(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2017 년 6 월 29 일 (29.06.2017)

WIPO | PCT

(10) 국제공개번호
WO 2017/111383 A1

(51) 국제특허분류:
H04L 9/32 (2006.01) *G06K 9/00* (2006.01)
H04L 9/08 (2006.01)

(21) 국제출원번호: PCT/KR2016/014628

(22) 국제출원일: 2016 년 12 월 14 일 (14.12.2016)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2015-0185450 2015 년 12 월 23 일 (23.12.2015) KR

(71) 출원인: **주식회사 케이티 (KT CORPORATION)** [KR/KR]; 13606 경기도 성남시 분당구 불정로 90, Gyeonggi-do (KR).

(72) 발명자: **김태균 (KIM, Tae-Gyun)**; 13618 경기도 성남시 분당구 미금로 215, 806 동 1502 호, Gyeonggi-do (KR). **조대성 (CHO, Daesung)**; 06113 서울시 강남구 강남대로 126 길 76, 302 호, Seoul (KR). **이인수 (LEE, In-Soo)**; 16936 경기도 용인시 수지구 상현로 88, 282 동 504 호, Gyeonggi-do (KR). **장덕문 (CHANG, Deok-Moon)**; 06762 서울시 서초구 바우뫼로 7 길 51, 104 동 1403 호, Seoul (KR).

(74) 대리인: **유미특허법인 (YOU ME PATENT AND LAW FIRM)**; 06134 서울시 강남구 테헤란로 115, Seoul (KR).

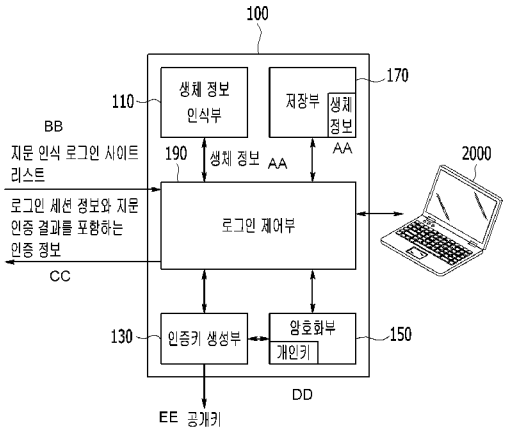
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[다음 쪽 계속]

(54) Title: BIOMETRIC DATA-BASED AUTHENTICATION DEVICE, CONTROL SERVER LINKED TO SAME, AND BIOMETRIC DATA-BASED LOGIN METHOD FOR SAME

(54) 발명의 명칭 : 생체 정보 기반 인증 장치, 이와 연동하는 제어 서버, 그리고 이들의 생체 정보 기반 로그인 방법



110 ... Biometric data recognition unit
130 ... Authentication key generation unit
150 ... Encoding unit
170 ... Storage unit
190 ... Login control unit
AA ... Biometric data
BB ... Fingerprint recognition login site list
CC ... Authentication information comprising fingerprint authentication result and login session information
DD ... Private key
EE ... Public key

(57) **Abstract**: The present invention relates to a method for a biometric data-based authentication device being linked to a control server and processing a website login requested from a computing device. The method comprises the steps of: detecting a login request message transmitted from the computing device to a website server which is for providing a website; extracting login session information from the login request message; outputting a biometric data authentication result on biometric data that has been received; and transmitting, to the control server, authentication information comprising the biometric data authentication result and the login session information, wherein the login session information is information transmitted from the control server to the website server and used when determining a login-permitted account by the website server.

(57) **요약서**: 생체 정보 기반 인증 장치가 제어 서버와 연동하여 컴퓨팅 장치에서 요청된 웹사이트의 로그인을 처리하는 방법으로서, 상기 컴퓨팅 장치로부터 상기 웹사이트를 제공하는 웹사이트 서버로 전달되는 로그인 요청 메시지를 탐지하는 단계, 상기 로그인 요청 메시지로부터 로그인 세션 정보를 추출하는 단계, 입력받은 생체 정보에 대한 생체 정보 인증 결과를 출력하는 단계, 그리고 상기 로그인 세션 정보와 상기 생체 정보 인증 결과를 포함하는 인증 정보를 상기 제어 서버로 전송하는 단계를 포함하고, 상기 로그인 세션 정보는 상기 제어 서버에서 상기 웹사이트 서버로 전달되어 상기 웹사이트 서버의 로그인 허용 대상 판단 시 사용되는 정보이다.

WO 2017/111383 A1

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

명세서

발명의 명칭: 생체 정보 기반 인증 장치, 이와 연동하는 제어 서버, 그리고 이들의 생체 정보 기반 로그인 방법

기술분야

[1] 본 발명은 생체 정보 기반 인증에 관한 것이다.

배경기술

[2] 웹사이트는 사용자 인증을 위해 지정된 로그인 방법을 정하고, 사용자에게 로그인을 요청한다. 지금까지의 로그인 방법은 사용자가 웹사이트 가입 시 등록한 아이디와 패스워드를 사용하는 방법, 또는 공인인증서를 사용하는 방법, 통신사에 가입된 사용자의 휴대 단말 번호를 사용하는 방법 등이 존재한다.

[3] 그러나, 아이디와 패스워드 기반 로그인은 해킹 등으로 노출될 가능성이 높고, 사용자가 웹사이트별 아이디와 패스워드를 기억해야 하는 불편함이 있다. 공인인증서 기반 로그인은 공인인증서가 저장된 단말에서만 사용 가능하므로, 사용자가 공인인증서로 로그인할 수 있는 환경이 제한적이다. 또한, 사용자의 휴대 단말 번호를 통한 로그인은 사용자가 자신의 휴대 단말 번호를 입력하여 인증번호를 요청하고, 수신한 인증번호를 다시 입력해야 하는 번거로움이 있다.

[4] 한편, 사용자의 고유한 생체 정보를 웹사이트에 등록하고, 생체 정보의 동일성 여부로 사용자를 인증할 수 있다. 그러나, 웹사이트가 생체 정보 기반 로그인을 위해 개별적으로 생체 정보 입력 및 인증 처리를 위한 각종 프로그램을 구현해야 하고, 사용자의 고유 정보를 관리해야 하는 부담이 있다. 또한, 웹사이트는 자신만의 로그인을 위해 생체 정보 센서를 사용자에게 발급해야 하므로 현실적으로 생체 정보 기반 로그인이 활성화되기 어렵다.

발명의 상세한 설명

기술적 과제

[5] 본 발명이 해결하고자 하는 과제는 생체 정보 기반 인증 장치, 이와 연동하는 제어 서버, 그리고 이들의 생체 정보 기반 로그인 방법을 제공하는 것이다.

과제 해결 수단

[6] 본 발명의 한 실시예에 따른 생체 정보 기반 인증 장치가 제어 서버와 연동하여 컴퓨팅 장치에서 요청된 웹사이트의 로그인을 처리하는 방법으로서, 상기 컴퓨팅 장치로부터 상기 웹사이트를 제공하는 웹사이트 서버로 전달되는 로그인 요청 메시지를 탐지하는 단계, 상기 로그인 요청 메시지로부터 로그인 세션 정보를 추출하는 단계, 입력받은 생체 정보에 대한 생체 정보 인증 결과를 출력하는 단계, 그리고 상기 로그인 세션 정보와 상기 생체 정보 인증 결과를 포함하는 인증 정보를 상기 제어 서버로 전송하는 단계를 포함하고, 상기 로그인 세션 정보는 상기 제어 서버에서 상기 웹사이트 서버로 전달되어 상기 웹사이트 서버에서 로그인 허용 대상 판단 시 사용되는 정보이다.

[7] 상기 로그인 방법은 상기 제어 서버로부터 생체 정보 로그인 사이트들의 정보를 포함하는 화이트 리스트를 수신하는 단계를 더 포함하고, 상기 로그인 세션 정보를 추출하는 단계는 상기 로그인 요청 메시지를 기초로 상기 웹사이트 서버가 상기 화이트 리스트에 해당하는지 판단하는 단계, 그리고 상기 웹사이트 서버가 상기 화이트 리스트에 해당하는 경우, 상기 로그인 요청 메시지에 포함된 세션키를 상기 로그인 세션 정보로 추출하는 단계를 포함할 수 있다.

[8] 상기 로그인 세션 정보는 상기 세션키와 상기 웹사이트의 식별 정보를 포함하고, 상기 웹사이트의 식별 정보는 상기 화이트 리스트에 포함되어 있을 수 있다.

[9] 상기 로그인 방법은 상기 웹사이트 서버가 상기 화이트 리스트에 해당하는 경우, 센서를 활성화하는 단계를 더 포함할 수 있다.

[10] 상기 생체 정보 인증 결과를 출력하는 단계는 저장된 생체 정보와 상기 입력받은 생체 정보를 비교하여 상기 생체 정보 인증 결과를 출력할 수 있다.

[11] 상기 인증 정보를 상기 제어 서버로 전송하는 단계는 상기 인증 정보를 개인키로 서명하여 상기 제어 서버로 전송하고, 상기 제어 서버는 상기 개인키와 쌍을 이루는 공개키를 저장하며, 상기 공개키와 상기 개인키는 상기 인증 장치를 등록할 때 생성되는 정보일 수 있다.

[12] 상기 로그인 요청 메시지를 탐지하는 단계 이전에 인증 장치 등록 단계를 더 포함하고, 상기 인증 장치 등록 단계는 상기 컴퓨팅 장치로부터 상기 제어 서버로 전달되는 제1 식별 정보를 탐지하는 단계, 상기 제1 식별 정보가 자신의 식별 정보와 같은지 판단하는 단계, 상기 제1 식별 정보가 자신의 식별 정보와 같은 경우, 센서를 활성화하는 단계, 상기 센서로부터 입력된 생체 정보를 등록하는 단계, 그리고 키 생성 알고리즘을 기초로 공개키와 개인키를 생성하는 단계를 포함할 수 있다.

[13] 본 발명의 한 실시예에 따른 제어 서버가 생체 정보 기반 인증 장치와 연동하여 컴퓨팅 장치에서 요청된 웹사이트의 로그인을 처리하는 방법으로서, 생체 정보 로그인 사이트들의 정보를 포함하는 화이트 리스트를 상기 인증 장치로 전송하는 단계, 상기 인증 장치로부터 로그인 세션 정보와 생체 정보 인증 결과를 포함하는 인증 정보를 수신하는 단계, 그리고 상기 로그인 세션 정보에 관련된 웹사이트 서버로 상기 로그인 세션 정보에 대한 로그인 허용을 요청하는 단계를 포함한다.

[14] 상기 로그인 세션 정보는 세션키와 상기 웹사이트의 식별 정보를 포함하고, 상기 세션키는 상기 컴퓨팅 장치와 상기 웹사이트 서버 사이에 연결된 세션을 특정하는 값이며, 상기 웹사이트는 상기 화이트 리스트에 포함되는 사이트일 수 있다.

[15] 상기 로그인 허용을 요청하는 단계는 상기 인증 정보의 진위 여부를 판단하는 단계, 상기 인증 정보가 신뢰 정보이고 상기 생체 정보 인증 결과가 성공인 경우, 상기 화이트 리스트에서 상기 인증 정보에 포함된 상기 웹사이트의 식별 정보에

해당하는 상기 웹사이트 서버를 찾는 단계, 그리고 상기 웹사이트 서버로 상기 세션키에 대한 로그인 허용을 요청하는 단계를 포함할 수 있다.

[16] 상기 인증 장치로부터 수신한 공개키를 저장하는 단계를 더 포함하고, 상기 인증 정보의 진위 여부를 판단하는 단계는 상기 공개키를 이용하여 상기 인증 정보를 복호하고, 복호 결과를 기초로 진위 여부를 판단하며, 상기 인증 정보는 상기 공개키와 쌍을 이루는 개인키로 서명되어 전송될 수 있다.

[17] 본 발명의 한 실시예에 따른 생체 정보 기반 인증 장치로서, 등록된 생체 정보를 저장하는 저장부, 키 생성 알고리즘을 기초로 공개키와 개인키를 생성하고, 상기 공개키를 제어 서버로 전송하는 인증 키 생성부, 그리고 컴퓨팅 장치로부터 웹사이트 서버로 전달되는 로그인 요청 메시지를 탐지하고, 상기 로그인 요청 메시지로부터 추출한 로그인 세션 정보와 생체 정보 인증 결과를 포함하는 인증 정보를 상기 제어 서버로 전송하는 로그인 제어부를 포함하고, 상기 생체 정보 인증 결과는 상기 등록된 생체 정보와 상기 로그인 요청 메시지를 탐지한 후 입력된 생체 정보를 비교한 결과이다.

[18] 상기 로그인 제어부는 상기 제어 서버로부터 생체 정보 로그인 사이트들의 정보를 포함하는 화이트 리스트를 수신하고, 상기 로그인 요청 메시지를 기초로 상기 웹사이트 서버가 상기 화이트 리스트에 포함되는지 판단하며, 상기 웹사이트 서버가 상기 화이트 리스트에 포함되는 경우, 상기 인증 정보를 상기 제어 서버로 전송할 수 있다.

[19] 상기 로그인 제어부는 상기 웹사이트 서버가 상기 화이트 리스트에 포함되는 경우, 상기 로그인 요청 메시지에 포함된 세션키를 파싱하고, 상기 세션키를 포함하는 상기 로그인 세션 정보를 생성할 수 있다.

[20] 상기 로그인 제어부는 상기 웹사이트 서버가 상기 화이트 리스트에 포함되는 경우, 상기 화이트 리스트에서 상기 웹사이트 서버의 식별 정보를 확인하고, 상기 웹사이트 서버의 식별 정보를 더 포함하는 상기 로그인 세션 정보를 생성할 수 있다.

[21] 상기 로그인 제어부는 상기 웹사이트 서버가 상기 화이트 리스트에 포함되는 경우, 생체 인식 센서를 활성화하고, 상기 생체 인식 센서로부터 생체 정보를 입력받을 수 있다.

[22] 상기 로그인 제어부는 상기 인증 정보를 상기 개인키로 서명하여 상기 제어 서버로 전송할 수 있다.

[23] 본 발명의 한 실시예에 따른 생체 정보 기반 인증 장치로서, 생체 정보를 인식하는 적어도 하나의 센서, 외부 장치와의 통신을 위한 적어도 하나의 통신 인터페이스, 프로그램을 저장하는 메모리, 입력 데이터를 암호화하여 출력하는 보안 모듈, 상기 센서, 상기 통신 인터페이스, 상기 메모리, 그리고 상기 보안 모듈과 연동하여 상기 프로그램에 구현된 동작을 실행하는 프로세서를 포함하고, 상기 프로그램은 생체 정보 기반 로그인을 위한 제1 프로그램을 포함하고, 상기 제1 프로그램은 컴퓨팅 장치로부터 웹사이트 서버로 전달되는

로그인 요청 메시지를 탐지하고, 상기 웹사이트 서버가 화이트 리스트에 해당하는지를 판단하여 상기 센서를 활성화시키며, 상기 센서로부터 입력된 제1 생체 정보의 생체 정보 인증 결과와 상기 로그인 요청 메시지로부터 추출한 로그인 세션 정보를 제어 서버로 전송하는 명령어들(instructions)을 포함하고, 상기 화이트 리스트는 상기 제어 서버로부터 수신한 생체 정보 로그인 사이트들의 정보이며, 상기 로그인 세션 정보는 세션키와 상기 웹사이트 서버의 식별 정보를 포함하고, 상기 세션키는 상기 컴퓨팅 장치와 상기 웹사이트 서버 사이에 연결된 세션을 특정하는 값이다.

[24] 상기 프로그램은 상기 인증 장치의 등록을 위한 제2 프로그램을 더 포함하고, 상기 제2 프로그램은 상기 컴퓨팅 장치로부터 상기 제어 서버로 전달되는 제1 식별 정보를 탐지하고, 상기 제1 식별 정보가 자신의 식별 정보와 같은지 판단하여 상기 센서를 활성화시키며, 상기 센서로부터 입력된 제2 생체 정보를 등록하고, 키 생성 알고리즘을 기초로 공개키와 개인키를 생성한 후, 상기 공개키를 상기 제어 서버로 전달하고, 상기 개인키를 상기 보안 모듈로 암호화하여 저장하는 명령어들을 포함할 수 있다.

[25] 상기 제1 프로그램은 상기 제1 생체 정보와 상기 제2 생체 정보를 비교하여 상기 생체 정보 인증 결과를 출력하고, 상기 개인키를 복호화하며, 상기 개인키로 상기 생체 정보 인증 결과와 상기 로그인 세션 정보를 서명하여 상기 제어 서버로 전송하는 명령어들을 더 포함할 수 있다.

발명의 효과

[26] 본 발명의 실시예에 따르면 사용자는 자신의 생체 정보 기반 인증 장치를 통해 다양한 웹사이트에 간편하게 로그인할 수 있다. 본 발명의 실시예에 따르면 웹사이트 서버는 생체 정보 기반 인증 장치와 연동하는 네트워크 장치로부터 수신한 로그인 허용 요청을 기초로 로그인을 허용하면 되므로, 생체 정보 기반 로그인을 위한 별도의 프로그램을 구현할 필요 없고, 해킹 등에 의한 아이디 도용에 의한 문제를 해결할 수 있다.

도면의 간단한 설명

[27] 도 1은 본 발명의 한 실시예에 따른 인증 장치의 블록도이다.

[28] 도 2는 본 발명의 한 실시예에 따른 인증 장치가 다른 장치들과 연결되는 모습을 예시적으로 나타내는 도면이다.

[29] 도 3은 본 발명의 한 실시예에 따른 지문 로그인 방법을 예시적으로 설명하는 도면이다.

[30] 도 4는 본 발명의 한 실시예에 따른 인증 장치의 하드웨어 구성도이다.

[31] 도 5는 본 발명의 한 실시예에 따른 인증 장치의 인증 정보 등록 방법의 흐름도이다.

[32] 도 6은 본 발명의 한 실시예에 따른 생체 정보 기반 로그인 방법의 흐름도이다.

발명의 실시를 위한 형태

[33] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[34] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "...부", "...기", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[35] 인증에 사용되는 생체 정보는 지문, 홍채, 정맥 등 다양할 수 있고, 앞으로는 설명을 위해 지문을 예로 들어 설명하나, 본 발명에서 사용하는 생체 정보가 지문으로 한정되는 것은 아니다. 또한, 복수의 생체 정보를 결합하여 인증에 사용할 수 있다.

[36] 도 1은 본 발명의 한 실시예에 따른 인증 장치의 블록도이고, 도 2는 본 발명의 한 실시예에 따른 인증 장치가 다른 장치들과 연결되는 모습을 예시적으로 나타내는 도면이며, 도 3은 본 발명의 한 실시예에 따른 지문 로그인 방법을 예시적으로 설명하는 도면이다.

[37] 도 1과 도 2를 참고하면, 인증 장치(100)는 프로세서(CPU)와 운영체제(OS)를 구비한 하드웨어 보안 장치로서, 컴퓨팅 장치(2000)에 연결되면 전기를 공급받아 부팅하고, 컴퓨팅 장치(2000)와 독립적인 시스템으로 동작한다. 또한, 인증 장치(100)는 컴퓨팅 장치(2000)에 연결되면 컴퓨팅 장치(2000)의 일부 기능을 비활성화(disable)시키고 인증 장치(100)의 내부 기능만을 활성화시킬 수 있다.

[38] 도 2를 참고하면, 인증 장치(100)는 통신 인터페이스(미도시)를 통해 컴퓨팅 장치(2000)와 연결될 수 있다. 통신 인터페이스는 다양한 유무선 인터페이스 중에서 선택될 수 있다. 예를 들면, 통신 인터페이스는 USB 인터페이스일 수 있으나, 컴퓨팅 장치(2000)와 연결될 수 있는 다른 통신 인터페이스도 가능하며, 또한 인증 장치(100)는 복수의 통신 인터페이스를 포함할 수 있다.

[39] 또한, 인증 장치(100)는 직접 통신망 연결이 가능한 통신 인터페이스(미도시), 즉 통신 모듈을 더 포함하고, 통신 모듈을 통해 각종 네트워크 장치에 접속할 수 있다. 네트워크 장치는 제어 서버(3000)와 복수의 웹사이트 서버(4000)를 포함한다. 통신 모듈은 유무선망에 접속할 수 있는 다양한 통신 모듈 중에서 선택될 수 있다. 예를 들면, 통신 모듈은 블루투스(Bluetooth)나 와이파이(Wifi) 등의 접속 장치(access point)에 무선 접속할 수 있는 무선 통신 모듈, 또는 유선 케이블로 통신망에 접속할 수 있는 유선 통신 모듈일 수 있다. 한편, 인증 장치(100)가 컴퓨팅 장치(2000)에 연결되면, 컴퓨팅 장치(2000)의 인터넷 연결

등을 위한 통신 모듈이 비활성화되고, 인증 장치(100)의 통신 모듈만으로 외부 통신망에 접속할 수 있도록 구현될 수 있다. 앞으로는, 인증 장치(100)가 컴퓨팅 장치(2000)에 연결되면, 컴퓨팅 장치(2000)의 인터넷 연결 등을 위한 통신 모듈이 비활성화되고, 인증 장치(100)의 통신 모듈만으로 외부 통신망에 접속한다. 컴퓨팅 장치(2000)에서 출력되는 패킷이나 컴퓨팅 장치(2000)로 입력되는 패킷은 인증 장치(100)를 거쳐 전송된다. 따라서, 인증 장치(100)는 컴퓨팅 장치(2000)에서 출력되는 패킷이나 컴퓨팅 장치(2000)로 입력되는 패킷을 탐지하고, 패킷의 데이터(메시지)를 확인할 수 있다.

[40] 다시 도 1을 참고하면, 인증 장치(100)는 생체 정보 인식부(110), 인증 키 생성부(130), 암호화부(150), 저장부(170), 로그인 제어부(190)를 포함한다.

[41] 생체 정보 인식부(110)는 사용자의 생체 정보를 인식(센싱)하는 센서이다. 생체 정보 인식부(110)는 인증 장치(100)가 전기를 공급받아 부팅되면 자동적으로 활성화되거나, 인증 장치(100)의 제어부(프로세서)로부터 제어 신호를 받아 활성화될 수 있다. 생체 정보 인식부(110)는 고유의 센서 식별 정보(sensor_id)를 가진다. 센서의 시리얼 정보를 센서 식별 정보로 이용할 수 있으나, 이에 한정되는 것은 아니다. 앞으로, 생체 정보로서 지문을 예로 들어 설명한다. 생체 정보 인식부(110)는 인식한 지문 정보를 저장부(170)에 저장한다.

[42] 인증 키 생성부(130)는 인증 정보 등록 단계에서 지문 정보를 등록(저장)하고, 공개키와 개인키를 생성한다. 인증 키 생성부(130)는 공개키를 제어 서버(3000)로 전송한다. 개인키는 지정된 장소에 저장된다. 이때, 개인키는 암호화부(150)의 암호화키로 개인키를 암호화되고, 암호화된 개인키가 저장될 수 있다. 암호화부(150)는 하드웨어 보안 모듈(Hardware Security Module, HSM)일 수 있다.

[43] 인증 키 생성부(130)는 키 생성 알고리즘에 따라 공개키와 개인키를 생성한다. 키 생성 알고리즘은 RSA 키 생성 알고리즘일 수 있다. 인증 키 생성부(130)가 공개키와 개인키 생성 시 입력받는 정보는 다양하게 설계될 수 있다. 예를 들면, 인증 키 생성부(130)는 난수를 입력받고, 난수를 기초로 공개키와 개인키를 생성할 수 있다. 인증 키 생성부(130)는 생체(지문) 정보를 기초로 공개키와 개인키를 생성할 수 있다. 또는 인증 키 생성부(130)는 생체 정보와 추가 식별 정보를 기초로 공개키와 개인키를 생성할 수 있다. 추가 식별 정보는 다양할 수 있는데, 인증 장치(100)의 식별 정보(예를 들면, 시리얼 번호 등) 또는 인증 장치(100) 내부에 포함된 특정 하드웨어의 식별 정보와 같은 장치 관련 식별 정보일 수 있다. 특정 하드웨어의 식별 정보는 예를 들면, 생체 정보 인식부(110)의 센서 식별 정보(sensor_id)일 수 있다. 추가 식별 정보는 사용자 비밀번호, 사용자 주민등록번호 등과 같은 사용자 관련 식별 정보일 수 있다. 또는 추가 식별 정보는 장치 관련 식별 정보와 사용자 관련 식별 정보의 조합일 수 있다.

[44] 암호화부(150)는 암호화키로 입력 정보를 암호화하는 하드웨어 보안 모듈일 수

있다. 암호화키는 개인키를 암호화/복호화하는데 사용될 수 있다. 암호화부(150)는 AES(Advanced Encryption Standard) 암호화 알고리즘을 사용하여 암호화할 수 있다.

[45] 로그인 제어부(190)는 제어 서버(3000)로부터 생체 정보 기반 로그인을 지원하는 지문 인식 로그인 사이트 리스트(화이트 리스트)를 수신한다. 로그인 제어부(190)는 주기적으로 제어 서버(3000)에 접속하여 지문 인식 로그인 사이트 리스트를 갱신하거나, 제어 서버(3000)로부터 지문 인식 로그인 사이트 리스트를 푸쉬받을 수 있다. 지문 인식 로그인 사이트 리스트는 지문 인식 로그인 사이트를 식별할 수 있는 각종 정보(예를 들면, 호스트명(Host), IP 주소, URI 등)들을 포함하고, 지문 인식 로그인 사이트별로 식별 정보(예를 들면, 0001, 0002 등)가 부여될 수 있다.

[46] 사용자가 컴퓨팅 장치(2000)를 통해 특정 웹사이트에 접속하거나, 특정 웹사이트에 접속한 후 지문 로그인 요청(선택)을 하면, 로그인 제어부(190)는 컴퓨팅 장치(2000)로부터 웹사이트 서버(4000)로 전달되는 지문 로그인 요청 메시지를 수신한다. 도 3을 참고하면, 지문 로그인 요청을 위한 메뉴 버튼(10)은 웹사이트의 로그인 화면 중 일부 영역에 표시될 수 있다.

[47] 로그인 제어부(190)는 지문 로그인 요청 메시지에 포함된 목적지 정보를 기초로 웹사이트 서버(4000)가 지문 인식 로그인 사이트 리스트에 포함되는지 확인한다. 컴퓨팅 장치(2000)에서 특정 웹사이트 서버(4000)로 전송하는 패킷은 인증 장치(100)의 통신 모듈을 통해 웹사이트 서버(4000)로 전달된다. 따라서, 로그인 제어부(190)는 지문 로그인 요청 메시지에 포함된 정보(예를 들면, HTTP 프로토콜의 호스트(host), 목적지 주소, URI 등)를 기초로 웹사이트 서버(4000)가 지문 인식 로그인 사이트인지 확인할 수 있다.

[48] 웹사이트 서버(4000)가 지문 인식 로그인 사이트 리스트에 포함되는 경우, 즉, 지문 인식 로그인을 허용하는 사이트인 경우, 로그인 제어부(190)는 지문 로그인 요청 메시지에 포함된 세션키(예를 들면, finger_login=flogin=ABCD)를 파싱해서 저장한다. 세션키는 웹사이트 서버(4000)에서 랜덤하게 생성하여 컴퓨팅 장치(2000)로 전송하는 값으로서, 컴퓨팅 장치(2000)와 웹사이트 서버(4000) 사이에 연결되는 세션을 특정하는 세션값이다. 이때, 컴퓨팅 장치(2000)의 지문 로그인 요청 메시지는 웹사이트 서버(4000)로 전달된다. 웹사이트 서버(4000)는 지문 로그인 요청 메시지에 포함된 세션키와 쿠키를 저장한다.

[49] 웹사이트 서버(4000)는 컴퓨팅 장치(2000)와 연결된 세션을 통해 지문 확인 요청 메시지를 전달한다. 지문 확인 요청 메시지는 인증 장치(100)를 거쳐 컴퓨팅 장치(2000)로 전달되고, 컴퓨팅 장치(2000)는 도 3과 같이 지문 확인 요청 화면(20)을 표시할 수 있다.

[50] 로그인 제어부(190)는 생체 정보 인식부(110)로부터 사용자의 지문 정보를 수신하여 지문 인증을 한다. 지문 인증 방법은 다양할 수 있으며, 예를 들면, 로그인 제어부(190)는 수신한 지문 정보와 저장부(170)에 저장된 지문 정보를

비교하여 지문 인증을 할 수 있다.

[51] 로그인 제어부(190)는 파싱한 세션키에 대한 지문 인증 정보를 제어 서버(3000)로 전달한다. 이때, 로그인 제어부(190)는 지문 인증 정보를 개인키로 서명(암호화)하여 제어 서버(3000)로 전달한다. 지문 인증 정보는 제어 서버(3000)에서 요구되는 데이터를 포함하고, 제어 서버(3000)에서 요구되는 데이터는 지문 인증 결과에 연관된 세션키, 지문 인증 결과(예를 들면, 0 또는 1), 그리고 웹사이트 식별정보를 포함할 수 있다.

[52] 제어 서버(3000)는 개인키로 서명(암호화)된 정보를 공개키로 복호하고, 복호 결과를 기초로 수신한 지문 인증 정보의 진위 여부를 판단한다. 제어 서버(3000)는 지문 인증 정보가 신뢰 정보인 경우, 지문 인증 정보에 포함된 지문 인증 결과를 기초로 지문 인증 성공 여부를 판단한다. 지문 인증이 성공한 경우, 제어 서버(3000)는 지문 인증 정보에 포함된 웹사이트 식별정보를 기초로 웹사이트 서버(4000)를 확인하고, 웹사이트 서버(4000)로 특정 세션키에 해당하는 세션에 대한 로그인 허용을 요청한다.

[53] 웹사이트 서버(4000)는 제어 서버(3000)로부터 로그인 허용 요청된 대상(세션)에 대해 로그인을 허용한다. 그러면, 컴퓨팅 장치(2000)는 웹사이트 서버(4000)에 접속하여 로그인 이후의 서비스를 이용할 수 있다.

[54] 이와 같이, 웹사이트 서버(4000)는 신뢰할 수 있는 제어 서버(3000)로부터의 로그인 허용 요청을 수신하면, 로그인 허용 요청된 세션에 대해 로그인을 허용한다. 따라서, 웹사이트 서버(4000)는 도 3에서 예시적으로 설명한 바와 같이, 생체 정보 기반 로그인을 사용자가 요청(선택)할 수 있는 메뉴 버튼(10), 그리고 사용자에게 인증 장치(100)에 지문을 인식하도록 요청하고, 지문 인식 결과를 사용자에게 알려주는 화면(20)을 제공하기만 하면 되고, 제어 서버(3000)로부터 수신한 로그인 허용 요청에 대해 로그인을 허용하면 된다. 따라서, 웹사이트 서버(4000)는 사용자의 지문 정보와 사용자의 공개키를 저장한 후, 사용자의 개인키로 암호화된 지문 정보를 수신하면, 암호화된 지문 정보를 공개키로 복호화하여 인증하는 일련의 절차를 수행할 필요 없고, 보안에 민감한 지문 정보 등의 개인 정보를 관리할 필요 없다.

[55] 도 4는 본 발명의 한 실시예에 따른 인증 장치의 하드웨어 구성도이다.

[56] 도 4를 참고하면, 인증 장치(100)의 하드웨어 구성은 설계에 따라 다양할 수 있다. 인증 장치(100)는 도 4와 같이, 프로세서(CPU)(200), 적어도 하나의 센서(300), 적어도 하나의 메모리(400), 적어도 하나의 통신 인터페이스(500), 그리고 보안 모듈(600)을 포함할 수 있다.

[57] 센서(300)는 생체 정보 인식부(110)의 기능을 수행하는 하드웨어로서, 지문을 생체 정보로 이용하는 인증인 경우, 센서(300)는 지문 센서일 수 있다.

[58] 메모리(400)는 프로세서(200)의 동작에 필요한 각종 정보를 저장하는 하드웨어이다. 메모리(400)는 프로세서(200)의 구동을 위한 운영체제(OS), 그리고 본 발명에서 설명하는 인증 장치(100)의 각종 동작을 위한 프로그램을

저장할 수 있다. 메모리(400)는 저장부(170)의 적어도 일부 기능을 수행할 수 있다. 메모리는 저장되는 데이터에 따라 분리되어 구현될 수 있음은 당연하다. 즉, 메모리(400)는 지문 정보, 지문 인식 로그인 사이트 리스트, 파싱한 세션키 등을 저장할 수 있다. 메모리(400)에 저장된 정보는 갱신되거나 일정 기간 이후에 삭제될 수 있다.

[59] 통신 인터페이스(500)는 외부 장치와의 물리적 연결을 위한 하드웨어이다. 통신 인터페이스(500)는 도 2를 참고로 설명한 바와 같이, 컴퓨팅 장치(2000)와의 연결을 위한 통신 인터페이스, 그리고 통신망 접속을 위한 유/무선 통신 인터페이스를 포함한다.

[60] 보안 모듈(600)은 암호화부(150)의 기능을 수행하는 하드웨어이다.

[61] 프로세서(200)는 센서(300), 메모리(400), 통신 인터페이스(500), 그리고 보안 모듈(600)과 통신하고, 이들을 제어한다. 프로세서(200)는 메모리(400)에 저장된 프로그램(예를 들면, 키 생성 알고리즘을 비롯한 인증 정보 등록 알고리즘을 구현한 프로그램, 생체 정보 기반 로그인을 위한 프로그램 등)을 로드하여 인증키 생성부(130)와 로그인 제어부(190)의 기능을 수행할 수 있다.

[62] 프로세서(200)가 인증 정보 등록(인증서 발급 또는 공개키 및 개인키 생성이라고 할 수 있음)을 요청받는 경우, 인증 정보 등록에 관련된 프로그램을 로드한다. 프로세서(200)는 키 생성 알고리즘에 따라 공개키와 개인키를 생성한다. 프로세서(200)는 통신 인터페이스(500)를 통해 공개키를 인증기관으로 전송한다. 그리고 프로세서(200)는 개인키를 저장시킨다. 이때, 프로세서(200)는 개인키를 보안 모듈(600)로 전송하여 암호화하고, 암호화한 개인키를 지정된 장소(예를 들면, 보안 모듈(600) 내부)에 저장할 수 있다. 프로세서(200)는 전자서명을 위해 개인키가 필요한 경우, 암호화에 사용한 암호화키를 기초로 개인키를 복호화할 수 있다.

[63] 키 생성 알고리즘은 다양할 수 있고, 예를 들면, 난수를 기초로 공개키와 개인키를 생성하는 알고리즘, 생체(지문) 정보를 포함하는 공개키와 개인키를 생성하는 알고리즘, 또는 생체 정보와 추가 식별 정보를 포함하는 공개키와 개인키를 생성하는 알고리즘 등 다양할 수 있다.

[64] 프로세서(200)는 컴퓨팅 장치(2000)로 입출입하는 패킷을 탐지한다. 만약, 프로세서(200)가 컴퓨팅 장치(2000)에서 특정 웹사이트 서버(4000)로 전송되는 지문 로그인 요청 메시지를 탐지한 경우, 생체 정보 기반 로그인 요청(예를 들면, 전자서명) 절차의 개시로 인식한다. 그러면, 프로세서(200)는 생체 정보 기반 로그인을 위한 프로그램을 로드하고, 센서(300)를 활성화한다. 이를 위해, 프로세서(200)는 제어 서버(3000)로부터 수신한 지문 인식 로그인 사이트를 미리 저장해 둔다. 그리고, 프로세서(200)는 컴퓨팅 장치(2000)로부터 수신한 지문 로그인 요청 메시지를 기초로 웹사이트 서버(4000)가 지문 인식 로그인 사이트인지 확인하고, 웹사이트 서버(4000)가 지문 인식 로그인 사이트이면, 지문 로그인 요청 메시지에 포함된 세션키를 파싱한다. 프로세서(200)는

센서(300)로부터 수신한 지문 정보에 대해 지문 인증을 하고, 파싱한 세션키와 지문 인증 결과를 개인키로 서명(암호화)하여 제어 서버(3000)로 전달한다.

[65] 도 5는 본 발명의 한 실시예에 따른 인증 장치의 인증 정보 등록 방법의 흐름도이다. 여기서, 인증 정보 등록 방법은 지문 저장이 정상적으로 수행된 후, 공개키와 개인키를 생성하고, 공개키를 제어 서버(3000)에 등록하는 방법으로서, 생체 정보 기반 로그인을 위한 초기 설정 단계이다.

[66] 도 5를 참고하면, 인증 장치(100)와 컴퓨팅 장치(2000)가 연결된다(S110).

[67] 컴퓨팅 장치(2000)는 인증 장치(100)를 인식하고, 인증 정보 등록 화면을 표시한다(S120). 컴퓨팅 장치(2000)는 인증 장치(100)에 관련된 프로그램을 구동하고, 인증 장치(100)와 통신하면서 인증 정보 등록 절차를 지원한다. 컴퓨팅 장치(2000)는 인증 장치(100)와 사용자 사이의 커뮤니케이션을 지원하는 장치로서, 인증 장치(100)에 관련된 프로그램을 구동하여 사용자 인터페이스 화면을 제공한다. 즉, 컴퓨팅 장치(2000)는 디스플레이 화면을 통해 사용자에게 인증 정보 등록 절차에 필요한 안내(예를 들면, 인증 장치(100)에 지문 입력 요청)를 할 수 있다. 특히, 인증 정보 등록 화면은 인증 장치(100)의 등록을 위해, 인증 장치(100)의 식별 정보, 예를 들면 시리얼 정보의 입력을 요청할 수 있다.

[68] 컴퓨팅 장치(2000)는 인증 장치(100)의 식별 정보를 입력받고, 인증 장치(100)의 식별 정보를 포함하는 메시지를 제어 서버(3000)로 전송한다(S130).

[69] 인증 장치(100)는 인증 장치(100)의 식별 정보를 포함하는 메시지를 탐지하여, 메시지에 포함된 식별 정보와 자신의 식별 정보를 비교한다(S140).

[70] 인증 장치(100)는 식별 정보가 일치하면 자신의 인증 정보 등록 절차를 인식하고, 인증 정보 등록 절차를 개시한다(S142). 인증 장치(100)는 센서를 활성화할 수 있다.

[71] 인증 장치(100)는 사용자의 지문 정보를 입력받고, 입력받은 지문 정보를 등록(저장)한다(S150). 인증 장치(100)는 사용자의 지문 정보를 복수 번 입력 받을 수 있고, 지문 정보를 성공적으로 입력받으면, 인증 장치(100)의 알림 장치(LED, 스피커 등)를 통해 지문 입력 성공을 알리거나, 컴퓨팅 장치(2000)의 인증 장치 등록 화면에 지문 입력 성공을 표시할 수 있다.

[72] 인증 장치(100)는 지문 등록한 후 공개키 및 개인키를 생성한다(S160). 인증 장치(100)는 키 생성 알고리즘을 기초로 공개키와 개인키를 생성한다). 키 생성 알고리즘은 RSA 키 생성 알고리즘일 수 있다. 인증 장치(100)는 RSA 키 생성 알고리즘의 입력으로 지문 정보를 포함하는 소수의 P값과 소수의 Q값을 사용할 수 있으나, 일반적인 RSA 키 생성 알고리즘에 따라 공개키와 개인키를 생성할 수 있다.

[73] 인증 장치(100)는 공개키를 제어 서버(3000)로 전송한다(S162). 인증 장치(100)는 개인키를 저장한다. 인증 장치(100)는 암호화키로 개인키를 암호화하여 저장할 수 있다. 인증 장치(100)는 HSM의 AES 알고리즘으로 개인키를 암호화하여 HSM 내부에 개인키를 저장할 수 있다.

[74] 제어 서버(3000)는 공개키를 저장한다(S164). 이때, 제어 서버(3000)는 인증 장치(100)의 식별 정보에 공개키를 매핑하여 저장할 수 있다.

[75] 인증 장치(100)는 컴퓨팅 장치(2000)로 인증 정보 등록 완료 메시지를 전달한다(S170).

[76] 컴퓨팅 장치(2000)는 인증 정보 등록 화면에 인증 정보 등록이 완료됨을 표시한다(S172).

[77] 도 6은 본 발명의 한 실시예에 따른 생체 정보 기반 로그인 방법의 흐름도이다.

[78] 도 6을 참고하면, 인증 장치(100)와 컴퓨팅 장치(2000)가 연결된다(S210).

[79] 인증 장치(100)는 제어 서버(3000)로부터 지문 인식 로그인 사이트 리스트(화이트 리스트)를 수신한다(S220). 인증 장치(100)는 컴퓨팅 장치(2000)와의 연결 여부에 관계없이 지문 인식 로그인 사이트 리스트를 갱신할 수 있다. 설명을 위해, 특정 웹사이트(www.kt.com/finger, flogin)가 지문 인식 로그인 사이트 리스트에 포함되어 있다고 가정한다. 여기서, flogin은 지문 로그인 요청에 관계된 세션을 특정하는 세션값(세션키)이라고 정의한다.

[80] 사용자가 컴퓨팅 장치(2000)에서 특정 웹사이트(www.kt.com/finger, flogin)에서 제공하는 지문 로그인 요청(선택)을 하면, 컴퓨팅 장치(2000)는 특정 웹사이트(www.kt.com)의 서버(4000)로 지문 로그인 요청 메시지를 전송한다(S230). 지문 로그인 요청 메시지는 웹사이트 식별 정보(예를 들면, 호스트(host), 목적지 주소, URI 등), 세션키(flogin), 그리고 쿠키 정보를 포함할 수 있다. 예를 들면, 지문 로그인 요청 메시지는 www.kt.com/finger?flogin=ABCD/cookie=1234라고 가정한다.

[81] 웹사이트 서버(4000)는 지문 로그인 요청 메시지에 포함된 세션키(flogin=ABCD), 그리고 쿠키 정보(cookie=1234)를 저장한다(S232).

[82] 인증 장치(100)는 지문 로그인 요청 메시지를 탐지하여, 메시지에 포함된 웹사이트 식별 정보와 지문 인식 로그인 사이트 리스트를 비교한다(S240). 인증 장치(100)는 메시지 탐지 기능(Intrusion Detection system, IDS)을 통해 HTTP 프로토콜로 전송되는 지문 로그인 요청 메시지에서 Host를 추출하고, 추출한 Host가 지문 인식 로그인 사이트 리스트에 있는지 확인한다. 일치하는 Host가 있으면, 인증 장치(100)는 지문 로그인 요청 메시지에서 목적지 주소를 추출하고, 추출한 목적지 주소가 지문 인식 로그인 사이트 리스트에 있는지 확인한다. 일치하는 목적지 주소가 있으면, 인증 장치(100)는 지문 로그인 요청 메시지에서 URI를 추출하고, 추출한 URI가 지문 인식 로그인 사이트 리스트에 있는지 확인한다.

[83] 인증 장치(100)는 메시지에 포함된 웹사이트가 지문 인식 로그인 사이트에 해당하면 생체 정보 기반 로그인 절차를 인식하고, 생체 정보 기반 로그인 절차를 개시한다(S242). 인증 장치(100)는 센서를 활성화할 수 있다.

[84] 인증 장치(100)는 지문 로그인 요청 메시지에서 세션키(flogin=ABCD)를 파싱하여 저장한다(S244).

[85] 웹사이트 서버(4000)는 컴퓨팅 장치(2000)와 연결된 세션을 통해 지문 확인 요청 메시지를 전달한다(S250). 그러면, 컴퓨팅 장치(2000)는 도 3과 같이 지문 확인 요청 화면(20)를 표시할 수 있다.

[86] 인증 장치(100)는 사용자의 지문 정보를 입력받는다(S260).

[87] 인증 장치(100)는 입력받은 지문 정보를 인증한다(S262). 인증 장치(100)는 입력받은 지문 정보와 저장된 지문 정보를 비교하여 지문 인증을 할 수 있다.

[88] 인증 장치(100)는 지문 로그인 요청 세션에 대한 지문 인증 정보를 개인키로 서명(암호화)하여 제어 서버(3000)로 전송한다(S264). 지문 인증 정보는 제어 서버(3000)에서 요구되는 데이터를 포함하고, 특히 지문 인증 결과(예를 들면, 0 또는 1)와 로그인 세션 정보를 포함한다. 로그인 세션 정보는 지문 로그인을 요청한 세션 정보을 나타내는 세션키(예를 들면, ABCD), 그리고 웹사이트 식별정보를 포함할 수 있다. 그리고, 지문 인증 정보는 시간 정보, 인증 장치(100)의 식별 정보(예를 들면, 시리얼 정보), 서비스 코드 등을 더 포함할 수 있다. 시간 정보는 메시지 재사용 방지를 위해 사용되고 16진수로 전송하여 자리수를 줄일 수 있다. 서비스 코드는 서버에서 사용하고자 하는 함수 코드이다. 지문 인증 정보는 메시지 암호화 및 복호화에 사용되는 랜덤키를 더 포함할 수 있다.

[89] 제어 서버(3000)는 수신한 지문 인증 정보를 공개키로 복호한 복호 결과를 기초로 지문 인증 정보의 진위 여부를 판단한다(S270). 개인키로 전자서명된 데이터의 진위 여부를 공개키로 검증하는 방법은 전자서명 관련된 기술을 사용할 수 있다.

[90] 제어 서버(3000)는 지문 인증 정보가 신뢰 정보로 확인되면, 지문 인증 정보를 확인하여 지문 인증 성공 여부를 판단한다(S280).

[91] 지문 인증이 성공한 경우, 제어 서버(3000)는 웹사이트 서버(4000)로 지문 인증 정보에 포함된 세션에 대해 로그인 허용을 요청한다(S282). 즉, 제어 서버(3000)는 수신한 지문 인증 정보가 공개키를 전송한 사용자에 의해 전송된 것으로 인증되면, 지문 인증 정보를 신뢰한다. 제어 서버(3000)는 지문 인증 정보에 포함된 지문 인증 결과가 성공(예를 들면, 0)이면, 웹사이트 식별정보에 해당하는 웹사이트 서버(4000)를 확인하고, 웹사이트 서버(4000)로 세션키(예를 들면, ABCD)에 대한 로그인 허용을 요청한다.

[92] 웹사이트 서버(4000)는 제어 서버(3000)로부터 수신한 로그인 허용 요청 대상(세션)에 대해 로그인을 허용한다(S290). 그러면, 컴퓨팅 장치(2000)는 웹사이트 서버(4000)에 접속하여 로그인 이후의 서비스를 이용할 수 있다. 이때, 컴퓨팅 장치(2000)는 자신이 저장하고 있는 쿠키 정보(cookie=1234)를 포함하는 로그인 요청 메시지(또는 접속 요청 메시지)(예를 들면, www.kt.com/cookie=1234)를 웹사이트 서버(4000)로 전송하므로, 웹사이트 서버(4000)는 로그인 허용 요청 대상의 세션키(ABCD)에 매핑된 쿠키 정보(cookie=1234)를 보고, 로그인 허용 대상 여부를 판단할 수 있다. 그리고,

웹사이트 서버(4000)는 접속 요청 메시지에 로그인 허용 대상으로 결정한 쿠키 정보가 포함되어 있으면, 접속 요청 메시지에 대해 로그인을 허용한다.

[93] 다음에서, 인증 장치(100)가 제어 서버(3000)로 지문 로그인 요청 세션에 대한 지문 인증 정보를 개인키로 서명(암호화)하여 전송하는 방법에 대해 예시적으로 설명한다.

[94] 전자서명은 서명자를 확인하고 서명자가 전송 데이터(문서)에 서명을 하였음을 나타내기 위하여 전송 데이터에 첨부되는 전자적 형태의 정보이다. 전송 데이터(본문)에 전송 데이터(본문)를 개인키로 암호화한 전자서명을 첨부하여 보내다. 수신자는 개인키로 암호화된 전자서명을 공개키로 복호화한 값과 전송 데이터(본문)가 일치하면 수신한 전송 데이터가 공개키를 전송한 사용자에 의해 전송된 것으로 인증한다.

[95] 인증 장치(100)는 HTTP 프로토콜의 GET 메소드를 사용하여 지문 인증 정보를 포함하는 메시지를 전송할 수 있다. 지문 인증 정보가 전송 데이터(본문)라고 가정한다. 전송 데이터는 [시간, 인증 장치의 식별 정보(시리얼 정보), 서비스 코드, 로그인 세션 정보, 지문 인증 결과, 랜덤키]를 포함한다. 예를 들면, 로그인 세션 정보와 지문 인증 결과는 [세션키:지문 인증 성공 여부(성공 0, 실패 1):웹사이트식별 정보]로 구성되고, 예를 들면, [ABCD:0:001]일 수 있다.

[96] 인증 장치(100)는 전송 데이터를 개인키로 암호화여 서명한다.

[97] 인증 장치(100)는 전송 데이터에 서명 정보를 첨부하여 제어 서버(3000)로 전송한다. 전송 데이터와 서명 정보는 암호화되어 전송될 수 있다.

[98] 제어 서버(3000)는 서명 정보를 공개키로 복호한 값이 전송 데이터와 동일한지 비교하여 전송 데이터의 진위 여부를 판단한다.

[99] 이와 같이, 본 발명의 실시예에 따르면 사용자는 자신의 생체 정보 기반 인증 장치를 통해 다양한 웹사이트에 로그인할 수 있다. 본 발명의 실시예에 따르면 웹사이트 제공자는 생체 정보 기반 인증 장치와 연동하는 네트워크 장치로부터 수신한 인증 결과를 기초로 사용자 로그인 여부를 결정하면 되므로, 생체 정보 기반 로그인을 위한 별도의 프로그램을 구현할 필요 없고, 해킹 등에 의한 아이디 도용에 의한 문제를 해결할 수 있다.

[100] 이상에서 설명한 본 발명의 실시예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있다.

[101] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

청구범위

[청구항 1] 생체 정보 기반 인증 장치가 제어 서버와 연동하여 컴퓨팅 장치에서 요청된 웹사이트의 로그인을 처리하는 방법으로서,
상기 컴퓨팅 장치로부터 상기 웹사이트를 제공하는 웹사이트 서버로 전달되는 로그인 요청 메시지를 탐지하는 단계,
상기 로그인 요청 메시지로부터 로그인 세션 정보를 추출하는 단계,
입력받은 생체 정보에 대한 생체 정보 인증 결과를 출력하는 단계, 그리고
상기 로그인 세션 정보와 상기 생체 정보 인증 결과를 포함하는 인증 정보를 상기 제어 서버로 전송하는 단계를 포함하고,
상기 로그인 세션 정보는 상기 제어 서버에서 상기 웹사이트 서버로 전달되어 상기 웹사이트 서버에서 로그인 허용 대상 판단 시 사용되는 정보인, 로그인 방법.

[청구항 2] 제1항에서,
상기 제어 서버로부터 생체 정보 로그인 사이트들의 정보를 포함하는 화이트 리스트를 수신하는 단계를 더 포함하고,
상기 로그인 세션 정보를 추출하는 단계는
상기 로그인 요청 메시지를 기초로 상기 웹사이트 서버가 상기 화이트 리스트에 해당하는지 판단하는 단계, 그리고
상기 웹사이트 서버가 상기 화이트 리스트에 해당하는 경우, 상기 로그인 요청 메시지에 포함된 세션키를 상기 로그인 세션 정보로 추출하는 단계
를 포함하는 로그인 방법.

[청구항 3] 제2항에서,
상기 로그인 세션 정보는 상기 세션키와 상기 웹사이트의 식별 정보를 포함하고, 상기 웹사이트의 식별 정보는 상기 화이트 리스트에 포함되어 있는, 로그인 방법.

[청구항 4] 제2항에서,
상기 웹사이트 서버가 상기 화이트 리스트에 해당하는 경우,
센서를 활성화하는 단계
를 더 포함하는 로그인 방법.

[청구항 5] 제1항에서,
상기 생체 정보 인증 결과를 출력하는 단계는
저장된 생체 정보와 상기 입력받은 생체 정보를 비교하여 상기 생체 정보 인증 결과를 출력하는 로그인 방법.

[청구항 6] 제1항에서,

상기 인증 정보를 상기 제어 서버로 전송하는 단계는
상기 인증 정보를 개인키로 서명하여 상기 제어 서버로 전송하고,
상기 제어 서버는 상기 개인키와 쌍을 이루는 공개키를 저장하며,
상기 공개키와 상기 개인키는 상기 인증 장치를 등록할 때
생성되는 정보인 로그인 방법.

[청구항 7] 제1항에서,
상기 로그인 요청 메시지를 탐지하는 단계 이전에 인증 장치 등록
단계를 더 포함하고,
상기 인증 장치 등록 단계는
상기 컴퓨팅 장치로부터 상기 제어 서버로 전달되는 제1 식별
정보를 탐지하는 단계,
상기 제1 식별 정보가 자신의 식별 정보와 같은지 판단하는 단계,
상기 제1 식별 정보가 자신의 식별 정보와 같은 경우, 센서를
활성화하는 단계,
상기 센서로부터 입력된 생체 정보를 등록하는 단계, 그리고
키 생성 알고리즘을 기초로 공개키와 개인키를 생성하는 단계
를 포함하는 로그인 방법.

[청구항 8] 제어 서버가 생체 정보 기반 인증 장치와 연동하여 컴퓨팅
장치에서 요청된 웹사이트의 로그인을 처리하는 방법으로서,
생체 정보 로그인 사이트들의 정보를 포함하는 화이트 리스트를
상기 인증 장치로 전송하는 단계,
상기 인증 장치로부터 로그인 세션 정보와 생체 정보 인증 결과를
포함하는 인증 정보를 수신하는 단계, 그리고
상기 로그인 세션 정보에 관련된 웹사이트 서버로 상기 로그인
세션 정보에 대한 로그인 허용을 요청하는 단계
를 포함하는 로그인 방법.

[청구항 9] 제8항에서,
상기 로그인 세션 정보는 세션키와 상기 웹사이트의 식별 정보를
포함하고,
상기 세션키는 상기 컴퓨팅 장치와 상기 웹사이트 서버 사이에
연결된 세션을 특정하는 값이며,
상기 웹사이트는 상기 화이트 리스트에 포함되는 사이트인,
로그인 방법.

[청구항 10] 제9항에서,
상기 로그인 허용을 요청하는 단계는
상기 인증 정보의 진위 여부를 판단하는 단계,
상기 인증 정보가 신뢰 정보이고 상기 생체 정보 인증 결과가
성공인 경우, 상기 화이트 리스트에서 상기 인증 정보에 포함된

상기 웹사이트의 식별 정보에 해당하는 상기 웹사이트 서버를 찾는 단계, 그리고
상기 웹사이트 서버로 상기 세션키에 대한 로그인 허용을 요청하는 단계
를 포함하는 로그인 방법.

[청구항 11] 제10항에서,
상기 인증 장치로부터 수신한 공개키를 저장하는 단계를 더 포함하고,
상기 인증 정보의 진위 여부를 판단하는 단계는
상기 공개키를 이용하여 상기 인증 정보를 복호하고, 복호 결과를 기초로 진위 여부를 판단하며,
상기 인증 정보는 상기 공개키와 쌍을 이루는 개인키로 서명되어 전송되는, 로그인 방법.

[청구항 12] 생체 정보 기반 인증 장치로서,
등록된 생체 정보를 저장하는 저장부,
키 생성 알고리즘을 기초로 공개키와 개인키를 생성하고, 상기 공개키를 제어 서버로 전송하는 인증 키 생성부, 그리고
컴퓨팅 장치로부터 웹사이트 서버로 전달되는 로그인 요청 메시지를 탐지하고, 상기 로그인 요청 메시지로부터 추출한 로그인 세션 정보와 생체 정보 인증 결과를 포함하는 인증 정보를 상기 제어 서버로 전송하는 로그인 제어부
를 포함하고,
상기 생체 정보 인증 결과는 상기 등록된 생체 정보와 상기 로그인 요청 메시지를 탐지한 후 입력된 생체 정보를 비교한 결과인 생체 정보 기반 인증 장치.

[청구항 13] 제12항에서,
상기 로그인 제어부는
상기 제어 서버로부터 생체 정보 로그인 사이트들의 정보를 포함하는 화이트 리스트를 수신하고,
상기 로그인 요청 메시지를 기초로 상기 웹사이트 서버가 상기 화이트 리스트에 포함되는지 판단하며, 상기 웹사이트 서버가 상기 화이트 리스트에 포함되는 경우, 상기 인증 정보를 상기 제어 서버로 전송하는 생체 정보 기반 인증 장치.

[청구항 14] 제13항에서,
상기 로그인 제어부는
상기 웹사이트 서버가 상기 화이트 리스트에 포함되는 경우, 상기 로그인 요청 메시지에 포함된 세션키를 파싱하고, 상기 세션키를 포함하는 상기 로그인 세션 정보를 생성하는 생체 정보 기반 인증

장치.

[청구항 15] 제14항에서,
상기 로그인 제어부는
상기 웹사이트 서버가 상기 화이트 리스트에 포함되는 경우, 상기 화이트 리스트에서 상기 웹사이트 서버의 식별 정보를 확인하고, 상기 웹사이트 서버의 식별 정보를 더 포함하는 상기 로그인 세션 정보를 생성하는 생체 정보 기반 인증 장치.

[청구항 16] 제13항에서,
상기 로그인 제어부는
상기 웹사이트 서버가 상기 화이트 리스트에 포함되는 경우, 생체 인식 센서를 활성화하고, 상기 생체 인식 센서로부터 생체 정보를 입력받는 생체 정보 기반 인증 장치.

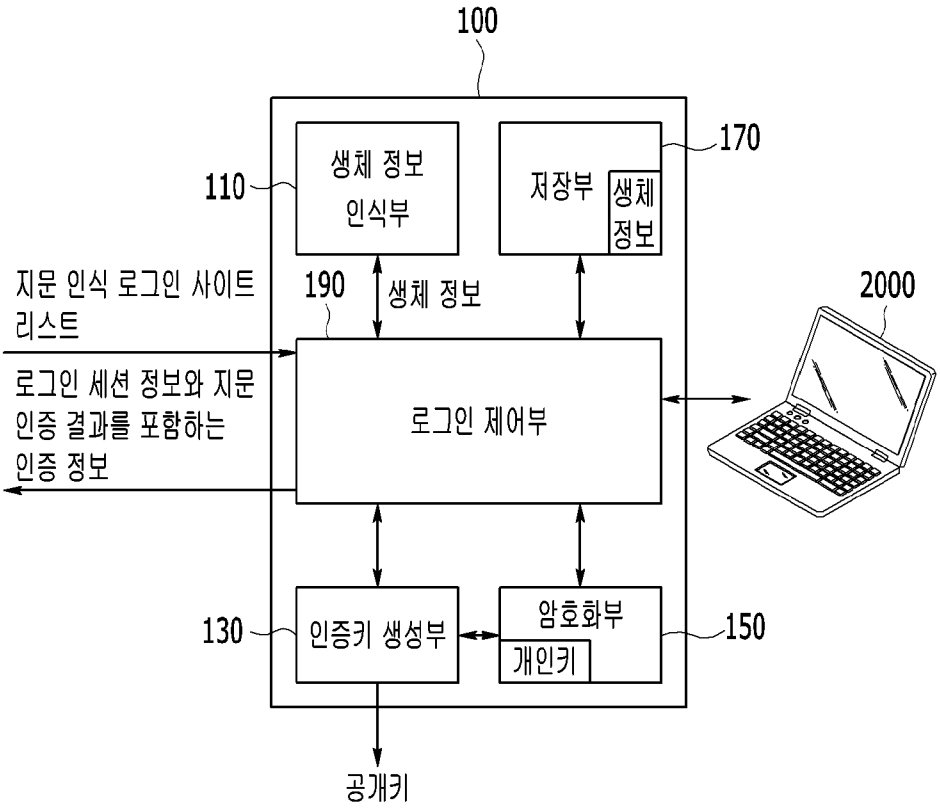
[청구항 17] 제12항에서,
상기 로그인 제어부는
상기 인증 정보를 상기 개인키로 서명하여 상기 제어 서버로 전송하는 생체 정보 기반 인증 장치.

[청구항 18] 생체 정보 기반 인증 장치로서,
생체 정보를 인식하는 적어도 하나의 센서,
외부 장치와의 통신을 위한 적어도 하나의 통신 인터페이스,
프로그램을 저장하는 메모리,
입력 데이터를 암호화하여 출력하는 보안 모듈, 그리고
상기 센서, 상기 통신 인터페이스, 상기 메모리, 그리고 상기 보안 모듈과 연동하여 상기 프로그램에 구현된 동작을 실행하는 프로세서를 포함하고,
상기 프로그램은 생체 정보 기반 로그인을 위한 제1 프로그램을 포함하고,
상기 제1 프로그램은
컴퓨팅 장치로부터 웹사이트 서버로 전달되는 로그인 요청 메시지를 탐지하고, 상기 웹사이트 서버가 화이트 리스트에 해당하는지를 판단하여 상기 센서를 활성화시키며, 상기 센서로부터 입력된 제1 생체 정보의 생체 정보 인증 결과와 상기 로그인 요청 메시지로부터 추출한 로그인 세션 정보를 제어 서버로 전송하는 명령어들(instructions)을 포함하고,
상기 화이트 리스트는 상기 제어 서버로부터 수신한 생체 정보 로그인 사이트들의 정보이며, 상기 로그인 세션 정보는 세션키와 상기 웹사이트 서버의 식별 정보를 포함하고, 상기 세션키는 상기 컴퓨팅 장치와 상기 웹사이트 서버 사이에 연결된 세션을 특정하는 값인, 생체 정보 기반 인증 장치.

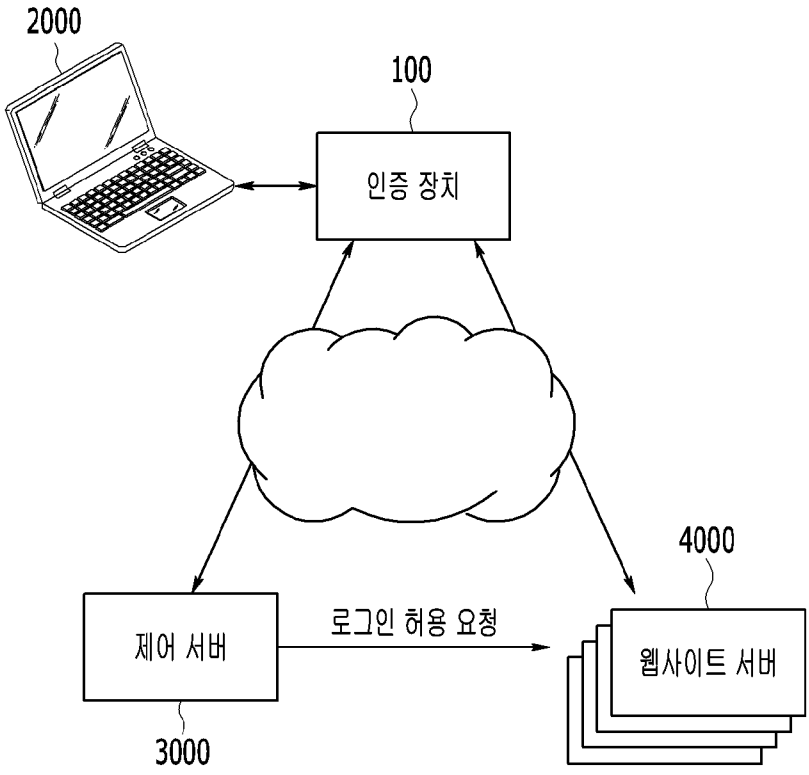
[청구항 19] 제18항에서,
상기 프로그램은 상기 인증 장치의 등록을 위한 제2 프로그램을 더 포함하고,
상기 제2 프로그램은
상기 컴퓨팅 장치로부터 상기 제어 서버로 전달되는 제1 식별 정보를 탐지하고, 상기 제1 식별 정보가 자신의 식별 정보와 같은지 판단하여 상기 센서를 활성화시키며, 상기 센서로부터 입력된 제2 생체 정보를 등록하고, 키 생성 알고리즘을 기초로 공개키와 개인키를 생성한 후, 상기 공개키를 상기 제어 서버로 전달하고, 상기 개인키를 상기 보안 모듈로 암호화하여 저장하는 명령어들을 포함하는 생체 정보 기반 인증 장치.

[청구항 20] 제19항에서,
상기 제1 프로그램은
상기 제1 생체 정보와 상기 제2 생체 정보를 비교하여 상기 생체 정보 인증 결과를 출력하고, 상기 개인키를 복호화하며, 상기 개인키로 상기 생체 정보 인증 결과와 상기 로그인 세션 정보를 서명하여 상기 제어 서버로 전송하는 명령어들을 더 포함하는 생체 정보 기반 인증 장치.

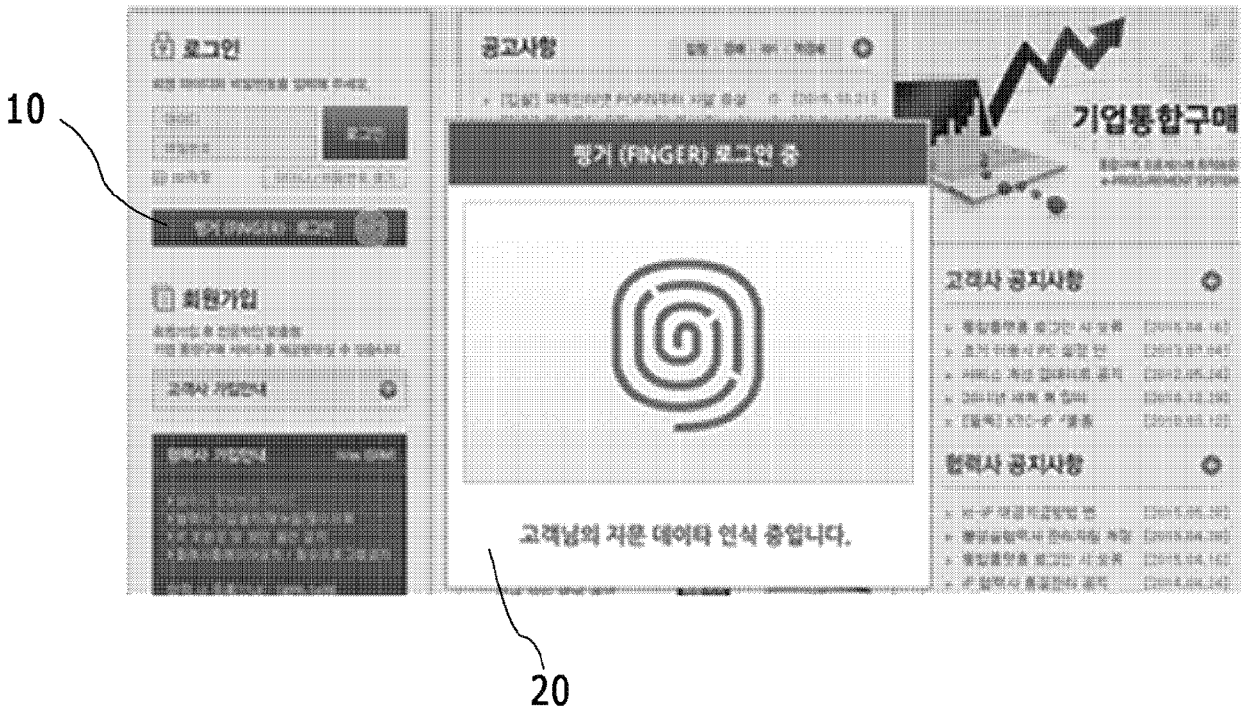
[Fig. 1]


100
생체 정보 인식부
110
저장부
생체 정보
170
지문 인식 로그인 사이트 리스트
190
생체 정보
2000
로그인 세션 정보와 지문 인증 결과를 포함하는 인증 정보
로그인 제어부
인증키 생성부
130
암호화부
개인키
150
공개키

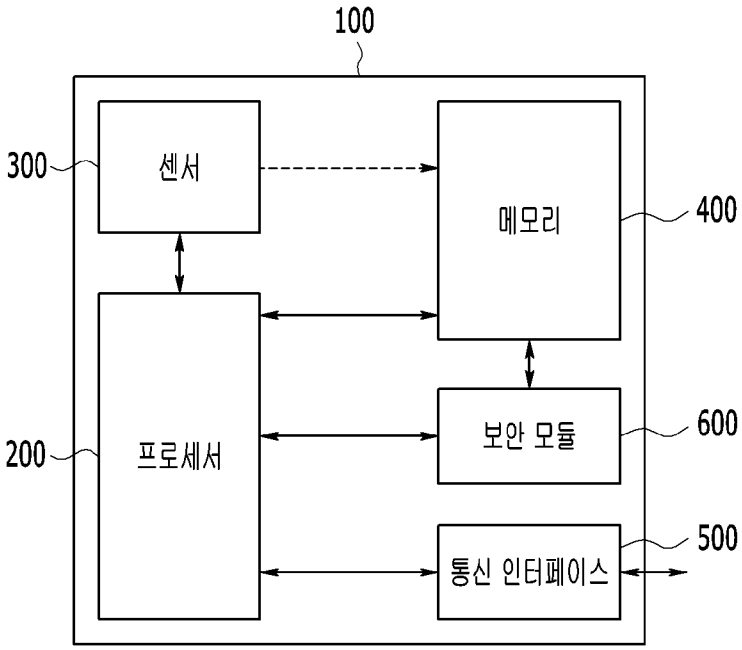
[Fig. 2]


2000
100
인증 장치
4000
제어 서버
로그인 허용 요청
웹사이트 서버
3000

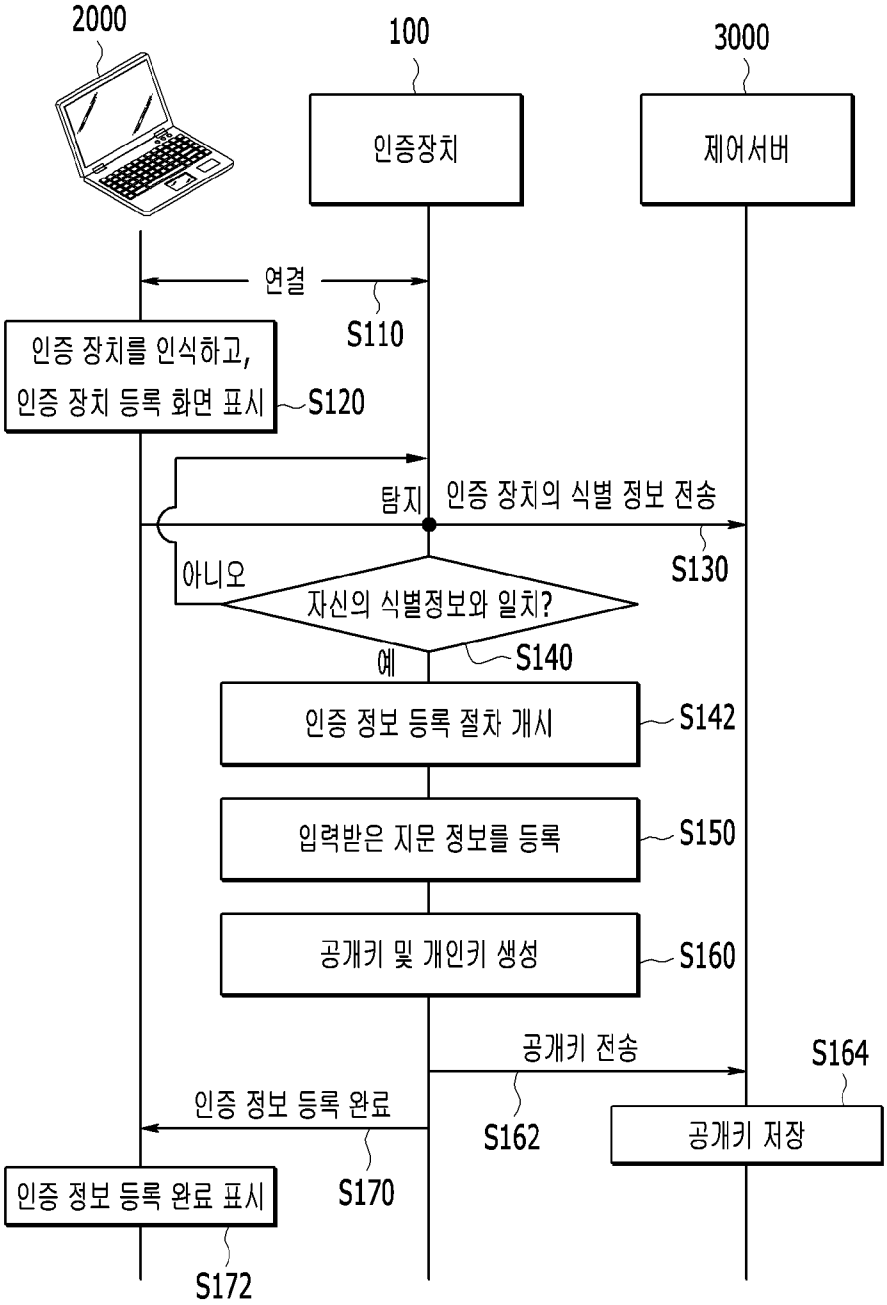
[Fig. 3]


10
로그인
공고사항
기업통합구매
핑거 (FINGER) 로그인 중
회원가입
고객사 공지사항
협력사 공지사항
고객님의 지문 데이타 인식 중입니다.
20

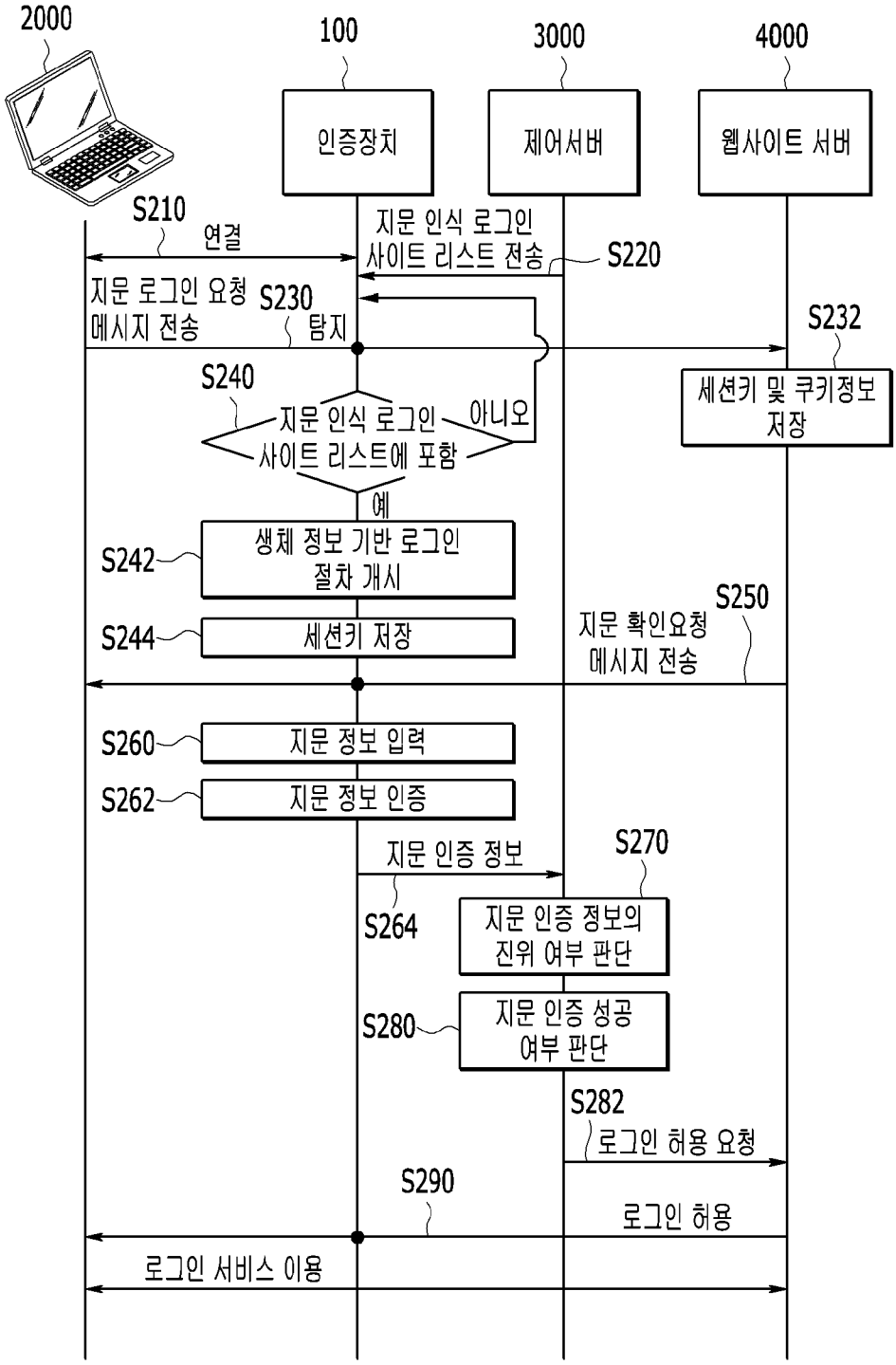
[Fig. 4]


100
300
센서
메모리
400
프로세서
200
보안 모듈
600
통신 인터페이스
500

[Fig. 5]


2000
100
3000
인증장치
제어서버
연결
S110
인증 장치를 인식하고,
인증 장치 등록 화면 표시
S120
탐지
인증 장치의 식별 정보 전송
S130
아니오
자신의 식별정보와 일치?
예
S140
인증 정보 등록 절차 개시
S142
입력받은 지문 정보를 등록
S150
공개키 및 개인키 생성
S160
공개키 전송
S164
인증 정보 등록 완료
S162
공개키 저장
인증 정보 등록 완료 표시
S170
S172

[Fig. 6]


2000
100
3000
4000
인증장치
제어서버
웹사이트 서버
S210
연결
지문 인식 로그인
사이트 리스트 전송
S220
지문 로그인 요청
메시지 전송
S230
탐지
S232
세션키 및 쿠키정보
저장
S240
지문 인식 로그인
사이트 리스트에 포함
아니오
예
S242
생체 정보 기반 로그인
절차 개시
S244
세션키 저장
S250
지문 확인요청
메시지 전송
S260
지문 정보 입력
S262
지문 정보 인증
지문 인증 정보
S270
S264
지문 인증 정보의
진위 여부 판단
S280
지문 인증 성공
여부 판단
S282
로그인 허용 요청
S290
로그인 허용
로그인 서비스 이용

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2016/014628

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i, H04L 9/08(2006.01)i, G06K 9/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/32; G06F 21/30; G06F 21/20; H04L 12/26; G06Q 50/00; H04L 12/22; H04L 9/08; G06K 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: biometrics data, authentication, website, login, permission, session information

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2014-0085295 A (ROWEM INC.) 07 July 2014 See paragraphs [0038]-[0048], [0075]-[0077], [0082]-[0084], [0092]; claim 1; and figures 1-2, 6-7.	1-20
Y	KR 10-0544217 B1 (NOMADIX, INC.) 23 January 2006 See paragraph [0023]; claims 3-7; and figure 1.	1-7,19-20
Y	KR 10-2011-0059963 A (SAMSUNG SDS CO., LTD.) 08 June 2011 See paragraphs [0057]-[0069], [0086]; and figures 1, 3-4.	2-4,8-11,13-16 ,18-20
Y	KR 10-0941321 B1 (FROM2 INFORMATION & COMMUNICATIONS CO., LTD.) 11 February 2010 See paragraph [0035]; claims 2-4; and figures 1-2.	6-7,10-20
A	KR 10-0998241 B1 (T-MONET. CO., LTD.) 06 December 2010 See paragraphs [0020]-[0028]; and figure 2.	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 MARCH 2017 (16.03.2017)	**16 MARCH 2017 (16.03.2017)**

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2016/014628

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2014-0085295 A	07/07/2014	CN 105027131 A	04/11/2015
		CN 105229655 A	06/01/2016
		EP 2940616 A2	04/11/2015
		EP 2940616 A4	16/11/2016
		EP 2940617 A1	04/11/2015
		EP 2940617 A4	24/08/2016
		JP 2016-508270 A	17/03/2016
		JP 2016-511855 A	21/04/2016
		JP 6055932 B2	27/12/2016
		KR 10-1416541 B1	09/07/2014
		KR 10-2014-0085280 A	07/07/2014
		US 2015-0341348 A1	26/11/2015
		US 2015-0350178 A1	03/12/2015
		WO 2014-104507 A1	03/07/2014
		WO 2014-104777 A2	03/07/2014
		WO 2014-104777 A3	31/07/2014
KR 10-0544217 B1	23/01/2006	AU 2001-57540 A1	20/11/2001
		CA 2408233 A1	15/11/2001
		CA 2408233 C	09/01/2007
		CN 1433615 A	30/07/2003
		CN 1433615 C	02/04/2008
		EP 1282955 A2	12/02/2003
		EP 1282955 B1	09/02/2005
		IL 152642 B	07/08/2008
		JP 2004-507908 A	11/03/2004
		JP 4471554 B2	02/06/2010
		WO 2001-86877 A3	15/11/2001
KR 10-2011-0059963 A	08/06/2011	NONE	
KR 10-0941321 B1	11/02/2010	KR 10-2009-0035968 A	13/04/2009
KR 10-0998241 B1	06/12/2010	KR 10-2009-0131967 A	30/12/2009

국 제 조 사 보 고 서

국제출원번호
PCT/KR2016/014628

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 9/32(2006.01)i, H04L 9/08(2006.01)i, G06K 9/00(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
H04L 9/32; G06F 21/30; G06F 21/20; H04L 12/26; G06Q 50/00; H04L 12/22; H04L 9/08; G06K 9/00

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: 생체 정보, 인증, 웹사이트, 로그인, 허용, 세션 정보

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-2014-0085295 A (주식회사 로웸) 2014.07.07 단락 [0038]-[0048], [0075]-[0077], [0082]-[0084], [0092]; 청구항 1; 및 도면 1-2, 6-7 참조.	1-20
Y	KR 10-0544217 B1 (노마딕스, 인코포레이티드) 2006.01.23 단락 [0023]; 청구항 3-7; 및 도면 1 참조.	1-7,19-20
Y	KR 10-2011-0059963 A (삼성에스디에스 주식회사) 2011.06.08 단락 [0057]-[0069], [0086]; 및 도면 1, 3-4 참조.	2-4,8-11,13-16 ,18-20
Y	KR 10-0941321 B1 (프롬투정보통신(주)) 2010.02.11 단락 [0035]; 청구항 2-4; 및 도면 1-2 참조.	6-7,10-20
A	KR 10-0998241 B1 (주식회사 티모넷) 2010.12.06 단락 [0020]-[0028]; 및 도면 2 참조.	1-20

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2017년 03월 16일 (16.03.2017)	2017년 03월 16일 (16.03.2017)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-481-8578

심사관
안정환
전화번호 +82-42-481-8633

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2016/014628

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2014-0085295 A	2014/07/07	CN 105027131 A	2015/11/04
		CN 105229655 A	2016/01/06
		EP 2940616 A2	2015/11/04
		EP 2940616 A4	2016/11/16
		EP 2940617 A1	2015/11/04
		EP 2940617 A4	2016/08/24
		JP 2016-508270 A	2016/03/17
		JP 2016-511855 A	2016/04/21
		JP 6055932 B2	2016/12/27
		KR 10-1416541 B1	2014/07/09
		KR 10-2014-0085280 A	2014/07/07
		US 2015-0341348 A1	2015/11/26
		US 2015-0350178 A1	2015/12/03
		WO 2014-104507 A1	2014/07/03
		WO 2014-104777 A2	2014/07/03
		WO 2014-104777 A3	2014/07/31
KR 10-0544217 B1	2006/01/23	AU 2001-57540 A1	2001/11/20
		CA 2408233 A1	2001/11/15
		CA 2408233 C	2007/01/09
		CN 1433615 A	2003/07/30
		CN 1433615 C	2008/04/02
		EP 1282955 A2	2003/02/12
		EP 1282955 B1	2005/02/09
		IL 152642 B	2008/08/07
		JP 2004-507908 A	2004/03/11
		JP 4471554 B2	2010/06/02
		WO 2001-86877 A3	2001/11/15
KR 10-2011-0059963 A	2011/06/08	없음	
KR 10-0941321 B1	2010/02/11	KR 10-2009-0035968 A	2009/04/13
KR 10-0998241 B1	2010/12/06	KR 10-2009-0131967 A	2009/12/30