(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0085295
(43) 공개일자 2014년07월07일

(51) 국제특허분류(Int. Cl.)
*G06F 21/30* (2013.01)
(21) 출원번호 10-2013-0137982
(22) 출원일자 2013년11월14일
심사청구일자 2013년11월14일
(30) 우선권주장
1020120155630 2012년12월27일 대한민국(KR)

(71) 출원인
**주식회사 로웸**
서울특별시 구로구 디지털로29길 38 ,201호(구로동,에이스테크노3차)
(72) 발명자
**양기호**
서울특별시 마포구 월드컵북로27길 10 (성산동)
**황재엽**
경기도 고양시 일산동구 고봉로 424, 106동 703호 (중산동, 중산마을)
(74) 대리인
**특허법인필앤온지**

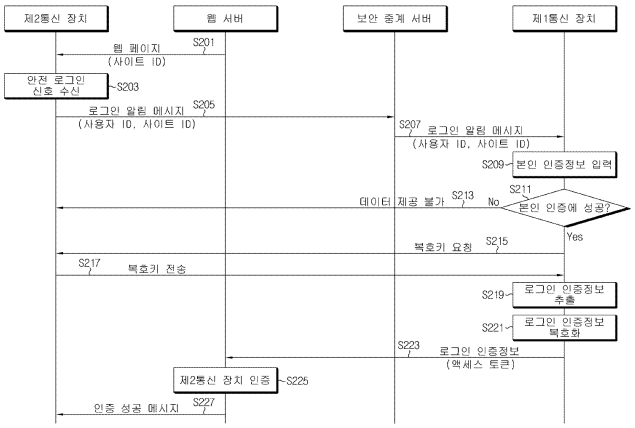
전체 청구항 수 : 총 29 항

(54) 발명의 명칭 **안전 로그인 시스템과 방법 및 이를 위한 장치**

## (57) 요 약

본 발명은 복수의 장치가 연동하여 사용자의 로그인을 진행하는 안전 로그인 시스템과 방법 및 이를 위한 장치에 관한 것이다. 본 발명에 따른 웹 사이트로 접속하는 통신 장치의 안전 로그인을 진행하는 방법은, 인증 데이터 제공 장치가, 상기 웹 사이트의 로그인에 필요한 인증 관련 데이터를 상기 통신 장치로부터 요청받는 단계; 상기 인증 데이터 제공 장치가, 상기 웹 사이트의 로그인에 필요한 인증 관련 데이터를 추출하는 단계; 상기 인증 데이터 제공 장치가, 상기 추출한 인증 관련 데이터를 상기 통신 장치로 전송하는 단계; 및 상기 통신 장치가, 상기 인증 관련 데이터를 이용하여 상기 웹 사이트로 로그인 인증을 시도하는 단계를 포함한다.

## 대 표 도



## *특허청구의 범위*

**청구항 1**

웹 사이트로 접속하는 통신 장치의 안전 로그인을 진행하는 방법으로서,

인증 데이터 제공 장치가, 상기 웹 사이트의 로그인에 필요한 인증 관련 데이터를 상기 통신 장치로부터 요청받는 단계;

상기 인증 데이터 제공 장치가, 상기 웹 사이트의 로그인에 필요한 인증 관련 데이터를 추출하는 단계;

상기 인증 데이터 제공 장치가, 상기 추출한 인증 관련 데이터를 상기 통신 장치로 전송하는 단계; 및

상기 통신 장치가, 상기 인증 관련 데이터를 이용하여 상기 웹 사이트로 로그인 인증을 시도하는 단계;를 포함하는 안전 로그인 방법.

**청구항 2**

제 1 항에 있어서,

상기 인증 관련 데이터를 추출하는 단계는, 상기 인증 관련 데이터로서 암호화된 로그인 인증정보를 추출하고,

상기 인증 관련 데이터를 전송하는 단계는, 상기 추출한 암호화된 로그인 인증정보를 상기 통신 장치로 전송하고,

상기 로그인 인증을 시도하는 단계는,

상기 통신 장치가, 상기 인증 데이터 제공 장치로부터 수신한 암호화된 로그인 인증정보를 보관중인 복호키를 이용하여 복호화하고, 이렇게 복호화된 로그인 인증정보를 이용하여 상기 웹 사이트로 로그인 인증을 시도하는 것을 특징으로 하는 안전 로그인 방법.

**청구항 3**

제 1 항에 있어서,

상기 인증 관련 데이터를 추출하는 단계는, 상기 인증 관련 데이터로서 복호키를 추출하고,

상기 인증 관련 데이터를 전송하는 단계는, 상기 추출한 복호키를 상기 통신 장치로 전송하고,

상기 로그인 인증을 시도하는 단계는,

상기 통신 장치가, 상기 인증 데이터 제공 장치로부터 수신한 복호키를 이용하여 저장중인 암호화된 로그인 인증정보를 복호화하고, 이렇게 복호화된 로그인 인증정보를 이용하여 상기 웹 사이트로 로그인 인증을 시도하는 것을 특징으로 하는 안전 로그인 방법.

**청구항 4**

제 1 항에 있어서,

상기 인증 관련 데이터를 추출하는 단계는, 상기 인증 관련 데이터로서 인증정보 보관주소를 추출하고,

상기 인증 관련 데이터를 전송하는 단계는, 상기 추출한 인증정보 보관주소를 상기 통신 장치로 전송하고,

상기 로그인 인증을 시도하는 단계는,

상기 통신 장치가, 상기 인증정보 보관주소에 보관된 인증정보를 인증정보 보관 서버로부터 수신하고, 이 수신한 인증정보를 이용하여 상기 웹 사이트로 로그인 인증을 시도하는 것을 특징으로 하는 안전 로그인 방법.

**청구항 5**

제 4 항에 있어서,

상기 통신 장치가, 상기 인증 데이터 제공 장치로부터 수신한 상기 인증정보 보관주소를 보관중인 복호키를 이

용하여 복호화하는 단계;를 더 포함하는 것을 특징으로 하는 안전 로그인 방법.

**청구항 6**

제 1 항 내지 제 5 항 중 어느 한 항에 있어서,

상기 인증 데이터 제공 장치가, 사용자로부터 본인인증 정보를 입력받아 사용자의 본인인증을 수행하는 단계;를 더 포함하고,

상기 인증 관련 데이터를 전송하는 단계는,

상기 사용자의 본인인증에 성공한 경우에 상기 인증 관련 데이터를 상기 통신 장치로 전송하는 것을 특징으로 하는 안전 로그인 방법.

**청구항 7**

제 6 항에 있어서,

상기 사용자의 본인인증을 수행하는 단계는,

상기 사용자의 생체정보를 입력받고, 이 입력받은 생체정보와 자체 저장중인 생채정보가 임계값 이상으로 일치하는 여부를 확인하는 것을 특징으로 하는 안전 로그인 방법.

**청구항 8**

인증 데이터 제공 장치에서 웹 사이트로 접속하는 통신 장치의 안전 로그인을 진행하는 방법으로서,

상기 웹 사이트의 로그인에 필요한 인증 관련 데이터를 상기 통신 장치로부터 요청받는 단계;

상기 웹 사이트의 로그인에 필요한 상기 통신 장치의 로그인 인증정보를 추출하는 단계; 및

상기 웹 사이트에서 상기 통신 장치의 로그인 인증이 수행되도록 상기 추출한 로그인 인증정보를 상기 웹 사이트로 전송하는 단계;를 포함하는 안전 로그인 방법.

**청구항 9**

제 8 항에 있어서,

상기 웹 사이트를 통해 부여받은 상기 통신 장치의 액세스 토큰을 확인하는 단계;를 더 포함하고,

상기 웹 사이트로 전송하는 단계는,

상기 확인한 액세스 토큰을 상기 로그인 인증정보와 함께 상기 웹 사이트로 전송하는 것을 특징으로 하는 안전 로그인 방법.

**청구항 10**

제 8 항에 있어서,

상기 로그인 인증정보를 추출하는 단계는,

상기 통신 장치로 복호키를 요청하여 수신하는 단계; 및

암호화된 로그인 인증정보를 추출하고, 상기 복호키를 이용하여 상기 추출한 로그인 인증정보를 복호화하는 단계;를 포함하고,

상기 웹 사이트로 전송하는 단계는,

상기 복호화한 로그인 인증정보를 상기 웹 사이트로 전송하는 것을 특징으로 하는 안전 로그인 방법.

**청구항 11**

제 8 항 내지 제 10 항 중 어느 한 항에 있어서,

사용자로부터 본인인증 정보를 입력받아 사용자의 본인인증을 수행하는 단계;를 더 포함하고,

상기 웹 사이트로 전송하는 단계는,

상기 사용자의 본인인증에 성공한 경우에 상기 로그인 인증정보를 상기 웹 사이트로 전송하는 것을 특징으로 하는 안전 로그인 방법.

**청구항 12**

웹 사이트의 로그인에 필요한 인증 관련 데이터를 상기 제2통신 장치로부터 요청받으면, 상기 제2통신 장치의 인증 관련 데이터를 추출하여 상기 제2통신 장치로 전송하는 제1통신 장치;

상기 제1통신 통신 장치로부터 수신한 인증 관련 데이터를 토대로, 상기 웹 사이트의 로그인 인증정보를 획득하는 제2통신 장치; 및

상기 제2통신 장치에서 획득한 로그인 인증정보를 수신하고, 상기 수신한 로그인 정보에 근거하여 상기 제2통신 장치의 로그인 인증을 수행하는 웹 서버;를 포함하는 안전 로그인 시스템.

**청구항 13**

제 12 항에 있어서,

상기 제1통신 장치는, 상기 인증 관련 데이터로서 암호화된 로그인 인증정보를 추출하여 상기 제2통신 장치로 제공하고,

상기 제2통신 장치는, 상기 제1통신 장치로부터 수신한 암호화된 로그인 인증정보를 보관중인 복호키로 복호화하여 상기 로그인 인증정보를 획득하는 것을 특징으로 하는 안전 로그인 시스템.

**청구항 14**

제 12 항에 있어서,

제1통신 장치는, 상기 인증 관련 데이터로서 복호키를 추출하고 상기 추출한 복호키를 상기 제2통신 장치로 제공하고,

상기 제2통신 장치는, 제1통신 장치로부터 수신한 복호키를 이용하여 자체 저장중인 암호화된 로그인 인증정보를 복호화하여 상기 로그인 인증정보를 획득하는 것을 특징으로 하는 안전 로그인 시스템.

**청구항 15**

제 12 항에 있어서,

상기 제1통신 장치는, 상기 인증 관련 데이터로서 인증정보가 보관된 인증정보 보관주소를 추출하여 상기 제2통신 장치로 전송하고,

상기 제2통신 장치는, 상기 인증정보 보관주소에 보관된 로그인 인증정보를 인증정보 보관 서버로부터 수신하여 상기 로그인 인증정보를 획득하는 것을 특징으로 하는 안전 로그인 시스템.

**청구항 16**

제 15 항에 있어서,

상기 제2통신 장치는,

상기 제1통신 장치로부터 수신한 상기 인증정보 보관주소를 보관중인 복호키를 이용하여 복호화한 후에, 이 복호화한 인증정보 보관주소에 보관된 인증정보를 상기 인증정보 보관 서버로부터 수신하는 것을 특징으로 하는 안전 로그인 시스템.

**청구항 17**

제 12 항 내지 제 16 항 중 어느 한 항에 있어서,

제1통신 장치는,

사용자로부터 본인인증 정보를 입력받아 사용자의 본인인증을 수행한 후, 상기 사용자의 본인인증에 성공한 경

우에 상기 인증 관련 데이터를 상기 제2통신 장치로 전송하는 것을 특징으로 하는 안전 로그인 시스템.

**청구항 18**

제 17 항에 있어서,

상기 제1통신 장치는,

상기 사용자의 생체정보를 입력받고, 이 입력받은 생체정보와 자체 저장중인 생채정보가 임계값 이상으로 일치하는 여부를 확인하여 상기 사용자의 본인인증을 수행하는 것을 특징으로 하는 안전 로그인 시스템.

**청구항 19**

웹 사이트로 접속하는 제2통신 장치;

상기 웹 사이트의 로그인에 필요한 인증 관련 데이터를 상기 제2통신 장치로부터 요청받아, 상기 웹 사이트에 대한 상기 제2통신 장치의 로그인 인증정보를 추출하는 제1통신 장치; 및

상기 제1통신 장치로부터 상기 제2통신 장치의 로그인 인증정보를 수신하여, 이 로그인 인증정보를 토대로 상기 제2통신 장치의 로그인 인증을 수행하는 웹 서버;를 포함하는 안전 로그인 시스템.

**청구항 20**

제 19 항에 있어서,

상기 제1통신 장치는,

상기 통신 장치의 액세스 토큰을 확인하고, 상기 액세스 토큰을 상기 로그인 인증정보와 함께 상기 웹 서버로 제공하고,

상기 웹 서버는,

상기 액세스 토큰을 토대로 상기 제2통신 장치를 식별하여 로그인 인증을 수행하는 것을 특징으로 하는 안전 로그인 시스템.

**청구항 21**

제 19 항에 있어서,

제1통신 장치는,

상기 제2통신 장치로 복호키를 요청하여 수신한 후, 암호화된 로그인 인증정보를 추출하고, 상기 복호키를 이용하여 상기 추출한 로그인 인증정보를 복호화하여 상기 웹 서버로 전송하는 것을 특징으로 하는 안전 로그인 시스템.

**청구항 22**

제 19 항 내지 제 21 항 중 어느 한 항에 있어서,

사용자로부터 본인인증 정보를 입력받아 사용자의 본인인증을 수행하여, 상기 사용자의 본인인증에 성공한 경우에 상기 로그인 인증정보를 상기 웹 서버로 전송하는 것을 특징으로 하는 안전 로그인 시스템.

**청구항 23**

하나 이상의 프로세서;

메모리; 및

상기 메모리에 저장되어 있으며 상기 하나 이상의 프로세서에 의하여 실행되도록 구성되는 하나 이상의 프로그램을 포함하는 인증 데이터 제공 장치에 있어서,

상기 프로그램은,

인증 관련 데이터를 저장하는 데이터 저장 모듈;

상기 인증 데이터 제공 장치와 연동하며 웹 사이트로 접속하는 통신 장치로부터 상기 웹 사이트의 로그인에 필요한 인증 관련 데이터를 요청받으면, 상기 데이터 저장 모듈에서 상기 통신 장치의 인증 관련 데이터를 추출하는 데이터 추출 모듈; 및

상기 데이터 추출 모듈에서 추출한 인증 관련 데이터를 상기 웹 사이트 또는 상기 통신 장치로 전송하는 인증 데이터 제공 모듈;을 포함하는 인증 데이터 제공 장치.

**청구항 24**

제 23 항에 있어서,

상기 데이터 저장 모듈은, 암호화된 로그인 인증정보를 저장하고,

상기 인증 데이터 추출 모듈은, 상기 통신 장치로 복호키를 요청하고 수신한 후, 상기 데이터 저장 모듈에 저장된 암호화된 로그인 인증정보를 추출하고, 상기 복호키를 이용하여 상기 추출한 암호화된 로그인 인증정보를 복호화하고,

상기 인증 데이터 제공 모듈은, 상기 복호화한 로그인 인증정보를 상기 웹 사이트 또는 상기 통신 장치로 전송하는 것을 특징으로 하는 인증 데이터 제공 장치.

**청구항 25**

제 24 항에 있어서,

상기 인증 데이터 제공 모듈은,

상기 통신 장치의 액세스 토큰을 확인하고, 이 액세스 토큰을 상기 로그인 인증정보와 함께 상기 웹 사이트로 전송하는 것을 특징으로 하는 인증 데이터 제공 장치.

**청구항 26**

제 23 항에 있어서,

상기 데이터 저장 모듈은, 암호화된 로그인 인증정보를 저장하고,

상기 인증 데이터 추출 모듈은, 상기 데이터 저장 모듈에 저장된 암호화된 로그인 인증정보를 추출하고,

상기 인증 데이터 제공 모듈은, 상기 추출한 암호화된 로그인 인증정보를 상기 통신 장치로 전송하는 것을 특징으로 하는 인증 데이터 제공 장치.

**청구항 27**

제 23 항에 있어서,

상기 데이터 저장 모듈은, 상기 통신 장치에서 보관하는 암호화된 로그인 인증정보를 복호화할 수 있는 복호키를 저장하고,

상기 인증 데이터 추출 모듈은, 상기 데이터 저장 모듈에서 복호키를 추출하고,

상기 인증 데이터 제공 모듈은, 상기 추출한 복호키를 상기 통신 장치로 전송하는 것을 특징으로 하는 인증 데이터 제공 장치.

**청구항 28**

제 23 항에 있어서,

상기 데이터 저장 모듈은, 상기 웹 사이트의 로그인 인증정보가 보관되는 인증정보 보관주소를 저장하고,

상기 인증 데이터 추출 모듈은, 상기 데이터 저장 모듈에서 상기 인증정보 보관주소를 추출하고,

상기 인증 데이터 제공 모듈은, 상기 추출한 인증정보 보관주소를 상기 통신 장치로 전송하는 것을 특징으로 하는 인증 데이터 제공 장치.

**청구항 29**

제 23 항 내지 제 28 항 중 어느 한 항에 있어서,

사용자로부터 본인인증 정보를 입력받아 사용자의 본인인증을 수행하는 본인 인증 모듈;을 더 포함하고,

상기 인증 데이터 제공 모듈은, 상기 사용자의 본인인증에 성공한 경우에 상기 인증 관련 데이터를 상기 통신 장치 또는 상기 웹 사이트로 전송하는 것을 특징으로 하는 인증 데이터 제공 장치.

## 명 세 서

### 기 술 분 야

[0001] 본 발명은 로그인 처리 기술에 관한 것으로서, 더욱 상세하게는 복수의 장치가 연동하여 사용자의 로그인을 진행하는 안전 로그인 시스템과 방법 및 이를 위한 장치에 관한 것이다.

### 배 경 기 술

[0002] 사용자 인증을 위한 보편적인 방법으로서 패스워드 인증 방식이 이용되고 있다. 패스워드 인증 방식은 사용자가 웹 서버에 접속하여 자신의 아이디와 패스워드를 설정한 후, 단말기에서 설정한 아이디와 패스워드를 입력함으로써 로그인을 수행하는 방식이다. 또한, 기존의 패스워드 인증 방식에서 더 나아가 사용자가 설정한 터치 패턴을 이용하여 사용자를 인증하는 기술이 개시되었다. 아래의 특허문헌은 패턴을 이용하여 사용자를 인증하는 휴대 단말기 및 그의 잠금 및 해제방법에 대해서 개시한다.

[0003] 그런데 이러한 방식은 엿보기 공격(shoulder surfing)에 의해 사용자의 인증정보, 즉 패스워드와 아이디가 타인에 의해 탈취될 수 있는 문제점이 있다. 게다가, 특정 사용자의 아이디와 패스워드를 타인이 탈취할 경우, 상기 특정 사용자가 아이디와 패스워드를 변경하거나 회원 탈퇴를 수행하지 않은 한, 상기 사용자의 개인 데이터가 상기 타인에게 계속적으로 노출되는 문제점도 있다.

### 선행기술문헌

#### 특허문헌

[0004] (특허문헌 0001) 한국공개특허 10-2009-0013432

## 발명의 내용

### 해결하려는 과제

[0005] 본 발명은 이러한 문제점을 해결하기 위하여 제안된 것으로, 엿보기 공격 등의 외부 해킹으로부터 사용자의 인증정보를 보호하고 인증정보의 보안성을 강화시킨 안전 로그인 시스템과 방법 및 이를 위한 장치를 제공하는데 그 목적이 있다.

[0006] 본 발명의 다른 목적 및 장점들은 하기의 설명에 의해서 이해될 수 있으며, 본 발명의 실시예에 의해 보다 분명하게 알게 될 것이다. 또한, 본 발명의 목적 및 장점들은 특허 청구 범위에 나타낸 수단 및 그 조합에 의해 실현될 수 있음을 쉽게 알 수 있을 것이다.

### 과제의 해결 수단

[0007] 상기 목적을 달성하기 위한 본 발명의 제 1 측면에 따른 웹 사이트로 접속하는 통신 장치의 안전 로그인을 진행하는 방법은, 인증 데이터 제공 장치가, 상기 웹 사이트의 로그인에 필요한 인증 관련 데이터를 상기 통신 장치로부터 요청받는 단계; 상기 인증 데이터 제공 장치가, 상기 웹 사이트의 로그인에 필요한 인증 관련 데이터를 추출하는 단계; 상기 인증 데이터 제공 장치가, 상기 추출한 인증 관련 데이터를 상기 통신 장치로 전송하는 단계; 및 상기 통신 장치가, 상기 인증 관련 데이터를 이용하여 상기 웹 사이트로 로그인 인증을 시도하는 단계를 포함하는 것을 특징으로 한다.

[0008] 상기 목적을 달성하기 위한 본 발명의 제 2 측면에 따른 인증 데이터 제공 장치에서 웹 사이트로 접속하는 통신 장치의 안전 로그인을 진행하는 방법은, 상기 웹 사이트의 로그인에 필요한 인증 관련 데이터를 상기 통신 장치로부터 요청받는 단계; 상기 웹 사이트의 로그인에 필요한 상기 통신 장치의 로그인 인증정보를 추출하는 단계;

및 상기 웹 사이트에서 상기 통신 장치의 로그인 인증이 수행되도록 상기 추출한 로그인 인증정보를 상기 웹 사이트로 전송하는 단계를 포함하는 것을 특징으로 한다.

[0009] 상기 목적을 달성하기 위한 본 발명의 제 3 측면에 따른 안전 로그인 시스템은, 웹 사이트의 로그인에 필요한 인증 관련 데이터를 상기 제2통신 장치로부터 요청받으면, 상기 제2통신 장치의 인증 관련 데이터를 추출하여 상기 제2통신 장치로 전송하는 제1통신 장치; 상기 제1통신 통신 장치로부터 수신한 인증 관련 데이터를 토대로, 상기 웹 사이트의 로그인 인증정보를 획득하는 제2통신 장치; 및 상기 제2통신 장치에서 획득한 로그인 인증정보를 수신하고, 상기 수신한 로그인 정보에 근거하여 상기 제2통신 장치의 로그인 인증을 수행하는 웹 서버를 포함하는 것을 특징으로 한다.

[0010] 상기 목적을 달성하기 위한 본 발명의 제 4 측면에 따른 안전 로그인 시스템은, 웹 사이트로 접속하는 제2통신 장치; 상기 웹 사이트의 로그인에 필요한 인증 관련 데이터를 상기 제2통신 장치로부터 요청받아, 상기 웹 사이트에 대한 상기 제2통신 장치의 로그인 인증정보를 추출하는 제1통신 장치; 및 상기 제1통신 장치로부터 상기 제2통신 장치의 로그인 인증정보를 수신하여, 이 로그인 인증정보를 토대로 상기 제2통신 장치의 로그인 인증을 수행하는 웹 서버를 포함하는 것을 특징으로 한다.

[0011] 상기 목적을 달성하기 위한 본 발명의 제 5 측면에 따른 하나 이상의 프로세서; 메모리; 및 상기 메모리에 저장되어 있으며 상기 하나 이상의 프로세서에 의하여 실행되도록 구성되는 하나 이상의 프로그램을 포함하는 인증 데이터 제공 장치에 있어서, 상기 프로그램은 인증 관련 데이터를 저장하는 데이터 저장 모듈; 상기 인증 데이터 제공 장치와 연동하며 웹 사이트로 접속하는 통신 장치로부터 상기 웹 사이트의 로그인에 필요한 인증 관련 데이터를 요청받으면, 상기 데이터 저장 모듈에서 상기 통신 장치의 인증 관련 데이터를 추출하는 데이터 추출 모듈; 및 상기 데이터 추출 모듈에서 추출한 인증 관련 데이터를 상기 웹 사이트 또는 상기 통신 장치로 전송하는 인증 데이터 제공 모듈을 포함하는 것을 특징으로 한다.

## *발명의 효과*

[0012] 본 발명은 제1통신 장치와 제2통신 장치가 연동하여 로그인 인증정보를 웹 서버로 제공함으로써, 엿보기 공격으로부터 사용자의 인증정보를 보호하고 사용자의 인증정보에 대한 보안을 강화시키는 장점이 있다.

[0013] 또한, 본 발명에 따른 제1통신 장치는, 사용자의 본인인증을 1차적으로 진행하고, 이 본인인증 결과에 따라 인증 관련 데이터를 제2통신 장치로 제공함으로써, 사용자의 인증정보에 대한 보안성을 더욱 강화시키는 장점이 있다.

[0014] 게다가, 본 발명은 로그인 인증에 필요한 데이터를 복수의 장치를 통해서 분산시켜 저장하기 때문에, 악의적인 의도를 가지는 타인이 특정 장치의 데이터를 탈취하더라도 완전하게 사용자의 로그인 인증정보를 획득할 수 없어, 사용자의 인증정보를 더욱 안전하게 보호하는 이점이 있다.

## *도면의 간단한 설명*

[0015] 본 명세서에 첨부되는 다음의 도면들은 본 발명의 바람직한 실시예를 예시하는 것이며, 발명을 실시하기 위한 구체적인 내용과 함께 본 발명의 기술사상을 더욱 이해시키는 역할을 하는 것이므로, 본 발명은 그러한 도면에 기재된 사항에만 한정되어 해석되어서는 아니 된다.

도 1은 본 발명의 일 실시예에 따른 안전 로그인 시스템의 구성을 나타내는 도면이다.

도 2는 본 발명의 일 실시예에 따른, 안전 로그인 시스템에서 로그인 인증을 수행하는 방법을 설명하는 흐름도이다.

도 3은 본 발명의 다른 실시예에 따른, 안전 로그인 시스템에서 로그인 인증을 수행하는 방법을 설명하는 흐름도이다.

도 4는 본 발명의 또 다른 실시예에 따른, 안전 로그인 시스템에서 로그인 인증을 수행하는 방법을 설명하는 흐름도이다.

도 5는 본 발명의 또 다른 실시예에 따른, 안전 로그인 시스템에서 로그인 인증을 수행하는 방법을 설명하는 흐름도이다.

도 6은 본 발명의 일 실시예에 따른, 인증 데이터 제공 장치의 구성을 나타내는 도면이다.

도 7은 본 발명의 일 실시예에 따른, 안전 로그인 프로그램의 구성을 나타내는 도면이다.

## *발명을 실시하기 위한 구체적인 내용*

[0016] 상술한 목적, 특징 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이며, 그에 따라 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에 그 상세한 설명을 생략하기로 한다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일 실시예를 상세히 설명하기로 한다.

[0017] 도 1은 본 발명의 일 실시예에 따른 안전 로그인 시스템의 구성을 나타내는 도면이다.

[0018] 도 1에 도시된 바와 같이, 본 발명의 실시예에 따른 안전 로그인 시스템은 제1통신 장치(10), 제2통신 장치(20), 보안 중계 서버(30), 웹 서버(40) 및 인증정보 보관 서버(50)를 포함한다.

[0019] 제1통신 장치(10), 제2통신 장치(20), 보안 중계 서버(30), 웹 서버(40), 인증정보 보관 서버(50) 각각은 네트워크(60)를 통해 서로 통신한다. 여기서 네트워크(60)는 이동통신망, 유선 인터넷망, 근거리 무선통신망 등을 포함하는 것으로서, 본 발명에 있어서 주지의 관용기술에 해당하므로 자세한 설명은 생략한다.

[0020] 웹 서버(40)는 포탈 서비스, 금융 서비스, 온라인 쇼핑 서비스, 전자 상거래 서비스 등과 같은 온라인 서비스를 사용자에게 제공하는 서버로서, 각 사용자의 아이디/패스워드 등과 같은 로그인 인증정보를 저장한다. 특히, 웹 서버(40)는 제2통신 장치(20)가 로그인을 시도한 경우, 상기 제2통신 장치(20)의 로그인 인증정보를 제1통신 장치(10) 또는 제2통신 장치(20)로부터 수신하여 이 로그인 인증정보를 토대로 제2통신 장치(20)의 로그인 인증을 수행한다.

[0021] 보안 중계 서버(30)는 하나 이상의 사용자 식별정보와 제1통신 장치(10)의 식별정보가 매핑된 테이블을 저장한다. 이때, 보안 중계 서버(30)는 제1통신 장치(10)의 식별정보로서 제1통신 장치(10)의 전화번호, IP 주소, MAC 주소, 제1통신 장치(10)에 설치된 안전 로그인 애플리케이션 식별정보 등 중에서 어느 하나를 저장할 수 있으며, 사용자 식별정보로서 안전 로그인 서비스 ID, 사용자의 주민등록번호, I-PIN(Internet Personal Identification Number), 이동통신 전화번호 등을 저장할 수 있다.

[0022] 특히, 보안 중계 서버(30)는 제2통신 장치(20)로부터 로그인 알림 메시지를 수신하면, 상기 제2통신 장치(20)의 사용자 식별정보와 매핑된 제1통신 장치(10)의 식별정보를 확인하고, 이 식별정보를 가지는 제1통신 장치(10)로 상기 로그인 알림 메시지를 전송한다. 바람직하게, 보안 중계 서버(30)는 상기 로그인 알림 메시지를 푸시 메시지 형태로 전송할 수 있다.

[0023] 인증정보 보관 서버(50)는 암호화 처리된 사이트별 로그인 인증정보를 사용자별로 구분하여 저장한다. 이때, 인증정보 보관 서버(50)는 로그인 인증정보의 보관주소를 설정하여, 상기 설정한 보관주소에 암호화한 로그인 인증정보를 각각 저장한다. 즉, 인증정보 보관 서버(50)는 각각의 로그인 인증정보에 대해서 유일한 보관주소를 설정하고, 이렇게 설정한 각 보관주소에 암호화된 로그인 인증정보를 각각 보관한다. 상기 인증정보 보관 서버(50)는 사용자로부터 암호화된 로그인 인증정보를 사용자로부터 수신하면, 상기 로그인 인증정보에 대한 보관주소를 설정하여 상기 설정한 보관주소를 가지는 저장영역에 상기 로그인 인증정보를 저장한다. 아울러, 인증정보 보관 서버(50)는 로그인 인증정보가 저장된 보관주소를 사용자에게 제공하여, 이 보관주소가 사용자의 제1통신 장치(10)에 저장되게 한다.

[0024] 제2통신 장치(20)는 웹 서버(40)로 로그인을 시도하는 장치로서, 안전 로그인 서비스를 위한 에이전트(21)를 탑재한다. 상기 에이전트(21)는 제2통신 장치(20)가 특정 사이트로의 로그인을 진행하는지 여부를 모니터링하여 진행한 경우, 로그인 시도하는 웹 사이트의 식별정보, 로그인 사용자의 식별정보 및 제2통신 장치(20)의 식별정보가 포함된 로그인 알림 메시지를 생성하여 보안 중계 서버(30)로 전송한다.

[0025] 바람직하게, 에이전트(21)는 일반 로그인 메뉴 이외에 본 발명에 따른 안전 로그인을 진행할 메뉴를 웹 브라우저 또는 웹 페이지에 출력할 수 있다. 예컨대, 에이전트(21)는 웹 페이지의 로그인 메뉴 아래에 추가적으로 안전 로그인 메뉴를 출력할 수도 있다.

[0026] 일 실시예에서, 제2통신 장치(20)는 복호키를 저장하고, 이 복호키를 지정된 제1통신 장치(10)로 제공할 수 있다. 바람직하게, 제2통신 장치(20)는 제1통신 장치(10)에서 저장중인 암호화된 로그인 인증정보를 복호화할 수

있는 고유의 복호키를 저장한다.

[0027] 다른 실시예에서, 제2통신 장치(20)는 제1통신 장치(10)로부터 암호화된 인증정보를 수신하고, 이 인증정보를 자체 저장중인 복호키를 이용하여 복호화한 후, 이 복호화된 인증정보를 이용하여 웹 서버(40)로의 로그인 인증을 수행할 수 있다.

[0028] 또 다른 실시예에서, 제2통신 장치(20)는 웹 사이트별로 암호화된 인증정보를 저장하고, 해당 인증정보를 해독할 수 있는 복호키를 제1통신 장치(10)로부터 수신하여, 이 복호키를 이용하여 인증정보를 복호화하여 웹 서버(40)로 제공할 수 있다.

[0029] 또한, 또 다른 실시예에서, 제2통신 장치(20)는 제1통신 장치(10)로부터 인증정보 보관 주소를 수신하고, 이 인증정보 보관 주소에 보관된 인증정보를 인증정보 보관 서버(50)로부터 수신할 수 있다.

[0030] 이러한 제2통신 장치(20)는 데스크톱 컴퓨터, 태블릿 컴퓨터, 노트북, 이동통신단말 등으로서, 네트워크(60)를 경유하여 웹 서버(40)로 접속할 수 있는 통신 장치라면 제한되지 않고 채택 가능하다. 또한, 상기 에이전트(21)는 안전 로그인 애플리케이션 또는 플러그인이 설치된 경우에 제2통신 장치(20)에 탑재될 수 있고, 또한 웹 페이지에 포함된 안전 로그인 스크립트가 실행되는 경우에 제2통신 장치(20)에 탑재될 수도 있다. 게다가, 상기 에이전트(21)는 또 다른 스크립트, 웹 저장소, 쿠키 등의 여타의 프로그램 또는 명령어를 통해서 구현될 수도 있다.

[0031] 제1통신 장치(10)는 인증 관련 데이터를 제2통신 장치(20) 또는 웹 서버(40)로 제공하는 기능을 수행한다. 상기 인증 관련 데이터는 복호키, 로그인 인증정보(예컨대, 아이디와 패스워드), 인증정보 보관 주소 중에서 하나 이상을 포함한다. 또한, 제1통신 장치(10)는 보안 중계 서버(30)로부터 로그인 알림 메시지를 수신하면, 사용자로부터 본인인증 정보(예컨대, 생체정보 등)를 입력받고, 입력받은 본인인증 정보가 저장중인 본인인증 정보와 일치하는 경우에, 인증 관련 데이터를 추출하여 제2통신 장치(20) 또는 웹 서버(40)로 전송한다.

[0032] 일 실시예에서, 제1통신 장치(10)는 각 웹 사이트의 로그인 인증정보가 기록된 보안 데이터를 통신 장치 식별정보별로 구분하여 저장하고, 제2통신 장치(20)로부터 복호키를 획득한 후 이 복호키를 이용하여 제2통신 장치(20)가 접속한 웹 사이트의 로그인 인증정보를 복호화하여 웹 서버(40) 또는 제2통신 장치(20)로 전송할 수 있다.

[0033] 다른 실시예에서, 제1통신 장치(10)는 각 웹 사이트의 로그인 인증정보가 암호화되어 기록된 보안 데이터를 통신 장치 식별정보별로 구분하여 저장하고, 제2통신 장치(20)가 접속 시도하는 웹 사이트의 로그인 인증정보를 제2통신 장치(20)로 전송할 수도 있다.

[0034] 또 다른 실시예에서, 제1통신 장치(10)는 암호화된 로그인 인증정보를 복호화되는데 사용하는 복호키를 통신 장치별로 구분하여 저장하고, 특정 복호키를 제2통신 장치(20)로 전송할 수 있다.

[0035] 또 다른 실시예에서, 제1통신 장치(10)는 웹 사이트별 인증정보 보관주소를 통신 장치 식별정보별로 구분하여 저장하고, 제2통신 장치(20)의 사용자가 접속 시도하는 웹 사이트를 확인한 후, 이 웹 사이트의 인증정보가 보관된 인증정보 보관주소를 제2통신 장치(20)로 제공할 수 있다.

[0036] 이러한 제1통신 장치(10)는 태블릿 컴퓨터, 노트북, 이동통신단말, 서버 등으로서, 바람직하게는 스마트폰이다. 또한, 제1통신 장치(10)와 제2통신 장치(20) 각각을 동일한 사용자가 보유하는 것이 더욱 바람직하다.

[0037] 도 2는 본 발명의 일 실시예에 따른, 안전 로그인 시스템에서 로그인 인증을 수행하는 방법을 설명하는 흐름도이다.

[0038] 도 2를 참조하면, 제2통신 장치(20)는 사용자가 입력한 웹 사이트 주소를 부여받은 웹 서버(40)로 접속하고, 웹 서버(40)는 아이디와 패스워드를 입력할 수 있는 로그인 메뉴가 포함된 웹 페이지를 제2통신 장치(20)로 전송한다(S201). 이때, 웹 서버(40)는 액세스 토큰을 생성하고, 이 액세스 토큰과 웹 사이트 식별정보(예컨대, 웹 서버의 사이트 주소)를 상기 웹 페이지와 함께 제2통신 장치(20)로 전송한다. 상기 액세스 토큰(access token)은 제2통신 장치(20)가 로그인 수행시 필요한 보안 정보가 기록된 일종의 객체로서, 고유의 식별정보(예컨대, 보안 식별정보)를 갖는다.

[0039] 다음으로, 제2통신 장치(20)는 웹 서버(40)로부터 수신한 웹 페이지를 화면에 출력한다. 이때, 제2통신 장치(20)의 에이전트(21)는 상기 웹 페이지의 로그인 메뉴 아래에 안전 로그인 메뉴를 출력할 수 있다. 바람직하게,

제2통신 장치(20)의 에이전트(21)는 쿠키 등의 저장공간에 안전 로그인 서비스의 닉네임 또는 아이디가 보관된 경우, 이 닉네임 또는 아이디를 상기 안전 로그인 메뉴와 함께 웹 페이지에 표시할 수 있다.

[0040] 이어서, 제2통신 장치(20)의 에이전트(21)는 안전 로그인 메뉴가 클릭되는지 여부를 모니터링하여 안전 로그인 메뉴가 클릭되면(S203), 로그인하고자 하는 웹 사이트의 식별정보(예컨대, 웹 사이트 주소), 웹 서버(40)로 접근할 수 있는 액세스 토큰, 사용자 식별정보 및 제2통신 장치(20)의 식별정보가 포함된 로그인 알림 메시지를 생성하여 보안 중계 서버(30)로 전송한다(S205). 이때, 에이전트(21)는 사용자 식별정보로서 안전 로그인 서비스 ID, 사용자의 주민등록번호, I-PIN(Internet Personal Identification Number), 이동통신 전화번호 등 중 어느 하나를 로그인 알림 메시지에 기록할 수 있다. 게다가, 에이전트(21)는 제2통신 장치(20)의 식별정보로서, 자신의 식별정보(즉, 에이전트 식별정보), 제2통신 장치(20)의 IP 주소, MAC 주소 등 중 어느 하나를 로그인 알림 메시지에 기록할 수 있다.

[0041] 그러면, 보안 중계 서버(30)는 상기 로그인 알림 메시지에 포함된 사용자 식별정보를 확인하고, 이 사용자 식별정보와 매핑된 제1통신 장치(10)의 식별정보를 확인한다. 그리고 보안 중계 서버(30)는 상기 확인한 식별정보를 가지는 제1통신 장치(10)로 상기 로그인 알림 메시지를 전송한다(S207).

[0042] 다음으로, 제1통신 장치(10)는 보안 중계 서버(30)로부터 수신한 로그인 알림 메시지에서 사용자 식별정보, 웹 사이트 식별정보, 액세스 토큰 및 제2통신 장치(20)의 식별정보를 추출한다.

[0043] 이어서, 제1통신 장치(10)는 사용자의 본인인증을 요청하는 알림창을 출력하여, 사용자로부터 본인인증 정보를 입력받는다(S209). 이때, 제1통신 장치(10)는 사용자가 사전에 설정한 본인인증 비밀번호를 입력받을 수 있고, 바람직하게는 카메라 또는 생체정보 입력수단 등을 통해 사용자의 지문, 홍체 등과 같은 생체정보를 사용자로부터 입력받는다.

[0044] 다음으로, 제1통신 장치(10)는 사전에 사용자로부터 입력받아 자체 저장하고 있는 본인인증 정보와 상기 사용자로부터 입력받은 본인인증 정보가 일치하는지 여부를 인증한다(S211). 제1통신 장치(10)는 상기 사용자로부터 입력받은 본인인증 정보와 자체 저장하고 있는 본인인증 정보가 일치하지 않으면, 제2통신 장치(20)로 인증 관련 데이터를 제공할 수 없음을 알리는 데이터 제공 불가 메시지를 전송한다(S213). 또는, 제1통신 장치(10)는 본인인증 정보를 재입력을 요구하는 메시지를 화면에 출력할 수도 있다.

[0045] 반면에, 제1통신 장치(10)는 상기 사용자로부터 입력받은 본인인증 정보와 자체 저장하고 있는 본인인증 정보가 일치하면, 제2통신 장치(20)로 복호키를 요청한다(S215). 그러면, 제2통신 장치(20)는 자체 보유하고 있는 복호키를 추출하여 제1통신 장치(10)로 전송한다(S217).

[0046] 이어서, 제1통신 장치(10)는 로그인 알림 메시지에 포함된 제2통신 장치 식별정보와 웹 사이트 식별정보를 확인하고, 상기 제2통신 장치 식별정보를 토대로 통신 장치별로 구분된 보안 데이터 중에서 상기 제2통신 장치 전용의 보안 데이터를 추출한다. 다음으로, 제1통신 장치(10)는 상기 추출한 보안 데이터에 포함된 로그인 인증정보 중에서 상기 웹 사이트 식별정보와 매핑되는 암호화된 로그인 인증정보(예컨대, 아이디와 패스워드)를 추출한다(S219). 이어서, 제1통신 장치(10)는 상기 추출한 로그인 인증정보를 상기 복호키를 이용하여 복호화한다(S221).

[0047] 다음으로, 제1통신 장치(10)는 상기 로그인 알림 메시지에서 추출한 웹 사이트 식별정보와 액세스 토큰을 확인하고, 이 웹 사이트 식별정보를 부여받은 웹 서버(40)로 상기 추출한 로그인 인증정보와 상기 액세스 토큰을 전송한다(S223).

[0048] 그러면, 웹 서버(40)는 제1통신 장치(10)로부터 수신한 액세스 토큰을 토대로, 로그인 시도하는 제2통신 장치(20)를 식별하고, 상기 로그인 인증정보가 정확한지 여부를 확인함으로써, 상기 제2통신 장치(20)의 로그인 인증을 수행한다(S225).

[0049] 다음으로, 웹 서버(40)는 로그인 인증에 실패하면, 제2통신 장치(20)의 로그인을 실패 처리하고, 반면에 로그인 인증에 성공하면 인증 성공 메시지를 제2통신 장치(20)로 전송한 후(S227), 제2통신 장치(20)가 요청한 온라인 서비스를 제공한다. 바람직하게, 웹 서버(40)는 로그인 인증에 성공한 경우, 제1통신 장치(10)로 제2통신 장치(20)가 로그인 성공하였음을 통보한다.

[0050] 또한, 제1통신 장치(10)는 복호화된 로그인 인증정보를 웹 서버(40)가 아닌 상기 제2통신 장치(20)로 전송할 수 있다. 이 경우, 제2통신 장치(20)는 상기 제1통신 장치(10)로부터 수신한 로그인 인증정보를 웹 서버(40)로 전송하여 로그인 인증을 직접 진행한다.

[0051] 이하, 도 3 내지 도 5를 참조한 설명에 있어서, 도 2와 동일한 참조부호를 가지는 각 단계는 도 2와 동일하게 적용되므로 공통되는 참조부호를 가지는 단계(S201 내지 S215)에 대한 설명은 생략한다.

[0052] 도 3은 본 발명의 다른 실시예에 따른, 안전 로그인 시스템에서 로그인 인증을 수행하는 방법을 설명하는 흐름도이다.

[0053] 도 3을 참조하면, 제1통신 장치(10)는 사용자의 본인인증에 성공하면, 자체 저장중인 암호화된 로그인 인증 정보를 추출한다(S319). 구체적으로, 제1통신 장치(10)는 S207 단계에서 수신한 로그인 알림 메시지에 포함된 제2통신 장치 식별정보와 웹 사이트 식별정보를 확인하고, 상기 제2통신 장치 식별정보를 토대로 통신 장치별로 구분된 보안 데이터 중에서 상기 제2통신 장치 전용의 보안 데이터를 추출한다. 다음으로, 제1통신 장치(10)는 상기 추출한 보안 데이터에 포함된 로그인 인증정보 중에서 상기 웹 사이트 식별정보와 매핑되는 암호화된 로그인 인증정보(예컨대, 아이디와 패스워드)를 추출한다. 상기 암호화된 로그인 인증정보는 상기 제2통신 장치(20)에서 보관중인 복호키를 통해서 정상적으로 복호화된다.

[0054] 이어서, 제1통신 장치(10)는 상기 추출한 암호화된 로그인 인증정보를 제2통신 장치(10)로 전송한다(S321).

[0055] 그러면, 제2통신 장치(20)는 제1통신 장치(10)로부터 수신한 암호화된 로그인 인증정보를 자체 보관중인 복호키를 통해서 복호화하고(S323), 이 복호화된 로그인 인증정보를 웹 서버(40)로 전송하여 로그인 인증을 요청한다(S325).

[0056] 다음으로, 웹 서버(40)는 제2통신 장치(20)로부터 수신한 로그인 인증정보가 정확한지 여부를 확인함으로써, 상기 제2통신 장치(20)의 로그인 인증을 수행한다(S327).

[0057] 다음으로, 웹 서버(40)는 로그인 인증에 실패하면, 제2통신 장치(20)의 로그인을 실패 처리하고, 반면에 로그인 인증에 성공하면 인증 성공 메시지를 제2통신 장치(20)로 전송한 후(S329), 제2통신 장치(20)가 요청한 온라인 서비스를 제공한다.

[0058] 도 4는 본 발명의 또 다른 실시예에 따른, 안전 로그인 시스템에서 로그인 인증을 수행하는 방법을 설명하는 흐름도이다.

[0059] 도 4를 참조하여 설명한 실시예에서는, 제1통신 장치(10)가 통신 장치별로 구분된 복호키를 저장하고, 제2통신 장치(20)가 암호화된 각 웹 사이트의 로그인 인증정보를 저장한다.

[0060] 도 4를 참조하면, 제1통신 장치(10)는 사용자의 본인인증에 성공하면, 통신 장치별로 구분된 복호키 중에서 로그인 알림 메시지에 포함된 제2통신 장치 식별정보와 대응되는 복호키를 추출한다(S419). 이어서, 제1통신 장치(10)는 상기 추출한 복호키를 제2통신 장치(20)로 전송한다(S421).

[0061] 이어서, 제2통신 장치(20)는 자체 저장중인 암호화된 사이트별 로그인 인증정보에서, 현재 접속중인 웹 사이트 식별정보와 매핑된 암호화된 로그인 인증정보를 추출한다(S423). 이어서, 제2통신 장치(20)는 상기 추출한 로그인 인증정보를 제1통신 장치(10)로부터 수신한 복호키를 이용하여 복호화한다(S425). 다음으로, 제2통신 장치(20)는 상기 복호화한 로그인 인증 정보를 웹 서버(40)로 전송하여 로그인 인증을 요청한다(S427).

[0062] 그러면, 웹 서버(40)는 제2통신 장치(20)로부터 수신한 로그인 인증정보가 정확한지 여부를 확인함으로써, 상기 제2통신 장치(20)의 로그인 인증을 수행한다(S429). 다음으로, 웹 서버(40)는 로그인 인증에 실패하면, 제2통신 장치(20)의 로그인을 실패 처리하고, 반면에 로그인 인증에 성공하면 인증 성공 메시지를 제2통신 장치(20)로 전송한 후(S431), 제2통신 장치(20)가 요청한 온라인 서비스를 제공한다.

[0063] 도 5는 본 발명의 또 다른 실시예에 따른, 안전 로그인 시스템에서 로그인 인증을 수행하는 방법을 설명하는 흐름도이다.

[0064] 도 5를 참조하여 설명한 실시예에서는, 제1통신 장치(10)가 암호화 처리된 웹 사이트별 인증정보 보관주소를 통신장치 식별정보별로 구분하여 저장한다.

[0065] 도 5를 참조하면, 제1통신 장치(10)는 사용자의 본인인증에 성공하면, S207 단계에서 수신한 로그인 알림 메시지에 포함된 제2통신 장치 식별정보를 토대로, 로그인 시도하는 제2통신 장치 전용의 보관주소 데이터를 확인한다. 그리고 제1통신 장치(10)는 상기 확인한 제2통신 장치 전용의 보관주소 데이터 중에서 로그인 알림 메시지에 포함된 사이트 식별정보와 매핑되는 암호화된 인증정보 보관주소를 추출한다(S519). 상기 암호화된 인증정보

보관주소는 제2통신 장치(20)에서 보유중인 복호키를 통해 정상적으로 복호화된다.

[0066] 이어서, 제1통신 장치(10)는 상기 추출한 암호화된 인증정보 보관주소를 제2통신 장치(20)로 전송한다(S521).

[0067] 그러면, 제2통신 장치(20)는 자체 저장중인 복호키를 추출하고, 이 복호키를 이용하여 제1통신 장치(10)로부터 수신한 암호화된 인증정보 보관주소를 복호화한다. 그리고 제2통신 장치(20)는 인증정보 보관 서버(50)로 상기 보관주소가 기록된 인증정보 요청 메시지를 전송한다(S523).

[0068] 그러면, 인증정보 보관 서버(50)는 상기 인증정보 요청 메시지에서 인증정보 보관주소를 확인하고, 이 보관주소에 보관된 암호화된 로그인 인증정보를 추출하여 제2통신 장치(20)로 전송한다(S525). 즉, 인증정보 보관 서버(50)는 저장중인 복수의 로그인 인증정보 중에서 상기 확인한 인증정보 보관주소를 가지는 로그인 인증정보를 추출하여 제2통신 장치(20)로 전송한다. 상기 암호화된 로그인 인증정보는 제2통신 장치(20)에서 보유하고 있는 복호키를 통해 정상적으로 복호화된다.

[0069] 이어서, 제2통신 장치(20)는 인증정보 보관 서버(50)로부터 수신한 상기 암호화된 인증정보를 자체 저장중인 복호키를 이용하여 복호화한다(S527). 다음으로, 제2통신 장치(20)는 상기 복호화한 로그인 인증 정보를 웹 서버(40)로 전송하여 로그인 인증을 요청한다(S529).

[0070] 그러면, 웹 서버(40)는 제2통신 장치(20)로부터 수신한 로그인 인증정보가 정확한지 여부를 확인함으로써, 상기 제2통신 장치(20)의 로그인 인증을 수행한다(S531). 다음으로, 웹 서버(40)는 로그인 인증에 실패하면, 제2통신 장치(20)의 로그인을 실패 처리하고, 반면에 로그인 인증에 성공하면 인증 성공 메시지를 제2통신 장치(20)로 전송한 후(S533), 제2통신 장치(20)가 요청한 온라인 서비스를 제공한다.

[0071] 한편, 제2통신 장치(20)는 제2통신 장치(20)가 로그인에 성공한 경우, 제2통신 장치(20)를 강제 로그아웃을 진행할 수도 있다. 구체적으로, 제1통신 장치(10)는 제2통신 장치(20)가 로그인에 성공한 후, 제2통신 장치(20)에 대한 로그아웃 조작신호를 사용자로부터 입력받으면, 제2통신 장치(20)의 로그아웃 요청 메시지를 웹 서버(40)로 전송한다. 이때, 제1통신 장치(10)는 로그인 알림 메시지에서 추출한 액세스 토큰을 상기 로그아웃 요청 메시지에 포함한다.

[0072] 그러면, 웹 서버(40)는 상기 로그아웃 요청 메시지에 포함된 액세스 토큰을 토대로, 로그인 성공한 제2통신 장치(20)를 식별하고, 상기 제2통신 장치(20)를 강제로 로그아웃 처리한다. 바람직하게, 웹 서버(40)는 로그아웃이 처리되었음을 알리는 메시지를 제2통신 장치(20)로 전송하고, 더불어 제1통신 장치(10)로 제2통신 장치(20)가 로그아웃 되었음을 통보한다.

[0073] 도 6은 본 발명의 일 실시예에 따른, 인증 데이터 제공 장치의 구성을 나타내는 도면이다.

[0074] 도 6에 도시된 인증 데이터 제공 장치(100)는 도 1 내지 도 5를 참조하여 설명한 제1통신 장치(10)의 동작을 수행한다.

[0075] 도 6에 도시된 바와 같이, 본 발명의 일 실시예에 따른 인증 데이터 제공 장치(100)는 메모리(110), 메모리 제어기(121), 하나 이상의 프로세서(CPU)(122), 주변 인터페이스(123), 입출력(I/O) 서브시스템(130), 디스플레이 장치(141), 입력 장치(142), 카메라(143), 통신 회로(150) 및 GPS 수신기(160)를 포함한다. 이러한 구성요소는 하나 이상의 통신 버스 또는 신호선을 통하여 통신한다. 도 6에 도시한 여러 구성요소는 하나 이상의 신호 처리 및/또는 애플리케이션 전용 집적 회로(application specific integrated circuit)를 포함하여, 하드웨어, 소프트웨어 또는 하드웨어와 소프트웨어 둘의 조합으로 구현될 수 있다.

[0076] 메모리(110)는 고속 랜덤 액세스 메모리를 포함할 수 있고, 또한 하나 이상의 자기 디스크 저장 장치, 플래시 메모리 장치와 같은 불휘발성 메모리, 또는 다른 불휘발성 반도체 메모리 장치를 포함할 수 있다. 일부 실시예에서, 메모리(110)는 하나 이상의 프로세서(122)로부터 멀리 떨어져 위치하는 저장 장치, 예를 들어 통신 회로(150)와, 인터넷, 인트라넷, LAN(Local Area Network), WLAN(Wide LAN), SAN(Storage Area Network) 등, 또는 이들의 적절한 조합과 같은 통신 네트워크를 통하여 액세스되는 네트워크 부착형(attached) 저장 장치를 더 포함할 수 있다. 프로세서(122) 및 주변 인터페이스(123)와 같은 인증 데이터 제공 장치(100)의 다른 구성요소에 의한 메모리(110)로의 액세스는 메모리 제어기(121)에 의하여 제어될 수 있다.

[0077] 주변 인터페이스(123)는 입출력 주변 장치를 프로세서(122) 및 메모리(110)와 연결시킨다. 하나 이상의 프로세서(122)는 다양한 소프트웨어 프로그램 및/또는 메모리(110)에 저장되어 있는 명령어 세트를 실행하여 인증 데

이터 제공 장치(100)를 위한 여러 기능을 수행하고 데이터를 처리한다.

[0078] 일부 실시예에서, 주변 인터페이스(123), 프로세서(122) 및 메모리 제어기(121)는 칩(120)과 같은 단일 칩 상에서 구현될 수 있다. 일부 다른 실시예에서, 이들은 별개의 칩으로 구현될 수 있다.

[0079] I/O 서브시스템(130)은 디스플레이 장치(141), 입력 장치(142), 카메라(143)와 같은 인증 데이터 제공 장치(100)의 입출력 주변장치와 주변 인터페이스(123) 사이에 인터페이스를 제공한다.

[0080] 디스플레이 장치(141)는 LCD(liquid crystal display) 기술 또는 LPD(light emitting polymer display) 기술을 사용할 수 있고, 이러한 디스플레이 장치(141)는 용량형, 저항형, 적외선형 등의 터치 디스플레이일 수 있다. 터치 디스플레이는 장치와 사용자 사이에 출력 인터페이스 및 입력 인터페이스를 제공한다. 터치 디스플레이는 사용자에게 시각적인 출력을 표시한다. 시각적 출력은 텍스트, 그래픽, 비디오와 이들의 조합을 포함할 수 있다. 시각적 출력의 일부 또는 전부는 사용자 인터페이스 대상에 대응할 수 있다. 터치 디스플레이는 사용자 입력을 수용하는 터치 감지면을 형성한다.

[0081] 입력 장치(142)는 키패드, 키보드 등과 같은 입력수단으로서, 사용자의 입력신호를 수신한다.

[0082] 카메라(143)는 렌즈를 구비하여 이 렌즈를 통해 주변 이미지를 촬영한다. 특히, 카메라(143)는 사용자의 지문, 홍체 등과 같은 사용자의 생체정보 이미지를 촬영할 수 있다.

[0083] 프로세서(122)는 인증 데이터 제공 장치(100)에 연관된 동작을 수행하고 명령어들을 수행하도록 구성된 프로세서로서, 예를 들어, 메모리(110)로부터 검색된 명령어들을 이용하여, 인증 데이터 제공 장치(100)의 컴포넌트 간의 입력 및 출력 데이터의 수신과 조작을 제어할 수 있다.

[0084] 통신 회로(150)는 안테나를 통해 무선 전자파를 송수신하거나 유선 케이블을 통해 데이터를 송수신한다. 통신 회로(150)는 전기 신호를 전자파로 또는 그 반대로 변환하며 이 전자파를 통하여 통신 네트워크, 다른 이동형 게이트웨이 장치 및 통신 장치와 통신할 수 있다. 통신 회로(150)는 예를 들어 안테나 시스템, RF 트랜시버, 하나 이상의 증폭기, 튜너, 하나 이상의 오실레이터, 디지털 신호 처리기, CODEC 칩셋, 가입자 식별 모듈(subscriber identity module, SIM) 카드, 메모리 등을 포함하지만 이에 한정되지 않는, 이러한 기능을 수행하기 위한 주지의 회로를 포함할 수 있다. 통신 회로(150)는 월드 와이드 웹(World Wide Web, WWW)으로 불리는 인터넷, 인트라넷과 네트워크 및/또는 이동통신 네트워크, 무선 LAN 및/또는 MAN(metropolitan area network) 그리고 근거리 무선 통신에 의하여 다른 장치와 통신할 수 있다. 무선 통신은 GSM(Global System for Mobile Communication), EDGE(Enhanced Data GSM Environment), WCDMA(wideband code division multiple access), CDMA(code division multiple access), TDMA(time division multiple access), VoIP(voice over Internet Protocol), Wi-MAX, LTE(Long Term Evolution), 블루투스(Bluetooth), 지그비(zigbee), 엔에프씨(NFC:Near Field Communication) 또는 본 출원의 출원 시점에 아직 개발되지 않은 통신 프로토콜을 포함하는 기타 다른 적절한 통신 프로토콜을 포함하지만 이에 한정되지 않는 복수의 통신 표준, 프로토콜 및 기술 중 어느 것을 이용할 수 있다.

[0085] GPS(Global Positioning System) 수신기(160)는 복수의 인공위성에서 발신하는 위성신호를 수신한다. 이러한 GPS 수신기(160)는 C/A코드 의사거리 수신기, C/A코드 반송파 수신기, P코드 수신기, Y코드 수신기 등이 채택될 수 있다.

[0086] 소프트웨어 구성요소인 운영 체제(111), 그래픽 모듈(명령어 세트)(112) 및 안전 로그인 프로그램(명령어 세트)(113)이 메모리(110)에 탑재(설치)된다.

[0087] 운영 체제(111)는, 예를 들어, 다윈(Darwin), RTXC, LINUX, UNIX, OS X, WINDOWS, VxWorks, Tizen, IOS 또는 안드로이드 등과 같은 내장 운영체제일 수 있고, 일반적인 시스템 태스크(task)(예를 들어, 메모리 관리, 저장 장치 제어, 전력 관리 등)를 제어 및 관리하는 다양한 소프트웨어 구성요소 및/또는 장치를 포함하고, 다양한 하드웨어와 소프트웨어 구성요소 사이의 통신을 촉진시킨다.

[0088] 그래픽 모듈(112)은 디스플레이 장치(141) 상에 그래픽을 제공하고 표시하기 위한 주지의 여러 소프트웨어 구성요소를 포함한다. "그래픽(graphics)"이란 용어는 텍스트, 웹 페이지, 아이콘, 디지털 이미지, 비디오, 애니메이션 등을 제한 없이 포함하여, 사용자에게 표시될 수 있는 모든 대상을 포함한다.

[0089] 안전 로그인 프로그램(113)은 제2통신 장치(20)가 웹 서버(40)로 로그인을 시도하는 경우, 인증 관련 데이터를 획득하여 웹 서버(40) 또는 제2통신 장치(20)로 제공한다. 상기 안전 로그인 프로그램(113)은 안전 로그인 애플

리케이션이 설치되는 경우에, 메모리(110)에 탑재된다.

[0090] 도 7은 본 발명의 일 실시예에 따른, 안전 로그인 프로그램의 구성을 나타내는 도면이다.

[0091] 도 7에 도시된 바와 같이, 본 발명의 일 실시예에 따른 안전 로그인 프로그램(113)은 데이터 저장 모듈(71), 본인 인증 모듈(72), 인증 데이터 추출 모듈(73) 및 인증 데이터 제공 모듈(74)을 포함한다.

[0092] 데이터 저장 모듈(71)은 사용자의 본인인증 정보를 저장한다. 상기 데이터 저장 모듈(71)은 본인인증 정보로서, 사용자의 비밀번호 또는 사용자의 생체정보 등을 저장할 수 있다. 일 실시예에서, 데이터 저장 모듈(71)은 각 웹 사이트의 로그인 인증정보(즉, 아이디와 패스워드)가 기록된 보안 데이터를 통신 장치 식별정보별로 구분하여 저장할 수 있다. 상기 로그인 인증정보는 암호화 처리되어 데이터 저장 모듈(71)에 저장되며, 제2통신 장치(20)에서 저장된 복호키를 토대로 정상적으로 복호화된다. 또 다른 실시예에서, 데이터 저장 모듈(71)은 하나 이상의 복호키를 통신 장치 식별정보별로 구분하여 저장할 수 있다. 또 다른 실시예에서, 데이터 저장 모듈(71)은 웹 사이트별 인증정보 보관주소가 기록된 보안 주소 데이터를 통신 장치 식별정보별로 구분하여 저장할 수 있다.

[0093] 본인 인증 모듈(72)은 사용자로부터 입력받은 본인 인증정보와 데이터 저장 모듈(71)에 저장된 본인 인증정보가 정확한지 여부를 확인하여, 사용자를 인증하는 기능을 수행한다. 즉, 본인 인증 모듈(72)은 통신 회로(150)를 통해 보안 중계 서버(30)로부터 로그인 알림 메시지를 수신하면, 본인인증 정보의 입력을 요청하는 알림창을 디스플레이 장치(141)에 출력한다. 아울러, 본인 인증 모듈(72)은 사용자로부터 본인 인증정보를 입력하면, 이 본인인증 정보와 데이터 저장 모듈(71)에 저장된 본인인증 정보가 일치하는지 여부를 확인한다. 상기 본인 인증 모듈(72)은 입력장치(142)를 통해 사용자로부터 본인인증을 위한 비밀 번호를 입력받을 수 있으며, 이 경우 사용자로부터 입력받은 비밀번호와 데이터 저장 모듈(71)에 저장된 비밀번호가 일치하는지 여부를 인증한다. 또한, 본인 인증 모듈(72)은 카메라(143) 또는 다른 생체정보 입력수단(도면에 도시되지 않음)을 통해 사용자의 생체정보를 입력받을 수 있으며, 이 경우 사용자로부터 입력받은 생체정보와 데이터 저장 모듈(71)에 저장된 생체정보가 임계값(예컨대, 70%) 이상으로 일치하는지 여부를 확인하여 사용자를 인증할 수 있다.

[0094] 인증 데이터 추출 모듈(73)은 본인 인증 모듈(72)에서 사용자 본인 인증에 성공하면, 데이터 저장 모듈(71)에서 인증 관련 데이터를 추출한다. 상기 인증 데이터 추출 모듈(73)은 로그인 알림 메시지에 포함된 통신 장치 식별정보를 토대로 다수의 보안 데이터 중에서 상기 제2통신 장치 전용의 보안 데이터를 데이터 저장 모듈(71)에서 확인하고, 이 보안 데이터 중에서 웹 사이트 식별정보와 매핑되는 암호화된 로그인 인증정보(즉, 아이디와 패스워드)를 인증 관련 데이터로서 추출할 수 있다.

[0095] 또 다른 실시예에서, 인증 데이터 추출 모듈(73)은 로그인 알림 메시지에 포함된 제2통신 장치 식별정보를 토대로, 상기 제2통신 장치(20)의 식별정보와 대응되는 복호키를 인증 관련 데이터로서 데이터 저장 모듈(71)에서 추출할 수 있다.

[0096] 또 다른 실시예에서, 인증 데이터 추출 모듈(73)은 로그인 알림 메시지에 포함된 제2통신 장치 식별정보를 토대로, 제2통신 장치 전용의 보관주소 데이터를 데이터 저장 모듈(71)에서 확인하고, 이 보관주소 데이터 중에서 웹 사이트 식별정보와 매핑되는 인증정보 보관주소를 인증 관련 데이터로서 추출할 수 있다.

[0097] 인증 데이터 제공 모듈(74)은 인증 데이터 추출 모듈(73)에서 추출한 인증 관련 데이터를 웹 서버(40) 또는 제2통신 장치(20)로 제공하는 기능을 수행한다. 일 실시예에서, 인증 데이터 제공 모듈(74)은 통신 회로(150)를 이용하여 제2통신 장치(20)로 복호키를 요청하고 수신하여, 이 복호키를 이용하여 인증 데이터 추출 모듈(73)에서 추출한 암호화된 로그인 인증정보를 복호화한 후에, 이렇게 복호화된 로그인 인증정보를 웹 서버(40) 또는 제2통신 장치(20)로 전송한다. 다른 실시예에서, 인증 데이터 제공 모듈(74)은 인증 데이터 추출 모듈(73)에서 추출한 암호화된 로그인 인증정보를, 통신 회로(150)를 이용하여 제2통신 장치(20)로 전송하여, 제2통신 장치(20)에서 보유하고 있는 복호키를 통해 상기 암호화된 로그인 인증정보가 복호화되게 한다.

[0098] 또 다른 실시예에서, 인증 데이터 제공 모듈(74)은 인증 데이터 추출 모듈(73)에서 추출한 복호키를, 통신 회로(150)를 통해 제2통신 장치(20)로 전송하여, 제2통신 장치(20)에서 저장하고 있는 암호화된 로그인 인증정보가 상기 전송한 복호키를 통해 복호화되게 한다. 또 다른 실시예에서, 인증 데이터 제공 모듈(74)은 인증 데이터 추출 모듈(73)에서 추출한 암호화된 인증정보 보관주소를 제2통신 장치(20)로 전송하여, 제2통신 장치(20)가 상기 인증정보 보관주소에 보관된 로그인 인증정보를 인증정보 보관 서버(50)로부터 수신하게 한다.

[0099] 상술한 바와 같이, 본 발명은 제1통신 장치(10)와 제2통신 장치(20)가 연동하여 로그인 인증정보를 웹 서버(40)로 제공함으로써, 엿보기 공격으로부터 사용자의 아이디와 패스워드를 보호하고 사용자의 인증정보에 대한 보

안을 강화시킨다. 또한, 본 발명에 따른 제1통신 장치(10)는, 사용자의 본인인증을 1차적으로 진행하고, 이 본인인증 결과에 따라 인증 관련 데이터를 제2통신 장치(20)로 제공함으로써, 사용자의 인증정보에 대한 보안성을 더욱 강화시킨다. 게다가, 본 발명은 로그인 인증에 필요한 인증 관련 데이터를 복수의 장치를 통해서 분산시켜 저장하기 때문에, 악의적인 의도를 가지는 타인이 특정 장치의 데이터를 탈취하더라도 완전하게 사용자의 로그인 인증정보를 획득할 수 없어, 사용자의 인증정보를 더욱 안전하게 보호한다.

[0100] 본 명세서는 많은 특징을 포함하는 반면, 그러한 특징은 본 발명의 범위 또는 특허청구범위를 제한하는 것으로 해석되어서는 안 된다. 또한, 본 명세서에서 개별적인 실시예에서 설명된 특징들은 단일 실시예에서 결합되어 구현될 수 있다. 반대로, 본 명세서에서 단일 실시예에서 설명된 다양한 특징들은 개별적으로 다양한 실시예에서 구현되거나, 적절히 결합되어 구현될 수 있다.

[0101] 도면에서 동작들이 특정한 순서로 설명되었으나, 그러한 동작들이 도시된 바와 같은 특정한 순서로 수행되는 것으로, 또는 일련의 연속된 순서, 또는 원하는 결과를 얻기 위해 모든 설명된 동작이 수행되는 것으로 이해되어서는 안 된다. 특정 환경에서 멀티태스킹 및 병렬 프로세싱이 유리할 수 있다. 아울러, 상술한 실시예에서 다양한 시스템 구성요소의 구분은 모든 실시예에서 그러한 구분을 요구하지 않는 것으로 이해되어야 한다. 상술한 프로그램 구성요소 및 시스템은 일반적으로 단일 소프트웨어 제품 또는 멀티플 소프트웨어 제품에 패키지로 구현될 수 있다.

[0102] 상술한 바와 같은 본 발명의 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 형태로 기록매체(시디롬, 램, 롬, 플로피 디스크, 하드 디스크, 광자기 디스크 등)에 저장될 수 있다. 이러한 과정은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있으므로 더 이상 상세히 설명하지 않기로 한다.

[0103] 이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니다.

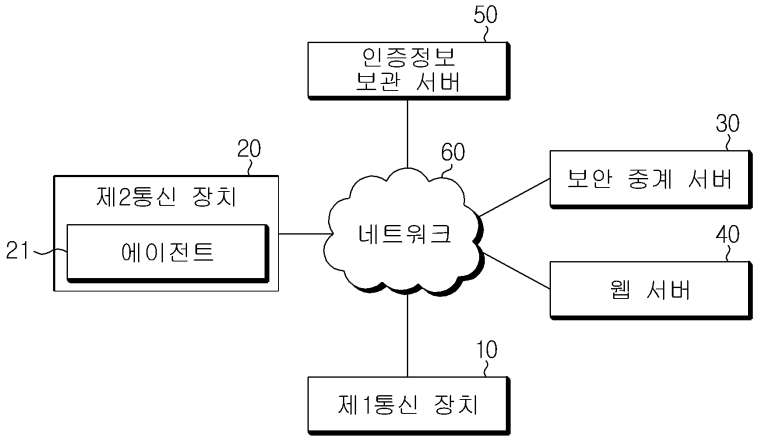
## *부호의 설명*

[0104]

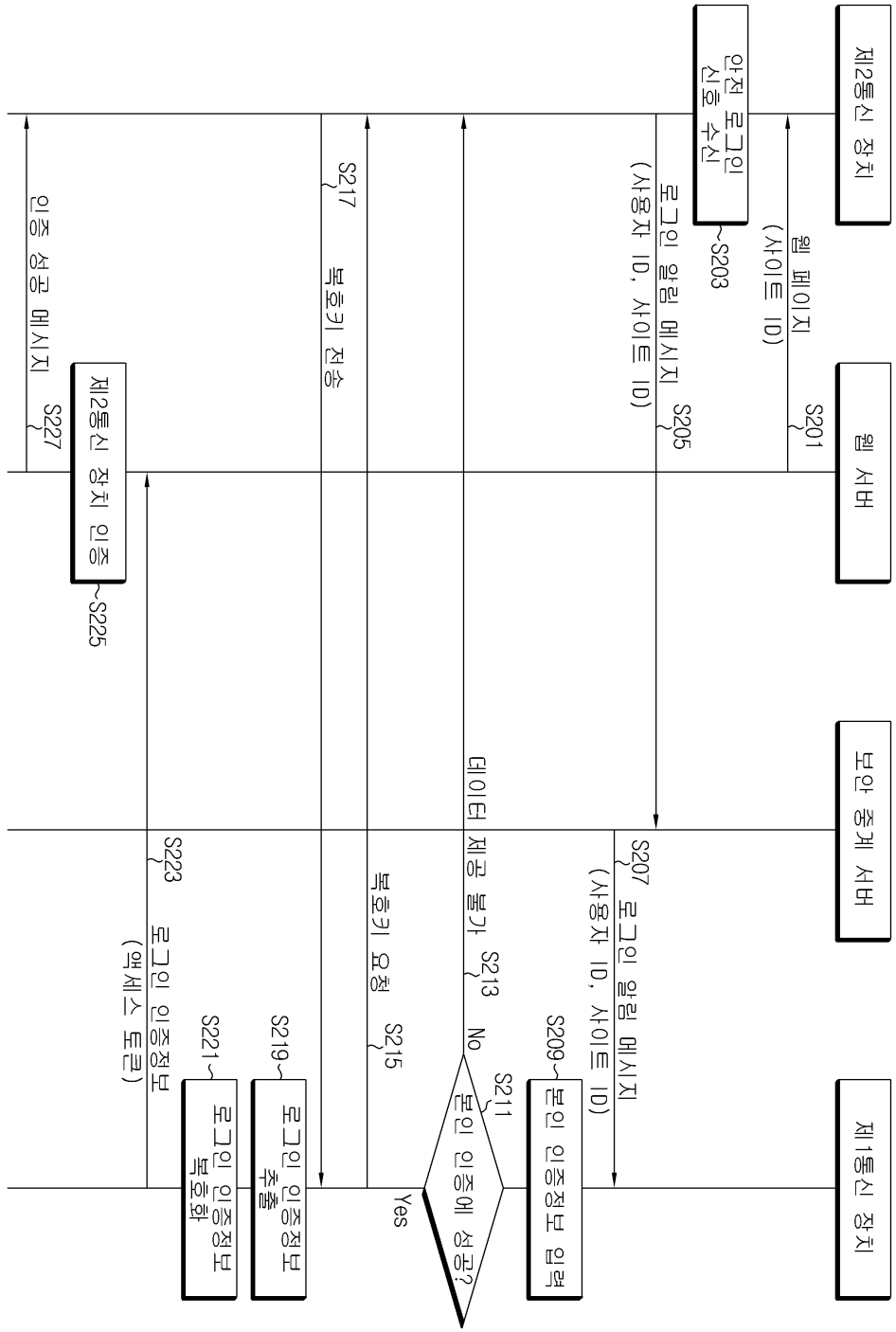
| | |
|---|---|
| 10 : 제1통신 장치 | 20 : 제2통신 장치 |
| 21 : 에이전트 | 30 : 보안 중계 서버 |
| 40 : 웹 서버 | 50 : 인증정보 보관 서버 |
| 60 : 네트워크 | 100 : 인증 데이터 제공 장치 |
| 110 : 메모리 | 111 : 운영 체제 |
| 112 : 그래픽 모듈 | 113 : 안전 로그인 프로그램 |
| 121 : 메모리 제어기 | 122 : CPU |
| 123 : 주변 인터페이스 | 130 : I/O 서브시스템 |
| 141 : 디스플레이 장치 | 142 : 입력장치 |
| 143 : 카메라 | 150 : 통신 회로 |
| 160 : GPS 수신기 | 71 : 데이터 저장 모듈 |
| 72 : 본인 인증 모듈 | 73 : 인증 데이터 추출 모듈 |
| 74 : 인증 데이터 제공 모듈 | |

## 도면

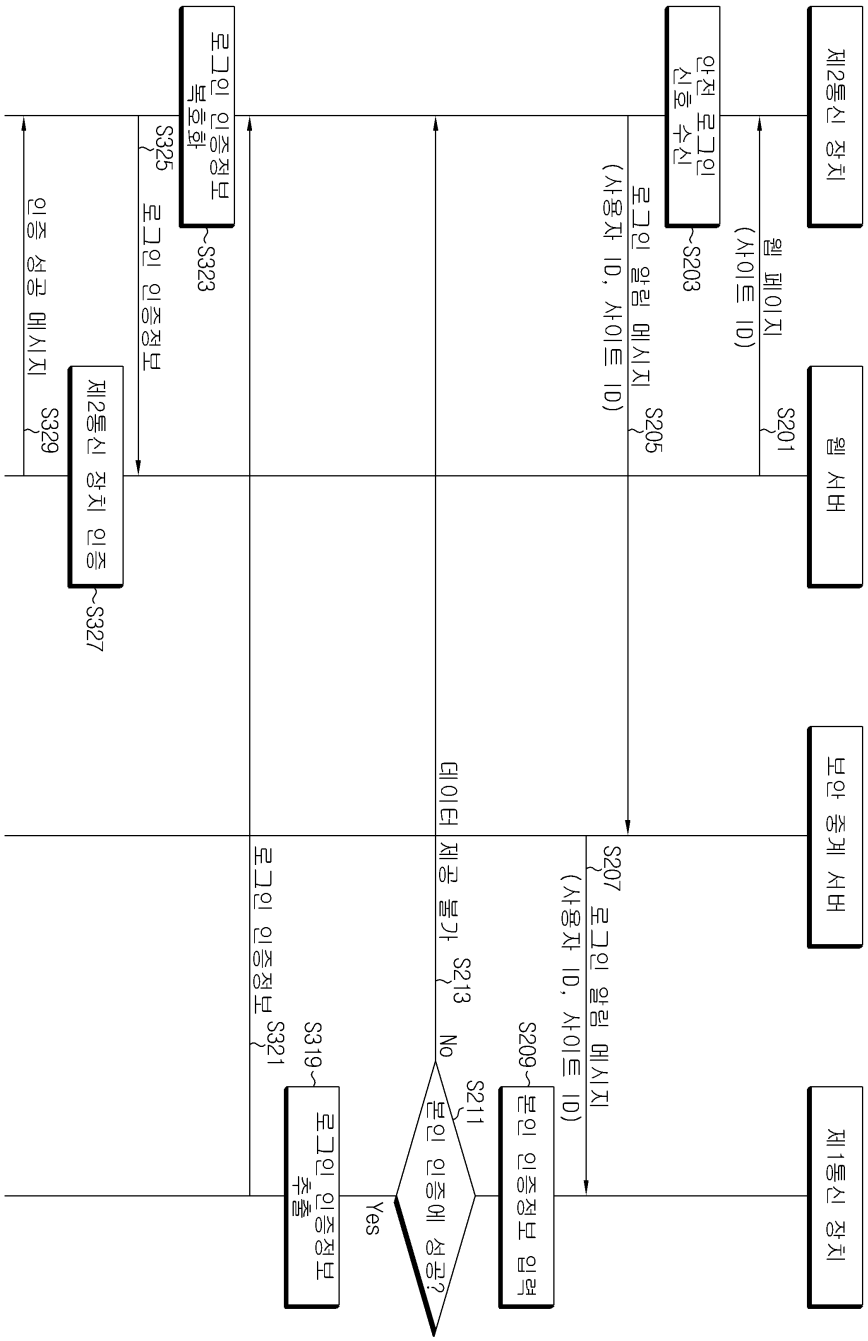
### 도면1


50
인증정보
보관 서버
30
보안 중계 서버
20
60
제2통신 장치
21
에이전트
네트워크
40
웹 서버
10
제1통신 장치

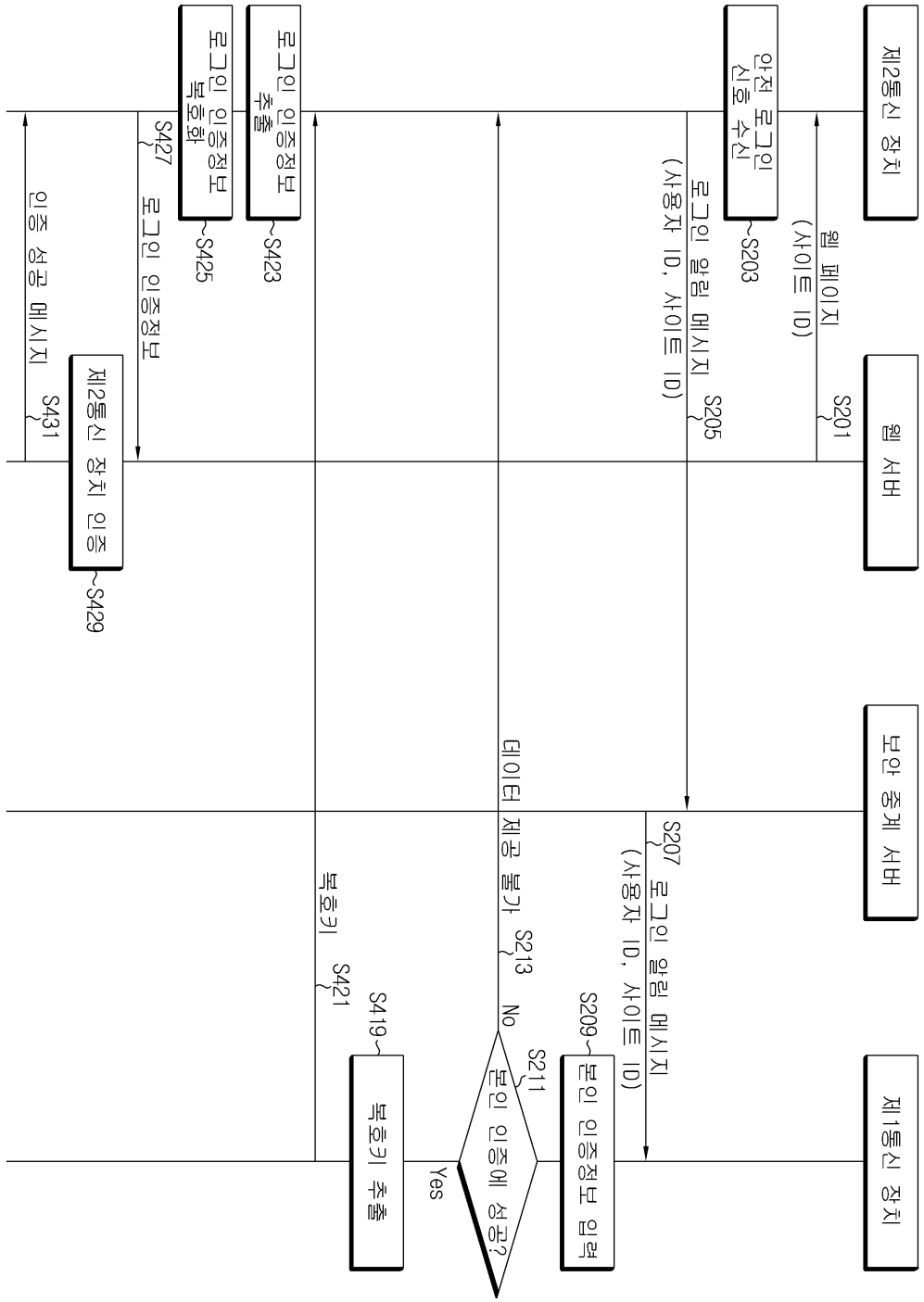
도면2


제2통신 장치
웹 서버
보안 중계 서버
제1통신 장치
웹 페이지 (사이트 ID)
S201
안전 로그인 신호 수신
S203
로그인 알림 메시지 (사용자 ID, 사이트 ID)
S205
S207 로그인 알림 메시지 (사용자 ID, 사이트 ID)
S209 본인 인증정보 입력
본인 인증에 성공?
S211
No
Yes
데이터 제공 불가
S213
복호키 요청
S215
S217 복호키 전송
로그인 인증정보 추출
S219
로그인 인증정보 복호화
S221
S223 로그인 인증정보 (액세스 토큰)
제2통신 장치 인증
S225
인증 성공 메시지
S227

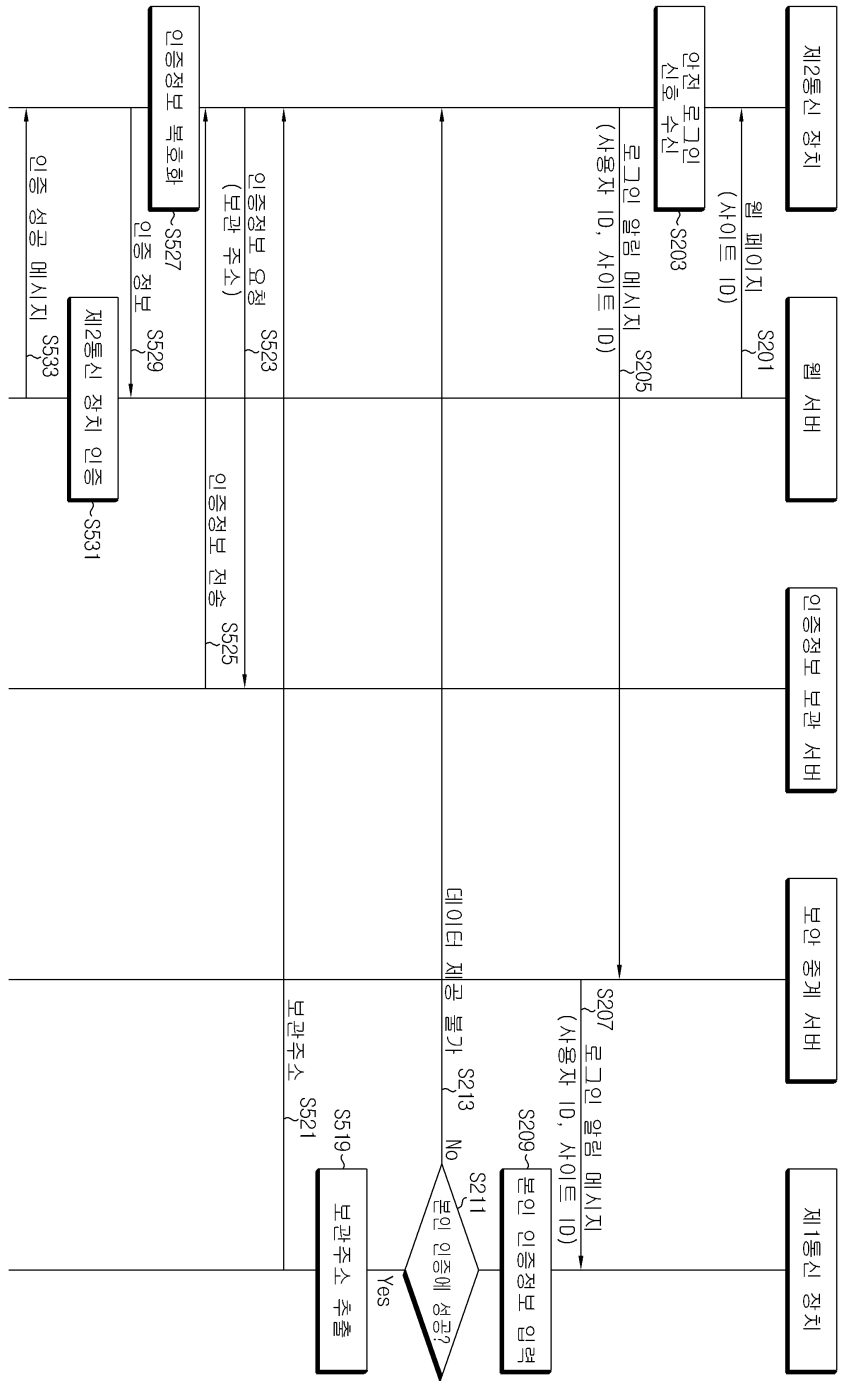
도면3


제2통신 장치
웹 서버
보안 중계 서버
제1통신 장치
안전 로그인 신호 수신
~S203
웹 페이지 (사이트 ID)
S201
로그인 알림 메시지 (사용자 ID, 사이트 ID)
S205
로그인 인증정보 복호화
~S323
S325
로그인 인증정보
제2통신 장치 인증
~S327
인증 성공 메시지
S329
S207
로그인 알림 메시지 (사용자 ID, 사이트 ID)
본인 인증정보 입력
S209~
데이터 제공 불가
S213
No
본인 인증에 성공?
S211
Yes
로그인 인증정보 추출
S319~
로그인 인증정보
S321

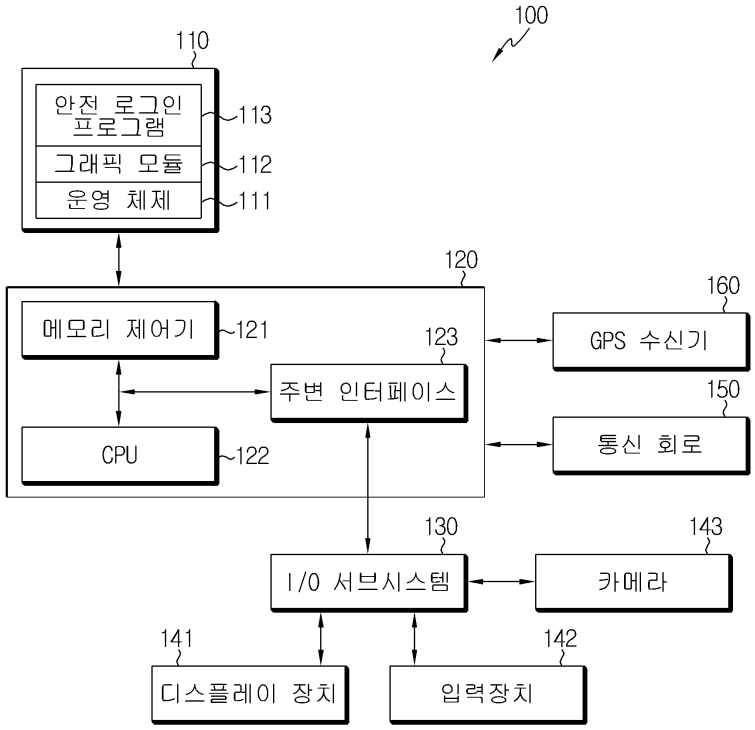
도면4


제2통신 장치
웹 서버
보안 중계 서버
제1통신 장치
안전 로그인 신호 수신
S203
웹 페이지 (사이트 ID)
S201
로그인 알림 메시지 (사용자 ID, 사이트 ID)
S205
로그인 인증정보 추출
S423
로그인 인증정보 복호화
S425
로그인 인증정보
S427
인증 성공 메시지
S431
제2통신 장치 인증
S429
S207
로그인 알림 메시지 (사용자 ID, 사이트 ID)
S209
본인 인증정보 입력
데이터 제공 불가
S213
No
S211
본인 인증에 성공?
Yes
S419
복호키 추출
복호키
S421

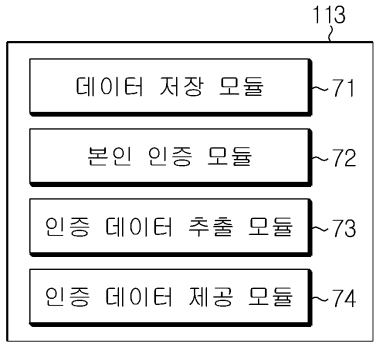
도면5


제2통신 장치
웹 서버
인증정보 보관 서버
보안 중계 서버
제1통신 장치
웹 페이지 (사이트 ID)
S201
안전 로그인 신호 수신
S203
로그인 알림 메시지 (사용자 ID, 사이트 ID)
S205
로그인 알림 메시지 (사용자 ID, 사이트 ID)
S207
분인 인증정보 입력
S209
분인 인증에 성공?
S211
No
Yes
데이터 제공 불가
S213
보관주소 S521
보관주소 추출
S519
인증정보 요청 (보관 주소)
S523
인증정보 전송
S525
인증정보 복호화
S527
인증 정보
S529
제2통신 장치 인증
S531
인증 성공 메시지
S533

도면6


100
110
안전 로그인 프로그램
113
그래픽 모듈
112
운영 체제
111
120
160
메모리 제어기
121
123
GPS 수신기
주변 인터페이스
150
CPU
122
통신 회로
130
143
I/O 서브시스템
카메라
141
142
디스플레이 장치
입력장치

도면7


113
데이터 저장 모듈
71
본인 인증 모듈
72
인증 데이터 추출 모듈
73
인증 데이터 제공 모듈
74