(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0032857
(43) 공개일자 2020년03월27일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 29/06* (2006.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/3226 (2013.01)
H04L 63/0853 (2013.01)
(21) 출원번호 10-2018-0111995
(22) 출원일자 2018년09월19일
심사청구일자 2018년09월19일

(71) 출원인
인하대학교 산학협력단
인천광역시 미추홀구 인하로 100(용현동, 인하대학교)
(72) 발명자
양대헌
서울특별시 서초구 서초중앙로 200, 17동 901호(서초동, 삼풍아파트)
정창훈
서울특별시 강서구 방화동로1길 14, 공항타워팰리스오피스텔3 606호(방화동)
민대홍
인천광역시 미추홀구 인하로 135, 금희, 403호(용현동)
(74) 대리인
양성보

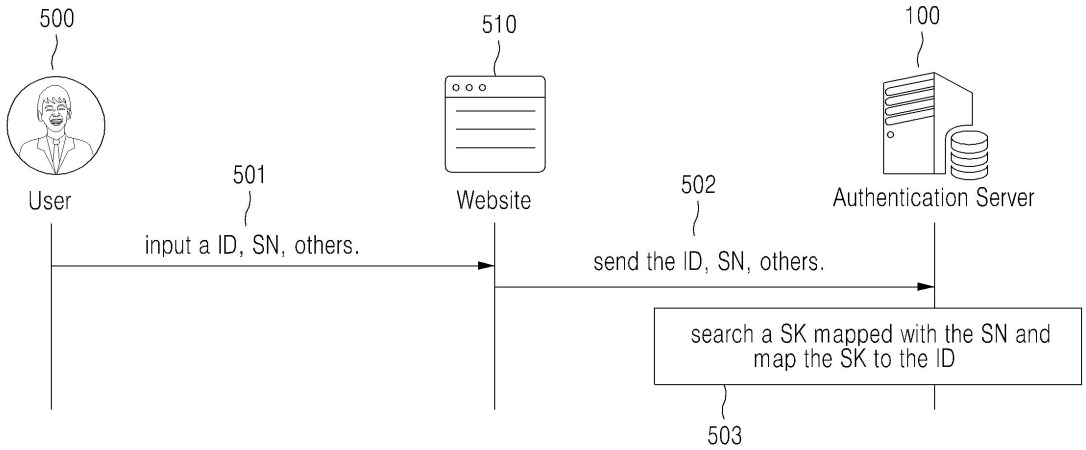
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 **디지털인감을 이용한 안전한 비밀번호 인증 프로토콜**

(57) 요 약

일 실시예에 따른 인증 서버에서 수행되는 비밀번호 인증 방법은, 디지털인감과 관련된 정보의 저장 유무에 따라 분류된 적어도 하나 이상의 프로토콜 중 어느 하나의 프로토콜을 설정하는 단계; 상기 설정된 프로토콜에 기반하여 사용자의 식별 정보가 입력됨에 따라 회원 가입을 완료하는 단계; 및 상기 설정된 프로토콜에 기반하여 상기 회원 가입이 완료된 서비스에 로그인이 수행됨에 따라 상기 사용자의 서비스 접근 권한을 제어하는 단계를 포함할 수 있다.

대 표 도



(52) CPC특허분류
H04L 63/10 (2013.01)
H04L 9/0866 (2013.01)
H04L 9/3242 (2013.01)
H04L 9/3271 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 2018055881
부처명 과학기술정보통신부
연구관리전문기관 한국연구재단
연구사업명 글로벌연구실(GRL)사업
연구과제명 [Ezbaro] 빅데이터 기반의 DDoS공격의 분석, 모델링, 방어 기술 연구
기 여 율 1/1
주관기관 인하대학교
연구기간 2018.05.01 ~ 2019.02.28

명 세 서

청구범위

청구항 1

인증 서버에서 수행되는 비밀번호 인증 방법에 있어서,

디지털인감과 관련된 정보의 저장 유무에 따라 분류된 적어도 하나 이상의 프로토콜 중 어느 하나의 프로토콜을 설정하는 단계;

상기 설정된 프로토콜에 기반하여 사용자의 식별 정보가 입력됨에 따라 회원 가입을 완료하는 단계; 및

상기 설정된 프로토콜에 기반하여 상기 회원 가입이 완료된 서비스에 로그인이 수행됨에 따라 상기 사용자의 서비스 접근 권한을 제어하는 단계

를 포함하는 비밀번호 인증 방법.

청구항 2

제1항에 있어서,

상기 디지털인감과 관련된 정보의 저장 유무에 따라 분류된 적어도 하나 이상의 프로토콜 중 어느 하나의 프로토콜을 설정하는 단계는,

상기 디지털인감의 비밀키가 저장되어 있는 프로토콜 및 상기 디지털인감의 비밀키가 저장되어 있지 않은 프로토콜로 분류하는 단계

를 포함하는 비밀번호 인증 방법.

청구항 3

제1항에 있어서,

상기 설정된 프로토콜에 기반하여 사용자의 식별 정보가 입력됨에 따라 회원 가입을 완료하는 단계는,

상기 디지털인감의 비밀키가 저장되어 있는 프로토콜에 기반하여 상기 사용자의 식별 정보, 상기 사용자가 소유하고 있는 디지털인감의 인감 정보(SN)를 포함하는 사용자 정보를 웹 사이트에 입력함에 따라 상기 웹 사이트에서 상기 사용자 정보가 전달됨을 수신하는 단계; 및

상기 디지털인감의 인감 정보와 매핑되어 있는 비밀키를 검색하고, 상기 사용자의 식별 정보와 상기 검색된 비밀키(SK)를 매핑하여 회원 가입을 완료하는 단계

를 포함하는 비밀번호 인증 방법.

청구항 4

제1항에 있어서,

상기 설정된 프로토콜에 기반하여 상기 회원 가입이 완료된 서비스에 로그인이 수행됨에 따라 상기 사용자의 서비스 접근 권한을 제어하는 단계는,

비밀키가 저장된 프로토콜에 기반하여, 상기 사용자로부터 웹 사이트에 로그인하기 위하여 사용자의 식별 정보가 입력됨에 따라 상기 웹 사이트에서 전송된 상기 사용자의 식별 정보를 수신하여 랜덤챌린지를 생성하고, 상기 생성된 랜덤챌린지와 상기 사용자의 식별 정보를 결합하여 바코드를 생성하여 상기 웹 사이트에게 상기 생성된 바코드를 전달하고, 상기 웹 사이트에서 상기 전달받은 바코드가 출력됨에 따라 상기 사용자로부터 상기 사용자의 디지털인감으로 상기 바코드가 스캔되는 단계

를 포함하고,

상기 디지털인감에서, 상기 사용자의 식별 정보, 상기 랜덤챌린지로 구성된 바코드 데이터 및 상기 디지털인감에 내장된 비밀키를 HOTP 알고리즘에 기반하여 제1 태그를 생성함에 따라 상기 디지털인감의 디스플레이에 상기

생성된 제1 태그가 출력되는

비밀번호 인증 방법.

청구항 5

제4항에 있어서,

상기 설정된 프로토콜에 기반하여 상기 회원 가입이 완료된 서비스에 로그인이 수행됨에 따라 상기 사용자의 서비스 접근 권한을 제어하는 단계는,

상기 사용자로부터 상기 디지털인감의 디스플레이에 출력된 제1 태그가 비밀번호로서 웹 사이트에 입력됨에 따라 상기 웹 사이트에서 상기 사용자로부터 입력된 제1 태그가 전송됨을 수신하고, 로그인 시 입력된 사용자의 식별 정보, 상기 생성된 랜덤챌린지 및 미리 공유된 비밀키를 HOTP 알고리즘에 기반하여 제2 태그를 생성하고, 상기 사용자로부터 입력된 제1 태그와 상기 생성된 제2 태그를 비교한 결과, 제1 태그 및 제2 태그가 일치할 경우, 상기 사용자에게 상기 웹 사이트와 관련된 서비스의 접근 권한을 허가하는 단계

를 포함하는 비밀번호 인증 방법.

청구항 6

제1항에 있어서,

상기 설정된 프로토콜에 기반하여 사용자의 식별 정보가 입력됨에 따라 회원 가입을 완료하는 단계는,

비밀키가 저장되어 있지 않은 프로토콜에 기반하여 사용자로부터 상기 웹 사이트에 로그인하기 위하여 사용자의 식별 정보가 입력됨에 따라 상기 웹 사이트에서 전송된 사용자의 식별 정보를 수신하여 랜덤챌린지를 생성하고, 상기 생성된 랜덤챌린지와 상기 사용자의 식별 정보와 결합하여 바코드를 생성하여 상기 웹 사이트에게 상기 생성된 바코드를 전달하고, 상기 웹 사이트에서 상기 전달받은 바코드가 출력됨에 따라 상기 사용자로부터 상기 사용자의 디지털인감으로 상기 바코드가 스캔되는 단계

를 포함하고,

상기 디지털인감에서, 상기 사용자의 식별 정보, 상기 랜덤챌린지로 구성된 바코드 데이터 및 상기 디지털인감에 내장된 비밀키를 HOTP 알고리즘에 기반하여 제3 태그를 생성함에 따라 상기 디지털인감의 디스플레이에 상기 생성된 제3 태그가 출력되는

비밀번호 인증 방법.

청구항 7

제6항에 있어서,

상기 설정된 프로토콜에 기반하여 사용자의 식별 정보가 입력됨에 따라 회원 가입을 완료하는 단계는,

상기 사용자로부터 상기 디지털인감의 디스플레이에 출력된 제3 태그가 상기 웹 사이트에 입력됨에 따라 상기 웹 사이트에서 전송된 상기 사용자로부터 입력된 제3 태그를 수신하고, 상기 사용자의 식별 정보, 상기 랜덤챌린지 및 상기 제3 태그를 저장한 후, 회원 가입을 완료하는 단계

를 포함하는 비밀번호 인증 방법.

청구항 8

제1항에 있어서,

상기 설정된 프로토콜에 기반하여 상기 회원 가입이 완료된 서비스에 로그인이 수행됨에 따라 상기 사용자의 서비스 접근 권한을 제어하는 단계는,

비밀키가 저장되어 있지 않은 프로토콜에 기반하여, 상기 사용자로부터 웹 사이트에 로그인하기 위하여 사용자의 식별 정보가 입력됨에 따라 상기 웹 사이트에서 전송된 상기 사용자의 식별 정보를 수신하고, 상기 수신된 사용자의 식별 정보와 매핑되어 있는 랜덤챌린지를 이용하여 바코드를 생성하여 상기 웹 사이트에게 상기 생성된 바코드를 전달하고, 상기 웹 사이트에서 상기 전달받은 바코드가 출력됨에 따라 상기 사용자로부터 상기 사

용자의 디지털인감으로 상기 바코드가 스캔되는 단계

를 포함하고,

상기 디지털인감에서, 상기 사용자의 식별 정보, 상기 랜덤챌린지로 구성된 바코드 데이터 및 상기 디지털인감에 내장된 비밀키를 HOTP 알고리즘에 기반하여 제4 태그를 생성함에 따라 상기 디지털인감의 디스플레이에 상기 생성된 제4 태그가 출력되는

비밀번호 인증 방법.

청구항 9

제8항에 있어서,

상기 설정된 프로토콜에 기반하여 상기 회원 가입이 완료된 서비스에 로그인이 수행됨에 따라 상기 사용자의 서비스 접근 권한을 제어하는 단계는,

상기 사용자로부터 상기 디지털인감의 디스플레이에 출력된 제4 태그가 비밀번호로서 웹 사이트에 입력됨에 따라 상기 웹 사이트에서 상기 사용자로부터 입력된 제4 태그가 전송됨을 수신하고, 상기 사용자의 회원 가입 요청 시 저장된 제3 태그와 상기 수신한 제4 태그를 비교한 결과, 상기 제3 태그와 상기 제4 태그가 일치할 경우, 상기 사용자에게 상기 웹 사이트와 관련된 서비스의 접근 권한을 허가하는 단계

를 포함하는 비밀번호 인증 방법.

청구항 10

제9항에 있어서,

상기 설정된 프로토콜에 기반하여 상기 회원 가입이 완료된 서비스에 로그인이 수행됨에 따라 상기 사용자의 서비스 접근 권한을 제어하는 단계는,

상기 로그인에 성공함에 따라 새로운 랜덤챌린지를 생성할 수 있고, 사용자의 식별 정보와 새로운 랜덤챌린지를 결합하여 새로운 바코드를 생성하고, 상기 새로운 바코드를 웹 사이트에 전송함에 따라 상기 웹 사이트가 상기 새로운 바코드를 사용자에게 출력하고 상기 사용자로부터 디지털인감으로 상기 새로운 바코드를 스캔함에 따라 입력된 제5 태그를 수신하면, 기 저장된 사용자의 식별 정보와 매핑되어 있는 랜덤챌린지와 HOTP Tag를 삭제하고, 새로운 랜덤챌린지와 상기 제5 태그를 저장하는 단계

를 포함하는 비밀번호 인증 방법.

청구항 11

비밀번호 인증을 위한 인증 서버에 있어서,

디지털인감과 관련된 정보의 저장 유무에 따라 분류된 적어도 하나 이상의 프로토콜 중 어느 하나의 프로토콜을 설정하는 프로토콜 설정부;

상기 설정된 프로토콜에 기반하여 사용자의 식별 정보가 입력됨에 따라 회원 가입을 완료하는 회원 가입부; 및

상기 설정된 프로토콜에 기반하여 상기 회원 가입이 완료된 서비스에 로그인이 수행됨에 따라 상기 사용자의 서비스 접근 권한을 제어하는 제어부

를 포함하는 인증 서버.

발명의 설명

기 술 분 야

[0001] 아래의 설명은 자가 로그인을 할 때 디지털인감을 이용하여 일회용 패스워드를 생성하고, 생성된 패스워드를 이용하여 안전하게 로그인을 할 수 있도록 하는 기술에 관한 것으로, 안전한 로그인 인증 프로토콜을 제공하기 위한 방법 및 시스템에 관한 것이다.

배 경 기 술

[0003] 인증 프로토콜이란, 사용자가 온라인 서비스를 이용하기 위하여 서비스를 제공해주는 웹사이트 등의 접근 권한을 얻는 절차를 의미한다. 예를 들어, 사용자는 온라인 서비스 제공자와 사전에 비밀번호를 공유하고, 서비스를 이용하고 싶을 때 비밀번호를 이용하여 접근 권한을 얻어 서비스를 이용할 수 있다. 초기 인증 프로토콜은 간단하게 비밀번호만을 이용했었지만, 공격자의 비밀번호 탈취 기술이 발전함에 따라 다양한 인증 기법 및 프로토콜이 개발되었다.

[0004] 일례로, 사용자가 PC에서 인증을 시도하는 경우에는, 키보드를 입력하는 패턴이 개인마다 다르다는데 기초한 키 입력 패턴 인식(Keystroke dynamics) 기술, 키보드를 입력할 때의 발생하는 소리를 이용한 인증 기술 등의 인증 기법 및 프로토콜이 연구되어 왔다. 이러한 인증 기법 및 프로토콜은 PC에서만 사용할 수 있다는 제한이 있으며, 올바른 사용자라고 하더라도 사용자의 상황이나 환경에 의해 인증에 실패할 가능성이 존재한다.

[0005] 다른 예로, 사용자가 스마트 폰에서 인증을 시도하는 경우에는, 검은색과 흰색 키패드를 사용하는 인증 기법, 진동을 이용한 인증 기법, 키 터치 위치 및 시간과 머신러닝을 이용한 인증 프로토콜 등이 연구되어 왔으나, 이러한 기술들은 스마트 폰에서만 한정적으로 사용할 수 있다는 단점과 사용자에게 패스워드뿐만 아니라 색 구분, 기호, 키 터치 위치 및 시간 등도 기억해야 한다는 부담이 존재한다.

[0006] 또 다른 예로, 원패스워드란 사용자가 여러 웹사이트 또는 어플리케이션에 등록해놓은 비밀번호를 관리해주는 비밀번호 통합관리 솔루션이다. 사용자는 웹사이트에 자신의 계정을 등록할 때 원패스워드를 이용하여 복잡한 비밀번호를 생성할 수 있고, 로그인을 시도할 때에는 원패스워드를 이용하여 비밀번호가 자동으로 입력되게 할 수 있다. 그러므로 사용자는 여러 사이트에 등록된 비밀번호를 일일이 관리하지 않아도 된다. 그런데 2015년 소프트웨어 엔지니어인 데일 마이어스는 원패스워드를 사용하던 중 애자일 키체인 파일에 문제가 있다는 것을 인지하였고, 그 결과 사용자가 원패스워드를 어떤 서비스 계정에 사용하는지 등의 개인정보가 유출될 수 있다는 것을 확인하였다. 뿐만 아니라 사용을 위해 서버와 통신을 해야 하는 솔루션이므로 네트워크 경로를 통해 비밀키가 유출될 수 있는 가능성도 존재한다.

[0007] 사용자는 로그인을 시도할 때 보안성을 향상시키기 위하여 소프트웨어적인 다양한 인증 기법 및 인증 프로토콜이 아닌, 하드웨어적인 보안 도구를 이용할 수도 있다. OTP(One Time Password), 보안카드 등은 사용자가 스마트폰, PC 등의 플랫폼 상관없이 사용할 수 있는 하드웨어적인 보안 도구이다. 따라서 사용을 위해서는 OTP 기기 또는 카드 형식으로 제작된 보안 카드를 소지하고 있어야만 한다. OTP는 무작위로 일회용 비밀번호를 생성하여 인증에 사용한다. 시간 동기화 방식을 사용하는 Time-synchronized OTP, HMAC을 사용하는 HOTP, 서버와 질의 응답 방식을 이용하는 Challenge-Response OTP 등이 있다. 이러한 OTP는 비밀키 관리 문제가 있을 수 있으며, MitM(Man in the Middle), MitB(Man in the Browser)등의 공격으로부터 안전하지 않다. 보안 카드는 4자리 숫자 30여개가 기록되어 있는 난수표이며, 로그인 또는 온라인 금융 거래 시마다 웹사이트에서 요구하는 보안번호를 올바르게 입력함으로서 안전하게 인증을 할 수 있다. 하지만 보안카드의 번호는 고정되어 있으므로 장시간의 스니핑(Sniffing), 피싱(Phishing), 파밍(Pharming) 공격에 취약하다. 또한 사용자가 이미지화하여 스마트폰 등에 저장하고 다닐 경우, 이미지 유출을 통해 보안카드 전체 난수표가 유출될 수 있다는 가능성도 존재한다.

[0008] 도 1은 아두이노를 이용하여 제작된 디지털인감의 프로토타입 형태로서, 데이터를 포함하고 있는 바코드를 스캔하면, 그 데이터와 비밀키 그리고 HOTP 알고리즘을 이용하여 HOTP Tag를 LCD에 출력해주는 보안 도구이다.

[0009] 디지털인감은 도 2와 같이, 모니터 스크린에 있는 바코드와 실제 종이에 출력된 바코드를 모두 스캔할 수 있기 때문에 온라인, 오프라인에 사용할 수 있으며, 따라서 스마트폰, PC 등과 같은 플랫폼과 상관없이 사용될 수 있다.

[0010] 종이가 아닌, 스마트폰, PC 등과 같은 온라인 플랫폼에서 사용하는 경우에는, 바코드 제공자가 바코드를 자동적으로 스크롤 되게 제작할 수 있고, 사용자는 디지털인감을 모니터 스크린에 가져다대기만 하면 자동적으로 스캔이 되며, 따라서 사용자는 간편하게 스캔을 할 수 있다. 종이 등과 같이 오프라인 플랫폼에서 스캔을 할 경우에는, 도 3 또는 도 2의 중앙에 위치한 그림처럼 스캔 보조 툴 등을 이용하여 직선으로 간편하게 스캔을 할 수 있다.

[0011] 디지털인감은 로그인, 온라인 뱅킹, 모바일 뱅킹, IoT 키 분배 등의 다양한 인증 프로토콜에 적용될 수 있으며

HMAC 알고리즘을 이용한 HOTP를 사용하기 때문에 MitM, MitB 공격 등에 강하며, 사용할 때에는 USB 또는 네트워크에 연결할 필요가 없으므로 비밀키 관리에도 안전하다고 할 수 있다.

발명의 내용

해결하려는 과제

[0013] 본 발명은 사용자가 온라인 웹사이트에 로그인을 시도할 때, 디지털인감을 이용하여 일회용 패스워드를 생성하고, 그 패스워드를 이용하여 안전하게 로그인을 할 수 있도록 제공한다. 즉, 사용자에게 안전한 로그인 시스템을 보장해주는 것이 목적이다. 따라서 악성 해커로부터 스니핑, 키로깅, 숄더서핑, 사회공학적 기법, MitM, MitB 등의 해킹 기법으로부터 안전할 수 있으며, 비밀키 관리에 대한 문제도 해결할 수 있다.

과제의 해결 수단

[0015] 인증 서버에서 수행되는 비밀번호 인증 방법은, 디지털인감과 관련된 정보의 저장 유무에 따라 분류된 적어도 하나 이상의 프로토콜 중 어느 하나의 프로토콜을 설정하는 단계; 상기 설정된 프로토콜에 기반하여 사용자의 식별 정보가 입력됨에 따라 회원 가입을 완료하는 단계; 및 상기 설정된 프로토콜에 기반하여 상기 회원 가입이 완료된 서비스에 로그인이 수행됨에 따라 상기 사용자의 서비스 접근 권한을 제어하는 단계를 포함할 수 있다.

[0016] 상기 디지털인감과 관련된 정보의 저장 유무에 따라 분류된 적어도 하나 이상의 프로토콜 중 어느 하나의 프로토콜을 설정하는 단계는, 상기 디지털인감의 비밀키가 저장되어 있는 프로토콜 및 상기 디지털인감의 비밀키가 저장되어 있지 않은 프로토콜로 분류하는 단계를 포함할 수 있다.

[0017] 상기 설정된 프로토콜에 기반하여 사용자의 식별 정보가 입력됨에 따라 회원 가입을 완료하는 단계는, 상기 디지털인감의 비밀키가 저장되어 있는 프로토콜에 기반하여 상기 사용자의 식별 정보, 상기 사용자가 소유하고 있는 디지털인감의 인감 정보(SN)를 포함하는 사용자 정보를 웹 사이트에 입력함에 따라 상기 웹 사이트에서 상기 사용자 정보가 전달됨을 수신하는 단계; 및 상기 디지털인감의 인감 정보와 매핑되어 있는 비밀키를 검색하고, 상기 사용자의 식별 정보와 상기 검색된 비밀키(SK)를 매핑하여 회원 가입을 완료하는 단계를 포함할 수 있다.

[0018] 상기 설정된 프로토콜에 기반하여 상기 회원 가입이 완료된 서비스에 로그인이 수행됨에 따라 상기 사용자의 서비스 접근 권한을 제어하는 단계는, 비밀키가 저장된 프로토콜에 기반하여, 상기 사용자로부터 웹 사이트에 로그인하기 위하여 사용자의 식별 정보가 입력됨에 따라 상기 웹 사이트에서 전송된 상기 사용자의 식별 정보를 수신하여 랜덤챌린지를 생성하고, 상기 생성된 랜덤챌린지와 상기 사용자의 식별 정보를 결합하여 바코드를 생성하여 상기 웹 사이트에게 상기 생성된 바코드를 전달하고, 상기 웹 사이트에서 상기 전달받은 바코드가 출력됨에 따라 상기 사용자로부터 상기 사용자의 디지털인감으로 상기 바코드가 스캔되는 단계를 포함하고, 상기 디지털인감에서, 상기 사용자의 식별 정보, 상기 랜덤챌린지로 구성된 바코드 데이터 및 상기 디지털인감에 내장된 비밀키를 HOTP 알고리즘에 기반하여 제1 태그를 생성함에 따라 상기 디지털인감의 디스플레이에 상기 생성된 제1 태그가 출력될 수 있다.

[0019] 상기 설정된 프로토콜에 기반하여 상기 회원 가입이 완료된 서비스에 로그인이 수행됨에 따라 상기 사용자의 서비스 접근 권한을 제어하는 단계는, 상기 사용자로부터 상기 디지털인감의 디스플레이에 출력된 제1 태그가 비밀번호로서 웹 사이트에 입력됨에 따라 상기 웹 사이트에서 상기 사용자로부터 입력된 제1 태그가 전송됨을 수신하고, 로그인 시 입력된 사용자의 식별 정보, 상기 생성된 랜덤챌린지 및 미리 공유된 비밀키를 HOTP 알고리즘에 기반하여 제2 태그를 생성하고, 상기 사용자로부터 입력된 제1 태그와 상기 생성된 제2 태그를 비교한 결과, 제1 태그 및 제2 태그가 일치할 경우, 상기 사용자에게 상기 웹 사이트와 관련된 서비스의 접근 권한을 허가하는 단계를 포함할 수 있다.

[0020] 상기 설정된 프로토콜에 기반하여 사용자의 식별 정보가 입력됨에 따라 회원 가입을 완료하는 단계는, 비밀키가 저장되어 있지 않은 프로토콜에 기반하여 사용자로부터 상기 웹 사이트에 로그인하기 위하여 사용자의 식별 정보가 입력됨에 따라 상기 웹 사이트에서 전송된 사용자의 식별 정보를 수신하여 랜덤챌린지를 생성하고, 상기 생성된 랜덤챌린지와 상기 사용자의 식별 정보와 결합하여 바코드를 생성하여 상기 웹 사이트에게 상기 생성된 바코드를 전달하고, 상기 웹 사이트에서 상기 전달받은 바코드가 출력됨에 따라 상기 사용자로부터 상기 사용자의 디지털인감으로 상기 바코드가 스캔되는 단계를 포함하고, 상기 디지털인감에서, 상기 사용자의 식별 정보,

상기 랜덤챌린지로 구성된 바코드 데이터 및 상기 디지털인감에 내장된 비밀키를 HOTP 알고리즘에 기반하여 제3 태그를 생성함에 따라 상기 디지털인감의 디스플레이에 상기 생성된 제3 태그가 출력될 수 있다.

[0021] 상기 설정된 프로토콜에 기반하여 사용자의 식별 정보가 입력됨에 따라 회원 가입을 완료하는 단계는, 상기 사용자로부터 상기 디지털인감의 디스플레이에 출력된 제3 태그가 상기 웹 사이트에 입력됨에 따라 상기 웹 사이트에서 전송된 상기 사용자로부터 입력된 제3 태그를 수신하고, 상기 사용자의 식별 정보, 상기 랜덤챌린지 및 상기 제3 태그를 저장한 후, 회원 가입을 완료하는 단계를 포함할 수 있다.

[0022] 상기 설정된 프로토콜에 기반하여 상기 회원 가입이 완료된 서비스에 로그인이 수행됨에 따라 상기 사용자의 서비스 접근 권한을 제어하는 단계는, 비밀키가 저장되어 있지 않은 프로토콜에 기반하여, 상기 사용자로부터 웹 사이트에 로그인하기 위하여 사용자의 식별 정보가 입력됨에 따라 상기 웹 사이트에서 전송된 상기 사용자의 식별 정보를 수신하고, 상기 수신된 사용자의 식별 정보와 매핑되어 있는 랜덤챌린지를 이용하여 바코드를 생성하여 상기 웹 사이트에게 상기 생성된 바코드를 전달하고, 상기 웹 사이트에서 상기 전달받은 바코드가 출력됨에 따라 상기 사용자로부터 상기 사용자의 디지털인감으로 상기 바코드가 스캔되는 단계를 포함하고, 상기 디지털인감에서, 상기 사용자의 식별 정보, 상기 랜덤챌린지로 구성된 바코드 데이터 및 상기 디지털인감에 내장된 비밀키를 HOTP 알고리즘에 기반하여 제4 태그를 생성함에 따라 상기 디지털인감의 디스플레이에 상기 생성된 제4 태그가 출력될 수 있다.

[0023] 상기 설정된 프로토콜에 기반하여 상기 회원 가입이 완료된 서비스에 로그인이 수행됨에 따라 상기 사용자의 서비스 접근 권한을 제어하는 단계는, 상기 사용자로부터 상기 디지털인감의 디스플레이에 출력된 제4 태그가 비밀번호로서 웹 사이트에 입력됨에 따라 상기 웹 사이트에서 상기 사용자로부터 입력된 제4 태그가 전송됨을 수신하고, 상기 사용자의 회원 가입 요청 시 저장된 제3 태그와 상기 수신한 제4 태그를 비교한 결과, 상기 제3 태그와 상기 제4 태그가 일치할 경우, 상기 사용자에게 상기 웹 사이트와 관련된 서비스의 접근 권한을 허가하는 단계를 포함할 수 있다.

[0024] 상기 설정된 프로토콜에 기반하여 상기 회원 가입이 완료된 서비스에 로그인이 수행됨에 따라 상기 사용자의 서비스 접근 권한을 제어하는 단계는, 상기 로그인에 성공함에 따라 새로운 랜덤챌린지를 생성할 수 있고, 사용자의 식별 정보와 새로운 랜덤챌린지를 결합하여 새로운 바코드를 생성하고, 상기 새로운 바코드를 웹 사이트에 전송함에 따라 상기 웹 사이트가 상기 새로운 바코드를 사용자에게 출력하고 상기 사용자로부터 디지털인감으로 상기 새로운 바코드를 스캔함에 따라 입력된 제5 태그를 수신하면, 기 저장된 사용자의 식별 정보와 매핑되어 있는 랜덤챌린지와 HOTP Tag를 삭제하고, 새로운 랜덤챌린지와 상기 제5 태그를 저장하는 단계를 포함할 수 있다.

[0025] 비밀번호 인증을 위한 인증 서버는, 디지털인감과 관련된 정보의 저장 유무에 따라 분류된 적어도 하나 이상의 프로토콜 중 어느 하나의 프로토콜을 설정하는 프로토콜 설정부; 상기 설정된 프로토콜에 기반하여 사용자의 식별 정보가 입력됨에 따라 회원 가입을 완료하는 회원 가입부; 및 상기 설정된 프로토콜에 기반하여 상기 회원 가입이 완료된 서비스에 로그인이 수행됨에 따라 상기 사용자의 서비스 접근 권한을 제어하는 제어부를 포함할 수 있다.

발명의 효과

[0027] 해킹으로부터 안전할 수 있으며, 디지털인감이 안전하게 비밀키를 보관하기 때문에 비밀키 관리에 있어서 향상된 보안성을 가질 수 있다.

[0028] 용자가 온라인 웹사이트에 로그인을 시도할 때, 디지털인감을 이용하여 일회용 패스워드를 생성하고, 생성된 패스워드를 이용하여 안전하게 로그인을 할 수 있도록 제공할 수 있다.

도면의 간단한 설명

[0030] 도 1 내지 도 3은 디지털인감을 설명하기 위한 예이다.

도 4는 일 실시예에 따른 인증 서버의 구성을 설명하기 위한 블록도이다.

도 5는 일 실시예에 따른 비밀키가 인증 서버에 저장되어 있는 프로토콜에 기반한 회원 가입 과정을 설명하기

위한 흐름도이다.

도 6은 일 실시예에 따른 비밀키가 인증 서버에 저장되어 있는 프로토콜에 기반하여 로그인하는 과정을 설명하기 위한 흐름도이다.

도 7은 일 실시예에 따른 비밀키가 인증 서버에 저장되어 있지 않은 프로토콜에 기반한 회원 가입 과정을 설명하기 위한 흐름도이다.

도 8은 일 실시예에 따른 비밀키가 인증 서버에 저장되어 있지 않은 프로토콜에 기반하여 로그인하는 과정을 설명하기 위한 흐름도이다.

도 9는 일 실시예에 따른 비밀키가 인증 서버에 저장되어 있지 않은 프로토콜에서 비밀번호를 재설정하는 과정을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0031] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0032] 아래의 실시예에서는 안전한 비밀번호 인증을 위하여 디지털인감을 사용하지만, 디지털인감은 사용에 있어서 네트워크 연결 또는 USB 연결 등과 같이 외부와의 접속이 필요 없는 바코드 스캐너로 대체될 수 있고, 또한 바코드 스캐너에 따라서 바코드도 QR코드 등으로 대체될 수 있다.

[0033] 도 4는 일 실시예에 따른 인증 서버의 구성을 설명하기 위한 블록도이다.

[0034] 인증 서버(100)는 디지털인감을 이용한 안전한 비밀번호 인증 프로토콜을 제공할 수 있다. 인증 서버(100)는 프로토콜 설정부(410), 회원 가입부(420) 및 제어부(430)를 포함할 수 있다. 이러한 인증 서버(100)는 비밀번호(패스워드) 로그인 인증 시스템에 적용될 수 있다.

[0035] 프로토콜 설정부(410)는 디지털인감과 관련된 정보의 저장 유무에 따라 분류된 적어도 하나 이상의 프로토콜 중 어느 하나의 프로토콜을 설정할 수 있다. 포로토콜 설정부(410)는 디지털인감의 비밀키가 저장되어 있는 프로토콜 및 디지털인감의 비밀키가 저장되어 있지 않은 프로토콜로 분류할 수 있다. 비밀키가 인증 서버에 저장되어 있는 경우는 상대적으로 사용성을 강조한 프로토콜이며, 저장되어 있지 않은 경우는 상대적으로 보안성을 강조한 프로토콜이다.

[0036] 회원 가입부(420)는 실행된 프로토콜에 기반하여 사용자의 식별 정보가 입력됨에 따라 회원 가입을 완료할 수 있다. 회원 가입부(420)는 디지털인감의 비밀키가 저장되어 있는 프로토콜에 기반하여 사용자의 식별 정보, 사용자가 소유하고 있는 디지털인감의 인감 정보(SN)를 포함하는 사용자 정보를 웹 사이트에 입력함에 따라 웹 사이트에서 사용자 정보가 전달됨을 수신하고, 디지 인감의 인감 정보와 매핑되어 있는 비밀키를 검색하고, 사용자의 식별 정보와 검색된 비밀키(SK)를 매핑하여 회원 가입을 완료할 수 있다.

[0037] 또한, 회원 가입부(420)는 비밀키가 저장되어 있지 않은 프로토콜에 기반하여 사용자로부터 웹 사이트에 로그인하기 위하여 사용자의 식별 정보가 입력됨에 따라 웹 사이트에서 전송된 사용자의 식별 정보를 수신하여 랜덤챌린지를 생성하고, 생성된 랜덤챌린지와 사용자의 식별 정보와 결합하여 바코드를 생성하여 웹 사이트에게 생성된 바코드를 전달하고, 웹 사이트에서 전달받은 바코드가 출력됨에 따라 사용자로부터 사용자의 디지털인감으로 바코드가 스캔될 수 있다. 회원 가입부(420)는 사용자로부터 디지털인감의 디스플레이에 출력된 제3 태그(HOTP Tag)가 웹 사이트에 입력됨에 따라 웹 사이트에서 전송된 사용자로부터 입력된 제3 태그를 수신하고, 사용자의 식별 정보, 랜덤챌린지 및 제3 태그를 저장한 후, 회원 가입을 완료할 수 있다.

[0038] 제어부(430)는 실행된 프로토콜에 기반하여 회원 가입이 완료된 서비스에 로그인이 수행됨에 따라 사용자의 서비스 접근 권한을 제어할 수 있다. 제어부(430)는 비밀키가 저장된 프로토콜에 기반하여, 사용자로부터 웹 사이트에 로그인하기 위하여 사용자의 식별 정보가 입력됨에 따라 웹 사이트에서 전송된 사용자의 식별 정보를 수신하여 랜덤챌린지를 생성하고, 생성된 랜덤챌린지와 사용자의 식별 정보를 결합하여 바코드를 생성하여 웹 사이트에게 생성된 바코드를 전달하고, 웹 사이트에서 전달받은 바코드가 출력됨에 따라 사용자로부터 사용자의 디지털인감으로 바코드가 스캔될 수 있다. 제어부(430)는 사용자로부터 디지털인감의 디스플레이에 출력된 제1 태그(HOTP Tag)가 비밀번호로서 웹 사이트에 입력됨에 따라 웹 사이트에서 사용자로부터 입력된 제1 태그가 전송됨을 수신하고, 로그인 시 입력된 사용자의 식별 정보, 생성된 랜덤챌린지 및 미리 공유된 비밀키를 HOTP 알고리즘에 기반하여 제2 태그(HOTP Tag')를 생성하고, 사용자로부터 입력된 제1 태그와 생성된 제2 태그를 비교한 결과, 제1 태그 및 제2 태그가 일치할 경우, 사용자에게 웹 사이트와 관련된 서비스의 접근 권한을 허가할

수 있다.

[0039] 또한, 제어부(430)는 비밀키가 저장되어 있지 않은 프로토콜에 기반하여, 사용자로부터 웹 사이트에 로그인하기 위하여 사용자의 식별 정보가 입력됨에 따라 웹 사이트에서 전송된 사용자의 식별 정보를 수신하고, 수신된 사용자의 식별 정보와 매핑되어 있는 랜덤챌린지를 이용하여 바코드를 생성하여 웹 사이트에게 생성된 바코드를 전달하고, 웹 사이트에서 전달받은 바코드가 출력됨에 따라 사용자로부터 사용자의 디지털인감으로 바코드가 스캔될 수 있다. 제어부(430)는 사용자로부터 디지털인감의 디스플레이에 출력된 제4 태그(HOTP Tag')가 비밀번호로서 웹 사이트에 입력됨에 따라 웹 사이트에서 사용자로부터 입력된 제4 태그가 전송됨을 수신하고, 사용자의 회원 가입 요청 시 저장된 제3 태그와 수신한 제4 태그를 비교한 결과, 제3 태그와 제4 태그가 일치할 경우, 사용자에게 서비스 접근 권한을 허가할 수 있다.

[0040] 또한, 제어부(430)는 비밀키가 저장되어 있지 않은 프로토콜에 기반하여 사용자가 로그인에 성공함에 따라 새로운 랜덤챌린지를 생성할 수 있고, 사용자의 식별 정보와 새로운 랜덤챌린지를 결합하여 새로운 바코드를 생성하고, 새로운 바코드를 웹 사이트에 전송함에 따라 웹 사이트에서 새로운 바코드를 사용자에게 출력하고, 사용자로부터 디지털인감으로 새로운 바코드를 스캔함에 따라 입력된 제5 태그를 수신하면, 기 저장된 사용자의 식별 정보와 매핑되어 있는 랜덤챌린지와 HOTP Tag를 삭제하고, 새로운 랜덤챌린지와 제5 태그를 저장할 수 있다.

[0041] 도 5는 일 실시예에 따른 비밀키가 인증 서버에 저장되어 있는 프로토콜에 기반한 회원 가입 과정을 설명하기 위한 흐름도이다.

[0042] 비밀키가 인증 서버에 저장되어 있는 프로토콜은 회원 가입 단계, 로그인 단계로 구성될 수 있으며, 다음과 같이 세 가지 사항을 가정한다.

[0043] (1) 사용자는 인증 서버를 관리하는 기관으로부터 고유의 시리얼넘버가 부여되고 시리얼넘버와 1:1로 매핑되어 있는(저장되어 있는) 비밀키와 HOTP 알고리즘이 내장된 디지털인감을 발급 받았다.

[0044] (2) 인증 서버는 내부 데이터베이스에 사용자에게 발급한 디지털인감의 비밀키를 안전하게 저장하고 있으며, HOTP 알고리즘을 사용할 수 있다.

[0045] (3) 사용자가 로그인하는 웹사이트는 안전하게 인증 서버와 연결되어 있다.

[0046] 이하, 비밀키가 인증 서버에 저장되어 있는 프로토콜에 기반하여 회원 가입, 로그인을 수행하는 과정을 도 5 및 도 6에서 상세히 설명하기로 한다.

[0047] 사용자(500)는 웹 사이트(510)에서 회원 가입을 할 때, 사용자의 식별 정보(예를 들면, ID)를 설정할 수 있다. 사용자는 사용자의 식별 정보, 디지털인감의 인감 정보(SN)를 포함하는 사용자 정보를 웹사이트(510)에 입력할 수 있다(501). 다시 말해서, 사용자(500)는 아이디를 설정하고, 사용자가 소유하고 있는 디지털인감의 시리얼넘버와 그 이외의 다른 기타 정보를 웹 사이트(510)에 입력할 수 있다. 이때, 웹 사이트에서는 비밀번호 설정을 요구하지 않는다.

[0048] 웹 사이트(510)는 사용자의 식별 정보, 디지털인감의 인감 정보(SN)를 포함하는 사용자 정보를 인증 서버(100)로 전송할 수 있다(502). 인증 서버(100)는 웹 사이트(510)를 통하여 전달받은 사용자가 소유하고 있는 디지털인감의 시리얼 넘버(SN)와 디지털인감의 시리얼 넘버와 매칭되어 있는 비밀키(SK)를 검색하여 사용자의 식별 정보와 매핑시킬 수 있다(503). 이러한 과정은 사용자와 인증 서버(100)가 안전하게 비밀키를 공유하는 것을 의미한다. 이러한 과정이 완료되면 회원 가입이 완료될 수 있다.

[0049] 도 6은 일 실시예에 따른 비밀키가 인증 서버에 저장되어 있는 프로토콜에 기반하여 로그인하는 과정을 설명하기 위한 흐름도이다.

[0050] 사용자(500)는 웹 사이트에 로그인하기 위하여 사용자의 식별 정보(예를 들면, ID)를 입력할 수 있다(601). 웹 사이트(510)는 사용자로부터 입력된 사용자의 식별 정보를 인증 서버(100)로 전송할 수 있다(602). 인증 서버(100)는 랜덤챌린지를 생성한 후, 생성된 랜덤챌린지를 사용자로부터 입력된 식별 정보와 결합하여 바코드를 생성할 수 있다(603). 인증 서버(100)는 생성된 바코드를 웹 사이트(510)에게 전달할 수 있다(604).

[0051] 웹 사이트(510)는 인증 서버(100)로부터 전달받은 바코드를 사용자(500)에게 출력할 수 있다(605). 사용자(500)는 사용자가 소유하고 있는 디지털인감으로 바코드를 스캔할 수 있다(606). 이때, 디지털인감은 사용자의 식별 정보(예를 들면, ID)와 랜덤챌린지(RC)로 구성된 바코드 데이터 및 디지털인감에 내장된 비밀키(SK)를 그 알고리즘으로 HOTP Tag를 생성하여 디스플레이에 출력할 수 있다. 사용자(500)는 디지털인감의 디스플레이에

출력된 HOTP Tag를 비밀번호로서 웹사이트(510)에 입력할 수 있다(607).

[0052] 웹사이트(510)는 사용자(500)로부터 입력받은 HOTP Tag를 인증 서버(100)로 전송할 수 있다(608). 인증 서버(100)는 사용자로부터 웹 사이트(510)에 로그인하기 위하여 입력된 사용자의 식별 정보(예를 들면, ID), 생성되어 있는 랜덤챌린지 및 미리 공유된 비밀키를 HOTP 알고리즘을 사용하여 HOTP Tag'을 생성할 수 있다(609). 인증 서버(100)는 사용자로부터 입력받은 HOTP Tag와 직접 생성한 HOTP Tag'을 비교할 수 있다. 인증 서버(100)는 입력받은 HOTP Tag와 직접 생성한 HOTP Tag'을 비교함에 따른 인증 결과를 웹 사이트(510)에 전달할 수 있고(610), 웹 사이트(510)에서 사용자에게 인증 서버(100)로부터 전달받은 인증 결과를 제공할 수 있다(611). 예를 들면, HOTP Tag와 HOTP Tag'이 동일하다면, 로그인을 시도한 사용자가 자신이 입력한 아이디와 매핑되어 있는 비밀키를 공유하고 있는 올바른 사용자라는 것이 증명되기 때문에, 인증 서버(100)는 사용자에게 서비스의 접근 권한을 허가하고, 그렇지 않으면 허가하지 않는다.

[0053] 도 7은 일 실시예에 따른 비밀키가 인증 서버에 저장되어 있지 않은 프로토콜에 기반한 회원 가입 과정을 설명하기 위한 흐름도이다.

[0054] 또한, 비밀키가 인증 서버에 저장되어 있지 않은 프로토콜은 회원 가입 단계, 로그인 단계, 비밀번호 재설정 단계로 구성되어 있으며, 다음과 같이 두 가지 사항을 가정한다.

[0055] (1) 사용자는 인증 서버를 관리하는 기관으로부터 고유의 비밀키와 HOTP 알고리즘이 내장된 디지털인감을 발급받았다.

[0056] (2) 사용자가 로그인하는 웹사이트는 안전하게 인증 서버와 연결되어 있다.

[0057] 이하, 비밀키가 인증 서버에 저장되어 있는 프로토콜에 기반하여 회원 가입, 로그인을 수행하는 과정을 도 7 및 도 8에서 상세히 설명하기로 한다.

[0058] 사용자(500)는 웹 사이트(510)에서 회원 가입을 할 때, 사용자의 식별 정보(예를 들면, ID)를 설정할 수 있다. 사용자는 사용자의 식별 정보를 웹사이트(510)에 입력할 수 있다(701). 웹 사이트(510)는 사용자(500)로부터 입력된 사용자의 식별 정보를 인증 서버(100)로 전송할 수 있다. 인증 서버(100)는 랜덤챌린지(RC)를 생성한 후, 생성된 랜덤챌린지와 사용자의 식별 정보를 결합하여 바코드를 생성할 수 있다(703). 인증 서버(100)는 생성된 바코드를 웹 사이트(510)로 전송할 수 있다(704). 웹 사이트(510)는 인증 서버(100)로부터 수신된 바코드를 사용자에게 출력할 수 있다(705). 사용자는 사용자가 소유하고 있는 디지털인감으로 바코드를 스캔할 수 있다(706). 이때, 디지털인감은 사용자의 식별 정보와 랜덤챌린지로 구성되어 있는 바코드의 바코드 데이터, 디지털인감에 내장된 비밀키 및 HOTP 알고리즘에 기반하여 HOTP Tag를 생성하여 바코드의 디스플레이(LCD)에 출력할 수 있다. 사용자(500)는 디지털인감의 디스플레이에 출력된 HOTP Tag를 웹 사이트(510)에 입력할 수 있다(707).

[0059] 웹 사이트(510)는 사용자(500)로부터 입력된 HOTP Tag를 인증 서버(100)로 전송할 수 있다(708). 인증 서버(100)는 사용자의 식별 정보, 랜덤챌린지 및 HOTP Tag를 저장할 수 있다(709). 이에 따라 인증 서버(100) 회원 가입을 완료할 수 있다. 이때, 회원 가입 시 비밀번호 설정은 요구되지 않는다.

[0060] 도 8은 일 실시예에 따른 비밀키가 인증 서버에 저장되어 있지 않은 프로토콜에 기반하여 로그인하는 과정을 설명하기 위한 흐름도이다.

[0061] 사용자(510)는 웹 사이트(510)에 로그인하기 위하여 사용자의 식별 정보(예를 들면, ID)를 입력할 수 있다(801). 웹 사이트(510)는 사용자의 식별 정보를 인증 서버(100)로 전송할 수 있다(802). 인증 서버(100)는 사용자로부터 입력받은 사용자의 식별 정보와 매핑되어 있는 랜덤챌린지(RC)를 탐색할 수 있고, 탐색된 랜덤챌린지와 사용자의 식별 정보를 이용하여 바코드를 생성할 수 있다(803). 인증 서버(100)는 바코드를 웹 사이트에게 전송할 수 있다(804). 웹 사이트(510)는 바코드를 사용자(500)에게 출력할 수 있다(805). 사용자(500)는 사용자가 소유하고 있는 디지털인감으로 바코드를 스캔할 수 있다(806). 이때, 디지털인감은 사용자의 식별 정보와 랜덤챌린지로 구성된 바코드 데이터 및 디지털인감에 내장된 비밀키를 HOTP 알고리즘으로 HOTP Tag`을 생성하여 디지털인감의 디스플레이에 HOTP Tag`를 출력할 수 있다. 사용자(500)는 생성된 HOTP Tag`를 비밀번호로서 웹 사이트(510)에 입력할 수 있다(807). 웹 사이트(510)는 인증 서버(100)로 사용자로부터 전달받은 HOTP Tag`를 전송할 수 있다(808).

[0062] 인증 서버(100)는 기존에 저장되어 있던 사용자의 HOTP Tag와 HOTP Tag`을 비교할 수 있다(809). 인증 서버(100)는 HOTP Tag와 HOTP Tag`를 비교한 인증 결과를 웹 사이트(510)에 전송할 수 있다(810). 웹 사이트(51

0)는 사용자에게 인증 결과를 전송할 수 있다(811). 만약 HOTP Tag와 HOTP Tag`이 동일하다면, 로그인을 시도한 사용자가 자신이 입력한 아이디에 매핑되어 있는 HOTP Tag와 같은 HOTP Tag`을 생성했다는 것이기 때문에, 올바른 사용자라는 것이 증명된다. 인증 서버(100)는 HOTP Tag와 HOTP Tag`를 비교한 결과가 동일할 경우, 사용자에게 서비스 접근 권한을 허가하고, 그렇지 않으면 허가하지 않는다.

[0063] 도 9는 일 실시예에 따른 비밀키가 인증 서버에 저장되어 있지 않은 프로토콜에서 비밀번호를 재설정하는 과정을 설명하기 위한 흐름도이다.

[0064] 비밀키가 인증 서버에 저장되어 있는 프로토콜은 사용자(500)가 로그인을 시도할 때마다, 인증 서버(100)는 매번 새로운 랜덤챌린지를 생성하여 사용할 수 있다. 그로 인해 HOTP Tag과 HOTP Tag`이 매번 변경되기 때문에, 매번 다른 비밀번호를 사용하게 된다.

[0065] 이에 반해, 비밀키가 인증 서버에 저장되어 있지 않은 프로토콜은 사용자(500)가 로그인을 시도할 때, 이전에 저장되어 있는 랜덤챌린지를 사용하기 때문에 매번 변경되지 않는 HOTP Tag와 HOTP Tag`이 사용되고, 그로 인해 고정된 비밀번호를 사용하게 된다. 이를 해결하기 위해 비밀번호 재설정 단계가 요구된다.

[0066] 사용자(500)가 로그인에 성공하면 인증 서버(100)는 새로운 랜덤챌린지를 생성할 수 있고, 사용자의 식별 정보와 새로운 랜덤챌린지를 결합하여 새로운 바코드를 생성할 수 있다(901). 인증 서버(100)는 새로운 바코드를 웹 사이트(510)에 전송할 수 있다(902). 웹 사이트는 인증 서버(100)로부터 전송받은 새로운 바코드를 사용자(500)에게 출력할 수 있다(903). 사용자는 사용자가 소유하고 있는 디지털인감으로 바코드를 스캔할 수 있다(904). 디지털인감으로 바코드를 스캔한 후, 사용자(500)가 디지털인감에 출력된 HOTP Tag를 확인하고 웹 사이트에 HOTP Tag를 입력할 수 있다(905). 웹 사이트(510)는 사용자로부터 입력된 HOTP Tag를 인증 서버(100)로 전송할 수 있다(906). 인증 서버(100)는 기존에 사용자의 식별 정보와 매핑되어 있는 랜덤챌린지와 HOTP Tag를 삭제하고, 새로운 랜덤챌린지와 HOTP Tag를 저장할 수 있다(907). 인증 서버(100)는 저장된 새로운 랜덤챌린지와 HOTP Tag는 다음번 로그인에 사용할 수 있다. 이때, 사용자로부터 로그인될 때마다 이러한 단계가 반복되어 매번 저장된 랜덤챌린지와 HOTP Tag는 매번 새로운 것으로 변경(업데이트)될 수 있다. 그에 따라 사용자는 매번 변경된 비밀번호를 사용할 수 있게 된다.

[0067] 기존에 연구되어 왔던 키 입력 패턴 인식, 스마트 폰에서 진동을 이용한 인증 방법 등의 다양한 인증 기법 및 프로토콜은 플랫폼(데스크탑, 스마트폰 등)에 제한적이었으나, 일 실시예에 따른 디지털인감을 이용한 안전한 비밀번호 인증 프로토콜은 플랫폼에 상관없이 어디에나 적용하여 사용이 가능하다.

[0068] 기존에 사용되고 있는 Time-synchronized OTP, HOTP, Challenge-Response OTP, 보안카드 등의 보안 도구는 비밀번호와 함께 사용해야 하기 때문에 2-FACTOR 인증인 반면, 일 실시예에 따른 디지털인감을 이용한 안전한 비밀번호 인증 프로토콜은 1-FACTOR 인증이기 때문에 더 간편하게 인증을 수행할 수 있다.

[0069] 일 실시예에 따른 디지털인감을 이용한 안전한 비밀번호 인증 프로토콜에서 비밀번호 역할을 하는 HOTP Tag는 로그인 할 때마다 변경이 되므로, 스니핑, 키로깅, 숄더서핑 공격으로부터 유출되어도 재사용될 수 없다. 또한 이러한 특징으로 사용자는 여러 사이트에 비밀번호를 각각 다르게 설정하는 것과 같은 효과를 획득할 수 있고, 따라서 향상된 보안성을 가질 수 있다.

[0070] 사용자가 로그인을 시도할 때에는, 공격자가 HOTP Tag를 유추하려고 시도해도 HOTP Tag의 엔트로피(무질서도)가 높기 때문에 쉽게 유추할 수 없다. 또한 사용자와 비밀번호간의 관계성이 낮으므로 공격자는 사회공학적 기법으로 HOTP Tag를 쉽게 유추할 수 없다.

[0071] 디지털인감에 내장되어 있는 비밀키는 디지털인감을 이용한 안전한 비밀번호 인증 프로토콜에서 HOTP Tag 생성에 필요한 요인 중 하나이므로 외부로부터 안전하게 보관되어야 한다. 사용자가 디지털인감을 사용할 때에는 네트워크에 연결하거나 USB에 연결하여 사용하지 않아도 되므로 공격자는 디지털인감에 내장되어 있는 비밀키를 탈취할 수 없다. 공격자가 침투할 수 있는 경로가 존재하지 않기 때문이다.

[0072] 기존에 연구되어 왔던 키 입력 패턴 인식, 스마트 폰에서 진동을 이용한 인증 방법 등의 다양한 인증 기법 및 프로토콜은 사용자의 비밀번호 또는 사용자의 패턴 입력 특징이 스니핑, 키로깅, 숄더서핑 등으로 유출되었을 때 보안 사고를 야기할 수 있지만, 일 실시예에 따른 디지털인감을 이용한 안전한 비밀번호 인증 프로토콜은 유출이 되어도 One Time Password 특징을 가지고 있기 때문에, 유출된 비밀번호를 다시 사용할 수 없다. 그리고 원패스워드는 소프트웨어 솔루션이므로 비밀키 관리에 취약할 수 있지만, 실시예에 따른 디지털인감을 이용한 안전한 비밀번호 인증 프로토콜에서는 디지털인감이 안전하게 비밀키를 보관하므로, 비밀키 관리에 있어서 더

향상된 보안성을 가질 수 있다.

[0073] 기존에 사용되고 있는 Time-synchronized OTP는 시간차 공격에 취약하고, 엔티티(Entity) 기반 인증이므로 MitM, MitB 공격에 취약하다. HOTP는 사용할 때 네트워크에 연결되어 있는 스마트 폰의 어플리케이션 또는 PC의 어플리케이션이 필요하므로, 비밀키 관리에 문제가 있을 수 있다. 공격자가 비밀키를 탈취할 수 있는 경로가 존재하기 때문이다. Challenge-Response OTP는 Exhaustive Key Search 공격에 취약하며, 스마트폰 또는 PC에서 Response를 하게 되면 HOTP와 같이 비밀키 관리에 문제가 있을 수 있다. 보안카드는 랜덤한 수가 제한적이므로 장기간 스니핑 등에 취약하고, 보안카드를 스마트 폰에 이미지로 저장하여 사용하는 경우에는 이미지 유출을 통해 보안카드 전체가 유출 될 수 있는 가능성도 존재한다. 이렇게 기존에 존재하는 여러 OTP들은 다양한 취약점이 존재하는 반면, 디지털인감을 이용한 안전한 비밀번호 인증 프로토콜은 HOTP를 이용하기 때문에 MitM, MitB 등의 공격을 방어할 수 있고, 네트워크 또는 USB 연결이 필요 없는 디지털인감 내부에 비밀키를 안전하게 보관하고 있기 때문에 비밀키 관리에 문제를 해결할 수 있다. 또한 사용될 수 있는 HOTP Tag의 수가 제한적이지 않기 때문에 보안카드보다 더욱 더 안전하다.

[0074] 사용자가 로그인을 시도할 때마다 매번 다른 비밀번호를 제공하는 안전한 비밀번호 인증 프로토콜을 제공하는 프로토콜로서, 온라인, 모바일 뱅킹, 메신저, 메일, 게임 서비스 등의 로그인이 필요한 모든 시스템에서 사용될 수 있다.

[0075] 온라인, 모바일 뱅킹, 게임, 메일, 메신저 서비스 등의 다양한 온라인 서비스 시장이 증가함에 따라 발생하는 금전적 피해 사례를 막기 위하여 사용될 수 있다. 현재 사용되고 있는 일반적인 비밀번호 인증 프로토콜보다 더 높은 보안성을 사용자들에게 가져다 줄 것으로 기대된다.

[0076] 인증 프로토콜이 사용되는 다양한 온라인, 모바일 뱅킹, 게임, 메일, 메신저, 방송 서비스에서 사용될 수 있다. 인증 프로토콜이라는 것은 국내에서 한정적으로 사용되는 것이 아니라 국제적으로 대부분의 온라인 서비스가 사용 중인 시스템이므로 대량 생산 시스템을 도입하여 작은 비용으로 디지털인감을 생산할 수 있다면 전 세계 사용자들이 안전하게 인증을 할 수 있는 효과를 도출할 수 있다.

[0077] 나날이 악성 해커들의 공격 기법이 발전함에 따라, 국내뿐만 아니라 세계적으로도 사용 중인 인증 프로토콜이 공격당하는 사례가 많아지고 있는 상황에서, 보안은 더 이상 선택적인 요소가 아니라 필수적인 요소이므로, 국내/외 시장에서 많은 호응을 얻을 수 있을 것이다.

[0078] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0079] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0080] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히

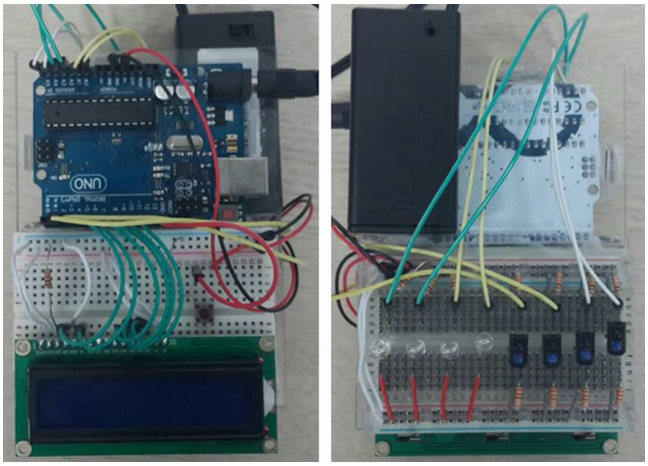
설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0081] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

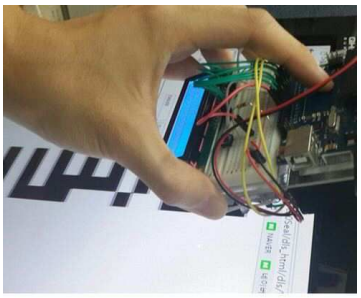
[0082] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

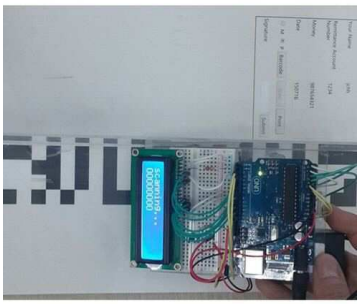
도면

도면1

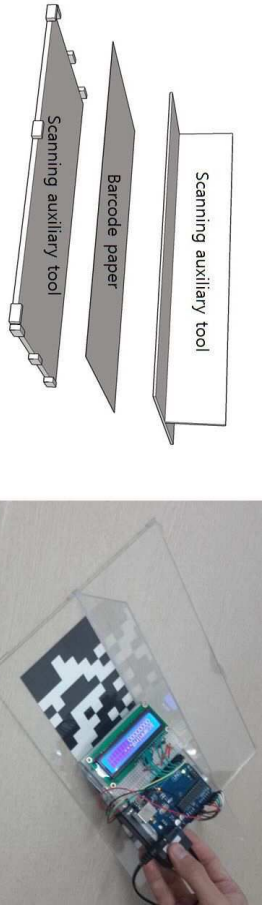


도면2

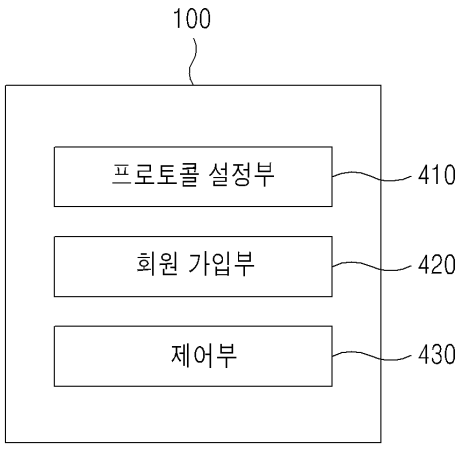




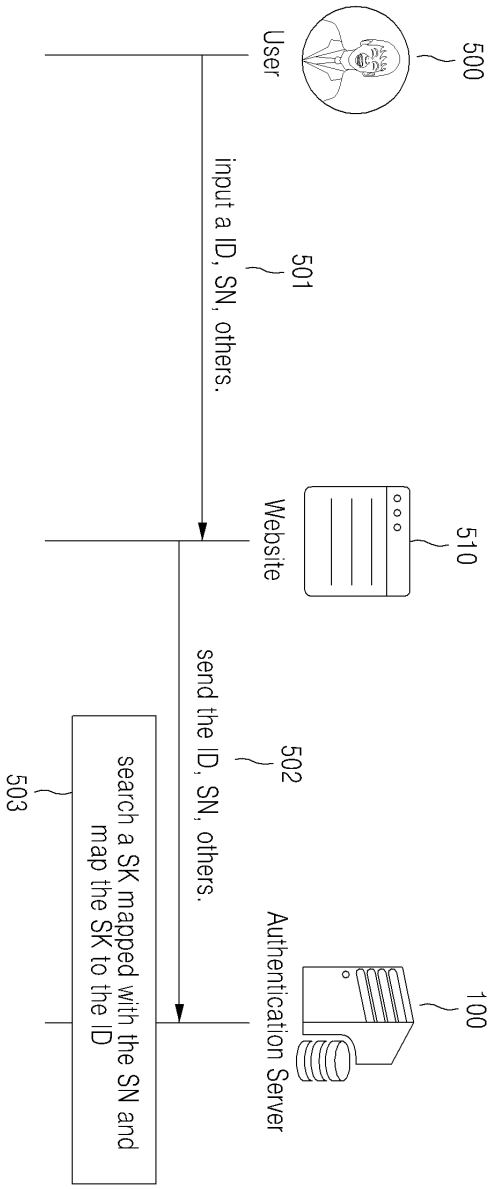
도면3


Scanning auxiliary tool
Barcode paper
Scanning auxiliary tool

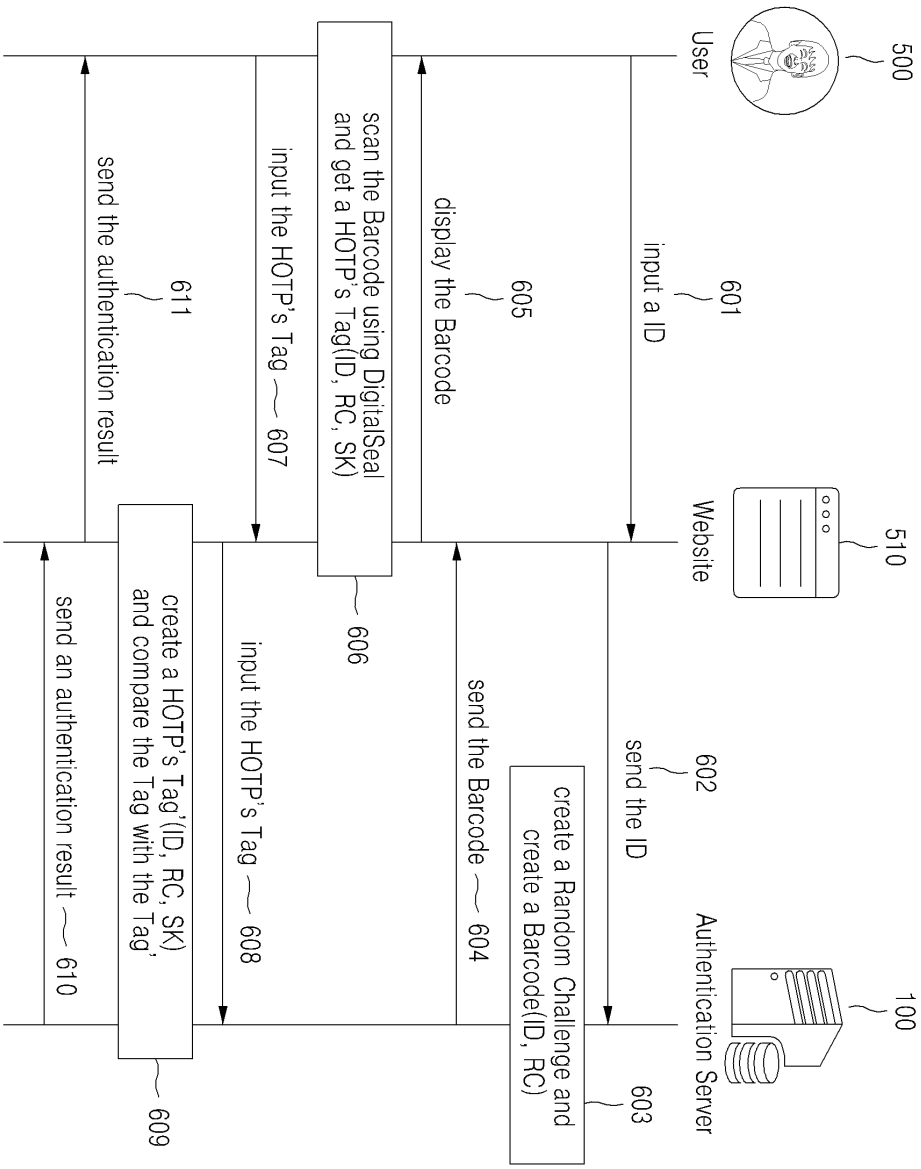
도면4


100
프로토콜 설정부
410
회원 가입부
420
제어부
430

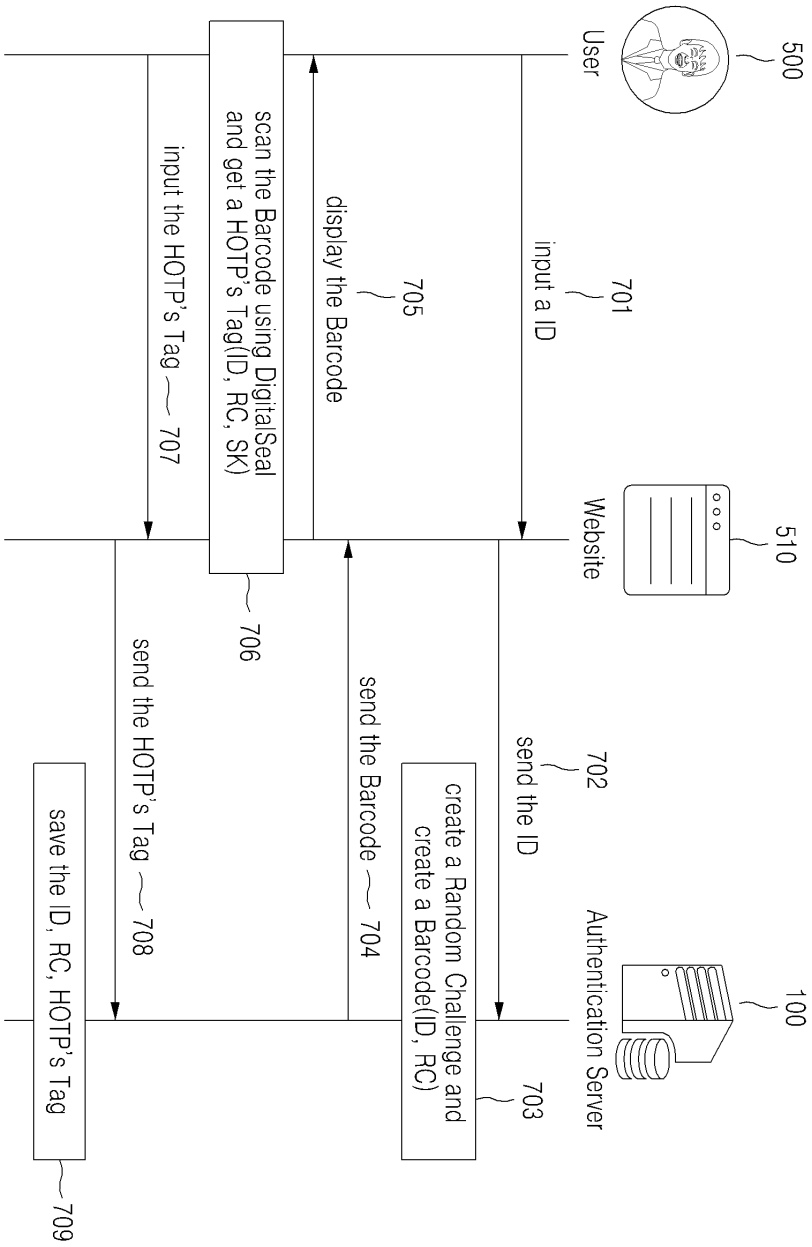
도면5


User
500
input a ID, SN, others.
501
Website
510
send the ID, SN, others.
502
search a SK mapped with the SN and map the SK to the ID
503
Authentication Server
100

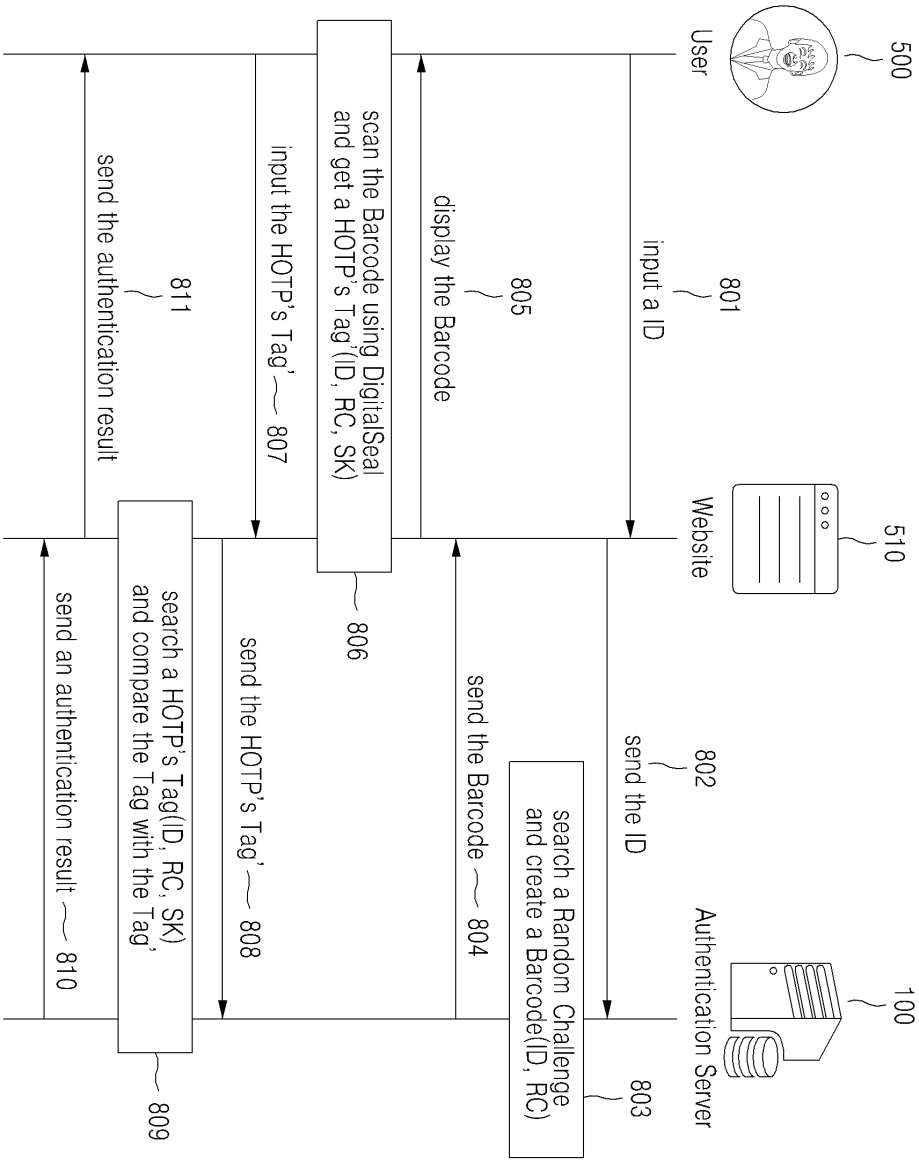
도면6


User
500
Website
510
Authentication Server
100
input a ID
601
send the ID
602
create a Random Challenge and
create a Barcode(ID, RC)
603
send the Barcode
604
display the Barcode
605
scan the Barcode using DigitalSeal
and get a HOTP's Tag(ID, RC, SK)
606
input the HOTP's Tag
607
input the HOTP's Tag
608
create a HOTP's Tag'(ID, RC, SK)
and compare the Tag with the Tag'
609
send an authentication result
610
send the authentication result
611

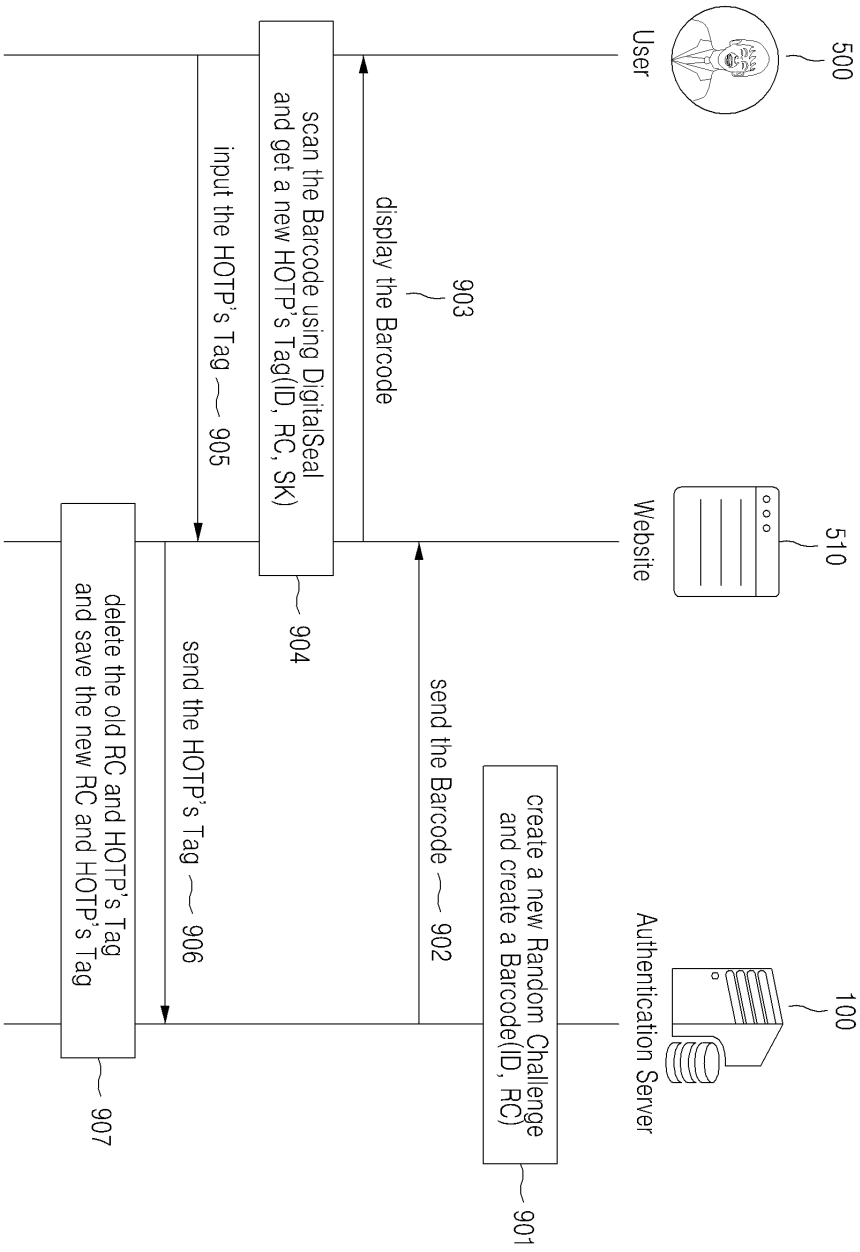
도면7


User
500
Website
510
Authentication Server
100
input a ID
701
send the ID
702
create a Random Challenge and
create a Barcode(ID, RC)
703
send the Barcode
704
display the Barcode
705
scan the Barcode using DigitalSeal
and get a HOTP's Tag(ID, RC, SK)
706
input the HOTP's Tag
707
send the HOTP's Tag
708
save the ID, RC, HOTP's Tag
709

도면8


User
500
Website
510
Authentication Server
100
input a ID
801
send the ID
802
search a Random Challenge and create a Barcode(ID, RC)
803
send the Barcode
804
display the Barcode
805
scan the Barcode using DigitalSeal and get a HOTP's Tag'(ID, RC, SK)
806
input the HOTP's Tag'
807
send the HOTP's Tag'
808
search a HOTP's Tag(ID, RC, SK) and compare the Tag with the Tag'
809
send an authentication result
810
send the authentication result
811

도면9


User
500
Website
510
Authentication Server
100
create a new Random Challenge and create a Barcode(ID, RC)
901
send the Barcode
902
display the Barcode
903
scan the Barcode using DigitalSeal and get a new HOTP's Tag(ID, RC, SK)
904
input the HOTP's Tag
905
send the HOTP's Tag
906
delete the old RC and HOTP's Tag and save the new RC and HOTP's Tag
907