(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2012 년 12 월 13 일 (13.12.2012)

WIPO | PCT

(10) 국제공개번호
WO 2012/169752 A2

(51) 국제특허분류:
G06F 21/20 (2006.01) *H04L 9/32* (2006.01)

(21) 국제출원번호: PCT/KR2012/004388

(22) 국제출원일: 2012 년 6 월 4 일 (04.06.2012)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2011-0054433 2011 년 6 월 7 일 (07.06.2011) KR

(71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): **(주) 잉카인터넷 (INCA INTERNET CO., LTD)** [KR/KR]; 서울특별시 구로구 구로 3 동 235-2 에이스하이엔드타워 1201 호, 152-740 Seoul (KR).

(72) 발명자; 겸
(75) 발명자/출원인 (US 에 한하여): **김영기 (KIM, Young-Gi)** [KR/KR]; 인천광역시 부평구 청천동 200, 403-030 Incheon (KR). **원현식 (WON, Hyun-Seek)** [KR/KR]; 인천광역시 부평구 부개 3 동 477, 403-813 Incheon (KR). **정명재 (JUNG, Myung-Jae)** [KR/KR]; 서울특별시 동작구 신대방동 366-231, 156-848 Seoul (KR). **유장선 (RYU, Jang-Seon)** [KR/KR]; 서울특별시 강서구 등촌 2 동 520-3, 157-032 Seoul (KR). **김인수 (KIM, In-Su)** [KR/KR]; 서울특별시 구로구 구로 3 동 1129-81, 152-880 Seoul (KR).

(74) 대리인: **특허법인 세아 (SEAH PARTNERS PATENT & LAW FIRM)**; 서울특별시 서초구 반포대로 118 우림빌딩 5 층, 137-872 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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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.

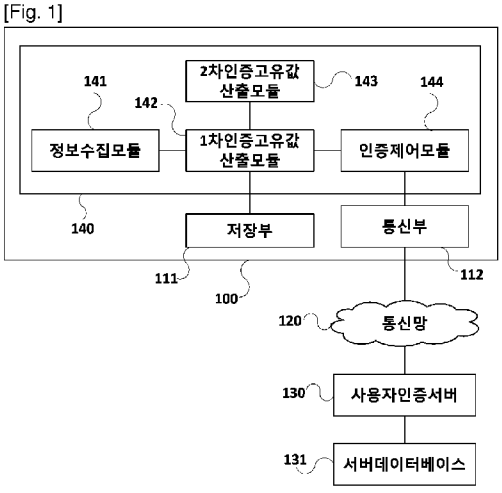
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE,

[다음 쪽 계속]

(54) **Title**: AUTHENTICATION SYSTEM AND METHOD FOR DEVICE ATTEMPTING CONNECTION

(54) **발명의 명칭** : 접속 시도 기기 인증 시스템 및 방법

[Fig. 1]



111 ... Storage unit
112 ... Communication unit
120 ... Communication network
130 ... User authentication server
131 ... Server database
141 ... Information collection module
142 ... First-round authentication eigenvalue production module
143 ... Second-round authentication eigenvalue production module
144 ... Authentication control module

(57) **Abstract**: The present invention relates to a system and a method for authenticating a device attempting connection in a PC environment or mobile environment which authenticate whether the device which is presently attempting connection to a web server is a registered device predetermined by a user. According to the present invention, the system for authenticating the device attempting connection, which is within a system for authenticating a device attempting connection while provided in a device connected to a user authentication server, includes: an information collection module which collects hardware environment and software environment information from the device; an authentication control module which performs a registration process for the device when a user requests device registration and performs a verification process for the device attempting connection with respect to the device of an online service request by the user; a first-round authentication eigenvalue production module which produces an eigenvalue for first-round authentication by combining at least two kinds of environment information collected by the information collection module according to an operating system provided in the device, and provides the first-round authentication eigenvalue for the authentication control module; and a second-round authentication eigenvalue production module which produces an eigenvalue for second-round authentication by combining at least two kinds of environment information collected by the information collection module, and provides the second-round authentication eigenvalue for the authentication control module.

(57) 요약서:

[다음 쪽 계속]

WO 2012/169752 A2

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, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

이 발명은 PC 환경 또는 모바일환경에서, 현재 웹서버에 접속 시도하는 기기가 사용자가 미리 지정해 놓은 등록 기기인지 여부를 인증하는 접속 시도 기기 인증 시스템 및 방법에 관한 것이다. 이 발명에 따른 접속 시도 기기 인증 시스템은, 사용자인증서버와 접속된 기기에 설치되는 접속 시도 기기 인증 시스템에 있어서, 상기 기기에 설치된 하드웨어 환경 및 소프트웨어 환경 정보를 수집하는 정보수집모듈과, 사용자의 기기 등록 요청시 상기 기기에 대한 등록 절차를 수행하고, 사용자가 온라인 서비스 요청시 상기 기기에 대한 접속 시도 기기 검증 절차를 수행하는 인증제어모듈과, 상기 기기에 설치된 운영체제에 따라 상기 정보수집모듈에서 수집된 적어도 둘 이상의 환경 정보를 조합하여 1 차인증고유값을 산출하고 상기 인증제어모듈에게 제공하는 1 차인증고유값산출모듈과, 상기 정보수집모듈에서 수집된 적어도 둘 이상의 환경 정보를 조합하여 2 차인증고유값을 산출하고 상기 인증제어모듈에게 제공하는 2 차인증고유값산출모듈을 포함한다.

명세서

발명의 명칭: 접속 시도 기기 인증 시스템 및 방법

기술분야

[1] 이 발명은 온라인 서비스를 이용하기 위해 접속을 시도하는 기기를 인증하는 시스템 및 방법에 관한 것으로서, 보다 상세하게는 PC환경 또는 모바일환경에서 현재 웹서버에 접속 시도하는 기기가 사용자가 미리 지정해 놓은 등록 기기인지 여부를 인증하는 접속 시도 기기 인증 시스템 및 방법에 관한 것이다.

배경기술

[2] 인터넷 통신망이 고속화됨에 따라, 인터넷 통신망을 이용하여 인터넷 뱅킹, 온라인 게임, 온라인 쇼핑 등과 같은 다양한 온라인 서비스가 활성화되고 있다. 통상적으로 사용자가 상술한 온라인 서비스를 이용하려면 해당 온라인 서비스를 제공하는 웹서버에 개인 인증 정보(사용자 아이디와 패스워드)를 입력하여 로그인 인증을 통과해야 한다. 정당사용자뿐만 아니라 명의도용자(정당사용자의 개인 인증 정보를 획득한 자)라 하더라도 컴퓨터나 모바일폰 등의 기기에 정당사용자의 개인 인증 정보를 이용하여 웹서버에 로그인하면, 현재 사용중인 기기를 통해 해당 웹서버에서 제공하는 정당사용자의 온라인 서비스를 이용할 수 있다.

[3] 명의도용자는 정당사용자의 의사에 반하여 부정한 방법으로 정당사용자의 개인 인증 정보를 탈취한 자일 수 있다. 이렇게 부정한 방법으로 정당사용자의 개인 인증 정보를 탈취한 명의도용자가 정당사용자의 계정에 불법적으로 접속하여 정당사용자의 온라인 서비스를 불법적으로 사용하는 피해 사례가 늘어나고 있다. 이에, 명의도용자가 사용자의 개인 인증 정보를 탈취하더라도 정당사용자에게 제공되는 온라인 서비스에는 접근하지 못하도록 차단하는 보완적인 보안 대책 마련이 시급하다.

[4] 이러한 보완적인 보안 대책으로서, 사용자가 미리 지정해 놓은 등록 PC에서만 온라인 서비스를 이용할 수 있도록 하는 기술(이하, PC 지정 서비스 기술이라 함)이 제안되었다.

[5] PC 지정 서비스에 관한 선행기술로서, 대한민국공개특허 제2010-125496호와 대한민국등록특허 제1023793호가 있다. 이 선행기술들은 고객의 사용자 아이디와 고객이 온라인 서비스(인터넷 뱅킹)를 위해 지정한 하나 이상의 컴퓨터 정보를 연계하여 웹서버에 등록한다. 웹서버는 임의의 컴퓨터가 접속을 시도하면, 그 접속을 시도한 컴퓨터가 온라인 서비스를 위해 사전 등록된 컴퓨터인지를 확인하여 사전 등록된 컴퓨터인 경우에만 상기 컴퓨터에게 온라인 서비스를 제공한다.

[6] 온라인 게임 웹사이트의 경우, 2006년 9월 엔씨소프트는 업체 최초로 온라인 게임 MMORPG(Massive Multiplayer Online Role Playing Game) 리니지 시리즈에

PC 지정 서비스를 적용하였으며, 다른 온라인 게임업체(NHN 한 게임, 넥슨 등)에서도 PC 지정 서비스를 서비스중이거나 서비스 검토중인 것으로 알려져 있다. 아울러, 인터넷 뱅킹 웹사이트의 경우도 일부 은행 웹사이트에서 PC 지정 서비스를 제공하고 있다. 일 예로서, KB 국민은행에 적용되는 PC 지정 서비스인 경우, 사용자는 인터넷 뱅킹을 사용할 컴퓨터를 최대 10개까지 등록할 수 있다. 미리 등록해 놓은 10개의 등록 컴퓨터를 통해서는 이체 서비스 등의 금융 거래를 할 수 있지만, 미등록 컴퓨터에서는 조회 서비스만이 가능하도록 한다.

[7] 상술한 선행기술들에 따른 PC 지정 서비스 기술을 간략하게 설명한다. 웹서버는 사용자로부터 PC 지정 서비스가 요청되고 신규 PC 등록이 요청되면, 그 등록 요청된 PC의 하드웨어 정보로부터 인증고유값을 산출하여 사용자의 개인 인증 정보(사용자 아이디)와 매칭시켜 사전 등록해 놓는다. 그 후, 웹서버는 상기 사용자의 개인 인증 정보(사용자 아이디)를 이용하여 웹서버에 접속을 시도하는 PC의 하드웨어 정보로부터 해당 접속 시도 PC의 인증고유값을 산출한다. 물론, 등록 PC의 인증고유값을 산출하는 방법과 접속 시도 PC의 인증고유값을 산출하는 방법은 동일한 것이 바람직하다. 다음, 웹서버는 산출된 접속 시도 PC의 인증고유값과, 상기 사용자의 개인 인증 정보와 매칭된 등록 PC의 인증고유값을 비교하여, 접속 시도 PC에게 해당 온라인 서비스를 허여 또는 거부할 지를 판단한다.

[8] 이러한 선행기술들은 웹서버가 사용자의 개인 인증 정보를 확인하는 것과 아울러 접속 시도 PC가 사전 등록된 PC인지 여부를 확인한 후, 접속 시도 PC에 온라인 서비스를 허여함으로써 종래에 대비하여 보안이 강화되는 잇점이 있다.

[9] 그러나, 네트워크로 전송되는 접속 시도 PC의 인증고유값은 해커에 의해 쉽게 해킹되어 변조될 수 있는 바, 명의도용자가 정당사용자의 등록 PC가 아닌 미등록 PC를 이용하여 웹서버에 접속을 시도하더라도 미등록 PC의 인증고유값이 등록 PC의 인증고유값으로 변조될 수 있다. 이 경우, 웹서버는 이를 인지하지 못하고 명의도용자가 이용하는 접속 시도 미등록 PC에 사용자의 온라인 서비스 사용을 허여하게 되는 문제점이 있다.

[10] 또한, 선행기술들은 등록 PC와 접속 시도 PC의 시스템 구성 상태와는 무관하게 모두 동일한 하드웨어 정보로부터 해당 PC의 인증고유값을 산출하기 때문에, 해당 PC의 CMOS 설정이나 운영체제(OS)의 사용계정자의 권한에 따라 일부 PC에서는 인증고유값 산출에 필요한 정보를 수집하지 못하는 경우도 발생한다. 그렇다고 모든 PC가 필수적으로 구비한 한정된 하드웨어 정보를 기반으로 인증고유값(예컨대 현재 웹사이트의 PC 지정 서비스에서 주로 사용되는 MAC 주소)을 산출한다면 그 인증고유값은 변조되기 쉬운 취약점을 가지게 되는 문제점이 있다. 또한, 종래의 기술은 사용자가 웹서버에 접속하기 위해 등록하는 기기가 PC에 한정되기 때문에 사용자의 편리성이 줄어드는 문제점이 있다.

[11] 이와 같이 선행기술들은 다기종의 하드웨어 기기(PC, 모바일폰, 태블릿 PC), 멀티플랫폼 환경(Windows, 리눅스, Mac, iOS, 안드로이드, 윈도우즈모바일 등)

및 멀티 브라우저(Multi Browser) 환경에 적용하기 어려우며, 많은 보안 취약점을 가지고 있기 때문에 현재의 해킹 기술과 금융 및 온라인 사고 등에 대처하기 어려운 문제점이 있다.

[12]

발명의 상세한 설명

기술적 과제

[13] 상술한 종래기술의 문제점을 해결하기 위하여 안출된 이 발명의 목적은, 접속 시도 기기가 자체적으로 등록 기기인지 여부를 1차 인증하고, 1차 인증 완료된 접속 시도 기기에 한해 웹서버가 등록 기기 여부를 2차 인증하며, 1차 인증과 2차 인증이 모두 성공된 접속 시도 기기에게 사용자의 온라인 서비스 이용이 허여되도록 하는 접속 시도 기기 인증 시스템 및 방법을 제공하기 위한 것이다.

[14]

과제 해결 수단

[15] 상술한 목적을 달성하기 위한 이 발명에 따른 접속 시도 기기 인증 시스템은, 사용자인증서버와 접속된 기기에 설치되는 접속 시도 기기 인증 시스템에 있어서,

[16] 상기 기기에 설치된 하드웨어 환경과 소프트웨어 환경 중 적어도 둘 이상의 환경 정보를 수집하는 정보수집모듈과,

[17] 사용자의 기기 등록 요청시 상기 기기에 대한 기기 등록 절차를 수행하고, 사용자가 온라인 서비스 요청시 상기 기기에 대한 접속 시도 기기 검증 절차를 수행하는 인증제어모듈과,

[18] 상기 기기의 종류 및 상기 기기에 설치된 운영체제의 종류에 따라 상기 정보수집모듈에서 수집된 적어도 둘 이상의 환경 정보를 조합하여 1차인증고유값을 산출하고 상기 인증제어모듈에게 제공하는 1차인증고유값산출모듈을 포함하고,

[19] 상기 인증제어모듈은 상기 기기 등록 절차시 상기 1차인증고유값산출모듈로부터 입력되는 등록용 1차인증고유값을 상기 기기의 저장부에 저장하고 상기 사용자인증서버에게 전송하여 저장되도록 하며, 상기 접속 시도 기기 검증 절차시 상기 1차인증고유값산출모듈로부터 입력되는 검증용 1차인증고유값을 상기 등록용 1차인증고유값과 비교하여 검증하고 상기 사용자인증서버에게 전송하여 검증되도록 하는 것을 특징으로 한다.

[20]

[21] 또한, 이 발명에 따른 접속 시도 기기 인증 방법은, 사용자인증서버와 접속된 기기에 설치되는 접속 시도 기기 인증 시스템의 접속 시도 기기 인증 방법에 있어서,

[22] 상기 기기에 대한 접속 시도 기기 검증이 요청되면, 상기 접속 시도 기기 인증 시스템이 상기 접속 시도 기기의 기기 종류 및 운영체제를 파악하는 제1단계와,

[23] 상기 접속 시도 기기 인증 시스템이 상기 접속 시도 기기의 기기 종류 및 운영체제별로 수집 가능한 하드웨어와 소프트웨어 환경 정보 중 적어도 둘 이상의 환경 정보를 수집하는 제2단계와,

[24] 상기 접속 시도 기기 인증 시스템이 상기 접속 시도 기기로부터 적어도 둘 이상의 환경 정보를 조합하여 검증용 1차인증고유값을 산출하는 제3단계와,

[25] 상기 접속 시도 기기 인증 시스템이 상기 검증용 1차 인증고유값과 상기 접속 시도 기기의 저장부에 저장된 등록용 1차인증고유값을 비교하는 제4단계와,

[26] 상기 제4단계의 비교결과 상기 검증용 1차인증고유값과 상기 등록용 1차인증고유값이 동일하면, 상기 접속 시도 기기 인증 시스템이 검증용 1차인증고유값을 상기 사용자인증서버에게 전송하는 제5단계와,

[27] 상기 접속 시도 기기 인증 시스템이 상기 제5단계 후 상기 사용자인증서버로부터의 인증이 성공되면 상기 접속 시도 기기에 온라인 서비스가 제공되도록 하는 제6단계와,

[28] 상기 접속 시도 기기 인증 시스템이 상기 제4단계의 비교결과 상기 검증용 1차인증고유값과 상기 등록용 1차인증고유값이 동일하지 않거나, 상기 제5단계 후 상기 사용자인증서버로부터의 인증이 실패되면, 상기 접속 시도 기기에 온라인 서비스가 차단되도록 하는 제7단계를 포함한 것을 특징으로 한다.

[29]

[30] 또한, 이 발명에 따른 컴퓨터로 읽을 수 있는 기록매체에 있어서, 사용자인증서버와 접속된 기기에 접속 시도 기기 인증 방법을 실행하기 위한 컴퓨터로 읽을 수 있는 기록매체에 있어서,

[31] 상기 접속 시도 기기 인증 방법은, 상기 기기에 대한 접속 시도 기기 검증이 요청되면, 상기 접속 시도 기기 인증 시스템이 상기 접속 시도 기기의 기기 종류 및 운영체제를 파악하는 제1단계와,

[32] 상기 접속 시도 기기 인증 시스템이 상기 접속 시도 기기의 기기 종류 및 운영체제별로 수집 가능한 하드웨어와 소프트웨어 환경 정보 중 적어도 둘 이상의 환경 정보를 수집하는 제2단계와,

[33] 상기 접속 시도 기기 인증 시스템이 상기 접속 시도 기기로부터 적어도 둘 이상의 환경 정보를 조합하여 검증용 1차인증고유값을 산출하는 제3단계와,

[34] 상기 접속 시도 기기 인증 시스템이 상기 검증용 1차 인증고유값과 상기 접속 시도 기기의 저장부에 저장된 등록용 1차인증고유값을 비교하는 제4단계와,

[35] 상기 제4단계의 비교결과 상기 검증용 1차인증고유값과 상기 등록용 1차인증고유값이 동일하면, 상기 접속 시도 기기 인증 시스템이 검증용 1차인증고유값을 상기 사용자인증서버에게 전송하는 제5단계와,

[36] 상기 접속 시도 기기 인증 시스템이 상기 제5단계 후 상기 사용자인증서버로부터의 인증이 성공되면 상기 접속 시도 기기에 온라인 서비스가 제공되도록 하는 제6단계와,

[37] 상기 접속 시도 기기 인증 시스템이 상기 제4단계의 비교결과 상기 검증용

1차인증고유값과 상기 등록용 1차인증고유값이 동일하지 않거나, 상기 제5단계 후 상기 사용자인증서버로부터의 인증이 실패되면, 상기 접속 시도 기기에 온라인 서비스가 차단되도록 하는 제7단계를 포함한 것을 특징으로 한다.

[38]

발명의 효과

[39] 이상과 같이 이 발명에 따르면 등록 기기가 소프트웨어 및/또는 하드웨어 환경 정보를 기반으로 1차인증고유값과 2차인증고유값을 산출하고 자체적인 1차 인증 후 웹서버를 통한 2차 인증을 수행하기 때문에 네트워크 패킷 해킹으로부터 보안을 강화할 수 있는 효과가 있다. 또한, 이 발명에 따르면 등록 기기 및 접속 시도 기기의 종류(PC, 모바일폰, 태블릿PC), 해당 기기에 설치된 운영체제(OS)의 종류에 따라 각각 수집 가능한 정보들을 조합하여 인증고유값을 산출하기 때문에, 인증고유값 변조가 어렵게 되어 보안이 강화되는 효과가 있다.

[40]

도면의 간단한 설명

[41] 도 1은 이 발명에 따른 접속 시도 기기 인증 시스템을 도시한 구성 블록도이다.

[42] 도 2 및 도 3은 이 발명에 따른 접속 시도 기기 인증 방법을 도시한 동작 흐름도이다.

[43] * 부호의 설명 *

[44] 110 : 컴퓨터 유저 기기 111 : 저장부

[45] 112 : 통신부 120 : 통신망

[46] 130 : 사용자인증서버 131 : 서버데이터베이스

[47] 140 : 접속 시도 기기 인증 시스템 141 : 정보수집모듈

[48] 142 : 1차인증고유값산출모듈 143 : 2차인증고유값산출모듈

[49] 144 : 인증제어모듈

[50]

발명의 실시를 위한 최선의 형태

[51] 이하, 첨부된 도면을 참조하여 이 발명에 따른 접속 시도 기기 인증 시스템 및 방법을 보다 상세하게 설명한다.

[52] 도 1은 이 발명에 따른 접속 시도 기기 인증 시스템을 도시한 구성 블록도이다.

[53] 기기(110)는 통신망(120)을 통해 사용자인증서버(130)와 접속된다. 사용자인증서버(130)는 기기(110)에 다양한 온라인 서비스를 제공하는 통상적인 웹서버와 물리적으로 병용될 수도 있다. 사용자인증서버(130)는 서버데이터베이스(131)와 연결되며 기기(110)에게 기기 지정 서비스를 제공한다. 서버데이터베이스(131)에는 사용자 식별정보(사용자 아이디)와 매칭되어 사용자가 지정해 놓은 등록 기기별 인증고유값이 저장된다. 하나의 사용자 식별정보에 다수의 등록 기기가 매칭되어 저장된 경우, 서버데이터베이스(131)에는 등록 기기별 고유식별명도 함께 저장될 수 있다.

여기서, 기기 지정 서비스라 함은 사용자가 임의의 기기를 사용자인증서버(130)에 온라인 서비스 이용을 위한 등록 기기로 지정하거나 취소하는 절차 또는 임의의 사용자 아이디로 웹서버에 접속을 시도하는 기기가 해당 사용자 아이디에 기지정된 등록 기기인지를 검증하는 절차를 포함한다.

[54] 기기(110)는 이 발명에 따른 접속 시도 기기 인증 시스템(140)을 포함한다. 이 접속 시도 기기 인증 시스템(140)은 소프트웨어로 제작되어 기기(110)에 설치되며 기기(110)의 하드웨어 장비를 이용하여 실행된다. 이 소프트웨어는 사용자인증서버(130) 또는 타 소프트웨어 공급서버를 통해 기기(110)에 다운로드되어 설치될 수 있다. 기기(110)가 웹서버를 통해 온라인 서비스(에컨대, 전자금융서비스, 전자입찰, 온라인게임, 온라인판매 등)을 이용하려면 반드시 접속 시도 기기 인증 시스템(140)을 설치하도록 한다.

[55] 접속 시도 기기 인증 시스템(140)은, 정보수집모듈(141)과, 1차인증고유값산출모듈(142)과, 2차인증고유값산출모듈(143)과, 인증제어모듈(144)을 포함한다.

[56] 정보수집모듈(141)은, 기기(110)에 설치된 하드웨어 환경 및 소프트웨어 환경 정보를 수집하는데, 여기에는 하드웨어 일련번호, UUID(Universally Unique ID), 하드디스크 시리얼넘버(HDD serial number), 하드디스크 볼륨 시리얼넘버(HDD volumn serial number), 하드디스크 모델 이름(HDD model name), 운영 체제(OS), OS 설치 아이디(ID), USIM(Universal Subscriber Identity Module)카드에 저장된 가입자식별번호(IMSI : Internatioal Mobile Subscriber Identity), 네트워크 세션키, 기기고유번호(IMEI : International Mobile Equipment Identity) 등이 포함된다. 정보수집모듈(141)은 기기의 종류가 모바일폰인지, PC인지, 아니면 태블릿PC에 따라 그리고, 기기에 설치된 운영체제(OS)가 윈도우즈(Windows)인지, 리눅스인지, iOS인지, 안드로이드인지, 아니면 윈도우즈모바일인지에 따라 서로 다른 환경 정보를 수집한다.

[57] 인증제어모듈(144)은 이 발명에 따른 기기 등록 절차와, 접속 시도 기기 검증 절차를 수행한다. 이 발명의 명세서에서, 등록 기기와 접속 시도 기기가 동일한 기기일지라도, 사용자에 의해 등록 기기로 지정되는 기기 등록 절차에서는 등록 기기로 명명하고, 사용자가 웹서버에 접속하여 온라인 서비스를 이용하고자 하는 접속 시도 기기 검증 절차에서는 접속 시도 기기로 명명한다.

[58] 기기 등록 절차에서, 인증제어모듈(144)은 1차인증고유값산출모듈(142)에서 산출된 등록용 1차인증고유값을 해쉬값으로 변환하여 저장부(111)에 파일로 저장한다. 그러면, 저장부(111)에는 1차인증고유값 파일이 저장되며 그 1차인증고유값 파일 생성시간이 기록된다. 다음, 인증제어모듈(144)은 2차인증고유값산출모듈(143)에서 산출된 등록용 2차인증고유값을 해쉬값으로 변환하여 사용자 식별정보와 함께 통신부(112)를 통해 사용자인증서버(130)에게 전달한다. 이때, 해당 등록 기기를 식별하기 위한 고유식별명을 함께 전송할 수도 있다. 그러면, 사용자인증서버(130)는 서버데이터베이스(131)에 사용자

식별정보와 등록 기기의 등록용 2차인증고유값 및 고유식별명을 연계하여 저장한다. 2차인증고유값산출모듈(143)은 생략 가능하며, 이 경우 1차인증고유값산출모듈(142)에서 산출된 등록용 1차인증고유값을 등록용 2차인증고유값으로 사용할 수 있다.

[59] 접속 시도 기기 검증 절차에서, 인증제어모듈(144)은 1차인증고유값산출모듈(142)에서 산출된 검증용 1차인증고유값을 해쉬값으로 변환하여 등록 기기 등록절차에서 파일로 저장된 등록용 1차인증고유값과 비교하여 접속 시도 기기가 등록 기기인지 여부를 1차 인증한다. 1차 인증이 통과되면, 인증제어모듈(144)은 2차인증고유값산출모듈(143)에서 산출된 검증용 2차인증고유값을 해쉬값으로 변환하여 사용자 식별정보와 함께 통신부(112)를 통해 사용자인증서버(130)에게 전달한다. 그러면, 사용자인증서버(130)는 수신된 검증용 2차인증고유값과 서버데이터베이스(131)에 저장된 등록용 2차인증고유값을 비교하여 접속 시도 기기가 등록 기기인지 여부를 2차 인증한다. 2차인증고유값산출모듈(143)이 생략된 경우 검증용 1차인증고유값과 검증용 2차인증고유값은 동일하다.

[60] 등록 기기와 접속 시도 기기가 동일하고 하드웨어 및 소프트웨어 환경이 변경되지 않은 경우, 등록용 1차인증고유값과 검증용 1차인증고유값이 동일하며 등록용 2차인증고유값과 검증용 2차인증고유값이 동일하기 때문에, 접속 시도 기기는 1차 인증 및 2차 인증에 모두 성공하여 온라인 서비스를 이용할 수 있게 된다. 그러나, 등록 기기와 접속 시도 기기가 다를 경우, 등록용 1차인증고유값(등록 기기에 저장된 인증고유값)과 검증용 1차인증고유값이 동일할 수 없기 때문에 1차 인증을 통과할 수 없게 되고, 설사 1차 인증을 통과하게 되더라도 등록용 2차인증고유값(사용자인증서버에 저장된 인증고유값)과 검증용 2차인증고유값(또는 검증용 1차인증고유값)이 동일하지 않기 때문에 2차 인증을 통과할 수 없게 된다. 접속 시도 기기가 1차 인증 또는 2차 인증에 성공하지 못하면 웹서버의 온라인 서비스를 이용할 수 없게 된다.

[61] 인증제어모듈(144)은 등록 기기와 접속 시도 기기의 다양한 하드웨어 환경 및 소프트웨어 환경 정보를 조합하여 인증고유값을 생성하기 때문에, 등록 기기의 하드웨어나 소프트웨어가 변경될 경우(예컨대, 하드디스크 교체, 운영체제 재설치, 파일 변경), 인증제어모듈(144)은 등록 기기와 접속 시도 기기가 동일하지 않는 것으로 판단한다. 이럴 경우, 인증제어모듈(144)은 하드웨어 및 소프트웨어 환경이 변경된 등록 기기를 신규 기기로 인식하고, 사용자로 하여금 신규 기기 등록 절차를 진행하도록 안내한다.

[62] 1차인증고유값산출모듈(142)은 정보수집모듈(141)에서 수집된 기기(110)의 하드웨어 및 소프트웨어 환경 정보 중, 기기에 설치된 운영체제(OS)에 따라 수집 가능한 정보들을 이용하여 1차인증고유값을 산출하고, 해쉬값으로 변환하여 파일로 생성한다.

[63] 여기서, 1차인증고유값은 기기의 종류 및 기기에 설치된 운영체제의 종류에

따라 각기 다른 기기 식별 정보들을 조합하여 생성된다.

[64] 제1실시예로서, 기기가 컴퓨터이고, 기기에 설치된 운영체제가 윈도우즈 운영체제(Windows OS)이면, 1차인증고유값산출모듈(142)은 OS 설치 아이디와 하드디스크 시리얼넘버와 파일 생성 시간 및 사용자 식별정보 등을 조합하여 1차인증고유값을 생성한다. 여기서, OS 설치 아이디라 함은 윈도우즈 OS 설치시 제품 ID와 하드웨어 식별자 정보를 기반으로 생성되는 고유 설치 아이디를 의미한다.

[65] 한편, 제2실시예로서, 기기가 컴퓨터이고, 기기에 설치된 운영체제가 리눅스 운영체제(Linux OS)이면, 1차인증고유값산출모듈(142)은 UUID와 하드디스크 모델 이름(HDD model name)과 생성 시간 및 사용자 식별정보 등을 조합하여 1차인증고유값을 생성한다. 여기서, 리눅스 운영체제에서 하드디스크 모델 이름을 조합하여 1차인증고유값을 생성하는 이유는, 리눅스 운영체제에서는 일반 사용자 권한으로는 하드디스크 시리얼넘버 정보에 접근할 수 없기 때문이다. 마지막으로 기기에 설치된 운영체제가 맥 운영체제(Mac OS)이면, 하드웨어 일련번호와 하드디스크 시리얼넘버와 생성 시간 및 사용자 식별정보 등을 조합하여 1차인증고유값을 생성한다.

[66] 제3실시예로서, 기기가 모바일폰일 때 1차인증고유값을 생성하는 방법을 설명한다. 통상적으로 모바일폰은 이동통신사에 가입하여야 사용 가능한데, 해당 이동통신사가 서비스하는 통신 규약 기술(W-CDMA 또는 GSM)에 따라 모바일폰에는 USIM(Universal Subscriber Identity Module)카드 또는 SIM(Subscriber Identity Module)카드가 장착된다. 이 USIM카드 또는 SIM카드에는 가입자식별번호(IMSI), 네트워크정보, 인증정보 등과 같은 중요 정보와 함께 텍스트메시지, 이메일, 폰북 등과 같은 개인부가컨텐츠가 저장된다.

[67] 기기가 모바일폰이고 OS가 안드로이드이면, 1차인증고유값산출모듈(142)은 가입자식별번호(IMSI), 기기고유번호(IMEI), 모델번호, 펌웨어버전, 기저대역버전, 커널버전, 빌드번호 등을 조합하여 1차인증고유값을 생성한다. 기기가 모바일폰이고 OS가 iOS이면 가입자식별번호(IMSI), 기기고유번호(IMEI), iOS버전, ICCID(Integrated Circuit Card IDentifier) 등을 조합하여 1차인증고유값을 생성한다. 기기가 모바일폰이고 OS가 윈도우즈모바일이면, 가입자식별번호(IMSI), 기기고유번호(IMEI) 등을 조합하여 1차인증고유값을 생성한다. 물론, 2차인증고유값산출모듈(143)도 상술한 바와 같이 기기로부터 하드웨어 정보 및/또는 소프트웨어 정보를 추출하여 2차인증고유값을 생성할 수도 있다.

[68] 기기 등록시, 1차인증고유값산출모듈(142)은 저장부에 등록용 1차인증고유값 파일이 기록되는 시간(생성 시간)을 기반으로 등록용 1차인증고유값을 산출하고 해쉬값으로 변환하여 파일로 저장하는데, 이때 저장부에는 해당 등록용 1차인증고유값 파일의 생성 시간이 기록된다. 이 후, 접근 시도 기기 검증시, 1차인증고유값산출모듈(142)은 저장부에 기록된 파일 생성 시간 정보를

기반으로 검증용 1차인증고유값을 산출하고 등록용 1차인증고유값과 비교한다. 이로 인해, 등록용 1차인증고유값 파일이 접근 시도 기기에 복사되어 사용되는 것을 방지할 수 있다. 즉, 등록 기기에 저장된 등록용 1차인증고유값 파일을 접근 시도 기기에 복사하게 되면, 그 등록용 1차인증고유값 산출시 이용된 생성 시간 정보와 접근 시도 기기의 저장부에 기록되는 생성 시간 정보가 달라지기 때문에, 접근 시도 기기 검증시 등록용 1차인증고유값과 검증용 1차인증고유값이 동일하지 않게 된다.

[69] 2차인증고유값산출모듈(143)은 정보수집모듈(141)에서 수집된 기기(110)의 하드웨어 환경 정보 중 기기 고유의 하드웨어 정보를 기반으로 2차인증고유값을 산출한다. 물론, 상술한 바와 같이 2차인증고유값산출모듈(143)은 생략 가능하며, 1차인증고유값산출모듈에서 생성된 1차인증고유값을 이용하여 2차인증(기기와 사용자인증서버간 통신을 통한 인증)을 수행할 수도 있다.

[70]

발명의 실시를 위한 형태

[71] 도 2와 도 3은 이 발명에 따른 접속 시도 기기 인증 방법을 도시한 동작 흐름도이다.

[72] 접속 시도 기기 인증 시스템(140)은, 사용자로부터 현 기기에 대한 기기 등록이 요청되면(S201), 기기의 종류 및 운영체제 종류를 파악하고(S202), 기기 종류 및 운영체제별로 수집 가능한 하드웨어 및/또는 소프트웨어 환경을 수집한다(S203). 여기서, 운영체제별로 수집 가능한 하드웨어 및/또는 소프트웨어 환경은 미리 설정해 놓을 수도 있다.

[73] 그리고, 수집된 하드웨어 및/또는 소프트웨어 환경 정보와, 생성 시간 정보 및 사용자 식별정보를 조합하여 등록용 1차인증고유값을 산출하고(S204), 그 등록용 1차인증고유값을 해쉬값으로 변환하며, 등록용 1차인증고유값 파일을 저장부에 저장한다(S205). 이때, 저장부에는 등록용 1차인증고유값 파일의 생성 시간이 기록된다. 여기서, 등록용 1차인증고유값을 산출하는데 조합되는 생성 시간 정보라 함은 등록용 1차인증고유값 파일의 생성 시간을 의미하는 바, 파일이 저장부에 기록되는 시간과 동일하도록 한다.

[74] 다음, 접속 시도 기기 인증 시스템(140)은 미리 설정해 놓은 하드웨어 및/또는 소프트웨어 환경 정보로부터 등록용 2차인증고유값을 산출하고(S206), 산출된 등록용 2차인증고유값을 사용자인증서버에게 전송한다(S207). 여기서, 단계 S206을 생략하고, 단계 S204에서 산출된 등록용 1차인증고유값을 단계 S207에서 등록용 2차인증고유값으로 설정하여 사용자인증서버에게 전송할 수도 있다. 이렇게 하여 사용자인증서버에 등록 기기의 2차인증고유값(1차인증고유값과 동일할 수도 있고, 다를 수도 있음)이 등록된다.

[75] 다음, 사용자가 임의의 기기(이하, 접속 시도 기기)를 이용하여 온라인 서비스에 접근하고자 접속 시도 기기 검증이 요청되면(S208), 접속 시도 기기

인증 시스템(140)은 접속 시도 기기의 기기 종류 및 운영체제를 파악하고(S209), 기기 종류 및 운영체제별 수집 가능한 하드웨어 및/또는 소프트웨어 환경을 수집한다(S210). 그리고, 수집된 하드웨어 및/또는 소프트웨어 환경 정보와, 저장부에 기록된 등록용 1차 인증고유값 파일의 생성 시간 정보와, 사용자 식별정보를 조합하여 검증용 1차인증고유값을 산출하고(S211), 검증용 1차인증고유값을 저장부에 저장된 등록용 1차인증고유값과 비교한다(S212).

[76] 검증용 1차인증고유값과 등록용 1차인증고유값이 동일하면(S213), 검증용 2차인증고유값을 산출하고(S214), 검증용 2차인증고유값을 사용자인증서버에게 전송한다(S215). 단계 S214를 생략하고, 단계 S211에서 산출된 검증용 1차인증고유값을 단계 S215에서 검증용 2차인증고유값으로 설정하여 사용자인증서버에게 전송할 수도 있다. 한편, 단계 S213에서 검증용 1차인증고유값과 등록용 1차인증고유값이 동일하지 않으면(S213), 접속 시도 기기의 온라인 서비스를 차단하고(S216), 현재 접속 시도 기기를 신규 기기로 인식하며 신규 기기에 대한 기기 등록을 안내한다(S217).

[77] 단계 S215 후 사용자인증서버로부터 2차인증이 성공하면(S218), 이 접속 시도 기기는 1차인증 및 2차인증을 모두 성공한 것이기 때문에 이 접속 시도 기기에 온라인 서비스를 제공한다(S219). 그러나, 사용자인증서버로부터의 2차인증이 실패하면(S218), 접속 시도 기기의 온라인 서비스를 차단하고(S216), 현재 접속 시도 기기를 신규 기기로 인식하며 인식된 신규 기기에 대한 기기 등록을 안내한다(S217).

[78]

청구범위

[청구항 1] 사용자인증서버와 접속된 기기에 설치되는 접속 시도 기기 인증 시스템에 있어서,
상기 기기에 설치된 하드웨어 환경과 소프트웨어 환경 중 적어도 둘 이상의 환경 정보를 수집하는 정보수집모듈과,
사용자의 기기 등록 요청시 상기 기기에 대한 기기 등록 절차를 수행하고, 사용자가 온라인 서비스 요청시 상기 기기에 대한 접속 시도 기기 검증 절차를 수행하는 인증제어모듈과,
상기 기기의 종류 및 상기 기기에 설치된 운영체제의 종류에 따라 상기 정보수집모듈에서 수집된 적어도 둘 이상의 환경 정보를 조합하여 1차인증고유값을 산출하고 상기 인증제어모듈에게 제공하는 1차인증고유값산출모듈을 포함하고,
상기 인증제어모듈은 상기 기기 등록 절차시 상기 1차인증고유값산출모듈로부터 입력되는 등록용 1차인증고유값을 상기 기기의 저장부에 저장하고 상기 사용자인증서버에게 전송하여 저장되도록 하며, 상기 접속 시도 기기 검증 절차시 상기 1차인증고유값산출모듈로부터 입력되는 검증용 1차인증고유값을 상기 등록용 1차인증고유값과 비교하여 검증하고 상기 사용자인증서버에게 전송하여 검증되도록 하는 것을 특징으로 하는 접속 시도 기기 인증 시스템.

[청구항 2] 제 1 항에 있어서, 상기 정보수집모듈에서 수집된 적어도 둘 이상의 환경 정보를 조합하여 2차인증고유값을 산출하고 상기 인증제어모듈에게 제공하는 2차인증고유값산출모듈을 더 포함하고,
상기 인증제어모듈은 상기 기기 등록 절차시 상기 등록용 1차인증고유값 대신 상기 2차인증고유값산출모듈로부터 입력되는 등록용 2차인증고유값을 상기 사용자인증서버에게 전송하여 저장되도록 하며, 상기 접속 시도 기기 검증 절차시 상기 검증용 1차인증고유값 대신 상기 2차인증고유값산출모듈로부터 입력되는 검증용 2차인증고유값을 상기 사용자인증서버에게 전송하여 검증되도록 하는 것을 특징으로 하는 접속 시도 기기 인증 시스템.

[청구항 3] 제 1 항에 있어서, 상기 1차인증고유값산출모듈은 상기 등록용 1차인증고유값이 상기 저장부에 파일로 생성되는 생성 시간을 더 조합하여 상기 등록용 1차인증고유값을 산출하고 상기 저장부에 상기 생성 시간을 기록하며, 상기 저장부에 기록된 상기 생성 시간을 더 조합하여 상기 검증용 1차인증고유값을 산출하는 것을

특징으로 하는 접속 시도 기기 인증 시스템.

[청구항 4] 제 2 항에 있어서, 상기 인증제어모듈은 상기 등록용 2차인증고유값 및 검증용 2차인증고유값과 함께 고유식별명을 더 전송하는 것을 특징으로 하는 접속 시도 기기 인증 시스템.

[청구항 5] 제 1 항에 있어서, 상기 1차인증고유값산출모듈은 상기 기기가 컴퓨터이고 상기 기기에 설치된 운영체제가 윈도우즈 운영체제(Windows OS)이면, OS 설치 아이디를 포함하는 환경 정보를 조합하여 1차인증고유값을 산출하는 것을 특징으로 하는 접속 시도 기기 인증 시스템.

[청구항 6] 제 1 항에 있어서, 상기 1차인증고유값산출모듈은 상기 기기가 컴퓨터이고 상기 기기에 설치된 운영체제가 리눅스 운영체제(Linux OS)이면, 하드디스크 모델 이름(HDD model name)을 포함하는 환경 정보를 조합하여 1차인증고유값을 산출하는 것을 특징으로 하는 접속 시도 기기 인증 시스템.

[청구항 7] 제 1 항에 있어서, 상기 1차인증고유값산출모듈은 상기 기기가 컴퓨터이고 상기 기기에 설치된 운영체제가 맥 운영체제(Mac OS)이면, 하드웨어 일련번호를 포함하는 환경 정보를 조합하여 1차인증고유값을 산출하는 것을 특징으로 하는 접속 시도 기기 인증 시스템.

[청구항 8] 제 1 항에 있어서, 상기 1차인증고유값산출모듈은 상기 기기가 모바일폰이면, 가입자식별번호(IMSI), 기기고유번호(IMEI)를 포함하는 환경 정보를 조합하여 1차인증고유값을 산출하는 것을 특징으로 하는 접속 시도 기기 인증 시스템.

[청구항 9] 사용자인증서버와 접속된 기기에 설치되는 접속 시도 기기 인증 시스템의 접속 시도 기기 인증 방법에 있어서,

상기 기기에 대한 접속 시도 기기 검증이 요청되면, 상기 접속 시도 기기 인증 시스템이 상기 접속 시도 기기의 기기 종류 및 운영체제를 파악하는 제1단계와,

상기 접속 시도 기기 인증 시스템이 상기 접속 시도 기기의 기기 종류 및 운영체제별로 수집 가능한 하드웨어와 소프트웨어 환경 정보 중 적어도 둘 이상의 환경 정보를 수집하는 제2단계와,

상기 접속 시도 기기 인증 시스템이 상기 접속 시도 기기로부터 적어도 둘 이상의 환경 정보를 조합하여 검증용 1차인증고유값을 산출하는 제3단계와,

상기 접속 시도 기기 인증 시스템이 상기 검증용 1차 인증고유값과 상기 접속 시도 기기의 저장부에 저장된 등록용 1차인증고유값을 비교하는 제4단계와,

상기 제4단계의 비교결과 상기 검증용 1차인증고유값과 상기

등록용 1차인증고유값이 동일하면, 상기 접속 시도 기기 인증 시스템이 검증용 1차인증고유값을 상기 사용자인증서버에게 전송하는 제5단계와,
상기 접속 시도 기기 인증 시스템이 상기 제5단계 후 상기 사용자인증서버로부터의 인증이 성공되면 상기 접속 시도 기기에 온라인 서비스가 제공되도록 하는 제6단계와,
상기 접속 시도 기기 인증 시스템이 상기 제4단계의 비교결과 상기 검증용 1차인증고유값과 상기 등록용 1차인증고유값이 동일하지 않거나, 상기 제5단계 후 상기 사용자인증서버로부터의 인증이 실패되면, 상기 접속 시도 기기에 온라인 서비스가 차단되도록 하는 제7단계를 포함한 것을 특징으로 하는 접속 시도 기기 인증 방법.

[청구항 10] 제 9 항에 있어서, 상기 제5단계는, 상기 제4단계의 비교결과 상기 검증용 1차인증고유값과 상기 등록용 1차인증고유값이 동일하면, 상기 접속 시도 기기 인증 시스템이 검증용 2차인증고유값을 산출하고, 상기 검증용 1차인증고유값 대신 상기 검증용 2차인증고유값을 상기 사용자인증서버에게 전송하는 것을 특징으로 하는 접속 시도 기기 인증 방법.

[청구항 11] 제 9 항에 있어서, 상기 제7단계는 상기 접속 시도 기기 인증 시스템이 상기 접속 시도 기기에 대한 기기 등록을 안내하는 것을 특징으로 하는 접속 시도 기기 인증 방법.

[청구항 12] 제 9 항에 있어서, 상기 제1단계 전 상기 기기에 대한 등록 기기 등록이 요청되면, 상기 접속 시도 기기 인증 시스템이 상기 등록 기기의 기기 종류 및 운영체제를 파악하는 제8단계와,
상기 접속 시도 기기 인증 시스템이 상기 등록 기기의 운영체제별로 수집 가능한 하드웨어와 소프트웨어 환경 정보 중 적어도 둘 이상의 환경 정보를 수집하는 제9단계와,
상기 접속 시도 기기 인증 시스템이 상기 등록 기기의 기기 종류 및 운영체제에 따라 수집된 적어도 둘 이상의 환경 정보를 조합하여 상기 등록용 1차인증고유값을 산출하는 제10단계와,
상기 접속 시도 기기 인증 시스템이 상기 등록용 1차 인증고유값을 상기 저장부에 저장하는 제11단계와,
상기 접속 시도 기기 인증 시스템이 상기 등록용 1차인증고유값을 상기 사용자인증서버에게 전송하는 제12단계를 더 포함한 것을 특징으로 하는 접속 시도 기기 인증 방법.

[청구항 13] 제 12 항에 있어서, 상기 제12단계는, 상기 접속 시도 기기 인증 시스템이 등록용 2차인증고유값을 산출하여 상기 등록용 1차인증고유값 대신 상기 등록용 2차인증고유값을 상기

사용자인증서버에게 전송하는 것을 특징으로 하는 접속 시도 기기 인증 방법.

[청구항 14] 제 12 항에 있어서, 상기 제10단계는 상기 등록용 1차인증고유값이 상기 저장부에 파일로 생성되는 생성 시간을 더 조합하여 상기 등록용 1차인증고유값을 산출하고 상기 제11단계는 상기 저장부에 상기 생성 시간을 기록하며, 상기 제3단계는 상기 저장부에 기록된 상기 생성 시간을 더 조합하여 상기 검증용 1차인증고유값을 산출하는 것을 특징으로 하는 접속 시도 기기 인증 방법.

[청구항 15] 제 12 항 또는 제 13 항에 있어서, 상기 제5단계와 상기 제12단계는, 상기 사용자인증서버에게 상기 기기의 고유식별명을 더 전송하는 것을 특징으로 하는 접속 시도 기기 인증 방법.

[청구항 16] 제 12 항에 있어서, 상기 제3단계와 제10단계는 상기 기기가 컴퓨터이고 상기 기기에 설치된 운영체제가 윈도우즈 운영체제(Windows OS)이면, OS 설치 아이디를 포함하는 환경 정보를 조합하여 1차인증고유값을 산출하는 것을 특징으로 하는 접속 시도 기기 인증 방법.

[청구항 17] 제 12 항에 있어서, 상기 제3단계와 제10단계는 상기 기기가 컴퓨터이고 상기 기기에 설치된 운영체제가 리눅스 운영체제(Linux OS)이면, 하드디스크 모델 이름(HDD model name)을 포함하는 환경 정보를 조합하여 1차인증고유값을 산출하는 것을 특징으로 하는 접속 시도 기기 인증 방법.

[청구항 18] 제 12 항에 있어서, 상기 제3단계와 제10단계는 상기 기기가 컴퓨터이고 상기 기기에 설치된 운영체제가 맥 운영체제(Mac OS)이면, 하드웨어 일련번호를 포함하는 환경 정보를 조합하여 1차인증고유값을 산출하는 것을 특징으로 하는 접속 시도 기기 인증 방법.

[청구항 19] 제 12 항에 있어서, 상기 제3단계와 제10단계는 상기 기기가 모바일폰이면, 가입자식별번호(IMSI), 기기고유번호(IMEI)를 포함하는 환경 정보를 조합하여 1차인증고유값을 산출하는 것을 특징으로 하는 접속 시도 기기 인증 방법.

[청구항 20] 사용자인증서버와 접속된 기기에 접속 시도 기기 인증 방법을 실행하기 위한 컴퓨터로 읽을 수 있는 기록매체에 있어서, 상기 접속 시도 기기 인증 방법은, 상기 기기에 대한 접속 시도 기기 검증이 요청되면, 상기 접속 시도 기기 인증 시스템이 상기 접속 시도 기기의 기기 종류 및 운영체제를 파악하는 제1단계와, 상기 접속 시도 기기 인증 시스템이 상기 접속 시도 기기의 기기 종류 및 운영체제별로 수집 가능한 하드웨어와 소프트웨어 환경

정보 중 적어도 둘 이상의 환경 정보를 수집하는 제2단계와,
상기 접속 시도 기기 인증 시스템이 상기 접속 시도 기기로부터 적어도 둘 이상의 환경 정보를 조합하여 검증용 1차인증고유값을 산출하는 제3단계와,
상기 접속 시도 기기 인증 시스템이 상기 검증용 1차 인증고유값과 상기 접속 시도 기기의 저장부에 저장된 등록용 1차인증고유값을 비교하는 제4단계와,
상기 제4단계의 비교결과 상기 검증용 1차인증고유값과 상기 등록용 1차인증고유값이 동일하면, 상기 접속 시도 기기 인증 시스템이 검증용 1차인증고유값을 상기 사용자인증서버에게 전송하는 제5단계와,
상기 접속 시도 기기 인증 시스템이 상기 제5단계 후 상기 사용자인증서버로부터의 인증이 성공되면 상기 접속 시도 기기에 온라인 서비스가 제공되도록 하는 제6단계와,
상기 접속 시도 기기 인증 시스템이 상기 제4단계의 비교결과 상기 검증용 1차인증고유값과 상기 등록용 1차인증고유값이 동일하지 않거나, 상기 제5단계 후 상기 사용자인증서버로부터의 인증이 실패되면, 상기 접속 시도 기기에 온라인 서비스가 차단되도록 하는 제7단계를 포함한 것을 특징으로 하는 컴퓨터로 읽을 수 있는 기록매체.

[청구항 21] 제 20 항에 있어서, 상기 제1단계 전 상기 기기에 대한 등록 기기 등록이 요청되면, 상기 접속 시도 기기 인증 시스템이 상기 등록 기기의 기기 종류 및 운영체제를 파악하는 제8단계와,
상기 접속 시도 기기 인증 시스템이 상기 등록 기기의 운영체제별로 수집 가능한 하드웨어와 소프트웨어 환경 정보 중 적어도 둘 이상의 환경 정보를 수집하는 제9단계와,
상기 접속 시도 기기 인증 시스템이 상기 등록 기기의 기기 종류 및 운영체제에 따라 수집된 적어도 둘 이상의 환경 정보를 조합하여 상기 등록용 1차인증고유값을 산출하는 제10단계와,
상기 접속 시도 기기 인증 시스템이 상기 등록용 1차 인증고유값을 상기 저장부에 저장하는 제11단계와,
상기 접속 시도 기기 인증 시스템이 상기 등록용 1차인증고유값을 상기 사용자인증서버에게 전송하는 제12단계를 더 포함한 것을 특징으로 하는 컴퓨터로 읽을 수 있는 기록매체.

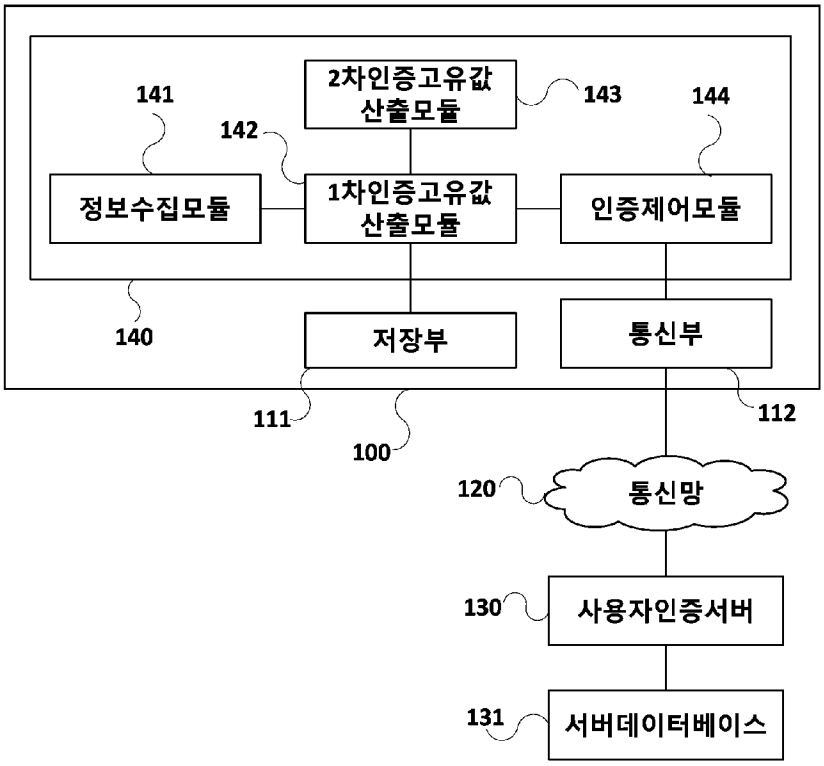
[청구항 22] 제 21 항에 있어서, 상기 제10단계는 상기 등록용 1차인증고유값이 상기 저장부에 파일로 생성되는 생성 시간을 더 조합하여 상기 등록용 1차인증고유값을 산출하고 상기 제11단계는 상기 저장부에 상기 생성 시간을 기록하며, 상기 제3단계는 상기

저장부에 기록된 상기 생성 시간을 더 조합하여 상기 검증용 1차인증고유값을 산출하는 것을 특징으로 하는 컴퓨터로 읽을 수 있는 기록매체.

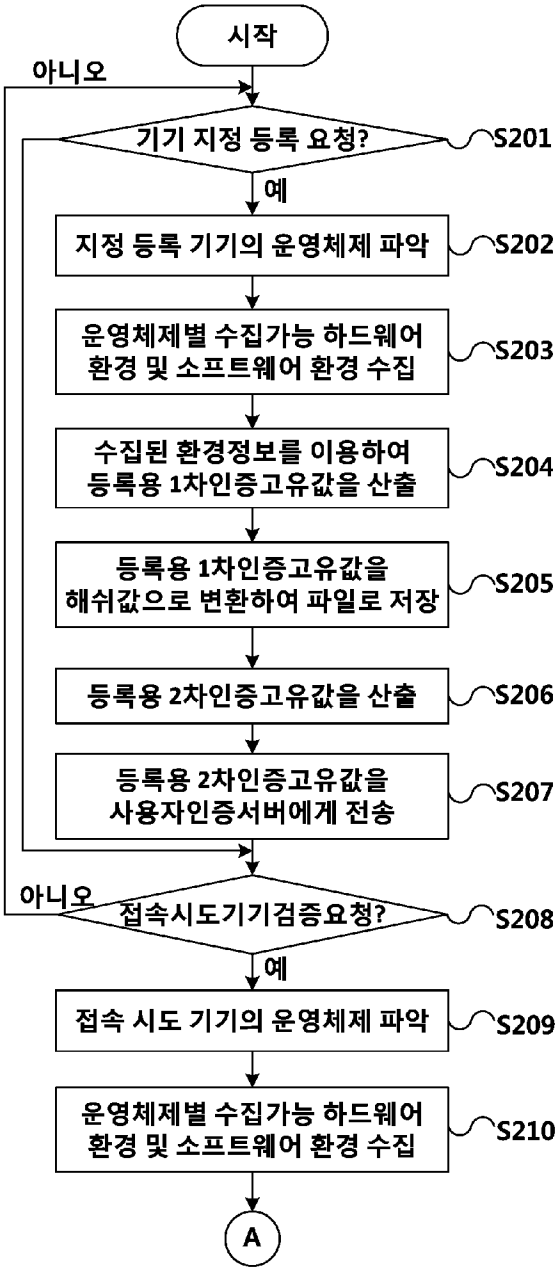
[청구항 23] 제 20 항에 있어서, 상기 제5단계는, 상기 제4단계의 비교결과 상기 검증용 1차인증고유값과 상기 등록용 1차인증고유값이 동일하면, 상기 접속 시도 기기 인증 시스템이 검증용 2차인증고유값을 산출하고, 상기 검증용 1차인증고유값 대신 상기 검증용 2차인증고유값을 상기 사용자인증서버에게 전송하는 것을 특징으로 하는 컴퓨터로 읽을 수 있는 기록매체.

[청구항 24] 제 21 항에 있어서, 상기 제12단계는, 상기 접속 시도 기기 인증 시스템이 등록용 2차인증고유값을 산출하여 상기 등록용 1차인증고유값 대신 상기 등록용 2차인증고유값을 상기 사용자인증서버에게 전송하는 것을 특징으로 하는 컴퓨터로 읽을 수 있는 기록매체.

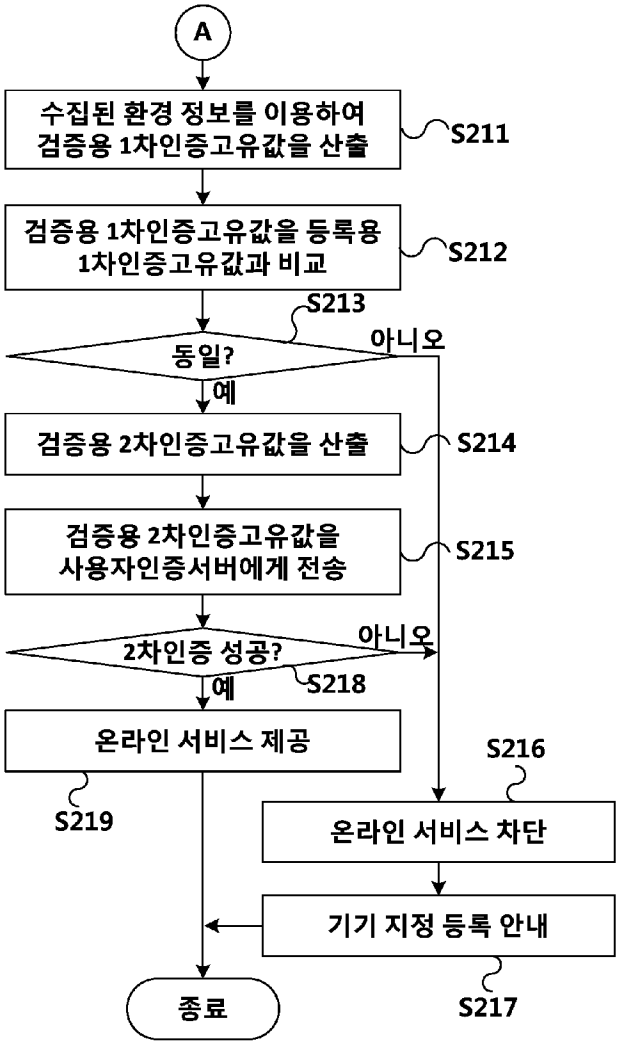
[Fig. 1]


141
142
2차인증고유값 산출모듈
143
144
정보수집모듈
1차인증고유값 산출모듈
인증제어모듈
140
저장부
통신부
111
100
112
120
통신망
130
사용자인증서버
131
서버데이터베이스

[Fig. 2]


시작
아니오
기기 지정 등록 요청?
S201
예
지정 등록 기기의 운영체제 파악
S202
운영체제별 수집가능 하드웨어 환경 및 소프트웨어 환경 수집
S203
수집된 환경정보를 이용하여 등록용 1차인증고유값을 산출
S204
등록용 1차인증고유값을 해쉬값으로 변환하여 파일로 저장
S205
등록용 2차인증고유값을 산출
S206
등록용 2차인증고유값을 사용자인증서버에게 전송
S207
아니오
접속시도기기검증요청?
S208
예
접속 시도 기기의 운영체제 파악
S209
운영체제별 수집가능 하드웨어 환경 및 소프트웨어 환경 수집
S210
A

[Fig. 3]


A
수집된 환경 정보를 이용하여 검증용 1차인증고유값을 산출
S211
검증용 1차인증고유값을 등록용 1차인증고유값과 비교
S212
S213
동일?
아니오
예
검증용 2차인증고유값을 산출
S214
검증용 2차인증고유값을 사용자인증서버에게 전송
S215
2차인증 성공?
아니오
S218
예
온라인 서비스 제공
S219
S216
온라인 서비스 차단
기기 지정 등록 안내
S217
종료