있다(S430).

[0066] 단말(100)로부터 아이디를 수신한 서버(300)는 수신된 아이디의 패스워드를 유출할 수 있는 힌트를 단말(100)로 송신할 수 있다(S440). 상기 힌트는 상기 아이디와 상기 패스워드를 등록하는 과정에서 단말(100)로부터 수신되어 서버(300)에 미리 저장되어 있을 수 있다.

[0067] 사용자 등록 단계에서 패스워드로 사용되거나 패스워드를 생성하는 과정에서 사용된 멀티미디어 파일은 클라우드 서버(500)에 저장되어 있다. 따라서, 단말(100)은 멀티미디어 파일 요청 메시지를 클라우드 서버(500)로 송신한다(S450).

[0068] 이때, 접근 권한이 없는 사용자의 접근을 차단하기 위해서 클라우드 서버(500)에 로그인하기 위한 인증 과정이 수행될 수 있다.

[0069] 클라우드 서버(500)와 단말(100) 간의 인증 과정이 완료되면, 클라우드 서버(500)는 적어도 하나의 제2 멀티미디어 파일을 단말(100)로 송신할 수 있다(S460). 상기 제2 멀티미디어 파일은 용량이 큰 원본 멀티미디어 파일의 송수신으로 인한 지연을 감소하기 위해 다운 사이징된(저용량의) 멀티미디어 파일을 의미할 수 있으며, 원본 멀티미디어 파일의 송수신 과정에서 원본 멀티미디어 파일의 유출로 인한 패스워드 노출을 방지하기 위하여 수정이나 솔트(salt)를 첨가한 멀티미디어 파일을 의미할 수 있다.

[0070] 클라우드 서버(500)로부터 수신된 상기 적어도 하나의 제2 멀티미디어 파일은 단말(100)에 구비된 디스플레이 장치를 통하여 디스플레이될 수 있고, 사용자는 소정의 입력 장치(예컨대, 터치 스크린)를 이용하여 상기 적어도 하나의 제2 멀티미디어 파일 중에서 서버(300)로부터 수신된 힌트에 대응하는, 즉 사용자 등록 단계에서 사용된 멀티미디어 파일에 대응하는 파일을 선택하고, 상기 사용자에 의해 입력된 선택 정보는 단말(100)에 의해 클라우드 서버(500)로 송신될 수 있다(S470).

[0071] 상기 선택 정보를 수신한 클라우드 서버(500)는 상기 선택 정보에 대응하는 멀티미디어 파일을 단말(100)로 송신할 수 있다(S480). 이후, 단말(100)은 상기 멀티미디어 파일을 암호화키를 이용하여 암호화하여 암호문을 생성하고, 생성된 암호문을 서버(300)로 송신한다(S490).

[0072] 서버(300)는 수신된 암호문을 이용하여 사용자 인증 여부를 결정한다(S500).

[0073] 구체적으로, 패스워드가 멀티미디어 파일 자체인 경우, 서버(300)는 복호화키(대칭키, 단말(100)의 공개키 또는 서버(300)의 개인키)를 이용하여 상기 암호문을 복호화하고, 복호화 결과로 생성된 멀티미디어 파일과 서버(300) 내에 저장되어 있는 멀티미디어 파일의 동일성 여부를 결정함으로써 사용자 인증 여부를 결정할 수 있다.

[0074] 패스워드가 상기 암호문 자체인 경우, 서버(300)는 복호화 과정을 수행할 필요가 없다. 즉, 수신된 암호문과 서버(300) 내에 저장되어 있는 암호문의 동일성 여부를 결정함으로써 사용자 인증 여부를 결정할 수 있다.

[0075] 인증이 완료된 경우, 서버(300)는 인증 완료 메시지를 단말(100)로 송신한다(S510). 인증 과정이 완료된 경우, 사용자는 서버(300)로부터 소정의 서비스를 제공받을 수 있다.

[0077] 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

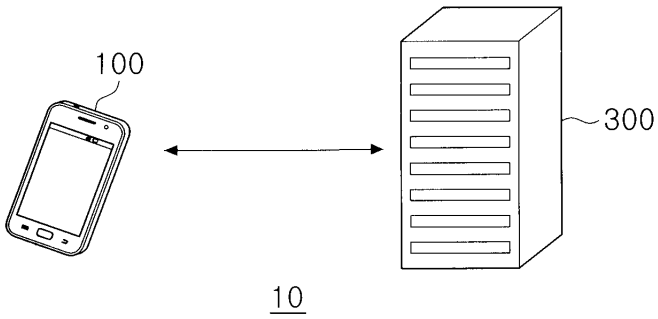
[0079] 100 : 단말

300 : 서버

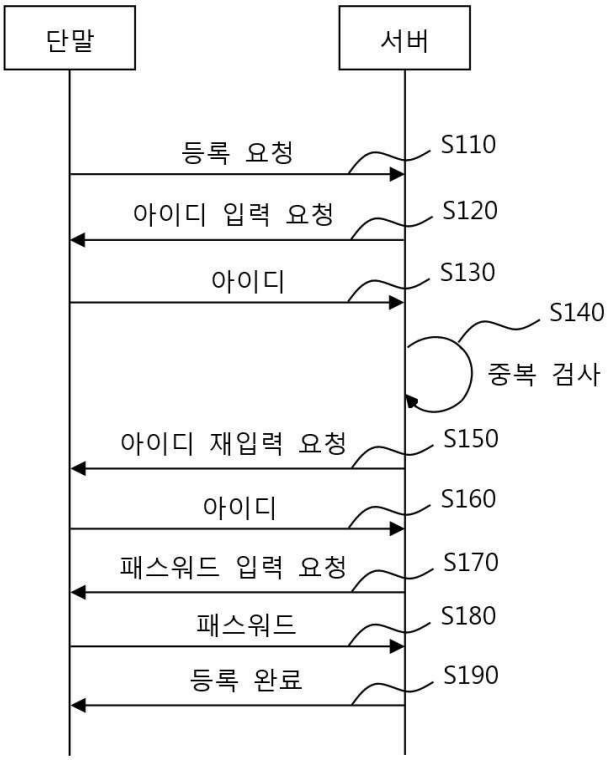
500 : 클라우드 서버

도면

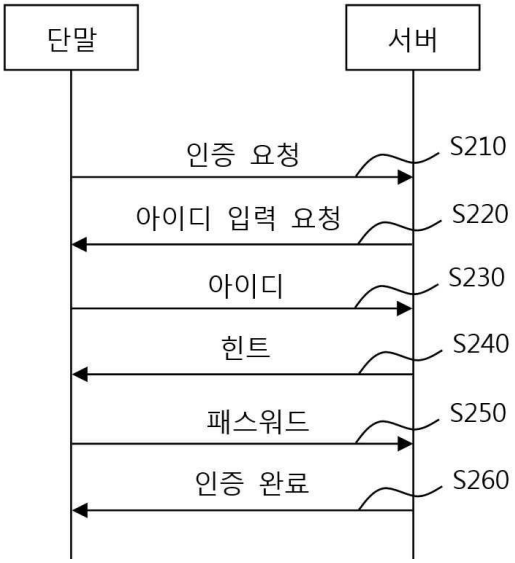
도면1


100
300
10

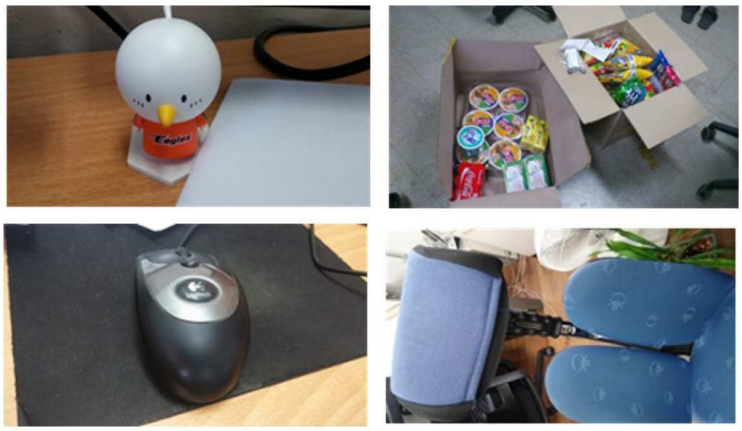
도면2


단말
서버
등록 요청
S110
아이디 입력 요청
S120
아이디
S130
S140
중복 검사
아이디 재입력 요청
S150
아이디
S160
패스워드 입력 요청
S170
패스워드
S180
등록 완료
S190

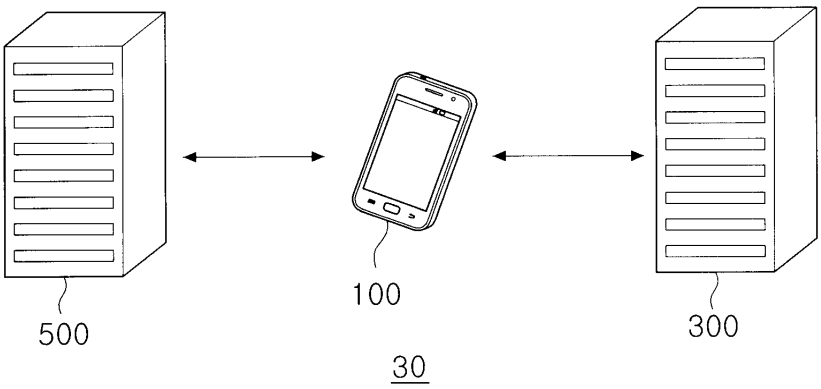
도면3


단말
서버
인증 요청
S210
아이디 입력 요청
S220
아이디
S230
힌트
S240
패스워드
S250
인증 완료
S260

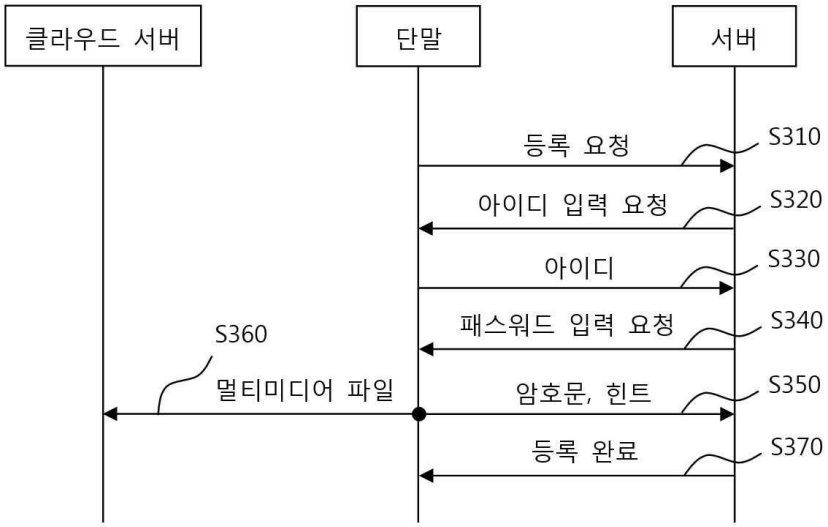
도면4



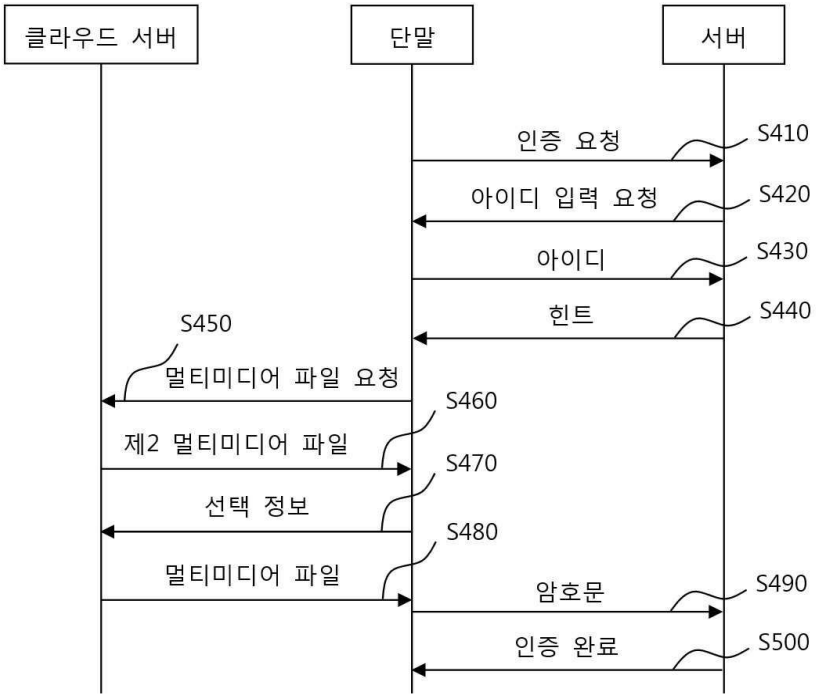
도면5


500
100
300
30

도면6


클라우드 서버
단말
서버
등록 요청
S310
아이디 입력 요청
S320
아이디
S330
패스워드 입력 요청
S340
S360
멀티미디어 파일
암호문, 힌트
S350
등록 완료
S370

도면7


클라우드 서버
단말
서버
인증 요청
S410
아이디 입력 요청
S420
아이디
S430
힌트
S440
S450
멀티미디어 파일 요청
S460
제2 멀티미디어 파일
S470
선택 정보
S480
멀티미디어 파일
암호문
S490
인증 완료
S500