(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0010016
(43) 공개일자 2019년01월30일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/06* (2006.01)
(52) CPC특허분류
H04L 9/3213 (2013.01)
H04L 9/0618 (2013.01)
(21) 출원번호 10-2017-0092111
(22) 출원일자 2017년07월20일
심사청구일자 2017년07월20일

(71) 출원인
중부대학교 산학협력단
충청남도 금산군 추부면 대학로 201
(72) 발명자
이병천
경기도 고양시 덕양구 동헌로 199-3, 대자그린시티빌 202호(대자동)
(74) 대리인
특허법인 남앤남

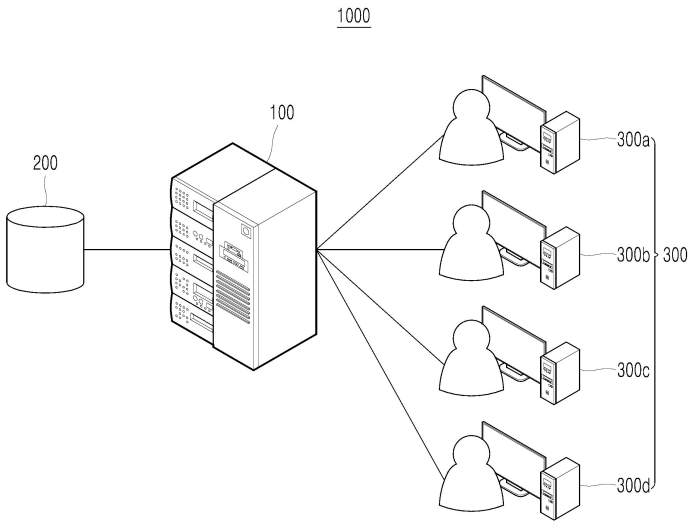
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 **사용자 인증 서버 및 시스템**

(57) 요 약

사용자 인증 시스템이 개시된다. 본 시스템은 적어도 하나의 사용자 단말, 및 적어도 하나의 단말에 로그인 서비스를 제공하는 인증 서버를 포함하며, 인증 서버는 특정 사용자 단말의 최초 로그인 요청에 대한 검증이 성공한 경우, 서명된 공개토큰(t_p) 및 비밀토큰(t_s)을 생성하여 상기 특정 사용자 단말로 전송하며, 상기 특정 사용자 단말은 최초 로그인 이후에 인증 서버에 접속하는 경우, 현재 시간 정보와 상기 비밀토큰(t_s)에 기초하여 계산되는 사용자 인증 정보를 공개토큰(t_p)과 함께 인증 서버로 전송하며, 상기 인증 서버는 수신된 상기 사용자 인증 정보를 검증할 수 있다. 이에 따라 장치 효율성 및 사용자 편의성이 향상될 수 있다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0869 (2013.01)
H04L 9/3242 (2013.01)

명 세 서

청구범위

청구항 1

사용자 인증 시스템에 있어서,

적어도 하나의 사용자 단말; 및

상기 적어도 하나의 사용자 단말에 로그인 서비스를 제공하는 인증 서버;를 포함하며,

상기 인증 서버는,

특정 사용자 단말의 최초 로그인 요청에 대한 검증이 성공한 경우, 서명된 공개토큰(t_p) 및 비밀토큰(t_s)을 생성하여 상기 특정 사용자 단말로 전송하며,

상기 특정 사용자 단말은,

최초 로그인 이후에 상기 인증 서버에 접속하는 경우, 현재 시간 정보와 상기 비밀토큰(t_s)에 기초하여 계산되는 사용자 인증 정보를 상기 공개토큰(t_p)과 함께 상기 인증 서버로 전송하며,

상기 인증 서버는,

수신된 상기 사용자 인증 정보를 검증하는, 사용자 인증 시스템.

청구항 2

제1항에 있어서,

상기 공개토큰(t_p)은 사용자 정보와 상기 인증 서버의 비밀키를 이용하여 계산되며, 상기 비밀토큰(t_s)은 상기 공개토큰(t_p)과 상기 인증 서버의 비밀키를 이용하여 계산되며,

상기 사용자 인증 정보는 상기 비밀토큰(t_s)과 현재시간을 이용하여 계산되는 것을 특징으로 하는 사용자 인증 시스템.

청구항 3

제2항에 있어서,

상기 공개토큰(t_p) 및 비밀토큰(t_s)은 아래 식에 의해 도출되는,

t_p = HMAC(ID, M, Ts, K),

t_s = HMAC(t_p, K),

여기서, HMAC는 서명 생성 함수이고, 상기 ID는 사용자의 ID, 상기 M은 특정 사용자 단말 정보, 상기 Ts는 토큰의 유효기간, 상기 K는 상기 인증 서버가 소유한 비밀키인, 사용자 인증 시스템.

청구항 4

제2항에 있어서,

상기 특정 사용자 단말은,

상기 사용자 인증 정보(auth)를 아래 식에 의해 산출하고,

auth = H(t_s, T), (여기서. H는 해쉬함수이고, T는 현재시간 정보임)

상기 사용자 인증 정보, 상기 공개토큰(t_p), 및 현재시간 정보(T)를 상기 인증 서버로 전송하며,

상기 인증 서버는,

상기 특정 사용자 단말이 전송한 상기 공개토큰(t_p)과 인증서버의 비밀키 K를 이용하여 비밀토큰을 식 t_s = HMAC(t_p, K)에 의해 계산하고, 이를 이용하여 상기 특정 사용자 단말이 전송한 사용자 인증정보 auth를 식 auth = H(t_s, T)에 의해 유효한지 확인하는, 사용자 인증 시스템.

청구항 5

제4항에 있어서,

상기 특정 사용자 단말은,

특정 메시지 Msg를 인증하기 위해 auth를 이용하여 메시지 인증 코드 mac 을 식 mac = HMAC(Msg, auth)에 의해 생성하고,

상기 메시지 인증 코드, 상기 특정 메시지 Msg, 공개토큰(t_p)을 상기 사용자 인증 서버로 전송하며,

상기 인증 서버는,

먼저 auth 을 계산한 후, mac의 유효성을 검증하는, 사용자 인증 시스템.

청구항 6

제5항에 있어서,

상기 특정 사용자 단말은,

특정 메시지 Msg을 암호화하여 전송하기 위해 auth 을 공유된 비밀키로 사용하여 암호문 C를 식 C = E(Msg, auth)에 의해 생성하여 전송하고,

상기 인증 서버는,

먼저 auth 을 계산한 후 복호화된 메시지 Msg' 를 식 Msg' = D(C, auth)에 의해 복호화하여 메시지를 복구하는, 사용자 인증 시스템.

청구항 7

사용자 인증 서버의 인증 방법에 있어서,

사용자 인증 서버는 특정 사용자 단말의 최초 로그인 요청에 대한 검증이 성공한 경우, 공개토큰(t_p) 및 비밀토큰(t_s)을 생성하여 상기 특정 사용자 단말로 전송하는 단계; 및

상기 특정 사용자 단말이 최초 로그인 이후에 접속하는 경우, 상기 비밀토큰(t_s) 및 현재 시간 정보에 기초한 사용자 인증 정보를 공개토큰(t_p)과 함께 상기 특정 단말로부터 수신하는 단계; 및

수신된 상기 사용자 인증 정보를 검증하는 단계를 포함하는, 사용자 인증 서버의 인증 방법.

발명의 설명

기 술 분 야

[0001] 본 개시는 사용자 인증 서버 및 시스템에 관한 것이다.

배 경 기 술

[0002] 로그인(Log-in)이란 사용자가 서버 컴퓨터 시스템을 사용하기 위해 서버 컴퓨터 시스템에 자신의 신원을 확인시키고 권한을 얻는 작업을 말한다. 다중 사용자 환경의 시스템에서는 작업을 시작하기 전에 자신의 아이디 및 패스워드를 입력하여 시스템에 접속하는 것이 전통적인 방식이라 할 수 있다.

[0003] 상기 전통적인 로그인 방식은 여러가지 불편 및 문제점이 있다. 사용자 측면에서는 항상 기억하고 있어야 하는 패스워드를 매번 입력해야 하는 불편함이 있고 패스워드가 서버로 전송됨으로 인해 도청 공격자에게 패스워드가

노출될 수 있으며 이 경우 공격자가 사용자의 신분을 쉽게 도용할 수 있는 문제점이 있다. 이러한 도청을 방지하기 위해서는 TLS(transport layer security), HTTPS(hypertext transfer protocol over secure socket layer) 등의 보안통신 환경을 이용해야 한다. 한편 서버 측면에서는 사용자의 신분을 확인하기 위해서는 사용자가 로그인할 때마다 사용자 인증 데이터베이스에 포함된 사용자 정보를 검색하여 패스워드 정보가 맞는지 확인해야 하는 시스템 로드(load)가 발생된다. 또한 서버는 사용자 단말기와 서버 사이의 보안통신 채널을 운영하기 위해 시스템 자원을 소모해야 한다.

[0004] 이런 문제점을 극복하기 위해 사용자 수가 많은 거대 웹 서비스에서는 인증토큰을 이용하는 자동 로그인 서비스를 이용하고 있다. 자동 로그인 서비스는 사용자가 한번 로그인에 성공하면 서버가 단말 시스템(브라우저)에 로그인 되어 있다는 의미의 서명된 인증토큰을 발급하고, 단말 시스템은 인증토큰을 저장하며, 다음에 서버에 접속하는 경우 패스워드를 입력하지 않고 인증토큰을 자동으로 제시하도록 함으로써 간편하게 로그인 상태를 유지할 수 있도록 하는 서비스이다. 이 경우 서버는 사용자 인증 데이터베이스를 검색할 필요가 없이 사용자가 제시하는 인증토큰의 서명을 확인함으로써 사용자의 신분을 확인할 수 있어서 서버 운영의 효율성을 크게 높일 수 있다.

[0005] 그러나, 이 방법은 고정된 인증토큰이 매번 반복 전송됨으로 인해 도청 공격자에게 노출될 수 있으며, 만일 도청 공격자가 사용자의 인증토큰을 획득하게 되면 사용자의 신분을 매우 쉽게 도용할 수 있는 문제점이 있다. 그러므로 이러한 자동 로그인 서비스는 TLS, HTTPS 등의 보안통신 환경에서만 적용되고 있는 실정이다.

[0006] 이에 따라, 보안통신 환경에 의존하지 않아도 되는 보다 개선되고 효율적인 자동 로그인 시스템이 필요하며 본 발명은 이러한 문제점을 해결하기 위해 제시되는 것이다.

[0007] 한편, 상기와 같은 정보는 본 발명의 이해를 돕기 위한 백그라운드(background) 정보로서만 제시될 뿐이다. 상기 내용 중 어느 것이라도 본 발명에 관한 종래 기술로서 적용 가능할지 여부에 관해, 어떤 결정도 이루어지지 않았고, 또한 어떤 주장도 이루어지지 않는다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 공개특허공보 제10-2015-0129869호(공개일: 2015.11.23)

발명의 내용

해결하려는 과제

[0009] 본 발명은 상술한 문제점을 해결하기 위해 안출된 것으로, 본 발명의 일 실시 예는 난수화된 토큰 인증을 이용한 효율적인 자동 로그인 서비스를 제공하는데, 이것은 보안통신을 사용하지 않아도 도청공격에 안전한 자동 로그인 서비스를 제공할 수 있다.

[0010] 본 발명에서 이루고자 하는 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급하지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0011] 상기한 과제를 실현하기 위한 사용자 인증 시스템은 적어도 하나의 사용자 단말; 및 상기 적어도 하나의 사용자 단말에 로그인 서비스를 제공하는 인증 서버;를 포함하며, 상기 인증 서버는 특정 사용자 단말의 최초 로그인 요청에 대한 검증이 성공한 경우, 서명된 공개토큰(t_p) 및 비밀토큰(t_s)을 생성하여 상기 특정 사용자 단말로 전송하며, 상기 특정 사용자 단말은 최초 로그인 이후에 상기 인증 서버에 접속하는 경우, 현재 시간 정보와 상기 비밀토큰(t_s)에 기초하여 계산되는 사용자 인증 정보를 상기 공개토큰(t_p)과 함께 상기 인증 서버로 전송하며, 상기 인증 서버는 수신된 상기 사용자 인증 정보를 검증할 수 있다.

발명의 효과

[0012] 본 발명의 다양한 실시예에 따르면 아래와 같은 효과가 도출될 수 있다.

[0013] 첫째, 난수화된 토큰 인증을 이용한 효율적인 자동 로그인 서비스가 제공될 수 있다. 매번 전송되는 사용자 인증 정보는 시간에 따라 달라지는 값이 되므로 공격자가 도청하여도 재사용할 수 없게 된다.

[0014] 둘째, 자동 로그인 서비스에서 암호화된 채널없이 평문 채널을 통해 로그인 서비스가 진행됨으로써, 장치 효율이 향상될 수 있고, 운영 비용 절감의 효과가 발생된다.

[0015] 셋째, 사용자 단말은 아이디 및 비밀번호의 입력없이 시스템에 자동 로그인이 가능하게 됨으로써, 사용자 편의성이 향상될 수 있다.

[0016] 네째, 서버는 사용자 인증 데이터베이스에 접근없이 사용자 인증을 수행 가능한 사용자 인증 시스템이 제공됨으로써, 서버의 효율성이 향상될 수 있다.

[0017] 본 발명에서 얻을 수 있는 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0018] 도 1은 실시 예에 사용자 인증 시스템을 개략적으로 나타낸다.

도 2는 실시 예에 따른 사용자 인증 시스템의 동작을 나타낸다.

도 3 및 도 4는 실시 예에 따른 사용자 단말의 동작을 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0019] 첨부되는 도면들을 참조하는 하기의 상세한 설명은 청구항들 및 청구항들의 균등들로 정의되는 본 개시의 다양한 실시 예들을 포괄적으로 이해하는데 있어 도움을 줄 것이다. 하기의 상세한 설명은 그 이해를 위해 다양한 특정 구체 사항들을 포함하지만, 이는 단순히 예로서만 간주될 것이다. 따라서, 해당 기술 분야의 당업자는 여기에서 설명되는 다양한 실시 예들의 다양한 변경들 및 수정들이 본 개시의 범위 및 사상으로부터 벗어남이 없이 이루어질 수 있다는 것을 인식할 것이다. 또한, 공지의 기능들 및 구성들에 대한 설명은 명료성 및 간결성을 위해 생략될 수 있다.

[0020] 도 1은 실시 예에 따른 사용자 인증 시스템(1000)을 개략적으로 나타낸다. 상기 사용자 인증 시스템(1000)은 사용자 인증 서버(100), 사용자 인증 데이터베이스(200) 및 복수의 사용자 단말들(300a~300d)을 포함한다.

[0021] 일단, 사용자 인증 서버(100)는 사용자 단말들(300a~300d)에 로그인 권한을 부여할 수 있다. 아울러, 사용자 인증 서버(100)는 인증 서비스 이외에 다양한 서비스(가령, 정보 제공 서비스, 결재 서비스 등)를 사용자 단말들(300a~300d)에 제공할 수 있다.

[0022] 아울러, 사용자 인증 서버(100)는 사용자에 대응되는 사용자 인증 정보(가령, 아이디 및 암호화된 패스워드)를 사용자 인증 데이터베이스(200)에 저장할 수 있다.

[0023] 사용자 인증 서버(100)은 사용자 단말들(300a~300d)이 최초에 사용자 인증 서버(100)에 접속하여 사용자 등록을 수행하는 경우, 아이디 및 암호화된 패스워드와 함께 다양한 사용자 정보, 가령, 사용자 이름, 주소, 생년월일 등을 사용자 인증 데이터베이스(200)에 저장할 수 있다. 이후 사용자 단말들(300a~300d)이 사용자 인증 서버(100)에 접속하여 로그인을 수행하는 경우 아이디 및 패스워드 입력을 요구할 수 있다.

[0024] 사용자 인증 서버(100)는 자동 로그인 서비스를 사용자 단말들(300a~300d)에게 제공할 수 있다. 사용자 단말들(300a~300d)은 최초 사용자 인증 서버(100)에 로그인한 후, 그 다음 상기 사용자 인증 서버(100)에 접속하는 경우 또는 로그인된 상태에서 사용자 인증 서버(100)가 제공하는 다른 페이지를 요청하는 경우, 토큰을 이용하여 간편하게 로그인을 수행할 수 있다.

[0025] 본 발명의 일 실시 예에 따른 사용자 인증 서버(100)는 자동 로그인 서비스를 제공하면서 사용자 인증 데이터베이스(200)에 저장된 정보를 이용하지 않고 자동 로그인 서비스를 제공할 수 있다. 또한, 자동로그인이 수행되는 채널은 암호화된 채널(HTTPS 등)이 아닌 평문 채널일 수 있다.

[0026] 이하에서는 상기 사용자 인증 시스템(1000)의 자동 로그인 프로세스를 도 2를 통해 자세히 설명하기로 한다. 사

용자 단말(300)은 단수로 설명하나, 실시 예는 이에 국한되지 않는다. 상기 프로세스는 등록 단계(S21), 최초 로그인 단계(S23) 및 자동 로그인 단계(S25)를 포함한다.

[0027] 등록 단계(S21)는 사용자 단말(300)의 사용자 정보를 사용자 정보 데이터베이스(200)에 등록하는 단계이다.

[0028] 일단, 사용자 단말(300)은 사용자 인증 정보(아이디 및 패스워드)를 사용자 인증 서버(100)로 전송한다(S210). 사용자 단말(300)은 아이디 및 패스워드 이외에 다양한 사용자 정보를 사용자 인증 서버(100)로 전송할 수 있으나, 실시 예는 이에 국한되지 않는다.

[0029] 그러면, 사용자 인증 서버(100)는 전송된 패스워드를 암호화한다(S215).

[0030] 전송된 패스워드를 사용자 인증 데이터베이스(200)에 바로 저장할 경우, 추후 사용자 인증 서버(100) 및 사용자 인증 데이터베이스(200)가 해킹되는 경우, 개인정보가 유출될 위험이 있으므로 전송된 패스워드는 암호화되어 저장될 수 있다.

[0031] 구체적으로, 사용자 인증 서버(100)는 솔트(salt) 값을 난수로 생성하고 해쉬함수의 반복횟수 I를 설정하여 전송된 패스워드(password)의 암호화 해쉬값을 산출하여 암호화된 패스워드(hpassword)를 생성할 수 있다. 이때, 유닉스의 경우 crypt 함수, 웹서비스의 경우 bcrypt, pbkdf2 함수 등이 사용될 수 있으나, 실시 예는 이에 국한되지 않는다.

[0032] 그런 후, 사용자 인증 서버(100)는 사용자의 아이디 및 암호화된 패스워드를 사용자 정보 데이터베이스(200)에 저장할 수 있다. 사용자 인증 서버(100)는 암호화된 패스워드(hpassword)를 이용하여 전송된 패스워드(password)를 검증할 수 있다. 이때, 사용자는 사람인 경우가 일반적이나 반드시 이에 국한되는 것은 아니다.

[0033] 등록단계(S21)의 마지막으로, 사용자 정보 데이터베이스(200)는 아이디 및 암호화된 패스워드를 저장한다(S225).

[0034] 등록단계(S21) 이후의 최초 로그인 단계(S23)를 설명하기로 한다. 최초 로그인 단계(S23)는 상기 등록단계(S21) 이후에 수행되는 것으로 설명하나, 상기 등록단계(S21) 및 상기 최초 로그인 단계(S21)가 동시에 수행될 수 있다.

[0035] 우선, 사용자 단말(300)은 사용자 인증 서버(100)에 접속하여 아이디 및 패스워드를 사용자 인증 서버(100)로 전송한다(S230). 상기 아이디 및 패스워드는 사용자에 의해 입력될 수 있으나, 실시 예는 이에 국한되지 않는다.

[0036] 사용자 인증 서버(100)는 사용자 인증 데이터베이스(200)에 입력된 아이디에 대한 암호화된 패스워드(hpassword)를 요청하여 사용자 인증 데이터베이스(200)로부터 수신한다(S235).

[0037] 사용자 인증 서버(100)는 사용자 단말(300)이 전송한 패스워드(password) 값과 암호화된 패스워드(hpassword)의 해쉬값이 일치하는지 확인함을 통해 제1 사용자 정보를 검증한다(S240).

[0038] 제1 사용자 정보 검증이 성공하면, 사용자 인증 서버(100)는 공개토큰(t_p) 및 비밀토큰(t_s)을 생성한다(S247). 그리고, 사용자 인증 서버(100)는 생성된 공개토큰(t_p) 및 비밀토큰(t_s)을 사용자 단말(300)에 전송한다(S250).

[0039] 그러면, 사용자 단말(300)은 수신한 공개토큰(t_p) 및 비밀토큰(t_s)을 저장한다(S253).

[0040] 참고로, 공개토큰(t_p) 및 비밀토큰(t_s)은 JWT(JSON Web Token) 토큰의 형식을 이용하여 생성될 수 있다. 종래의 JWT 토큰은 토큰이 공격자에 의해 도청 및 획득되어 재전송되면, 사용자 신분이 위장되는 문제가 있었다. 이에 따라 종래 JWT 토큰을 이용한 인증과정이 모두 암호화된 채널(가령, HTTPS, SSL/TLS, SSH 등)을 통해야 했는데 실시 예는 상기의 제약이 극복될 수 있다. 아울러, JWT 토큰의 서명 t는 t = HMAC(H, P, secret)의 형식으로 표현될 수 있는데, 여기서 HMAC의 경우 전송하는 메시지의 인증성을 제공하기 위해 비밀키 secret을 이용하여 HMAC(keyed-hash message authentication code)을 계산하여 전송하는 기술이다.

[0041] 여기서, H는 헤더, P는 페이로드, secret은 사용자 인증 서버가 소유한 비밀값이다. 여기서, H와 P는 공개가능하고 secret 값은 어느 누구에게도 공개되지 않는다.

[0042] 상술한 바와 같이, 사용자 인증 서버(100)는 사용자 단말(300)의 최초 로그인이 확인되면 공개토큰(t_p) 및 비밀토큰(t_s)을 생성할 수 있다. 우선 공개토큰(t_p)은 아래와 같이 생성될 수 있다.

[0043] t_p = HMAC(ID, M, Ts, K)

[0044] 여기서, ID는 사용자의 ID, M은 사용자 단말(300) 정보, Ts는 토큰의 유효기간, K는 사용자 인증 서버(100)의 비밀키다. HMAC은 서명 생성함수이고, 공개토큰(t_p)은 사용자 인증서버(100)가 HMAC 함수로 서명한 정보이며 공개될 수 있는 정보에 해당된다.

[0045] 또한, 비밀토큰(t_s)은 공개토큰(t_p)을 사용자 인증 서버(100)의 비밀키(K)로 HMAC 서명한 정보로서 아래와 같이 생성될 수 있다.

[0046] t_s = HMAC(t_p, K)

[0047] 비밀토큰(t_s)은 외부에 노출되지 않고, 사용자 단말(300)의 브라우저 등의 로컬스토리지에 저장되어 사용되는 비밀정보에 해당된다.

[0048] 사용자 인증 서버(100)는 공개토큰(t_p) 및 비밀토큰(t_s)을 생성하고, 이것을 사용자 단말(300)에 전달하게 되며, 사용자 단말(300)은 이것을 브라우저의 로컬스토리지 등의 안전한 장소에 저장하게 된다. 최초 로그인 단계(S23)는 패스워드 전달, 토큰 전달이 이루어지는 단계로서 네트워크 통신을 도청하는 공격자로부터 안전성을 보장하기 위해 인증된 보안통신 채널을 통해 수행되어야 한다.

[0049] 사용자 인증 서버(100)는 공개토큰(t_p)으로부터 언제든지 비밀토큰(t_s)을 산출할 수 있는데 이 계산을 위해서는 비밀키 K를 이용하게 된다.

[0050] 한편, 이하에서는 사용자 단말(300)의 최초 로그인 단계(S23) 이후의 자동 로그인 단계(S25)를 설명하기로 한다. 상기 자동 로그인은 사용자 단말(300) 내의 프로그램(가령, 특정 브라우저)에 의해 트리거될 수 있으나, 실시 예는 이에 한정되지 않는다.

[0051] 사용자 단말(300)이 사용자 인증 서버(100)에 접속하거나, 로그인 상태에서 다른 페이지를 사용자 인증 서버(100)에 요청하는 경우, 자동로그인이 수행될 수 있다.

[0052] 우선, 사용자 단말(300)은 현재 시간 T를 추출하고(S255), 제2 사용자 인증 정보(auth)를 생성한다(S260).

[0053] 제2 사용자 인증 정보(auth)는 아래와 같이 산출될 수 있다.

[0054] auth = H(t_s, T)

[0055] 여기서, H는 해쉬함수 또는 HMAC 함수가 될 수 있으며 현재 시간 T와 비밀토큰(t_s)으로부터 계산된 해쉬값이 제2 사용자 인증 정보(auth)가 될 수 있다.

[0056] 상기 사용자 단말(300)은 제2 사용자 인증 정보를 포함하는 정보를 사용자 인증 서버(100)로 전송한다(S265). 실제 전송되는 정보는 공개토큰(t_p), T, auth 가 될 수 있다.

[0057] 사용자 인증 서버(100)는 상기 제2 사용자 인증 정보를 검증한다(S270).

[0058] 구체적으로, 사용자 인증 서버(100)는 전송된 공개토큰(t_p)으로부터 토큰의 유효성을 검증할 수 있고, 사용자 정보도 확인할 수 있다. 공개토큰(t_p)이 사용자 정보와 사용자 인증 서버(100)의 비밀키를 이용하여 계산되기 때문이다. 이에 따라 사용자 인증 서버(100)는 사용자 인증 데이터베이스(200)를 검색할 필요가 없게 된다.

[0059] 또한, 사용자 인증 서버(100)는 공개토큰(t_p)으로부터 비밀토큰(t_s)을 용이하게 계산 가능하고, 이를 이용하여 제2 사용자 인증 정보(auth)의 유효성을 검증할 수 있다. 아울러 전송된 시간정보 T가 현재시간인지 확인할 수 있다.

[0060] 사용자 인증 서버(100)는 자동 로그인이 수행된 후, 사용자 단말(300)의 다양한 요청에 대해 서비스를 제공할 수 있다(S275).

[0061] 위에서 살핀 바와 같이, 자동 로그인 프로세스에서 전달되는 제 2 사용자 인증 정보는 현재시간 T에 따라 계속 바뀌는 값이 되므로 네트워크 공격자가 도청을 하더라도 재사용할 수 없게 된다. 그러므로 자동 로그인 프로세스는 암호화 채널이 아닌 평문 채널을 통해 수행될 수 있으며, 평문 채널이 사용되는 경우에도 보안성이 유지되어 비용 면이나 안정성 면에서 효과적이다. 또한, 상기의 인증 프로세스는 메시지 인증, 메시지 암호화 등에도

사용될 수 있으나, 실시 예는 이에 국한되지 않는다.

[0062] 한편, 본 발명의 다른 실시 예에 따르면, 제2 사용자 인증 정보 auth는 TOTP(Time-based One time password) 표준의 계산 방식을 차용하여 적용할 수도 있다. 사용자 단말(300)이 로그인된 상태에서 다른 페이지를 요청할 경우, 요청 패킷에 다음과 같이 계산되는 <t_p, auth>를 덧붙여 사용자 인증 서버(100)로 전송한다.

[0063] auth = HMAC(t_p, t_s, T), T = floor((T_{curr} - T_0)/X)

[0064] X는 시간간격을 초단위로 나타낸 것이며, 기본값은 30초일 수 있으나, 실시 예는 이에 국한되지 않는다. T_0는 유닉스 시간의 시점을 Tcurr는 현재 시간을 나타내며 floor 함수를 이용하여 정수의 T를 계산할 수 있다.

[0065] 그러면 사용자 인증 서버(100)는 전송된 공개토큰(t_p)의 서명을 검증하고 페이로드를 디코딩하여 사용자의 정보를 확인할 수 있으며 공개토큰(t_p)을 이용하여 비밀토큰(t_s)를 계산할 수 있다. 이후 제2 사용자 인증정보(auth)를 같은 수식을 이용하여 계산하고 사용자로부터 전송된 값과 일치하는지 확인하여 사용자의 유효성을 검증할 수 있다. 이 방식은 시간정보 T를 직접 전송하지 않으므로 효율성이 있다고 볼 수 있으나 사용자 인증 서버와 사용자 단말의 시간이 동기화되어 있어야 하고 동일 시간 대역에 있어야 인증이 되므로 구현상에 복잡성이 있다.

[0066] 상술한 바와 같이 이와 같은 자동로그인 기술은 사용자의 편의성 향상, 서버의 효율성, 확장성 향상에 도움이 될 수 있다. 사용자 인증 서버(100)는 사용자가 전송하는 토큰을 기반으로 사용자 정보를 확인하므로 사용자 인증 데이터베이스(200)를 검색할 필요가 없으며 시간에 따라 매번 달라지는 인증정보의 유효성을 확인하여 로그인 판단을 하므로 보안통신채널을 사용하지 않아도 되기 때문에 많은 사용자를 가지는 서비스의 확장성에 유리하게 된다.

[0067] 한편, 이하에서는 본 발명의 확장된 실시 예를 설명하기로 한다.

[0068] 상술한 제2 사용자 인증 정보(auth)는 인증된 사용자 단말(300)의 브라우저와 사용자 인증 서버(100) 사이에 공유화된 난수화된 비밀정보로 생각될 수 있다. 비밀정보를 직접 전송함으로써 자동로그인에 이용할 수도 있지만, 이것을 전송하지 않고 메시지 인증 및 암호화에 이용할 수도 있다.

[0069] 가령, 사용자 단말(300)이 사용자 인증 서버(100)에게 보내는 메시지 Msg 을 인증하기 위해서 메시지 인증코드를 mac = HMAC(Msg, auth)와 같이 생성하여 < t_p, T, mac, Msg>을 사용자 인증 서버(100)에 전송할 수 있다. 사용자 인증 서버(100)는 먼저 auth 을 계산한 후, mac의 유효성을 검증할 수 있다.

[0070] 사용자 단말(300)이 사용자 인증 서버(100)에 보내는 메시지 Msg 자체를 암호화할 필요가 있는 경우, auth 을 공유된 비밀키로 사용하여 암호문 C = E(Msg, auth) 을 생성하여 전송할 수 있고, 사용자 인증 서버(100)는 auth 을 계산한 후 Msg' =D(C, auth)와 같이 복호화할 수 있다. SSL/TLS를 이용한 암호화, 인증과 비교할 때, SSL/TLS방식은 사용자 단말(300)과 사용자 인증 서버(100)가 인증세션을 맺고 유지해야 하는 부담이 있으며 특히 사용자 인증 서버(100) 측면에서 많은 사용자들과의 인증세션 정보를 관리해야할 필요가 있다. 이에 반해, auth 를 이용한 방식은 평상시 비암호화 통신을 하다가 필요한 경우에만 암호화, 인증을 이용할 수 있고, 사용자 인증 서버(100)는 세션 정보를 유지할 필요가 없는 비접속형(stateless) 프로토콜로서의 장점이 있다.한편, 도 3 및 도 4는 실시 예에 따른 사용자 단말(300)의 동작을 나타낸다.

[0071] 도 3에 따르면, 사용자 단말(300)은 특정 사이트에 자동 로그인된 상태를 디스플레이(310)에 표시할 수 있다. 자동 로그인된 상태(320)가 디스플레이(310)에 명확하게 표시될 수 있다.

[0072] 아울러, 상술한 바와 같이, 사용자 단말(300)은 상술한 공개토큰(t_p), 현재시간정보(T), 제 2 인증정보(auth)를 사용자 인증 서버(100)에 전송할 수 있다.

[0073] 도 4에 따르면, 사용자 단말(300)은 즐겨찾기 리스트(420) 및 자동 로그인 설정 여부(430)를 디스플레이(310)에 표시할 수 있다.

[0074] 즐겨찾기 리스트(420)에는 쿠글, 네이모, 코코아, 17번가 등이 표시되고, 각각의 사이트에 대해 자동 로그인 상태인지 표시될 수 있다. 쿠글, 네이모, 코코아가 자동 로그인되도록 설정된 것이 표시될 수 있다.

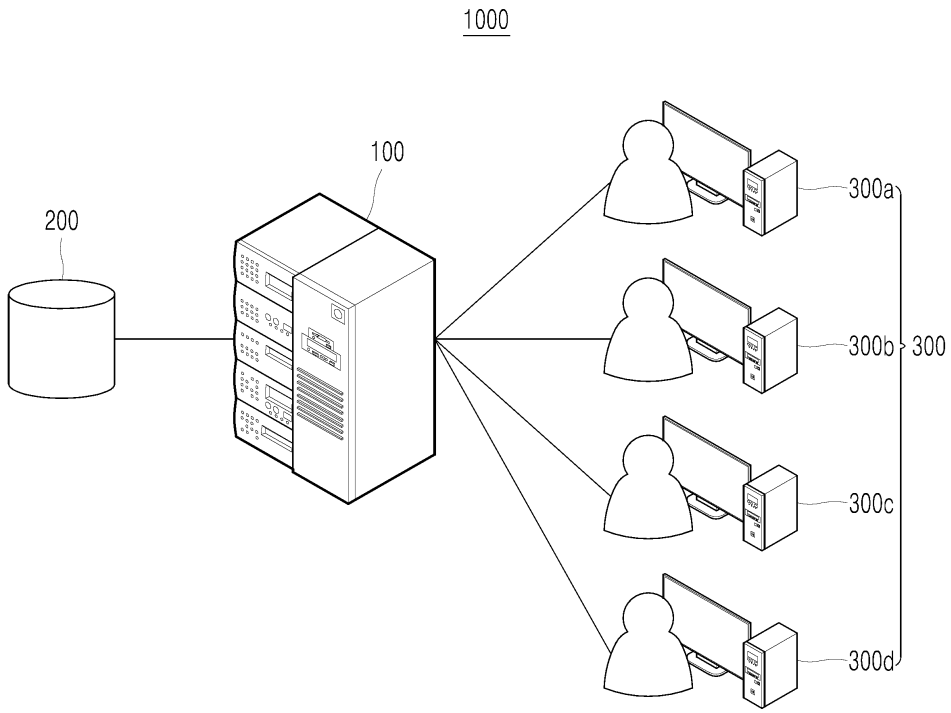
[0075] 한편 사용자 단말(300)에는 휴대폰, 스마트폰(smart phone), 노트북 컴퓨터(laptop computer), 디지털방송용 단말기, PDA(personal digital assistants), PMP(portable multimedia player), 네비게이션, 슬레이트

PC(slate PC), 태블릿 PC(tablet PC), 울트라북(ultrabook), 웨어러블 디바이스(wearable device, 예를 들어, 워치형 단말기 (smartwatch), 글래스형 단말기 (smart glass), HMD(head mounted display)) 등이 포함될 수 있다. 그러나, 본 명세서에 기재된 실시 예에 따른 구성은 사용자 단말(300)에만 적용 가능한 경우를 제외하면, 디지털 TV, 데스크탑 컴퓨터, 디지털 사이니지 등과 같은 고정 단말기에도 적용될 수도 있음을 본 기술분야의 당업자라면 쉽게 알 수 있을 것이다.

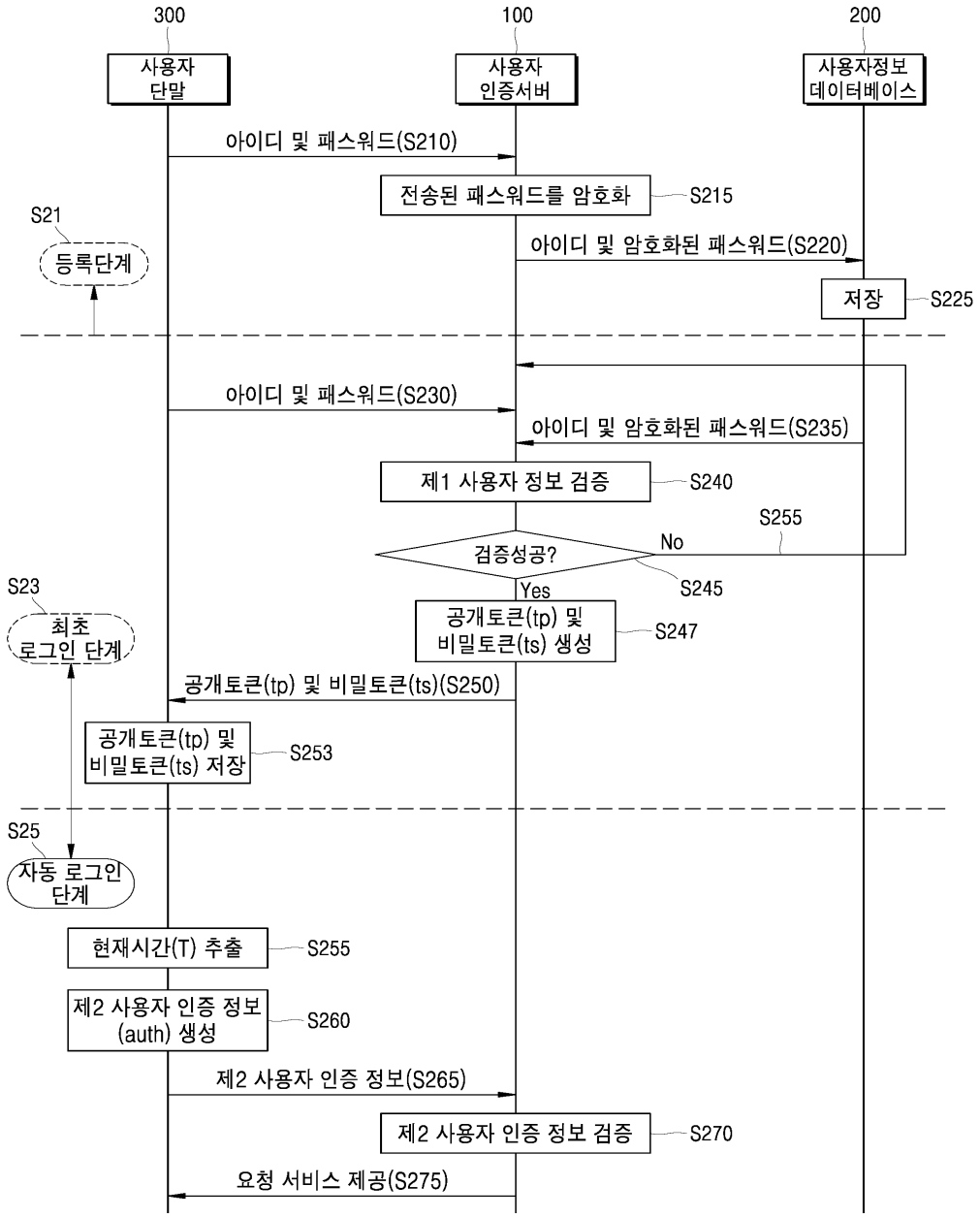
[0076] 한편, 본 발명의 기술 분야에서 통상의 지식을 가진 자는 여기에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 프로세서들, 수단들, 회로들 및 알고리즘 단계들이 전자 하드웨어, (편의를 위해, 여기에서 "소프트웨어"로 지칭되는) 다양한 형태들의 프로그램 또는 설계 코드 또는 이들 모두의 결합에 의해 구현될 수 있다는 것을 이해할 것이다. 하드웨어 및 소프트웨어의 이러한 상호 호환성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 이들의 기능과 관련하여 위에서 일반적으로 설명되었다. 이러한 기능이 하드웨어 또는 소프트웨어로서 구현되는지 여부는 특정한 애플리케이션 및 전체 시스템에 대하여 부과되는 설계 제약들에 따라 좌우된다. 본 발명의 기술 분야에서 통상의 지식을 가진 자는 각각의 특정한 애플리케이션에 대하여 다양한 방식들로 설명된 기능을 구현할 수 있으나, 이러한 구현 결정들은 본 발명의 범위를 벗어나는 것으로 해석되어서는 안 될 것이다.

도면

도면1



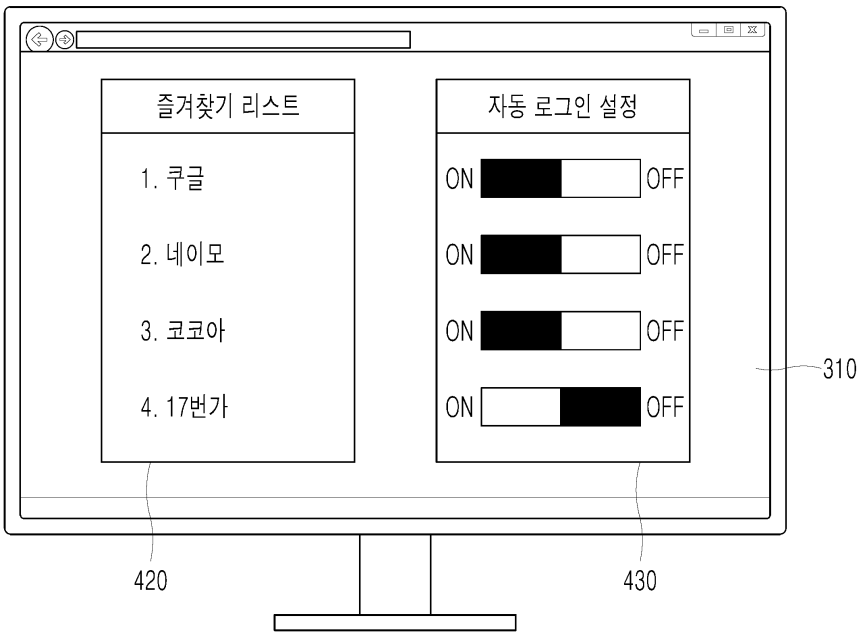
도면2


300
100
200
사용자 단말
사용자 인증서버
사용자정보 데이터베이스
아이디 및 패스워드(S210)
전송된 패스워드를 암호화
S215
S21
등록단계
아이디 및 암호화된 패스워드(S220)
저장
S225
아이디 및 패스워드(S230)
아이디 및 암호화된 패스워드(S235)
제1 사용자 정보 검증
S240
S255
검증성공?
No
Yes
S245
S23
최초 로그인 단계
공개토큰(tp) 및 비밀토큰(ts) 생성
S247
공개토큰(tp) 및 비밀토큰(ts)(S250)
공개토큰(tp) 및 비밀토큰(ts) 저장
S253
S25
자동 로그인 단계
현재시간(T) 추출
S255
제2 사용자 인증 정보 (auth) 생성
S260
제2 사용자 인증 정보(S265)
제2 사용자 인증 정보 검증
S270
요청 서비스 제공(S275)

도면3


Kmail
이미지
로그인됨
320
Koogle
한국
310
Koogle 검색 또는 URL 입력

도면4


즐겨찾기 리스트
1. 쿠글
2. 네이모
3. 코코아
4. 17번가
자동 로그인 설정
ON
OFF
ON
OFF
ON
OFF
ON
OFF
310
420
430