(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

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

WIPO | PCT

(10) 국제공개번호
WO 2017/111483 A1

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

(21) 국제출원번호: PCT/KR2016/015074

(22) 국제출원일: 2016 년 12 월 22 일 (22.12.2016)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2015-0185448 2015 년 12 월 23 일 (23.12.2015) KR
10-2016-0175017 2016 년 12 월 20 일 (20.12.2016) 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). 김명우 (KIM, Myung Woo); 11940 경기도 구리시 체육관로 40, 301 동 1903 호, Gyeonggi-do (KR). 장덕문 (CHANG, Deok-Moon); 06762 서울시 서초구 바우뫼로 7 길 51, 104 동 1403 호, Seoul (KR).

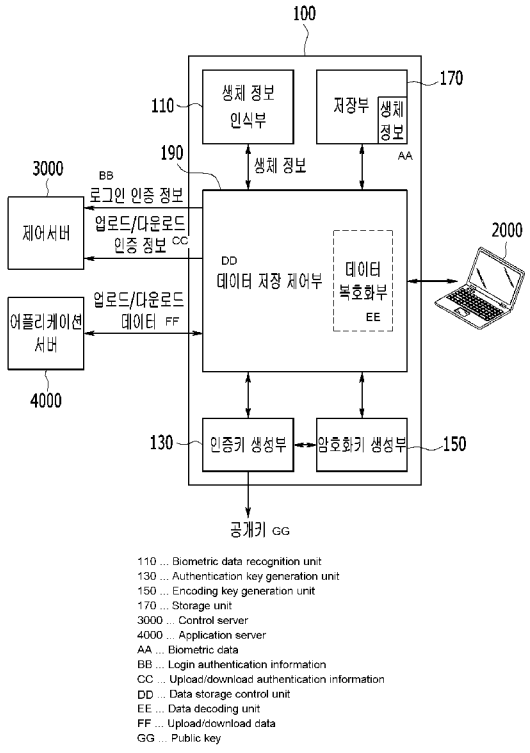
(74) 대리인: 유미특허법인 (YOU ME PATENT AND LAW FIRM); 06134 서울시 강남구 테헤란로 115, Seoul (KR).

(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.

[다음 쪽 계속]

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

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



(57) **Abstract**: The present invention relates to a method for a biometric data-based authentication device, which is connected to a computing device, being linked to a control server and processing data upload and download, to and from an application server, requested from the computing device. The method comprises the steps of: detecting an upload request message transmitted to the application server from the computing device; extracting a first identifier comprised in the upload request message; outputting a first biometric data authentication result on first biometric data that has been received; and transmitting, to the control server, upload authentication information comprising a first data encoding key, the first biometric data authentication result and the first identifier.

(57) **요약서**: 컴퓨팅 장치에 연결된 생체 정보 기반 인증 장치가 제어 서버와 연동하여 컴퓨팅 장치에서 요청된 어플리케이션 서버로의 데이터 업로드 및 다운로드를 처리하는 방법으로서, 컴퓨팅 장치로부터 어플리케이션 서버로 전달되는 업로드 요청 메시지를 탐지하는 단계, 업로드 요청 메시지에 포함된 제 1 식별자를 추출하는 단계, 입력받은 제 1 생체 정보에 대한 제 1 생체 정보 인증 결과를 출력하는 단계, 그리고 제 1 식별자, 제 1 생체 정보 인증 결과, 그리고 제 1 데이터 암호화키를 포함하는 업로드 인증 정보를 제어 서버로 전송하는 단계를 포함한다.

WO 2017/111483 A1

(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).

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

명세서

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

기술분야

[1] 본 발명은 생체 정보 기반 인증에 관한 것이다.

배경기술

[2] 데이터를 원격의 서버에 저장하고, 네트워크를 통해 서버에 접속하여 데이터를 열람하고 다운로드할 수 있는 클라우드 저장 서비스가 널리 사용되고 있다.

[3] 대부분의 클라우드 저장 서비스는 사용자의 접근 권한을 확인하기 위해 지정된 로그인 방법을 정하고, 사용자에게 로그인을 요청한다. 지금까지의 로그인 방법은 사용자가 클라우드 저장 서비스 가입 시 등록한 아이디와 패스워드를 사용하는 방법이 일반적이다.

[4] 또한 대부분의 클라우드 저장 서비스는 데이터를 평문으로 보관한다. 따라서, 해킹 등으로 아이디와 패스워드가 노출되는 경우, 클라우드 저장 서비스에 저장된 데이터가 유출될 가능성이 있다. 이렇게, 타인이 아이디와 패스워드만 알아 낸다면 데이터를 쉽게 확인할 수 있다. 이와 같이, 클라우드 저장 서비스는 데이터 접근성을 높이는 장점이 있으나, 보안성이 보장되지 않으므로, 업무상 보안이나 프라이버시 보안이 요구되는 데이터를 원격의 저장소에 저장할 수 없는 한계가 있다.

발명의 상세한 설명

기술적 과제

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

과제 해결 수단

[6] 한 실시예에 따른 컴퓨팅 장치에 연결된 생체 정보 기반 인증 장치가 제어 서버와 연동하여 상기 컴퓨팅 장치에서 요청된 어플리케이션 서버로의 로그인을 처리하는 방법으로서, 상기 컴퓨팅 장치로부터 상기 어플리케이션 서버로 전달되는 로그인 요청 메시지를 탐지하는 단계, 상기 로그인 요청 메시지에 포함된 식별자를 추출하는 단계, 입력받은 생체 정보에 대한 생체 정보 인증 결과를 출력하는 단계, 그리고 상기 식별자와 상기 생체 정보 인증 결과를 포함하는 로그인 인증 정보를 상기 제어 서버로 전송하는 단계를 포함한다. 상기 식별자는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 로그인 허용 대상 판단 시 사용된다. 상기 생체 정보 인증 결과는 상기 제어 서버에서 로그인 허용 여부 판단 시 사용된다.

[7] 상기 로그인 인증 정보는 사용자 식별정보를 더 포함하고, 상기 사용자 식별정보는 상기 제어 서버와 상기 어플리케이션 서버 중 적어도 하나의

서버에서 등록된 사용자 여부 판단 시 사용될 수 있다.

[8] 상기 식별자는 상기 컴퓨팅 장치에서 랜덤하게 생성된 정보일 수 있다.

[9] 다른 실시예에 따른 컴퓨팅 장치에 연결된 생체 정보 기반 인증 장치가 제어 서버와 연동하여 상기 컴퓨팅 장치에서 요청된 어플리케이션 서버로의 데이터 업로드 및 다운로드를 처리하는 방법으로서, 상기 컴퓨팅 장치로부터 상기 어플리케이션 서버로 전달되는 업로드 요청 메시지를 탐지하는 단계, 상기 업로드 요청 메시지에 포함된 제1 식별자를 추출하는 단계, 입력받은 제1 생체 정보에 대한 제1 생체 정보 인증 결과를 출력하는 단계, 그리고 상기 제1 식별자, 상기 제1 생체 정보 인증 결과, 그리고 제1 데이터 암호화키를 포함하는 업로드 인증 정보를 상기 제어 서버로 전송하는 단계를 포함한다. 상기 제1 식별자는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 업로드 허용 대상 판단 시 사용된다. 상기 제1 생체 정보 인증 결과는 상기 제어 서버에서 업로드 허용 여부 판단 시 사용된다. 상기 제1 데이터 암호화키는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 업로드 요청된 데이터를 암호화하는데 사용된다.

[10] 상기 업로드 인증 정보는 사용자 식별정보를 더 포함하고, 상기 사용자 식별정보는 상기 제어 서버와 상기 어플리케이션 서버 중 적어도 하나의 서버에서 등록된 사용자 여부 판단 시 사용될 수 있다.

[11] 상기 데이터 업로드 및 다운로드 방법은 상기 제1 생체 정보 인증 결과가 성공이면, 저장된 상기 제1 데이터 암호화키를 가져오는 단계를 더 포함할 수 있다.

[12] 상기 데이터 업로드 및 다운로드 방법은 상기 컴퓨팅 장치로부터 상기 어플리케이션 서버로 전달되는 다운로드 요청 메시지를 탐지하는 단계, 상기 다운로드 요청 메시지에 포함된 제2 식별자를 추출하는 단계, 입력받은 제2 생체 정보에 대한 제2 생체 정보 인증 결과를 출력하는 단계, 상기 제2 식별자, 상기 제2 생체 정보 인증 결과, 그리고 제2 데이터 암호화키를 포함하는 다운로드 인증 정보를 상기 제어 서버로 전송하는 단계, 상기 어플리케이션 서버로부터 상기 다운로드 요청 메시지에 관련된 다운로드 데이터를 수신하는 단계, 그리고 상기 다운로드 데이터를 상기 컴퓨팅 장치로 전달하는 단계를 더 포함할 수 있다. 상기 제2 식별자는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 다운로드 허용 대상 판단 시 사용될 수 있다. 상기 제2 생체 정보 인증 결과는 상기 제어 서버에서 다운로드 허용 여부 판단 시 사용될 수 있다. 상기 제2 데이터 암호화키는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 다운로드 요청된 데이터를 복호화하는데 사용될 수 있다.

[13] 상기 데이터 업로드 및 다운로드 방법은 상기 컴퓨팅 장치로부터 상기 어플리케이션 서버로 전달되는 다운로드 요청 메시지를 탐지하는 단계, 상기 다운로드 요청 메시지에 포함된 제2 식별자를 추출하는 단계, 입력받은 제2 생체

정보에 대한 제2 생체 정보 인증 결과를 출력하는 단계, 상기 제2 식별자, 그리고 상기 제2 생체 정보 인증 결과를 포함하는 다운로드 인증 정보를 상기 제어 서버로 전송하는 단계, 상기 어플리케이션 서버로부터 상기 다운로드 요청 메시지에 관련된 다운로드 데이터를 수신하는 단계, 그리고 상기 다운로드 데이터를 상기 제1 데이터 암호화키에 관련된 제2 데이터 암호화키로 복호화하여 상기 컴퓨팅 장치로 전달하는 단계를 더 포함할 수 있다. 상기 제2 식별자는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 다운로드 허용 대상 판단 시 사용될 수 있다. 상기 제2 생체 정보 인증 결과는 상기 제어 서버에서 다운로드 허용 여부 판단 시 사용될 수 있다.

[14] 또 다른 실시예에 따른 제어 서버가 생체 정보 기반 인증 장치 및 어플리케이션 서버와 연동하여 컴퓨팅 장치에서 요청된 절차를 처리하는 방법으로서, 상기 생체 정보 기반 인증 장치로부터 제1 식별자, 제1 생체 정보 인증 결과, 그리고 제1 데이터 암호화키를 포함하는 업로드 인증 정보를 수신하는 단계, 상기 업로드 인증 정보를 기초로 상기 제1 식별자를 업로드 허용 대상으로 판단하는 단계, 그리고 상기 제1 식별자와 상기 제1 데이터 암호화키를 포함하는 업로드 허용 요청 메시지를 상기 어플리케이션 서버로 전송하는 단계를 포함한다. 상기 제1 식별자는 상기 어플리케이션 서버에서 업로드 허용 대상 판단 시 사용된다. 상기 제1 데이터 암호화키는 상기 어플리케이션 서버에서 업로드 요청된 데이터를 암호화하는데 사용된다.

[15] 상기 처리 방법은 상기 생체 정보 기반 인증 장치로부터 제2 식별자그리고 제2 생체 정보 인증 결과를 포함하는 다운로드 인증 정보를 수신하는 단계, 상기 다운로드 인증 정보를 기초로 상기 제2 식별자를 다운로드 허용 대상으로 판단하는 단계, 그리고 상기 제2 식별자를 포함하는 다운로드 허용 요청 메시지를 상기 어플리케이션 서버로 전송하는 단계를 더 포함하고, 상기 제2 식별자는 상기 어플리케이션 서버에서 다운로드 허용 대상 판단 시 사용될 수 있다.

[16] 상기 제1 식별자를 업로드 허용 대상으로 판단하는 단계는 상기 업로드 인증 정보에 사용자 식별정보가 더 포함된 경우, 상기 사용자 식별정보가 등록된 정보이고, 상기 제1 생체 정보 인증 결과가 성공이면, 상기 제1 식별자를 업로드 허용 대상으로 판단하고, 상기 제2 식별자를 다운로드 허용 대상으로 판단하는 단계는 상기 다운로드 인증 정보에 상기 사용자 식별정보가 더 포함된 경우, 상기 사용자 식별정보가 등록된 정보이고, 상기 제2 생체 정보 인증 결과가 성공이면, 상기 제2 식별자를 다운로드 허용 대상으로 판단할 수 있다.

[17] 또 다른 실시예에 따른 어플리케이션 서버가 제어 서버와 연동하여 컴퓨팅 장치에서 요청된 절차를 처리하는 방법으로서, 상기 제어 서버로부터 제1 식별자와 제1 데이터 암호화키를 포함하는 업로드 허용 요청 메시지를 수신하는 단계, 상기 컴퓨팅 장치로부터 상기 제1 식별자와 업로드 요청된 데이터를

포함하는 업로드 요청 메시지를 수신하는 단계, 그리고 상기 제1 식별자에 대응된 상기 제1 데이터 암호화키를 이용하여 상기 업로드 요청된 데이터를 암호화하여 저장하는 단계를 포함하고, 상기 제1 데이터 암호화키는 생체 정보 기반 인증 장치에서 생성되어 상기 제어 서버로 전송된 정보이다.

[18] 상기 처리 방법은 상기 업로드 허용 요청 메시지는 사용자 식별정보를 더 포함하고, 상기 업로드 요청된 데이터를 암호화하여 저장하는 단계는 상기 사용자 식별정보가 등록된 정보인 경우, 상기 업로드 요청된 데이터를 암호화하고, 암호화한 데이터를 상기 사용자 식별정보에 대응된 데이터 저장소에 저장할 수 있다.

[19] 상기 처리 방법은 상기 제어 서버로부터 제2 식별자와 제2 데이터 암호화키를 포함하는 다운로드 허용 요청 메시지를 수신하는 단계, 상기 컴퓨팅 장치로부터 상기 제2 식별자와 특정 데이터에 대한 다운로드 요청을 포함하는 다운로드 요청 메시지를 수신하는 단계, 상기 제2 식별자에 대응된 상기 제2 데이터 암호화키를 이용하여 상기 특정 데이터를 복호화하는 단계, 그리고 복호화한 데이터를 상기 컴퓨팅 장치로 전송하는 단계를 더 포함하고, 상기 제2 데이터 암호화키는 상기 생체 정보 기반 인증 장치에서 생성되어 상기 제어 서버로 전송된 정보일 수 있다.

[20] 상기 업로드 요청된 데이터를 암호화하여 저장하는 단계는 상기 업로드 허용 요청 메시지에 사용자 식별정보가 더 포함되고 상기 사용자 식별정보가 등록된 정보인 경우, 상기 업로드 요청된 데이터를 암호화하고, 암호화한 데이터를 상기 사용자 식별정보에 대응된 데이터 저장소에 저장할 수 있다. 상기 특정 데이터를 복호화하는 단계는 상기 다운로드 허용 요청 메시지에 상기 사용자 식별정보가 더 포함되고 상기 사용자 식별정보가 등록된 정보인 경우, 상기 사용자 식별정보에 대응된 데이터 저장소에서 상기 특정 데이터를 찾고, 상기 특정 데이터를 상기 제2 데이터 암호화키로 복호화할 수 있다.

[21] 상기 처리 방법은 상기 제어 서버로부터 제2 식별자를 포함하는 다운로드 허용 요청 메시지를 수신하는 단계, 상기 컴퓨팅 장치로부터 상기 제2 식별자와 특정 데이터에 대한 다운로드 요청을 포함하는 다운로드 요청 메시지를 수신하는 단계, 그리고 상기 제2 식별자에 대응된 상기 특정 데이터를 상기 생체 정보 기반 인증 장치로 전송하는 단계를 더 포함하고, 상기 특정 데이터는 상기 생체 정보 기반 인증 장치에서 복호화될 수 있다.

[22] 또 다른 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 데이터 업로드 인증을 위한 제1 프로그램을 포함한다. 상기 제1 프로그램은 컴퓨팅 장치로부터 어플리케이션 서버로

전달되는 업로드 요청 메시지를 탐지하면, 상기 센서를 활성화하고, 상기 보안 모듈로부터 제1 데이터 암호화키를 획득한 후, 업로드 인증 정보를 생성하고, 상기 업로드 인증 정보를 제어 서버로 전송하는 명령어들(instructions)을 포함한다. 상기 업로드 인증 정보는 상기 업로드 요청 메시지에서 추출한 제1 식별자, 상기 센서로부터 입력된 제1 생체 정보의 제1 생체 정보 인증 결과, 그리고 상기 제1 데이터 암호화키를 포함하며, 상기 제1 식별자는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 업로드 허용 대상 판단 시 사용되고, 상기 제1 생체 정보 인증 결과는 상기 제어 서버에서 업로드 허용 여부 판단 시 사용되며, 상기 제1 데이터 암호화키는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 업로드 요청된 데이터를 암호화하는데 사용된다.

[23] 상기 프로그램은 데이터 다운로드 인증을 위한 제2 프로그램을 포함하고, 상기 제2 프로그램은 상기 컴퓨팅 장치로부터 상기 어플리케이션 서버로 전달되는 다운로드 요청 메시지를 탐지하면, 상기 센서를 활성화하고, 상기 보안 모듈로부터 제2 데이터 암호화키를 획득한 후, 다운로드 인증 정보를 생성하고, 상기 다운로드 인증 정보를 상기 제어 서버로 전송하는 명령어들을 포함한다. 상기 다운로드 인증 정보는 상기 다운로드 요청 메시지에서 추출한 제2 식별자, 그리고 상기 센서로부터 입력된 제2 생체 정보의 제2 생체 정보 인증 결과를 포함하며, 상기 제2 식별자는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 다운로드 허용 대상 판단 시 사용되고, 상기 제2 생체 정보 인증 결과는 상기 제어 서버에서 다운로드 허용 여부 판단 시 사용될 수 있다.

[24] 상기 제2 프로그램은 상기 어플리케이션 서버로부터 상기 다운로드 요청 메시지에 관련된 다운로드 데이터를 수신하면, 상기 다운로드 데이터를 상기 제1 데이터 암호화키에 관련된 제2 데이터 암호화키로 복호화하여 상기 컴퓨팅 장치로 전달하는 명령어들을 더 포함할 수 있다.

[25] 상기 프로그램은 로그인 인증을 위한 제3 프로그램을 포함하고, 상기 제3 프로그램은 상기 컴퓨팅 장치로부터 상기 어플리케이션 서버로 전달되는 로그인 요청 메시지를 탐지하면, 상기 센서를 활성화하고, 로그인 인증 정보를 생성하며, 상기 로그인 인증 정보를 상기 제어 서버로 전송하는 명령어들을 포함할 수 있다. 상기 로그인 인증 정보는 상기 로그인 요청 메시지에서 추출한 제3 식별자와 상기 센서로부터 입력된 제3 생체 정보의 제3 생체 정보 인증 결과를 포함하며, 상기 제3 식별자는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 로그인 허용 대상 판단 시 사용되고, 상기 제3 생체 정보 인증 결과는 상기 제어 서버에서 로그인 허용 여부 판단 시 사용될 수 있다.

발명의 효과

[26] 본 발명의 실시예에 따르면 어플리케이션 서버는 데이터를 암호화하여 저장하므로 암호화된 데이터가 노출될 수는 있어도 본인 이외에는 암호화된 데이터를 복호화할 수 없다. 본 발명의 실시예에 따르면 어플리케이션 서버는 데이터 업로드/다운로드 시에 메모리에 일시적으로 존재하는 암호화키를 이용하여 암호화/복호화하므로, 암호화키는 어느 네트워크 장치에도 저장되지 않는다. 따라서, 본 발명의 실시예에 따르면 보안성을 높일 수 있다. 또한, 본 발명의 실시예에 따르면 인증 장치와 어플리케이션 서버 사이의 통신 구간은 암호화되므로, 인증 장치와 어플리케이션 서버 사이에서 전송되는 데이터는 통신 구간 암호화 및 암호화키에 의한 암호화로 보호되므로 모든 전송 구간과 저장 위치에서 데이터 보안성이 매우 높다.

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 인증 장치의 하드웨어 구성도이다.

[30] 도 4는 본 발명의 한 실시예에 따른 인증 장치의 인증 정보 등록 방법의 흐름도이다.

[31] 도 5는 본 발명의 한 실시예에 따른 로그인 방법의 흐름도이다.

[32] 도 6은 본 발명의 한 실시예에 따른 데이터 업로드 방법의 흐름도이다.

[33] 도 7은 본 발명의 한 실시예에 따른 데이터 다운로드 방법의 흐름도이다.

[34] 도 8은 본 발명의 다른 실시예에 따른 데이터 다운로드 방법의 흐름도이다.

발명의 실시를 위한 형태

[35] 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.

[36] 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.

[37] 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.

[38] 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 도면이다.

[39] 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.

[40] 도 2를 참고하면, 네트워크 장치는 제어 서버(3000)와 어플리케이션 서버(4000), 그리고 데이터 저장소를 포함한다. 여기서, 데이터 저장소는 어플리케이션 서버(4000)와 연동하는 적어도 하나의 데이터 저장소로서, 어플리케이션 서버(4000)의 저장 요청(업로드 요청)에 의해 데이터를 저장하고, 출력 요청(다운로드 요청)에 의해 저장된 데이터를 어플리케이션 서버(4000)로 전달한다.

[41] 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.

[42] 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. 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.

[43] 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 접속하는 것으로 설명한다. 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 내용(메시지)를 확인할 수 있다.

[44] 다시 도 1을 참고하면, 인증 장치(100)는 생체 정보 인식부(110), 인증키 생성부(130), 암호화키 생성부(150), 저장부(170), 데이터 저장 제어부(190)를 포함한다.

[45] 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.

[46] 인증키 생성부(130)는 인증 정보 등록 단계에서 지문 정보를 등록(저장)하고, 공개키와 개인키를 생성한다. 인증키 생성부(130)는 공개키를 제어 서버(3000)로 전송한다. 개인키는 지정된 장소에 저장된다. 이때, 개인키는 암호화되어 저장될 수 있다. 개인키는 하드웨어 보안 모듈(Hardware Security Module, HSM)에 의해 암호화될 수 있다.

[47] 인증키 생성부(130)는 키 생성 알고리즘에 따라 공개키와 개인키를 생성한다. 키 생성 알고리즘은 RSA 키 생성 알고리즘일 수 있다. 인증키 생성부(130)가 공개키와 개인키 생성 시 입력받는 정보는 다양하게 설계될 수 있다. 예를 들면, 인증키 생성부(130)는 난수를 입력받고, 난수를 기초로 공개키와 개인키를 생성할 수 있다. 인증키 생성부(130)는 생체(지문) 정보를 기초로 공개키와 개인키를 생성할 수 있다. 또는 인증키 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.

[48] 암호화키 생성부(150)는 데이터 암호화에 사용되는 데이터 암호화키를 생성한다. 데이터 암호화키는 인증 정보 등록 시 생성될 수 있다. 암호화키 생성부(150)가 데이터 암호화키 생성 시 입력받는 정보는 다양하게 설계될 수 있다. 예를 들면, 암호화키 생성부(150)는 생체 정보와 추가 식별 정보 중 적어도 하나를 기초로 데이터 암호화키를 생성할 수 있다. 암호화키 생성부(150)가 생체 정보를 입력받고, 생체 정보를 기초로 데이터 암호화키를 생성할 수 있으나, 이에 한정되는 것은 아니다. 또한, 데이터 암호화키는 인증 장치(100)의 내부에 저장될 수 있고, 또는 인증 장치(100)의 내부에 저장되지 않고 데이터 암호화/복호화가 필요할 때마다 사용자가 입력한 생체 정보를 기초로 생성될 수 있다. 저장된 데이터 암호화키는 지문 입력을 통해 호출될 수 있다. 데이터 암호화키는 지문 정보, 비밀번호, 개인키 등으로 암호화되어 저장될 수 있다. 암호화키 생성부(150)는 하드웨어 보안 모듈(HSM)일 수 있다. 암호화키

생성부(150)는 AES(Advanced Encryption Standard) 암호화 알고리즘을 사용하여 데이터 암호화키를 생성할 수 있다.

[49] 데이터 저장 제어부(190)는 제어 서버(3000)로부터 생체 정보 기반 로그인을 지원하는 지문 인식 로그인 사이트 리스트(화이트 리스트)를 수신할 수 있다. 여기서는, 데이터 저장 제어부(190)가 어플리케이션 서버(4000)가 지문 인식 로그인 사이트임을 알고 있고, 어플리케이션 서버(4000)를 식별할 수 있는 각종 정보(예를 들면, 호스트명(Host), IP 주소, URI 등)들을 저장하고 있다고 가정한다.

[50] 사용자가 컴퓨팅 장치(2000)를 통해 어플리케이션 서버(4000)에 접속하거나, 어플리케이션 서버(4000)에 접속한 후 로그인 요청(선택)을 하면, 컴퓨팅 장치(2000)로부터 어플리케이션 서버(4000)로 로그인 요청 메시지가 전달된다.

[51] 로그인 요청 메시지는 인증 대상을 나타내는 식별자(ID)를 포함하고, 식별자는 컴퓨팅 장치(2000)에서 랜덤하게 생성될 수 있다. 식별자가 유효한 시간 동안, 인증 장치(100), 제어 서버(3000), 어플리케이션 서버(4000)는 수신 메시지에 포함된 식별자를 확인하여 인증 대상을 공통적으로 식별한다. 식별자는 컴퓨팅 장치(2000)에서 생성되므로, 컴퓨팅 장치(2000)에서 전송된 메시지임을 나타내는 정보일 수 있다. 로그인 요청 메시지는 사용자 식별정보를 더 포함할 수 있다. 사용자 식별정보는 인증 장치의 식별정보(시리얼 정보), 사용자 아이디와 패스워드 또는 전화 번호 등 사용자를 구분할 수 있는 다양한 정보일 수 있다. 컴퓨팅 장치(2000)는 사용자로부터 사용자 식별정보를 입력 받을 수 있다. 또는 컴퓨팅 장치(2000)는 인증 장치(100)로부터 사용자 식별정보(예를 들면, 시리얼 정보)를 가져올 수 있다.

[52] 데이터 저장 제어부(190)는 컴퓨팅 장치(2000)로부터 어플리케이션 서버(4000)로 전달되는 로그인 요청 메시지를 탐지한다.

[53] 데이터 저장 제어부(190)는 로그인 요청 메시지를 탐지하여 어플리케이션 서버(4000)로의 로그인 요청 단계를 개시한다. 컴퓨팅 장치(2000)에서 어플리케이션 서버(4000)로 전송하는 패킷은 인증 장치(100)의 통신 모듈을 통해 어플리케이션 서버(4000)로 전달된다. 따라서, 데이터 저장 제어부(190)는 로그인 요청 메시지에 포함된 정보(예를 들면, HTTP 프로토콜의 호스트(host), 목적지 주소, URI 등)를 기초로 지문 인식 로그인 사이트인 어플리케이션 서버(4000)로 전송되는 메시지이고, 로그인 요청 단계라는 것을 확인할 수 있다.

[54] 로그인 요청 단계인 경우, 데이터 저장 제어부(190)는 로그인 요청 메시지에 포함된 식별자를 파싱해서 저장한다. 그리고 데이터 저장 제어부(190)는 생체 정보 인식부(110)의 센서를 활성화하고, 생체 정보 인식부(110)로부터 사용자의 지문 정보를 수신하여 지문 인증을 한다. 지문 인증 방법은 다양할 수 있으며, 예를 들면, 데이터 저장 제어부(190)는 수신한 지문 정보와 저장부(170)에 저장된 지문 정보를 비교하여 지문 인증을 할 수 있다. 이때, 컴퓨팅 장치(2000)는 지문 확인 요청 화면을 표시하여, 사용자가 생체 정보 인식부(110)로 지문을

인식하도록 안내할 수 있다.

[55] 데이터 저장 제어부(190)는 파싱한 식별자에 대한 지문 인증 결과를 포함하는 로그인 인증 정보를 제어 서버(3000)로 전달한다. 이때, 데이터 저장 제어부(190)는 로그인 인증 정보를 개인키로 서명(암호화)하여 제어 서버(3000)로 전달할 수 있다. 로그인 인증 정보는 식별자, 지문 인증 결과(예를 들면, 0 또는 1), 그리고 사용자 식별정보를 포함할 수 있다. 사용자 식별정보는 인증 장치의 식별정보(시리얼 정보), 사용자 아이디와 패스워드 또는 전화 번호 등 사용자를 구분할 수 있는 다양한 정보일 수 있다. 사용자 식별정보는 컴퓨팅 장치(2000)로부터 전송되는 정보이거나, 인증 장치(100)가 알고 있는 정보일 수 있다. 사용자 식별정보는 인증 장치(100), 제어 서버(3000), 어플리케이션 서버(4000), 데이터 저장소가 공유하는 정보이다. 앞으로는 인증 장치(100)가 사용자 식별정보를 알고 있고, 제어 서버(3000)로 전달하는 인증 정보에 사용자 식별정보를 포함하여 전송하는 것으로 설명한다. 특히, 사용자 식별정보는 인증 장치의 식별정보(시리얼 정보)일 수 있고, 인증 장치 등록 시 제어 서버(3000)에 등록될 수 있다. 또한, 어플리케이션 서버(4000)와 데이터 저장소 역시 등록된 사용자 식별정보를 알고 있고, 사용자 식별정보에 매핑하여 데이터를 저장한다고 가정한다. 어플리케이션 서버(4000)와 데이터 저장소가 사용자 식별정보를 등록하는 방법은 다양할 수 있다.

[56] 제어 서버(3000)는 로그인 인증 정보에 포함된 정보를 기초로 로그인 허용 대상인지 판단한다. 제어 서버(3000)는 로그인 인증 정보에 포함된 사용자 식별정보가 등록된 정보이고, 지문 인증 결과가 성공이면, 어플리케이션 서버(4000)로 로그인 인증 정보에 포함된 식별자에 대한 로그인 허용을 요청한다. 제어 서버(3000)는 사용자 식별정보, 지문 인증 결과 정보, 그리고 로그인 허용 식별자를 어플리케이션 서버(4000)로 전송할 수 있다. 이때, 제어 서버(3000)는 개인키로 서명(암호화)된 로그인 인증 정보를 공개키로 복호화하고, 복호 결과를 기초로 수신한 로그인 인증 정보의 진위 여부를 판단할 수 있다. 제어 서버(3000)는 로그인 인증 정보가 신뢰 정보인 경우, 로그인 인증 정보에 포함된 정보를 기초로 로그인 허용 대상인지 판단한다.

[57] 어플리케이션 서버(4000)는 제어 서버(3000)로부터 수신한 로그인 허용 대상(식별자)에 대해 로그인을 허용한다. 즉, 컴퓨팅 장치(2000)가 로그인 허용 대상 식별자를 포함하여 어플리케이션 서버(4000)에 접속하면, 로그인 허용 대상 식별자를 포함하는 컴퓨팅 장치(2000)의 로그인을 허용한다.

[58] 어플리케이션 서버(4000)는 요청 서비스별로 권한을 부여할 수 있다. 따라서, 어플리케이션 서버(4000)는 로그인 허용된 컴퓨팅 장치(2000)로부터 디렉토리 정보 요청 등을 수신하면 추가적인 인증 절차 없이 해당 요청에 대한 응답(디렉토리 정보 제공 등)을 할 수 있다. 추가적인 인증을 요구하는 요청은 정책에 따라 설정되는데, 여기서는 데이터 업로드 및 데이터 다운로드 시 추가적인 인증 절차를 진행한다고 가정한다.

[59] 다음에서, 로그인 이후 사용자가 어플리케이션 서버(4000)에 데이터를 업로드하는 방법에 대해 설명한다.

[60] 데이터 저장 제어부(190)는 컴퓨팅 장치(2000)로부터 어플리케이션 서버(4000)로 전달되는 업로드 요청 메시지를 수신한다. 데이터 저장 제어부(190)는 업로드 요청 메시지를 탐지하여 어플리케이션 서버(4000)로의 업로드 요청 단계를 개시한다. 데이터 저장 제어부(190)는 업로드 요청 메시지에 포함된 식별자를 파싱해서 저장한다. 데이터 저장 제어부(190)는 생체 정보 인식부(110)의 센서를 활성화하고, 생체 정보 인식부(110)로부터 사용자의 지문 정보를 수신하여 지문 인증을 한다. 이때, 컴퓨팅 장치(2000)는 지문 확인 요청 화면을 표시하여, 사용자가 생체 정보 인식부(110)로 지문을 인식하도록 안내할 수 있다.

[61] 데이터 저장 제어부(190)는 지문 인증을 한 후, 암호화키 생성부(150)로 데이터 암호화에 사용되는 데이터 암호화키를 요청한다. 데이터 암호화키는 예를 들면, AES 알고리즘에 의해 생성된 32바이트의 키일 수 있다.

[62] 데이터 저장 제어부(190)는 데이터 암호화키와 식별자에 대한 지문 인증 결과를 포함하는 업로드 인증 정보를 제어 서버(3000)로 전달한다. 이때, 데이터 저장 제어부(190)는 업로드 인증 정보를 개인키로 서명(암호화)하여 제어 서버(3000)로 전달할 수 있다. 업로드 인증 정보는 식별자, 지문 인증 결과(예를 들면, 0 또는 1), 사용자 식별정보, 그리고 데이터 암호화키를 포함할 수 있다.

[63] 제어 서버(3000)는 업로드 인증 정보에 포함된 정보를 기초로 업로드 허용 대상인지 판단한다. 이때, 제어 서버(3000)는 개인키로 서명(암호화)된 업로드 인증 정보를 공개키로 복호화하고, 복호 결과를 기초로 수신한 업로드 인증 정보의 진위 여부를 판단할 수 있다. 제어 서버(3000)는 업로드 인증 정보가 신뢰 정보인 경우, 업로드 인증 정보에 포함된 정보를 기초로 업로드 허용 대상인지 판단한다.

[64] 제어 서버(3000)는 업로드 인증 정보에 포함된 사용자 식별정보가 등록된 정보이고, 지문 인증 결과가 성공이면, 어플리케이션 서버(4000)로 업로드 인증 정보에 포함된 식별자에 대한 업로드 허용을 요청한다. 이때, 제어 서버(3000)는 사용자 식별정보, 지문 인증 결과 정보, 업로드 허용 식별자, 그리고 데이터 암호화키를 어플리케이션 서버(4000)로 전송할 수 있다.

[65] 어플리케이션 서버(4000)는 제어 서버(3000)로부터 수신한 업로드 허용 대상(식별자)에 대해 업로드를 허용한다. 즉, 컴퓨팅 장치(2000)가 업로드 허용 대상 식별자를 포함하여 어플리케이션 서버(4000)에 접속하면, 업로드 허용 대상 식별자를 포함하는 컴퓨팅 장치(2000)의 업로드를 허용한다. 이때, 어플리케이션 서버(4000)는 업로드 허용에 포함된 사용자 식별정보가 등록된 정보인지 확인하고, 등록된 사용자 식별정보인 경우, 제어 서버(3000)로부터 수신한 업로드 허용 대상(식별자)에 대해 업로드를 허용한다.

[66] 어플리케이션 서버(4000)는 컴퓨팅 장치(2000)로부터 업로드 데이터를

수신한다. 인증 장치(100)에서 업로드 데이터를 어플리케이션 서버(4000)로 전송할 때, 업로드 데이터는 인증 장치(100)와 어플리케이션 서버(4000) 사이의 암호화된 통신 구간으로 전송된다. 따라서, 업로드/다운로드 데이터는 통신 구간 암호화에 의해 보안성이 유지된다.

[67] 어플리케이션 서버(4000)는 업로드 허용 대상 식별자에 해당하는 데이터 암호화키를 기초로 업로드 데이터를 암호화한다. 그리고, 어플리케이션 서버(4000)는 암호화한 데이터를 사용자 식별정보에 대응된 데이터 저장소에 저장한다. 이때, 어플리케이션 서버(4000)는 데이터 암호화키를 저장하지 않는다. 즉, 데이터 암호화키는 어플리케이션 서버(4000)의 메모리에 일시적으로 존재하다가, 어플리케이션 서버(4000)가 통신 구간 암호화로 전송된 업로드 데이터를 복호하는 순간에 메모리의 데이터 암호화키로 데이터를 암호화한다. 그리고, 메모리에 일시적으로 존재한 데이터 암호화키는 저장되지 않고 사라진다.

[68] 다음에서, 로그인 이후 사용자가 어플리케이션 서버(4000)에서 데이터를 다운로드하는 방법에 대해 설명한다.

[69] 데이터 저장 제어부(190)는 컴퓨팅 장치(2000)로부터 어플리케이션 서버(4000)로 전달되는 다운로드 요청 메시지를 수신한다. 데이터 저장 제어부(190)는 다운로드 요청 메시지를 탐지하여 어플리케이션 서버(4000)로의 다운로드 요청 단계를 개시한다. 데이터 저장 제어부(190)는 다운로드 요청 메시지에 포함된 식별자를 파싱해서 저장한다. 데이터 저장 제어부(190)는 생체 정보 인식부(110)의 센서를 활성화하고, 생체 정보 인식부(110)로부터 사용자의 지문 정보를 수신하여 지문 인증을 한다. 이때, 컴퓨팅 장치(2000)는 지문 확인 요청 화면을 표시하여, 사용자가 생체 정보 인식부(110)로 지문을 인식하도록 안내할 수 있다.

[70] 데이터 저장 제어부(190)는 암호화키 생성부(150)로 데이터 복호화에 사용되는 데이터 복호화키를 요청한다. 대칭키를 사용하는 경우, 데이터 복호화키는 데이터 암호화키와 동일하다. 이때 데이터 저장 제어부(190)는 데이터 업로드 시 사용한 데이터 암호화키를 저장하고, 지문 인증 후 저장된 데이터 암호화키를 가져와서 사용할 수 있다.

[71] 한 실시예에 따라 데이터 복호화를 어플리케이션 서버(4000)가 담당하는 경우, 데이터 저장 제어부(190)는 데이터 암호화키와 식별자에 대한 지문 인증 결과를 포함하는 다운로드 인증 정보를 제어 서버(3000)로 전달한다. 이때, 데이터 저장 제어부(190)는 다운로드 인증 정보를 개인키로 서명(암호화)하여 제어 서버(3000)로 전달할 수 있다. 다운로드 인증 정보는 식별자, 지문 인증 결과(예를 들면, 0 또는 1), 사용자 식별정보, 그리고 데이터 암호화키를 포함할 수 있다.

[72] 다른 실시예에 따라 데이터 복호화를 인증 장치(100)가 담당하는 경우, 데이터 저장 제어부(190)는 데이터 암호화키를 전송할 필요 없이, 식별자, 지문 인증

결과(예를 들면, 0 또는 1), 그리고 사용자 식별정보를 포함하는 다운로드 인증 정보를 제어 서버(3000)로 전달한다. 데이터 저장 제어부(190)는 데이터 복호화부를 더 포함할 수 있다.

[73] 제어 서버(3000)는 다운로드 인증 정보에 포함된 정보를 기초로 다운로드 허용 대상인지 판단한다. 이때, 제어 서버(3000)는 개인키로 서명(암호화)된 다운로드 인증 정보를 공개키로 복호화하고, 복호 결과를 기초로 수신한 다운로드 인증 정보의 진위 여부를 판단할 수 있다. 제어 서버(3000)는 다운로드 인증 정보가 신뢰 정보인 경우, 다운로드 인증 정보에 포함된 정보를 기초로 업로드 허용 대상인지 판단한다.

[74] 제어 서버(3000)는 다운로드 인증 정보에 포함된 사용자 식별정보가 등록된 정보이고, 지문 인증 결과가 성공이면, 어플리케이션 서버(4000)로 다운로드 인증 정보에 포함된 식별자에 대한 다운로드 허용을 요청한다. 이때, 제어 서버(3000)는 사용자 식별정보, 지문 인증 결과 정보, 다운로드 허용 식별자, 그리고 데이터 암호화키를 어플리케이션 서버(4000)로 전송할 수 있다.

[75] 어플리케이션 서버(4000)는 제어 서버(3000)로부터 수신한 다운로드 허용 대상(식별자)에 대해 다운로드를 허용한다. 즉, 컴퓨팅 장치(2000)가 다운로드 허용 대상 식별자를 포함하여 어플리케이션 서버(4000)에 접속하면, 다운로드 허용 대상 식별자를 포함하는 컴퓨팅 장치(2000)의 다운로드를 허용한다. 이때, 어플리케이션 서버(4000)는 다운로드 허용에 포함된 사용자 식별정보가 등록된 정보인지 확인하고, 등록된 사용자 식별정보인 경우, 제어 서버(3000)로부터 수신한 다운로드 허용 대상(식별자)에 대해 다운로드를 허용한다.

[76] 다운로드를 위해, 어플리케이션 서버(4000)는 데이터 저장소로부터 사용자 식별정보에 대응하여 저장된 데이터를 가져온다. 데이터는 데이터 암호화키로 암호화되어 있는데, 어플리케이션 서버(4000)는 제어 서버(3000)로부터 수신한 데이터 암호화키를 기초로 암호화된 데이터를 복호화할 수 있다. 그리고, 어플리케이션 서버(4000)는 컴퓨팅 장치(2000)에 연결된 인증 장치(100)로 복호화된 데이터를 전송한다. 인증 장치(100)는 수신한 데이터를 컴퓨팅 장치(2000)로 전달한다. 이때, 어플리케이션 서버(4000)는 데이터 암호화키를 저장하지 않는다. 즉, 데이터 암호화키는 어플리케이션 서버(4000)의 메모리에 일시적으로 존재하다가, 어플리케이션 서버(4000)가 암호화된 데이터를 데이터 암호화키로 복호화한 후, 저장되지 않고 사라진다. 이때, 데이터 암호화키로 복호화된 데이터는 통신 구간 암호화로 암호화되어 전송된다.

[77] 한편, 어플리케이션 서버(4000)는 제어 서버(3000)로부터 데이터 암호화키를 수신하지 않을 수 있다. 이 경우, 어플리케이션 서버(4000)는 암호화된 데이터를 컴퓨팅 장치(2000)에 연결된 인증 장치(100)로 전송한다. 그러면, 인증 장치(100)의 데이터 저장 제어부(190)가 암호화키 생성부(150)로 데이터 복호화에 사용되는 데이터 복호화키를 요청한다. 대칭키를 사용하는 경우, 데이터 복호화키는 데이터 암호화키와 동일하다. 이때 데이터 저장

제어부(190)는 데이터 업로드 시 사용한 데이터 암호화키를 저장하고, 지문 인증 후 저장된 데이터 암호화키를 가져와서 사용할 수 있다. 그 다음 인증 장치(100)는 복호화한 데이터를 컴퓨팅 장치(2000)로 전달한다. 어플리케이션 서버(4000)와 컴퓨팅 장치(2000) 사이의 전송 구간은 다양한 통신 구간 암호화를 사용하고, 이 전송 구간을 통해 전송되는 데이터는 통신 구간 암호화를 통해 보호된다.

[78] 도 3은 본 발명의 한 실시예에 따른 인증 장치의 하드웨어 구성도이다.

[79] 도 3을 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.

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

[81] 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 식별자, 사용자 식별번호 등을 저장할 수 있다. 메모리(400)에 저장된 정보는 갱신되거나 일정 기간 이후에 삭제될 수 있다.

[82] 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.

[83] 보안 모듈(600)은 암호화키 생성부(150)의 기능을 수행하는 하드웨어이다.

[84] 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, 데이터 저장을 위한 프로그램 등)을 로드하여 인증키 생성부(130)와 데이터 저장 제어부(190)의 기능을 수행할 수 있다.

[85] 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.

[86] 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.

[87] 프로세서(200)는 컴퓨팅 장치(2000)로 입출입하는 패킷을 탐지한다. 만약, 프로세서(200)가 컴퓨팅 장치(2000)에서 어플리케이션 서버(4000)로 전송되는 로그인 요청 메시지, 업로드 요청 메시지, 다운로드 요청 메시지 등을 탐지한 경우, 로그인 인증 절차, 업로드 인증 절차, 다운로드 인증 절차의 개시로 인식한다. 그러면, 프로세서(200)는 해당 프로그램을 로드하고, 센서(300)를 활성화한 후, 프로그램에 따라 동작한다.

[88] 도 4는 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, 초기 설정 단계이다.

[89] 도 4를 참고하면, 인증 장치(100)와 컴퓨팅 장치(2000)가 연결된다(S110).

[90] 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.

[91] 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). 예를 들면, 인증 장치(100)의 식별 정보는 시리얼 정보일 수 있다. 또한, 인증 장치(100)의 식별 정보는 사용자 식별정보일 수 있다.

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

[93] 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.

[94] 인증 장치(100)는 사용자의 지문 정보를 입력받고, 입력받은 지문 정보를 등록(저장)한다(S150). 인증 장치(100)는 사용자의 지문 정보를 복수 번 입력받을 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.

[95] 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.

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

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

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

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

[100] 도 5는 본 발명의 한 실시예에 따른 로그인 방법의 흐름도이다.

[101] 도 5를 참고하면, 인증 장치(100)와 컴퓨팅 장치(2000)가 연결된다(S210).

[102] 컴퓨팅 장치(2000)는 사용자로부터 어플리케이션 서버(4000)로의 로그인 요청(선택)을 수신한다(S220). 컴퓨팅 장치(2000)는 로그인 화면에 로그인 요청 버튼을 표시할 수 있다.

[103] 컴퓨팅 장치(2000)는 식별자를 생성한다(S222). 식별자는 랜덤하게 생성될 수 있고, 예를 들면, 시간 정보와 컴퓨팅 장치(2000)의 IP 주소를 기초로 생성될 수 있다. 식별자는 인증 장치(100), 제어 서버(3000), 어플리케이션 서버(4000)에서 인증 대상을 특정하기 위해 사용된다. 여기서 식별자를 포함하는 메시지는 컴퓨팅 장치(2000)에서 전송된 메시지를 나타내므로, 식별자는 컴퓨팅 장치의 식별자라고 볼 수 있다.

[104] 컴퓨팅 장치(2000)는 어플리케이션 서버(4000)로 식별자(ID)를 포함하는 로그인 요청 메시지를 전송한다(S224). 예를 들면, 로그인 요청 메시지(http://어플리케이션 서버(4000)의 URL/login/?ID)는 어플리케이션 서버(4000)의 URL, 로그인 요청을 나타내는 정보(login), 그리고 식별자(ID)를 포함할 수 있다.

[105] 인증 장치(100)는 로그인 요청 메시지를 탐지하여, 로그인 인증 절차를 개시한다(S230).

[106] 인증 장치(100)는 센서를 활성화한다(S232).

[107] 인증 장치(100)는 로그인 요청 메시지에서 식별자를 파싱하여 저장한다(S234).

[108] 인증 장치(100)는 사용자의 지문 정보를 입력받는다(S240).

[109] 인증 장치(100)는 입력받은 지문 정보를 인증한다(S242). 인증 장치(100)는 입력받은 지문 정보와 저장된 지문 정보를 비교하여 지문 인증을 할 수 있다.

[110] 인증 장치(100)는 식별자에 대한 지문 인증 결과를 포함하는 로그인 인증 정보를 제어 서버(3000)로 전달한다(S250). 이때, 인증 장치(100)는 로그인 인증 정보를 개인키로 서명(암호화)하여 제어 서버(3000)로 전달할 수 있다. 로그인 인증 정보는 식별자, 지문 인증 결과(예를 들면, 0 또는 1), 그리고 사용자 식별정보를 포함할 수 있다. 사용자 식별정보는 로그인 요청 메시지와 같이 컴퓨팅 장치(2000)로부터 전송된 메시지에 포함되는 경우, 인증 장치(100)가 컴퓨팅 장치(2000)로부터 전송된 메시지로부터 사용자 식별정보를 파싱할 수 있으나, 여기서는 인증 장치(100)가 사용자 식별정보를 알고 있다고 가정한다.

[111] 제어 서버(3000)는 로그인 인증 정보에 포함된 정보를 기초로 로그인 허용 대상인지 판단한다(S260). 제어 서버(3000)는 로그인 인증 정보에 포함된 사용자 식별정보가 등록된 정보이고, 지문 인증 결과가 성공이면, 로그인 인증 정보에 포함된 식별자를 로그인 허용 식별자로 판단한다. 이때, 제어 서버(3000)는 개인키로 서명(암호화)된 로그인 인증 정보를 공개키로 검증하고, 검증된 로그인 인증 정보를 기초로 로그인 허용 대상인지 판단한다.

[112] 제어 서버(3000)는 어플리케이션 서버(4000)로 로그인 인증 정보에 포함된 식별자에 대한 로그인 허용을 요청한다(S270). 제어 서버(3000)는 사용자 식별정보, 지문 인증 결과 정보, 그리고 로그인 허용 식별자를 어플리케이션 서버(4000)로 전송할 수 있다.

[113] 어플리케이션 서버(4000)는 제어 서버(3000)로부터 수신한 로그인 허용 식별자를 대해 로그인을 허용한다(S280). 어플리케이션 서버(4000)는 로그인 허용 요청에 포함된 사용자 식별정보가 등록된 정보이면, 로그인 허용 식별자를 저장하고, 로그인 허용 식별자에 대해 로그인을 허용한다.

[114] 컴퓨팅 장치(2000)가 어플리케이션 서버(4000)로 로그인 허용 대상 식별자를 포함하여 디렉토리 정보를 요청한다(S290).

[115] 어플리케이션 서버(4000)는 로그인 허용 대상 식별자에 대응된 사용자 식별정보를 검색하고, 사용자 식별정보에 일치하는 디렉토리 정보를 컴퓨팅 장치(2000)에 제공한다(S292).

[116] 도 6은 본 발명의 한 실시예에 따른 데이터 업로드 방법의 흐름도이다.

[117] 도 6을 참고하면, 컴퓨팅 장치(2000)는 어플리케이션 서버(4000)에 로그인한 후, 데이터 업로드를 할 수 있다.

[118] 컴퓨팅 장치(2000)는 사용자로부터 어플리케이션 서버(4000)로의 데이터 업로드 요청을 수신한다(S310). 컴퓨팅 장치(2000)는 업로드 요청 버튼과 업로드할 파일을 선택할 수 있는 화면을 표시할 수 있다. 특히, 컴퓨팅 장치(2000)는 어플리케이션 서버(4000)로 디렉토리 정보를 요청하고, 사용자 식별정보에 일치하는 디렉토리 정보를 확인할 수 있다.

[119] 컴퓨팅 장치(2000)는 어플리케이션 서버(4000)로 식별자를 포함하는 업로드 요청 메시지를 전송한다(S312). 예를 들면, 업로드 요청 메시지(http://어플리케이션 서버(4000)의 URL/upload/?ID)는 어플리케이션

서버(4000)의 URL, 업로드 요청을 나타내는 정보(upload), 그리고 식별자(ID)를 포함할 수 있다. 업로드 요청 메시지에 포함되는 식별자는 로그인 요청 메시지에 포함되는 식별자와 같거나 다를 수 있다.

[120] 인증 장치(100)는 업로드 요청 메시지를 탐지하여, 업로드 인증 절차를 개시한다(S320).

[121] 인증 장치(100)는 센서를 활성화한다(S322).

[122] 인증 장치(100)는 업로드 요청 메시지에서 식별자를 파싱하여 저장한다(S324).

[123] 인증 장치(100)는 사용자의 지문 정보를 입력받는다(S330).

[124] 인증 장치(100)는 입력받은 지문 정보를 인증한다(S332). 인증 장치(100)는 입력받은 지문 정보와 저장된 지문 정보를 비교하여 지문 인증을 할 수 있다.

[125] 인증 장치(100)는 식별자에 대한 지문 인증 결과를 포함하는 업로드 인증 정보를 제어 서버(3000)로 전달한다(S340). 이때, 인증 장치(100)는 업로드 인증 정보를 개인키로 서명(암호화)하여 제어 서버(3000)로 전달할 수 있다. 업로드 인증 정보는 식별자, 지문 인증 결과(예를 들면, 0 또는 1), 사용자 식별정보, 그리고 데이터 암호화키를 포함할 수 있다. 인증 장치(100)는 제어 서버(3000)에서 자신이 업로드한 파일을 암호화하여 저장하도록 데이터 암호화키를 전송한다. 인증 장치(100)는 지문 인증 결과가 성공이면, 인증 등록 시 저장한 데이터 암호화키를 꺼내온다.

[126] 제어 서버(3000)는 업로드 인증 정보에 포함된 정보를 기초로 업로드 허용 대상인지 판단한다(S350). 제어 서버(3000)는 업로드 인증 정보에 포함된 사용자 식별정보가 등록된 정보이고, 지문 인증 결과가 성공이면, 업로드 인증 정보에 포함된 식별자를 업로드 허용 식별자로 판단한다.

[127] 제어 서버(3000)는 어플리케이션 서버(4000)로 업로드 인증 정보에 포함된 식별자에 대한 업로드 허용을 요청한다(S360). 제어 서버(3000)는 식별자, 지문 인증 결과(예를 들면, 0 또는 1), 사용자 식별정보, 그리고 데이터 암호화키를 어플리케이션 서버(4000)로 전송할 수 있다. 이때, 제어 서버(3000)는 개인키로 서명(암호화)된 업로드 인증 정보를 공개키로 검증하고, 검증된 업로드 인증 정보를 기초로 업로드 허용 대상인지 판단한다.

[128] 어플리케이션 서버(4000)는 제어 서버(3000)로부터 수신한 업로드 허용 식별자를 저장한다(S370).

[129] 어플리케이션 서버(4000)는 컴퓨팅 장치(2000)로부터 업로드 허용 식별자와 특정 데이터에 대한 업로드 요청을 수신한다(S380). 이때, 데이터는 별도의 소켓(socket)을 통해 업로드될 수 있다. 업로드 데이터는 통신 구간 암호화되어 전송된다.

[130] 어플리케이션 서버(4000)는 업로드 허용 식별자에 대응된 데이터 암호화키로 업로드 요청된 데이터를 암호화한다(S382). 이때 어플리케이션 서버(4000)는 수신한 데이터를 패킷단위로 암호화한다. 즉, 업로드 요청된 데이터는 어플리케이션 서버(4000)에 도달한 패킷마다 개별적으로 암호화되어 저장된다.

따라서, 패킷 전체를 일회적으로 암호화하는 종래 기술에 비해 보안성을 높일 수 있다.

[131] 어플리케이션 서버(4000)는 암호화한 데이터를 사용자 식별정보에 대응된 데이터 저장소에 저장한다(S390). 이때, 어플리케이션 서버(4000)는 데이터 암호화키를 저장하지 않는다.

[132] 도 7은 본 발명의 한 실시예에 따른 데이터 다운로드 방법의 흐름도이다.

[133] 도 7을 참고하면, 컴퓨팅 장치(2000)는 어플리케이션 서버(4000)에 로그인한 후, 데이터 다운로드를 할 수 있다. 여기서, 어플리케이션 서버(4000)가 다운로드 요청된 데이터 복호화하여 인증 장치(100)로 전송하는 실시예에 대해 설명한다.

[134] 컴퓨팅 장치(2000)는 사용자로부터 어플리케이션 서버(4000)로의 데이터 다운로드 요청을 수신한다(S410). 컴퓨팅 장치(2000)는 다운로드 요청 버튼과 다운로드할 파일을 선택할 수 있는 화면을 표시할 수 있다. 특히, 컴퓨팅 장치(2000)는 어플리케이션 서버(4000)로 디렉토리 정보를 요청하고, 사용자 식별정보에 일치하는 디렉토리 정보를 확인할 수 있다.

[135] 컴퓨팅 장치(2000)는 어플리케이션 서버(4000)로 식별자를 포함하는 다운로드 요청 메시지를 전송한다(S412). 예를 들면, 다운로드 요청 메시지(http://어플리케이션 서버(4000)의 URL/download/?ID)는 어플리케이션 서버(4000)의 URL, 다운로드 요청을 나타내는 정보(download), 그리고 식별자(ID)를 포함할 수 있다. 다운로드 요청 메시지에 포함되는 식별자는 로그인 요청 메시지에 포함되는 식별자나 업로드 요청 메시지에 포함되는 식별자와 같거나 다를 수 있다.

[136] 인증 장치(100)는 다운로드 요청 메시지를 탐지하여, 다운로드 인증 절차를 개시한다(S420).

[137] 인증 장치(100)는 센서를 활성화한다(S422).

[138] 인증 장치(100)는 다운로드 요청 메시지에서 식별자를 파싱하여 저장한다(S424).

[139] 인증 장치(100)는 사용자의 지문 정보를 입력받는다(S430).

[140] 인증 장치(100)는 입력받은 지문 정보를 인증한다(S432). 인증 장치(100)는 입력받은 지문 정보와 저장된 지문 정보를 비교하여 지문 인증을 할 수 있다.

[141] 인증 장치(100)는 식별자에 대한 지문 인증 결과를 포함하는 다운로드 인증 정보를 제어 서버(3000)로 전달한다(S440). 이때, 인증 장치(100)는 다운로드 인증 정보를 개인키로 서명(암호화)하여 제어 서버(3000)로 전달할 수 있다. 다운로드 인증 정보는 식별자, 지문 인증 결과(예를 들면, 0 또는 1), 사용자 식별정보, 그리고 데이터 암호화키를 포함할 수 있다. 인증 장치(100)는 제어 서버(3000)에서 암호화된 파일을 복호화할 수 있는 데이터 암호화키를 전송한다. 인증 장치(100)는 지문 인증 결과가 성공이면, 인증 등록 시 저장한 데이터 암호화키를 꺼내온다.

[142] 제어 서버(3000)는 다운로드 인증 정보에 포함된 정보를 기초로 다운로드 허용

대상인지 판단한다(S450). 제어 서버(3000)는 다운로드 인증 정보에 포함된 사용자 식별정보가 등록된 정보이고, 지문 인증 결과가 성공이면, 다운로드 인증 정보에 포함된 식별자를 다운로드 허용 식별자로 판단한다.

[143] 제어 서버(3000)는 어플리케이션 서버(4000)로 다운로드 인증 정보에 포함된 식별자에 대한 다운로드 허용을 요청한다(S460). 제어 서버(3000)는 식별자, 지문 인증 결과(예를 들면, 0 또는 1), 사용자 식별정보, 그리고 데이터 암호화키를 어플리케이션 서버(4000)로 전송할 수 있다.

[144] 어플리케이션 서버(4000)는 제어 서버(3000)로부터 수신한 다운로드 허용 식별자를 저장한다(S470).

[145] 어플리케이션 서버(4000)는 컴퓨팅 장치(2000)로부터 다운로드 허용 식별자와 특정 데이터에 대한 다운로드 요청을 수신한다(S480). 다운로드 요청은 어플리케이션 서버(4000)에서 제공한 디렉토리 정보에 저장된 파일명과 같이 데이터를 특정할 수 있는 정보를 포함한다.

[146] 어플리케이션 서버(4000)는 데이터 저장소에서 다운로드 요청된 데이터를 가져온다(S482). 어플리케이션 서버(4000)는 다운로드 허용 식별자에 대응된 사용자 식별정보를 확인하고, 사용자 식별정보에 대응된 데이터 저장소에서 다운로드 요청된 데이터를 가져온다.

[147] 어플리케이션 서버(4000)는 다운로드 허용 식별자에 대응된 데이터 암호화키로 다운로드 요청된 데이터를 복호화한다(S484).

[148] 어플리케이션 서버(4000)는 컴퓨팅 장치(2000)로 다운로드 요청된 데이터를 전송한다(S490). 다운로드 요청된 데이터는 인증 장치(100)를 거쳐 컴퓨팅 장치(2000)로 전송된다. 이때, 어플리케이션 서버(4000)는 데이터 암호화키를 저장하지 않는다. 이때, 데이터는 별도의 소켓을 통해 전송될 수 있다. 다운로드 데이터는 통신 구간 암호화되어 전송될 수 있다.

[149] 도 8은 본 발명의 다른 실시예에 따른 데이터 다운로드 방법의 흐름도이다.

[150] 도 8을 참고하면, 컴퓨팅 장치(2000)는 어플리케이션 서버(4000)에 로그인한 후, 데이터 다운로드를 할 수 있다. 여기서, 어플리케이션 서버(4000)가 암호화된 데이터를 인증 장치(100)로 전송하면, 인증 장치(100)가 암포화된 데이터를 복호화하여 컴퓨팅 장치(2000)로 전달하는 실시예에 대해 설명한다.

[151] 컴퓨팅 장치(2000)는 사용자로부터 어플리케이션 서버(4000)로의 데이터 다운로드 요청을 수신한다(S510). 컴퓨팅 장치(2000)는 다운로드 요청 버튼과 다운로드할 파일을 선택할 수 있는 화면을 표시할 수 있다. 특히, 컴퓨팅 장치(2000)는 어플리케이션 서버(4000)로 디렉토리 정보를 요청하고, 사용자 식별정보에 일치하는 디렉토리 정보를 확인할 수 있다.

[152] 컴퓨팅 장치(2000)는 어플리케이션 서버(4000)로 식별자를 포함하는 다운로드 요청 메시지를 전송한다(S512). 예를 들면, 다운로드 요청 메시지(http://어플리케이션 서버(4000)의 URL/download/?ID)는 어플리케이션 서버(4000)의 URL, 다운로드 요청을 나타내는 정보(download), 그리고

식별자(ID)를 포함할 수 있다. 다운로드 요청 메시지에 포함되는 식별자는 로그인 요청 메시지에 포함되는 식별자나 업로드 요청 메시지에 포함되는 식별자와 같거나 다를 수 있다.

[153] 인증 장치(100)는 다운로드 요청 메시지를 탐지하여, 다운로드 인증 절차를 개시한다(S520).

[154] 인증 장치(100)는 센서를 활성화한다(S522).

[155] 인증 장치(100)는 다운로드 요청 메시지에서 식별자를 파싱하여 저장한다(S524).

[156] 인증 장치(100)는 사용자의 지문 정보를 입력받는다(S530).

[157] 인증 장치(100)는 입력받은 지문 정보를 인증한다(S532). 인증 장치(100)는 입력받은 지문 정보와 저장된 지문 정보를 비교하여 지문 인증을 할 수 있다.

[158] 인증 장치(100)는 식별자에 대한 지문 인증 결과를 포함하는 다운로드 인증 정보를 제어 서버(3000)로 전달한다(S540). 이때, 인증 장치(100)는 다운로드 인증 정보를 개인키로 서명(암호화)하여 제어 서버(3000)로 전달할 수 있다. 다운로드 인증 정보는 식별자, 지문 인증 결과(예를 들면, 0 또는 1), 사용자 식별정보를 포함할 수 있다. 이때, 인증 장치(100)가 데이터 복호화하므로, 인증 등록 시 저장한 데이터 암호화키를 제어 서버(3000)로 전송하지 않아도 된다.

[159] 제어 서버(3000)는 다운로드 인증 정보에 포함된 정보를 기초로 다운로드 허용 대상인지 판단한다(S550). 제어 서버(3000)는 다운로드 인증 정보에 포함된 사용자 식별정보가 등록된 정보이고, 지문 인증 결과가 성공이면, 다운로드 인증 정보에 포함된 식별자를 다운로드 허용 식별자로 판단한다.

[160] 제어 서버(3000)는 어플리케이션 서버(4000)로 다운로드 인증 정보에 포함된 식별자에 대한 다운로드 허용을 요청한다(S560). 제어 서버(3000)는 식별자, 지문 인증 결과(예를 들면, 0 또는 1), 사용자 식별정보를 어플리케이션 서버(4000)로 전송할 수 있다.

[161] 어플리케이션 서버(4000)는 제어 서버(3000)로부터 수신한 다운로드 허용 식별자를 저장한다(S570).

[162] 어플리케이션 서버(4000)는 컴퓨팅 장치(2000)로부터 다운로드 허용 식별자와 특정 데이터에 대한 다운로드 요청을 수신한다(S580). 다운로드 요청은 어플리케이션 서버(4000)에서 제공한 디렉토리 정보에 저장된 파일명과 같이 데이터를 특정할 수 있는 정보를 포함한다.

[163] 어플리케이션 서버(4000)는 데이터 저장소에서 다운로드 요청된 데이터를 가져온다(S582). 어플리케이션 서버(4000)는 다운로드 허용 식별자에 대응된 사용자 식별정보를 확인하고, 사용자 식별정보에 대응된 데이터 저장소에서 다운로드 요청된 데이터를 가져온다.

[164] 어플리케이션 서버(4000)는 컴퓨팅 장치(2000)에 연결된 인증 장치(100)로 다운로드 요청된 데이터를 전송한다(S584). 이때, 데이터는 암호화된 상태로 전송된다. 데이터는 별도의 소켓을 통해 전송될 수 있다. 다운로드 데이터는

통신 구간 암호화되어 전송될 수 있다.

[165] 인증장치(100)는 인증 등록 시 저장한 데이터 암호화키를 이용하여 수신한 데이터를 복호화한다(S590).

[166] 인증장치(100)는 복호화한 데이터를 컴퓨팅 장치(2000)에 전달한다(S592).

[167] 이와 같이, 본 발명의 실시예에 따르면 어플리케이션 서버는 데이터를 암호화하여 저장하므로 암호화된 데이터가 노출될 수는 있어도 본인 이외에는 암호화된 데이터를 복호화할 수 없다. 본 발명의 실시예에 따르면 어플리케이션 서버는 데이터 업로드/다운로드 시에 메모리에 일시적으로 존재하는 암호화키를 이용하여 암호화/복호화하므로, 암호화키는 어느 네트워크 장치에도 저장되지 않는다. 따라서, 본 발명의 실시예에 따르면 보안성을 높일 수 있다. 또한, 본 발명의 실시예에 따르면 인증 장치와 어플리케이션 서버 사이의 통신 구간은 암호화되므로, 인증 장치에서 어플리케이션 서버 사이에서 전송되는 데이터는 통신 구간 암호화 및 암호화키에 의한 암호화로 보호되므로 모든 전송 구간과 저장 위치에서 데이터 보안성이 매우 높다.

[168] 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.

[169] 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] 컴퓨팅 장치에 연결된 생체 정보 기반 인증 장치가 제어 서버와 연동하여 상기 컴퓨팅 장치에서 요청된 어플리케이션 서버로의 로그인을 처리하는 방법으로서,
상기 컴퓨팅 장치로부터 상기 어플리케이션 서버로 전달되는 로그인 요청 메시지를 탐지하는 단계,
상기 로그인 요청 메시지에 포함된 식별자를 추출하는 단계,
입력받은 생체 정보에 대한 생체 정보 인증 결과를 출력하는 단계, 그리고
상기 식별자와 상기 생체 정보 인증 결과를 포함하는 로그인 인증 정보를 상기 제어 서버로 전송하는 단계를 포함하고,
상기 식별자는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 로그인 허용 대상 판단 시 사용되고,
상기 생체 정보 인증 결과는 상기 제어 서버에서 로그인 허용 여부 판단 시 사용되는, 로그인 방법.

[청구항 2] 제1항에서,
상기 로그인 인증 정보는 사용자 식별정보를 더 포함하고,
상기 사용자 식별정보는 상기 제어 서버와 상기 어플리케이션 서버 중 적어도 하나의 서버에서 등록된 사용자 여부 판단 시 사용되는, 로그인 방법.

[청구항 3] 제1항에서,
상기 식별자는 상기 컴퓨팅 장치에서 랜덤하게 생성된 정보인 로그인 방법.

[청구항 4] 컴퓨팅 장치에 연결된 생체 정보 기반 인증 장치가 제어 서버와 연동하여 상기 컴퓨팅 장치에서 요청된 어플리케이션 서버로의 데이터 업로드 및 다운로드를 처리하는 방법으로서,
상기 컴퓨팅 장치로부터 상기 어플리케이션 서버로 전달되는 업로드 요청 메시지를 탐지하는 단계,
상기 업로드 요청 메시지에 포함된 제1 식별자를 추출하는 단계,
입력받은 제1 생체 정보에 대한 제1 생체 정보 인증 결과를 출력하는 단계, 그리고
상기 제1 식별자, 상기 제1 생체 정보 인증 결과, 그리고 제1 데이터 암호화키를 포함하는 업로드 인증 정보를 상기 제어 서버로 전송하는 단계를 포함하고,
상기 제1 식별자는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 업로드 허용 대상 판단 시

사용되고,
상기 제1 생체 정보 인증 결과는 상기 제어 서버에서 업로드 허용 여부 판단 시 사용되며,
상기 제1 데이터 암호화키는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 업로드 요청된 데이터를 암호화하는데 사용되는, 데이터 업로드 및 다운로드 방법.

[청구항 5] 제4항에서,
상기 업로드 인증 정보는 사용자 식별정보를 더 포함하고,
상기 사용자 식별정보는 상기 제어 서버와 상기 어플리케이션 서버 중 적어도 하나의 서버에서 등록된 사용자 여부 판단 시 사용되는, 데이터 업로드 및 다운로드 방법.

[청구항 6] 제4항에서,
상기 제1 생체 정보 인증 결과가 성공이면, 저장된 상기 제1 데이터 암호화키를 가져오는 단계
를 더 포함하는 데이터 업로드 및 다운로드 방법.

[청구항 7] 제4항에서,
상기 컴퓨팅 장치로부터 상기 어플리케이션 서버로 전달되는 다운로드 요청 메시지를 탐지하는 단계,
상기 다운로드 요청 메시지에 포함된 제2 식별자를 추출하는 단계,
입력받은 제2 생체 정보에 대한 제2 생체 정보 인증 결과를 출력하는 단계,
상기 제2 식별자, 상기 제2 생체 정보 인증 결과, 그리고 제2 데이터 암호화키를 포함하는 다운로드 인증 정보를 상기 제어 서버로 전송하는 단계,
상기 어플리케이션 서버로부터 상기 다운로드 요청 메시지에 관련된 다운로드 데이터를 수신하는 단계, 그리고
상기 다운로드 데이터를 상기 컴퓨팅 장치로 전달하는 단계
를 더 포함하고,
상기 제2 식별자는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 다운로드 허용 대상 판단 시 사용되고,
상기 제2 생체 정보 인증 결과는 상기 제어 서버에서 다운로드 허용 여부 판단 시 사용되며,
상기 제2 데이터 암호화키는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 다운로드 요청된 데이터를 복호화하는데 사용되는, 데이터 업로드 및 다운로드 방법.

[청구항 8] 제4항에서,
상기 컴퓨팅 장치로부터 상기 어플리케이션 서버로 전달되는 다운로드 요청 메시지를 탐지하는 단계,
상기 다운로드 요청 메시지에 포함된 제2 식별자를 추출하는 단계,
입력받은 제2 생체 정보에 대한 제2 생체 정보 인증 결과를 출력하는 단계,
상기 제2 식별자, 그리고 상기 제2 생체 정보 인증 결과를 포함하는 다운로드 인증 정보를 상기 제어 서버로 전송하는 단계,
상기 어플리케이션 서버로부터 상기 다운로드 요청 메시지에 관련된 다운로드 데이터를 수신하는 단계, 그리고
상기 다운로드 데이터를 상기 제1 데이터 암호화키에 관련된 제2 데이터 암호화키로 복호화하여 상기 컴퓨팅 장치로 전달하는 단계를 더 포함하고,
상기 제2 식별자는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 다운로드 허용 대상 판단 시 사용되고,
상기 제2 생체 정보 인증 결과는 상기 제어 서버에서 다운로드 허용 여부 판단 시 사용되는 데이터 업로드 및 다운로드 방법.

[청구항 9] 제어 서버가 생체 정보 기반 인증 장치 및 어플리케이션 서버와 연동하여 컴퓨팅 장치에서 요청된 절차를 처리하는 방법으로서,
상기 생체 정보 기반 인증 장치로부터 제1 식별자, 제1 생체 정보 인증 결과, 그리고 제1 데이터 암호화키를 포함하는 업로드 인증 정보를 수신하는 단계,
상기 업로드 인증 정보를 기초로 상기 제1 식별자를 업로드 허용 대상으로 판단하는 단계, 그리고
상기 제1 식별자와 상기 제1 데이터 암호화키를 포함하는 업로드 허용 요청 메시지를 상기 어플리케이션 서버로 전송하는 단계를 포함하고,
상기 제1 식별자는 상기 어플리케이션 서버에서 업로드 허용 대상 판단 시 사용되며,
상기 제1 데이터 암호화키는 상기 어플리케이션 서버에서 업로드 요청된 데이터를 암호화하는데 사용되는, 처리 방법.

[청구항 10] 제9항에서,
상기 생체 정보 기반 인증 장치로부터 제2 식별자그리고 제2 생체 정보 인증 결과를 포함하는 다운로드 인증 정보를 수신하는 단계,
상기 다운로드 인증 정보를 기초로 상기 제2 식별자를 다운로드 허용 대상으로 판단하는 단계, 그리고
상기 제2 식별자를 포함하는 다운로드 허용 요청 메시지를 상기

어플리케이션 서버로 전송하는 단계를 더 포함하고,
상기 제2 식별자는 상기 어플리케이션 서버에서 다운로드 허용 대상 판단 시 사용되는, 처리 방법.

[청구항 11] 제10항에서,
상기 제1 식별자를 업로드 허용 대상으로 판단하는 단계는 상기 업로드 인증 정보에 사용자 식별정보가 더 포함된 경우, 상기 사용자 식별정보가 등록된 정보이고, 상기 제1 생체 정보 인증 결과가 성공이면, 상기 제1 식별자를 업로드 허용 대상으로 판단하고,
상기 제2 식별자를 다운로드 허용 대상으로 판단하는 단계는 상기 다운로드 인증 정보에 상기 사용자 식별정보가 더 포함된 경우, 상기 사용자 식별정보가 등록된 정보이고, 상기 제2 생체 정보 인증 결과가 성공이면, 상기 제2 식별자를 다운로드 허용 대상으로 판단하는, 처리 방법.

[청구항 12] 어플리케이션 서버가 제어 서버와 연동하여 컴퓨팅 장치에서 요청된 절차를 처리하는 방법으로서,
상기 제어 서버로부터 제1 식별자와 제1 데이터 암호화키를 포함하는 업로드 허용 요청 메시지를 수신하는 단계,
상기 컴퓨팅 장치로부터 상기 제1 식별자와 업로드 요청된 데이터를 포함하는 업로드 요청 메시지를 수신하는 단계, 그리고
상기 제1 식별자에 대응된 상기 제1 데이터 암호화키를 이용하여 상기 업로드 요청된 데이터를 암호화하여 저장하는 단계
를 포함하고,
상기 제1 데이터 암호화키는 생체 정보 기반 인증 장치에서 생성되어 상기 제어 서버로 전송된 정보인, 처리 방법.

[청구항 13] 제12항에서,
상기 업로드 허용 요청 메시지는 사용자 식별정보를 더 포함하고,
상기 업로드 요청된 데이터를 암호화하여 저장하는 단계는 상기 사용자 식별정보가 등록된 정보인 경우, 상기 업로드 요청된 데이터를 암호화하고, 암호화한 데이터를 상기 사용자 식별정보에 대응된 데이터 저장소에 저장하는, 처리 방법.

[청구항 14] 제12항에서,
상기 제어 서버로부터 제2 식별자와 제2 데이터 암호화키를 포함하는 다운로드 허용 요청 메시지를 수신하는 단계,
상기 컴퓨팅 장치로부터 상기 제2 식별자와 특정 데이터에 대한 다운로드 요청을 포함하는 다운로드 요청 메시지를 수신하는 단계,
상기 제2 식별자에 대응된 상기 제2 데이터 암호화키를 이용하여

상기 특정 데이터를 복호화하는 단계, 그리고
복호화한 데이터를 상기 컴퓨팅 장치로 전송하는 단계
를 더 포함하고,
상기 제2 데이터 암호화키는 상기 생체 정보 기반 인증 장치에서
생성되어 상기 제어 서버로 전송된 정보인, 처리 방법.

[청구항 15] 제14항에서,
상기 업로드 요청된 데이터를 암호화하여 저장하는 단계는
상기 업로드 허용 요청 메시지에 사용자 식별정보가 더 포함되고
상기 사용자 식별정보가 등록된 정보인 경우, 상기 업로드 요청된
데이터를 암호화하고, 암호화한 데이터를 상기 사용자 식별정보에
대응된 데이터 저장소에 저장하고,
상기 특정 데이터를 복호화하는 단계는
상기 다운로드 허용 요청 메시지에 상기 사용자 식별정보가 더
포함되고 상기 사용자 식별정보가 등록된 정보인 경우, 상기
사용자 식별정보에 대응된 데이터 저장소에서 상기 특정 데이터를
찾고, 상기 특정 데이터를 상기 제2 데이터 암호화키로
복호화하는, 처리 방법.

[청구항 16] 제12항에서,
상기 제어 서버로부터 제2 식별자를 포함하는 다운로드 허용 요청
메시지를 수신하는 단계,
상기 컴퓨팅 장치로부터 상기 제2 식별자와 특정 데이터에 대한
다운로드 요청을 포함하는 다운로드 요청 메시지를 수신하는
단계, 그리고
상기 제2 식별자에 대응된 상기 특정 데이터를 상기 생체 정보
기반 인증 장치로 전송하는 단계
를 더 포함하고,
상기 특정 데이터는 상기 생체 정보 기반 인증 장치에서
복호화되는, 처리 방법.

[청구항 17] 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 데이터 업로드 인증을 위한 제1 프로그램을
포함하고,

상기 제1 프로그램은
컴퓨팅 장치로부터 어플리케이션 서버로 전달되는 업로드 요청 메시지를 탐지하면, 상기 센서를 활성화하고, 상기 보안 모듈로부터 제1 데이터 암호화키를 획득한 후, 업로드 인증 정보를 생성하고, 상기 업로드 인증 정보를 제어 서버로 전송하는 명령어들(instructions)을 포함하고,
상기 업로드 인증 정보는 상기 업로드 요청 메시지에서 추출한 제1 식별자, 상기 센서로부터 입력된 제1 생체 정보의 제1 생체 정보 인증 결과, 그리고 상기 제1 데이터 암호화키를 포함하며,
상기 제1 식별자는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 업로드 허용 대상 판단 시 사용되고,
상기 제1 생체 정보 인증 결과는 상기 제어 서버에서 업로드 허용 여부 판단 시 사용되며,
상기 제1 데이터 암호화키는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 업로드 요청된 데이터를 암호화하는데 사용되는, 생체 정보 기반 인증 장치.

[청구항 18] 제17항에서,
상기 프로그램은 데이터 다운로드 인증을 위한 제2 프로그램을 포함하고,
상기 제2 프로그램은
상기 컴퓨팅 장치로부터 상기 어플리케이션 서버로 전달되는 다운로드 요청 메시지를 탐지하면, 상기 센서를 활성화하고, 상기 보안 모듈로부터 제2 데이터 암호화키를 획득한 후, 다운로드 인증 정보를 생성하고, 상기 다운로드 인증 정보를 상기 제어 서버로 전송하는 명령어들을 포함하고,
상기 다운로드 인증 정보는 상기 다운로드 요청 메시지에서 추출한 제2 식별자, 그리고 상기 센서로부터 입력된 제2 생체 정보의 제2 생체 정보 인증 결과를 포함하며,
상기 제2 식별자는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 다운로드 허용 대상 판단 시 사용되고,
상기 제2 생체 정보 인증 결과는 상기 제어 서버에서 다운로드 허용 여부 판단 시 사용되는, 생체 정보 기반 인증 장치.

[청구항 19] 제17항에서,
상기 제2 프로그램은
상기 어플리케이션 서버로부터 상기 다운로드 요청 메시지에

관련된 다운로드 데이터를 수신하면, 상기 다운로드 데이터를 상기 제1 데이터 암호화키에 관련된 제2 데이터 암호화키로 복호화하여 상기 컴퓨팅 장치로 전달하는 명령어들을 더 포함하는 생체 정보 기반 인증 장치.

[청구항 20] 제17항에서,

상기 프로그램은 로그인 인증을 위한 제3 프로그램을 포함하고,

상기 제3 프로그램은

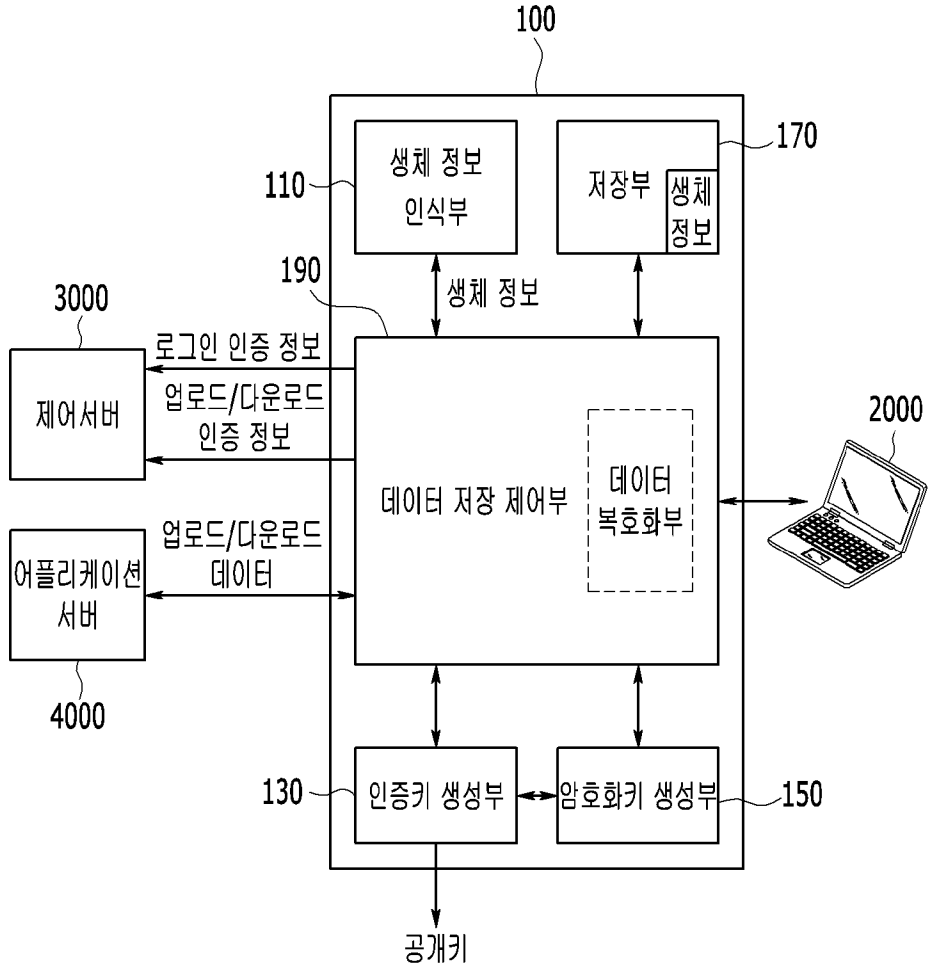
상기 컴퓨팅 장치로부터 상기 어플리케이션 서버로 전달되는 로그인 요청 메시지를 탐지하면, 상기 센서를 활성화하고, 로그인 인증 정보를 생성하며, 상기 로그인 인증 정보를 상기 제어 서버로 전송하는 명령어들을 포함하고,

상기 로그인 인증 정보는 상기 로그인 요청 메시지에서 추출한 제3 식별자와 상기 센서로부터 입력된 제3 생체 정보의 제3 생체 정보 인증 결과를 포함하며,

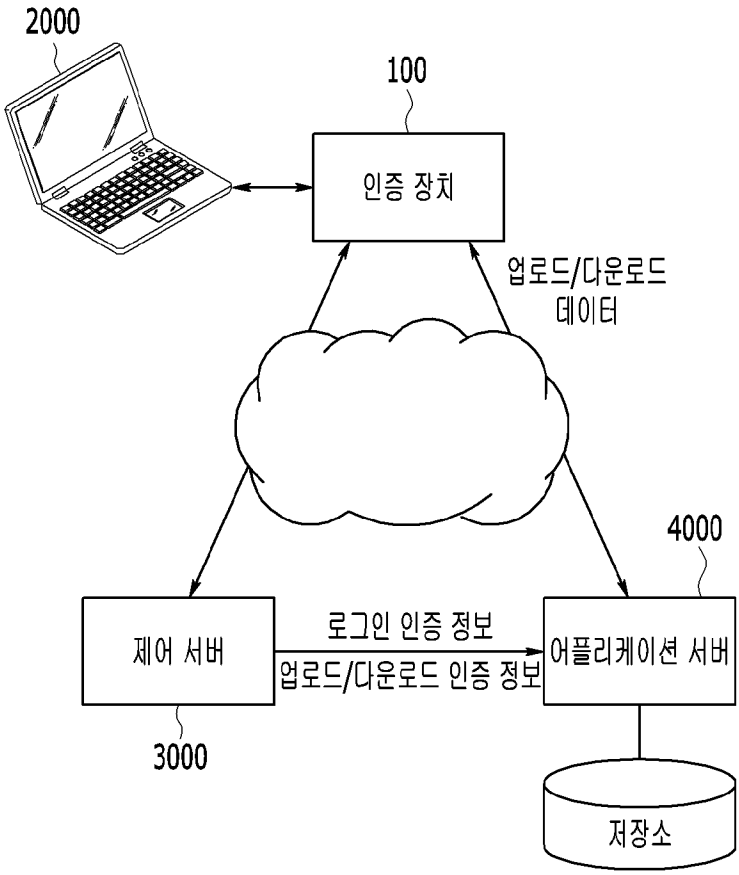
상기 제3 식별자는 상기 제어 서버에서 상기 어플리케이션 서버로 전달되어 상기 어플리케이션 서버에서 로그인 허용 대상 판단 시 사용되고,

상기 제3 생체 정보 인증 결과는 상기 제어 서버에서 로그인 허용 여부 판단 시 사용되는, 생체 정보 기반 인증 장치.

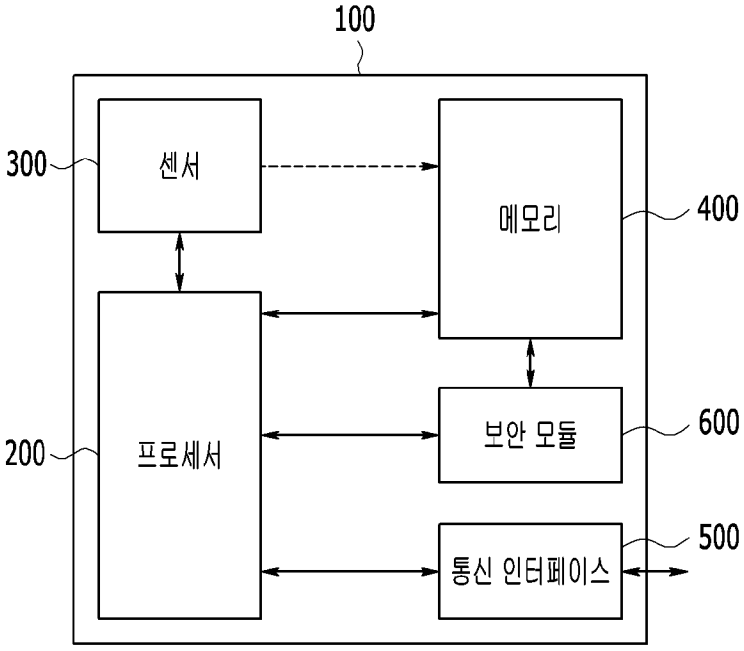
[Fig. 1]


100
생체 정보 인식부
110
저장부
생체 정보
170
190
생체 정보
3000
로그인 인증 정보
제어서버
업로드/다운로드 인증 정보
데이터 저장 제어부
데이터 복호화부
2000
업로드/다운로드 데이터
어플리케이션 서버
4000
130
인증키 생성부
암호화키 생성부
150
공개키

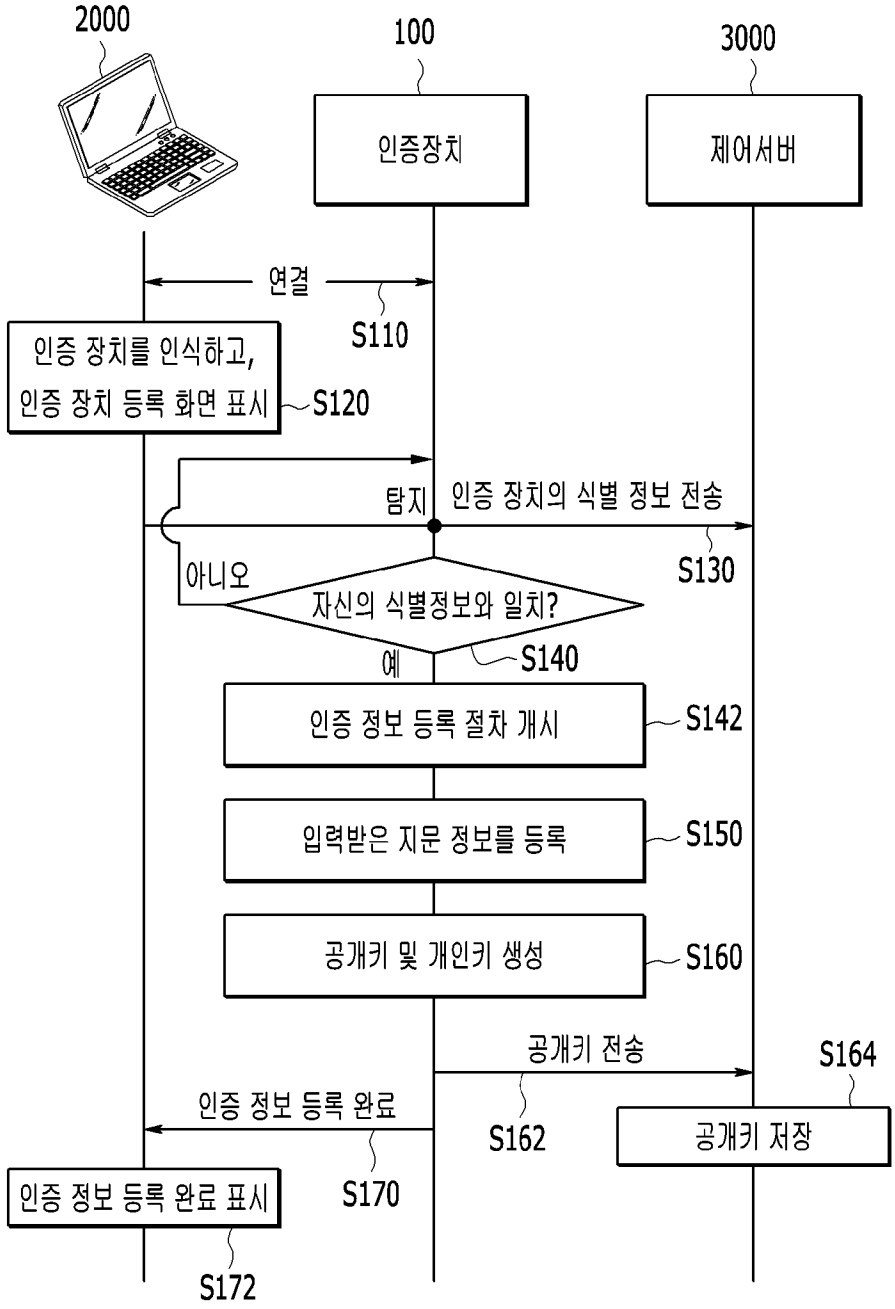
[Fig. 2]


2000
100
인증 장치
업로드/다운로드
데이터
4000
제어 서버
로그인 인증 정보
업로드/다운로드 인증 정보
어플리케이션 서버
3000
저장소

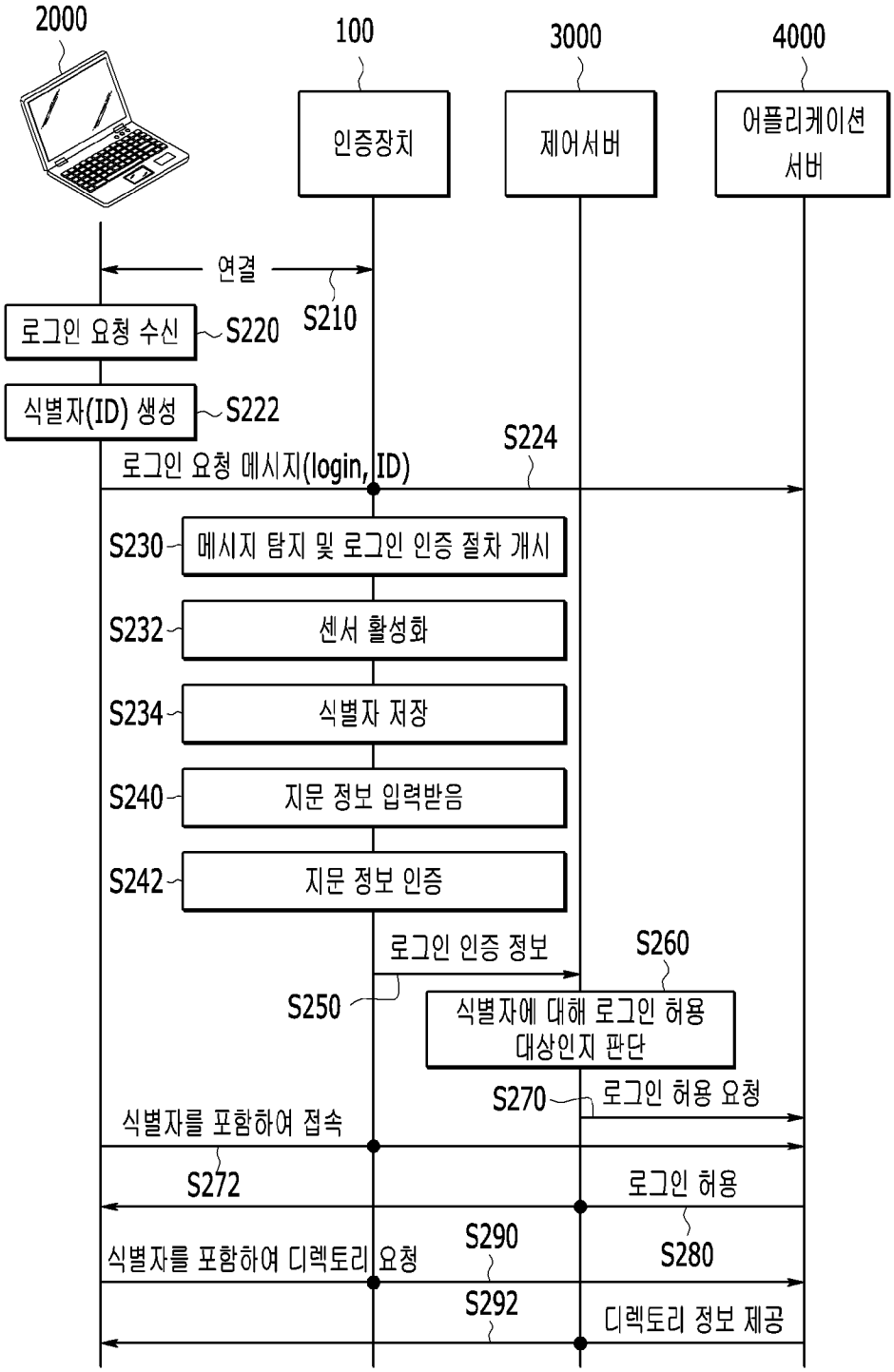
[Fig. 3]


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

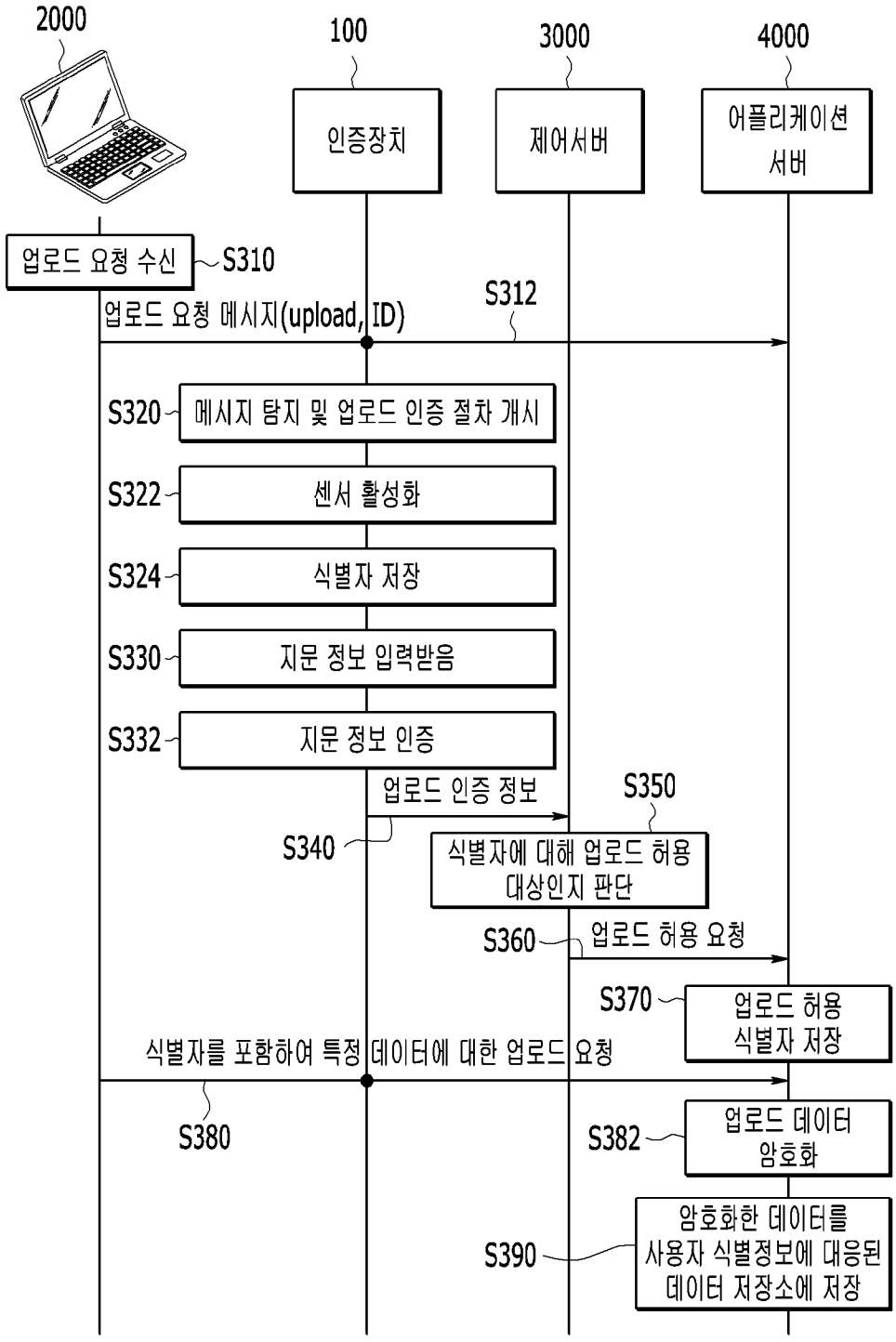
[Fig. 4]


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

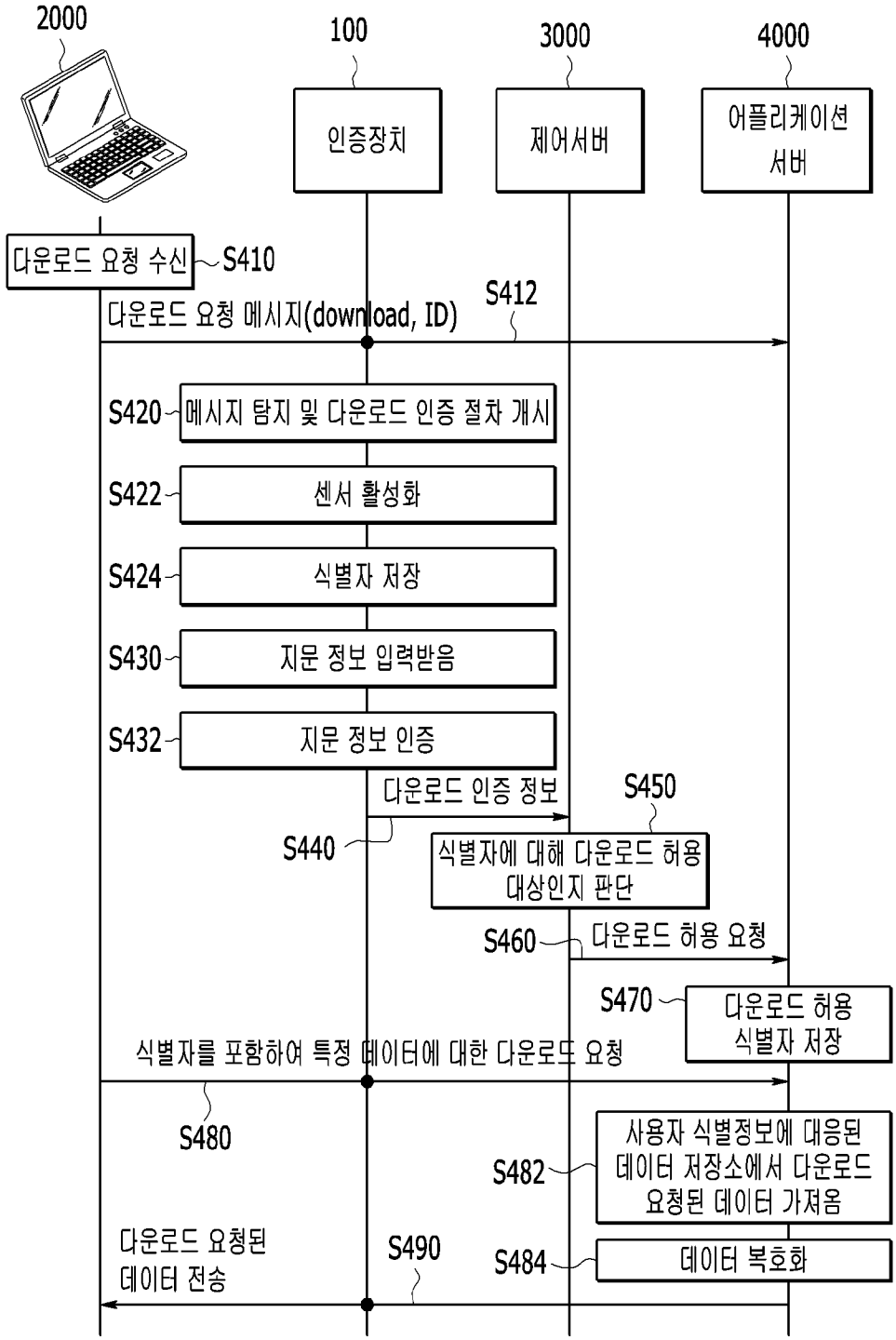
[Fig. 5]


2000
100
3000
4000
인증장치
제어서버
어플리케이션 서버
연결
S210
로그인 요청 수신
S220
식별자(ID) 생성
S222
S224
로그인 요청 메시지(login, ID)
S230
메시지 탐지 및 로그인 인증 절차 개시
S232
센서 활성화
S234
식별자 저장
S240
지문 정보 입력받음
S242
지문 정보 인증
로그인 인증 정보
S260
S250
식별자에 대해 로그인 허용 대상인지 판단
S270
로그인 허용 요청
식별자를 포함하여 접속
S272
로그인 허용
S290
S280
식별자를 포함하여 디렉토리 요청
S292
디렉토리 정보 제공

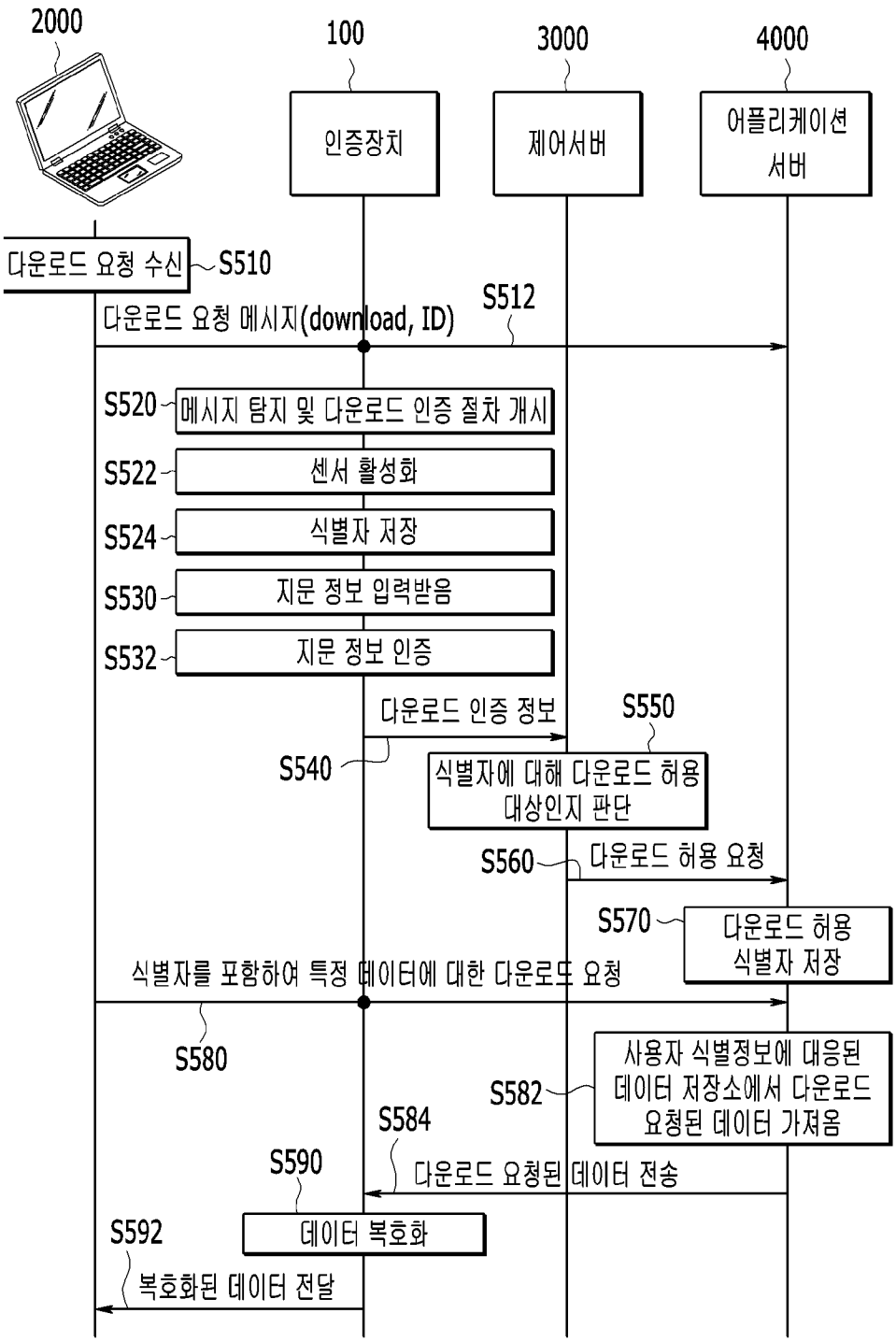
[Fig. 6]


2000
100
3000
4000
인증장치
제어서버
어플리케이션 서버
업로드 요청 수신
S310
업로드 요청 메시지(upload, ID)
S312
S320
메시지 탐지 및 업로드 인증 절차 개시
S322
센서 활성화
S324
식별자 저장
S330
지문 정보 입력받음
S332
지문 정보 인증
업로드 인증 정보
S350
S340
식별자에 대해 업로드 허용 대상인지 판단
S360
업로드 허용 요청
S370
업로드 허용 식별자 저장
식별자를 포함하여 특정 데이터에 대한 업로드 요청
S380
S382
업로드 데이터 암호화
암호화한 데이터를 사용자 식별정보에 대응된 데이터 저장소에 저장
S390

[Fig. 7]


2000
100
3000
4000
인증장치
제어서버
어플리케이션 서버
다운로드 요청 수신
S410
다운로드 요청 메시지(download, ID)
S412
S420
메시지 탐지 및 다운로드 인증 절차 개시
S422
센서 활성화
S424
식별자 저장
S430
지문 정보 입력받음
S432
지문 정보 인증
다운로드 인증 정보
S450
S440
식별자에 대해 다운로드 허용 대상인지 판단
S460
다운로드 허용 요청
S470
다운로드 허용 식별자 저장
식별자를 포함하여 특정 데이터에 대한 다운로드 요청
S480
사용자 식별정보에 대응된 데이터 저장소에서 다운로드 요청된 데이터 가져옴
S482
다운로드 요청된 데이터 전송
S490
S484
데이터 복호화

[Fig. 8]


2000
100
3000
4000
인증장치
제어서버
어플리케이션 서버
다운로드 요청 수신
S510
다운로드 요청 메시지(download, ID)
S512
S520
메시지 탐지 및 다운로드 인증 절차 개시
S522
센서 활성화
S524
식별자 저장
S530
지문 정보 입력받음
S532
지문 정보 인증
다운로드 인증 정보
S550
S540
식별자에 대해 다운로드 허용 대상인지 판단
S560
다운로드 허용 요청
S570
다운로드 허용 식별자 저장
식별자를 포함하여 특정 데이터에 대한 다운로드 요청
S580
사용자 식별정보에 대응된 데이터 저장소에서 다운로드 요청된 데이터 가져옴
S582
S584
다운로드 요청된 데이터 전송
S590
데이터 복호화
S592
복호화된 데이터 전달

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2016/015074

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 21/24; G06F 21/30; H04L 12/26; G06F 21/22; G06F 21/34; 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, login, application, authentication, user

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 [0040]-[0048]; claim 1; and figure 2.	1-20
Y	KR 10-0544217 B1 (NOMADIX, INC.) 23 January 2006 See paragraphs [0023], [0046]; claim 5; and figures 1, 3.	1-8,17-20
Y	KR 10-2010-0062827 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 10 June 2010 See paragraphs [0033]-[0048]; and figures 2-3.	4-20
A	KR 10-1458820 B1 (SOONCHUNHYANG UNIVERSITY INDUSTRY ACADEMY COOPERATION FOUNDATION) 07 November 2014 See paragraphs [0040]-[0060]; and figures 1-3.	1-20
A	KR 10-1418797 B1 (SAFERZONE CO., LTD.) 11 July 2014 See paragraphs [0041]-[0045]; and figure 4.	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 FEBRUARY 2017 (16.02.2017)	**17 FEBRUARY 2017 (17.02.2017)**

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/KR2016/015074

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
		JP 2004-507908 A	11/03/2004
		JP 4471554 B2	02/06/2010
		WO 2001-086877 A3	02/05/2002
KR 10-2010-0062827 A	10/06/2010	KR 10-1059144 B1	25/08/2011
KR 10-1458820 B1	07/11/2014	NONE	
KR 10-1418797 B1	11/07/2014	CN 104615929 A	13/05/2015
		EP 2869232 A1	06/05/2015
		US 2015-0127942 A1	07/05/2015

국 제 조 사 보 고 서

국제출원번호
PCT/KR2016/015074

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 21/24; G06F 21/30; H04L 12/26; G06F 21/22; G06F 21/34; 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, 로그인, 어플리케이션, 인증, 사용자

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 [0040]-[0048]; 청구항 1; 및 도면 2 참조.	1-20
Y	KR 10-0544217 B1 (노마딕스, 인코포레이티드) 2006.01.23 단락 [0023], [0046]; 청구항 5; 및 도면 1, 3 참조.	1-8,17-20
Y	KR 10-2010-0062827 A (한국전자통신연구원) 2010.06.10 단락 [0033]-[0048]; 및 도면 2-3 참조.	4-20
A	KR 10-1458820 B1 (순천향대학교 산학협력단) 2014.11.07 단락 [0040]-[0060]; 및 도면 1-3 참조.	1-20
A	KR 10-1418797 B1 ((주)세이퍼존) 2014.07.11 단락 [0041]-[0045]; 및 도면 4 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 02월 16일 (16.02.2017)	2017년 02월 17일 (17.02.2017)

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

심사관
이은규
전화번호 +82-42-481-3580

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2016/015074

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
		JP 2004-507908 A	2004/03/11
		JP 4471554 B2	2010/06/02
		WO 2001-086877 A3	2002/05/02
KR 10-2010-0062827 A	2010/06/10	KR 10-1059144 B1	2011/08/25
KR 10-1458820 B1	2014/11/07	없음	
KR 10-1418797 B1	2014/07/11	CN 104615929 A	2015/05/13
		EP 2869232 A1	2015/05/06
		US 2015-0127942 A1	2015/05/07