(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2016 년 7 월 21 일 (21.07.2016)

WIPO | PCT

(10) 국제공개번호
WO 2016/114566 A1

(51) 국제특허분류:
H04L 12/24 (2006.01) *H04L 29/06* (2006.01)
H04L 12/26 (2006.01)

(21) 국제출원번호: PCT/KR2016/000318

(22) 국제출원일: 2016 년 1 월 13 일 (13.01.2016)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2015-0006030 2015 년 1 월 13 일 (13.01.2015) KR
10-2016-0003719 2016 년 1 월 12 일 (12.01.2016) KR

(71) 출원인: **부산대학교 산학협력단 (PUSAN NATIONAL UNIVERSITY INDUSTRY-UNIVERSITY COOPERATION FOUNDATION)** [KR/KR]; 46241 부산시 금정구 부산대학로 63 번길 2 (장전동, 부산대학교), Busan (KR).

(72) 발명자: **최윤호 (CHOI, Yoon Ho)**; 46242 부산시 금정구 금샘로 262, 210 동 1002 호 (구서동, 쌍용예가 2 단지), Busan (KR). **김호원 (KIM, Ho Won)**; 49497 부산시 사하구 다대낙조 2 길 100, 218 동 1603 호 (다대동, 롯데캐슬몰운대아파트), Busan (KR).

(74) 대리인: **특허법인 무한 (MUHANN PATENT & LAW FIRM)**; 06044 서울시 강남구 학동로 3 길 9, 5 층 (논현동, 명림빌딩), Seoul (KR).

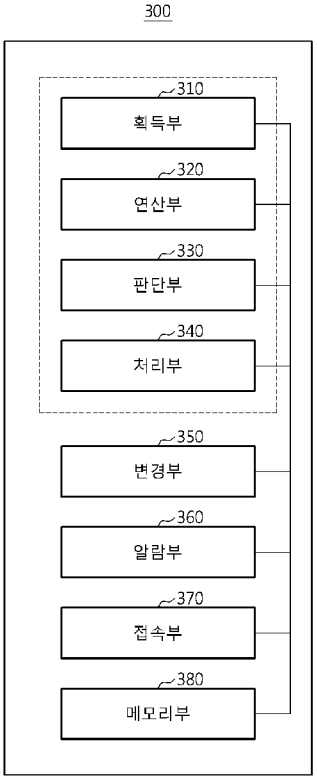
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LU, LY, MA, 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,

[다음 쪽 계속]

(54) **Title**: DUPLICATE LOGIN DETECTION METHOD AND DUPLICATE LOGIN DETECTION SYSTEM

(54) **발명의 명칭** : 이중 로그인 탐지 방법 및 이중 로그인 탐지 시스템



310 ... Acquisition unit
320 ... Calculation unit
330 ... Determination unit
340 ... Processing unit
350 ... Change unit
360 ... Alarm unit
370 ... Connection unit
380 ... Memory unit

(57) **Abstract**: Disclosed are a duplicate login detection method and a duplicate login detection system. A duplicate login detection method according to an embodiment of the present invention comprises the steps of: acquiring login information on a client terminal logging-in to a server to be managed, in response to an occurrence of a request for monitoring a duplicate login; comparing the login information with previous login information on the client terminal collected by the server to be managed, and calculating a velocity value relating to the logging-in; determining a duplicate login of the client terminal as the calculated velocity value exceeds a predetermined threshold value; and performing a logout process for the client terminal having been determined as the duplicate login.

(57) **요약서**: 이중 로그인 탐지 방법 및 이중 로그인 탐지 시스템이 개시된다. 본 발명의 일실시예에 따른 이중 로그인 탐지 방법은, 이중 로그인 모니터링 요청이 발생 함에 연동하여, 관리대상서버에 로그인하는 클라이언트 단말에 관한 로그인 정보를 획득하는 단계와, 상기 로그인 정보를, 상기 관리대상서버로부터 수집된 상기 클라이언트 단말에 관한 이전 로그인 정보와 비교하여, 상기 로그인과 관련한 속도값을 연산하는 단계와, 상기 연산한 속도값이, 지정된 임계치를 초과 함에 따라, 상기 클라이언트 단말에 대해 이중 로그인으로 판단하는 단계, 및 상기 이중 로그인으로 판단된 클라이언트 단말을, 로그아웃 처리하는 단계를 포함한다.

WO 2016/114566 A1

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))

— 청구범위 보정 기한 만료 전의 공개이며, 보정서를 접수하는 경우 그에 관하여 별도 공개함 (규칙 48.2(h))

명세서

발명의 명칭: 이중 로그인 탐지 방법 및 이중 로그인 탐지 시스템

기술분야

[1] 본 발명은 모바일 기기에서 동작하는 제어 어플리케이션을 통해, 관리대상서버에 로그인하는 클라이언트 단말의 로그인 상태를 용이하게 모니터링 할 수 있도록 하기 위한 기술에 관한 것입니다.

[2] 특히, 본 발명은 관리대상서버에 접속하는 클라이언트 단말의 이중 로그인(Duplicated Login) 여부를, 이전 로그인 정보와의 비교를 통해 간단하게 탐지하고, 해당 클라이언트 단말을 로그아웃 처리하여 이중 로그인을 자동 차단할 수 있는 이중 로그인 탐지 방법 및 이중 로그인 탐지 시스템에 관한 것이다.

배경기술

[3] 인가된 사용자를 확인하고 사용자의 안전한 통신을 보장하기 위한 원격 인증 프로토콜이 제안된 이래로, 인터넷과 같은 공개된 네트워크 통신 환경에서 클라이언트가 서버에 접속하여 자신의 아이디를 입증하고 계정에 접근하기 위한 방안으로 패스워드 인증이 널리 사용되고 있다. 하지만, 패스워드 인증이 훔친 검증자 공격, 중간자 공격, 재전송 공격 및 피싱 공격에 취약한 문제점이 발견되면서 이들 취약점을 해결하여 안정성과 효율성을 강화하기 위한 연구가 이루어져 왔다.

[4] 훔친 검증자 공격은 서버에 저장된 사용자 계정 정보(아이디와 패스워드)를 훔쳐서 로그인하는 것으로, 이를 막기 위해 서버에 사용자 계정 정보를 해쉬(hash)하거나 암호화하여 저장하는 방안이 제안되고 있다.

[5] 중간자 공격은 공개된 네트워크 통신 환경에서 평문으로 전송되는 사용자 계정 정보를 제3자가 가로채어 재전송하는 것으로, 이를 막기 위해 훔친 검증자 공격과 마찬가지로, 전송되는 사용자 계정 정보를 해쉬하거나 암호화하는 방안이 사용될 수 있다.

[6] 하지만, 사용자 계정 정보를 해쉬 값으로 변환하거나 암호화하는 경우, 재전송 공격에 취약할 수 있다. 재전송 공격은 공개된 네트워크 통신 환경에서 평문이나 암호화하여 전송되는 인가된 사용자의 계정 정보를 캡쳐하여 이를 다시 재전송하여 서버에 로그인하는 것으로, 이를 막기 위해 OTP(one time password)와 OTP를 활용한 S/KEY 패스워드, 동적 패스워드(dynamic password) 등이 제안되고 있다.

[7] 하지만, OTP 및 이를 활용한 스킴(scheme)은 가짜 웹 사이트를 만들어 사용자의 계정 정보를 획득하는 피싱 공격을 방어하기 어려울 수 있다. 피싱 공격을 막기 위해 그리드 기법(GRID analysis)을 사용하여 동적 패스워드를 발생하는 DPASS가 제안되고 있으나, OPT를 만들기 위한 복잡한 연산을

수행해야 하므로 사용자 친화적이지 않다는 단점을 가질 수 있다.

[8] 최근 이러한 문제점을 해결하기 위하여 안전 토큰(security token), 모바일 폰, SMS 메시지 등의 수단을 통해, 서버가 OTP를 만들어 사용자에게 배포하는 방안이 제안되었다. 하지만, 이 경우에도, 인가된 사용자의 정상적인 로그인 후 혹은 훔친 로그인 정보를 사용해 공격자가 로그인한 경우, 인가된 사용자의 계정 정보가 노출되거나 변경되는 경우를 막을 수는 없다.

[9] 또한, 종래에는 사용자가 각각의 웹 사이트에 모두 접속해야만 각 웹 사이트에 대한 사용자 로그인 상태 제어가 가능하였다. 로그인 상태를 제어하기 위한 설정 메뉴에 접근 시, 일부의 웹 사이트에서는 별도의 인증 과정을 요구하므로 사용이 불편하다는 단점이 있다. 또한 일부의 웹 사이트에서는 최초 로그인 상태에서 설정 메뉴에 접근할 수 있으나, 인증 정보 도용 시 사용자 계정 정보가 유출될 수 있는 문제점이 있다.

[10] 사용자의 로그인 상태 제어 절차의 경우, 설정 메뉴에서는 로그인 상태, 로그아웃 기능, 로그인 기록 등 사용자의 계정 정보를 관리하고 보호하기 위한 기능들이 존재한다.

[11] 도 1은 종래의 일실시예에 따른 사용자 로그인 상태 제어 절차를 도시한 도면이다.

[12] 도 1에는 현재 웹 사이트에서 인가된 사용자의 로그인 상태를 제어하기 위한 방법이 도시되어 있다. 도 1을 참조하여, 사용자 로그인 상태 제어 기능을 단계별로 요약하면, 우선, 사용자는 모바일 기기에 설치된 웹 브라우저(Web Browser)를 통해 웹 사이트에 접속 후, 인가된 접속 아이디(ID)와 패스워드를 입력하고 로그인을 시도한다(단계 (1)). 이때, 로그인 요청 정보가 해당 웹 사이트 운영 서버에 전달되고, 로그인 제어 서비스에 의해 사용자는 해당 웹 사이트에 로그인한다. 로그인에 성공한 사용자의 로그인 관련 정보는, 인증 서버의 데이터베이스에 저장된다(단계 (2)). 사용자는 웹 사이트에 로그인한 상태에서 단계 (1)을 반복하여 로그인 상태 제어를 위한 설정 메뉴에 접근한다. 사용자는 자신의 접속 아이디와 패스워드를 이용해 웹 사이트에 로그인한 세션을 확인하고, 해당 세션에 대해 로그아웃 또는 접속한 IP 주소를 차단한다(단계 (3)).

[13] 하지만 이러한 로그인 상태 제어 절차의 경우, 사용자가 해당 웹 사이트를 자주 접속하여 자신의 로그인 상태를 수시로 확인해야 하며 여러 웹 사이트에 대한 로그인 상태 제어를 위해서는 해당 웹 사이트를 모두 방문해야 한다는 문제점이 있다.

[14] 또한, 종래의 대부분의 웹 사이트에서는 프록시(proxy) 및 IP 스푸핑(spoofing)을 통해 IP 주소를 변경하여 접속하는 이중 로그인 세션을 차단하는 것이 용이하지 않다는 문제점이 있다.

[15] 일부의 웹 사이트에서 이중 로그인 세션에 대한 차단 기능이 제공되기도 하지만, 단지 로그인 컨트롤 서비스(login control service) 모듈을 통해, 현재 로그인한 기기의 IP 주소, 접속 국가, 접속 시간 등을 알려주는 것에 한정될 뿐,

사용자가 해당 웹 사이트에 접속해서 이중 로그인 세션을 판단하여 직접 차단을 수행해야 하는 불편함이 있다.

발명의 상세한 설명

기술적 과제

[16] 본 발명은 상술한 문제점을 해결하기 위한 것으로, 관리대상서버에 의해 운영되는 웹 사이트에 대한 클라이언트 단말의 로그인 상태(예컨대, 로그인 발생, 로그아웃, 이중 로그인 여부, 로그인 세션의 정상 종료 여부 등)를, 사용자가 해당 웹 사이트에서 운영되는 로그인 상태 제어를 위한 설정 메뉴에 일일이 접근할 필요 없이, 휴대가 용이한 모바일 기기에서 동작하는 제어 어플리케이션(제어 앱)을 통해 용이하게 모니터링 할 수 있도록 하는 것을 목적으로 한다.

[17] 특히, 본 발명의 실시예는 이중 로그인 모니터링 요청이 발생 함에 따라, 관리대상서버에 로그인하는 클라이언트 단말에 대한 로그인 정보(로그인 아이디, IP 주소, 로그인 시간, 국가코드 등)를, 이전 로그인 정보와 비교하여 산출한 상기 로그인에 대한 속도값에 기초하여, 상기 클라이언트 단말에 대해 이중 로그인 여부를 간단하게 판단할 수 있도록 하는 것을 목적으로 한다.

[18] 또한, 본 발명의 실시예는 이중 로그인으로 판단되는 클라이언트 단말에 대한 로그인 정보를, 제어 어플리케이션을 통해 화면 상에 표시하여, 사용자에게 이중 로그인에 대해 용이하게 알람할 수 있도록 하는 것을 목적으로 한다.

[19] 또한, 본 발명의 실시예는 이중 로그인으로 판단되는 클라이언트 단말을 로그아웃 처리하여, 관리대상서버에 대한 클라이언트 단말의 이중 로그인을 자동 차단 함으로써, 부정한 로그인에 따른 피해를 최소화 하는 것을 목적으로 한다.

[20] 또한, 본 발명의 실시예는 클라이언트 단말이 관리대상서버에 로그인 함에 따라 생성되는 로그인 정보가, 선정된 블록 조건(예, 로그인 지역, 로그인 시간)을 만족하는 경우, 해당 클라이언트 단말을 자동으로 로그아웃 처리(차단)할 수 있도록 하는 것을 목적으로 한다.

[21] 또한, 본 발명의 실시예는 관리대상서버에서 로그인 세션이 정상적으로 종료되지 않은 클라이언트 단말을 모니터링하여, 제어 어플리케이션을 통해 사용자에게 알람하고, 사용자의 선택(예컨대, 로그인 차단)에 따라 해당 클라이언트 단말을 로그아웃 처리하여, 개인 정보 유출에 따른 피해를 방지하는 것을 목적으로 한다.

[22] 또한, 본 발명의 실시예는 로그인 모니터링 요청이 발생 함에 연동하여 관리대상서버에 로그인하는 클라이언트 단말에 대한 로그인 정보를 제어 어플리케이션을 통해 화면 상에 표시하여, 관리대상서버에 로그인하는 클라이언트 단말을 손쉽게 모니터링할 수 있게 하고, 사용자의 선택에 따라 부정 로그인으로 의심되는 클라이언트 단말을 로그아웃 처리할 수 있도록 하는 것을

목적으로 한다.

과제 해결 수단

[23] 본 발명의 일실시예에 따른 이중 로그인 탐지 방법은, 이중 로그인 모니터링 요청이 발생 함에 연동하여, 관리대상서버에 로그인하는 클라이언트 단말에 관한 로그인 정보를 획득하는 단계와, 상기 로그인 정보를, 상기 관리대상서버로부터 수집된 상기 클라이언트 단말에 관한 이전 로그인 정보와 비교하여, 상기 로그인과 관련한 속도값을 연산하는 단계와, 상기 연산한 속도값이, 지정된 임계치를 초과 함에 따라, 상기 클라이언트 단말에 대해 이중 로그인으로 판단하는 단계, 및 상기 이중 로그인으로 판단된 클라이언트 단말을, 로그아웃 처리하는 단계를 포함한다.

[24] 또한, 본 발명의 일실시예에 따른 이중 로그인 탐지 시스템은, 이중 로그인 모니터링 요청이 발생 함에 연동하여, 관리대상서버에 로그인하는 클라이언트 단말에 관한 로그인 정보를 획득하는 획득부와, 상기 로그인 정보를, 상기 관리대상서버로부터 수집된 상기 클라이언트 단말에 관한 이전 로그인 정보와 비교하여, 상기 로그인과 관련한 속도값을 연산하는 연산부와, 상기 연산한 속도값이, 지정된 임계치를 초과 함에 따라, 상기 클라이언트 단말에 대해 이중 로그인으로 판단하는 판단부, 및 상기 이중 로그인으로 판단된 클라이언트 단말을, 로그아웃 처리하는 처리부를 포함한다.

발명의 효과

[25] 본 발명의 일실시예에 따르면, 관리대상서버에 의해 운영되는 웹 사이트에 대한 클라이언트 단말의 로그인 상태(예컨대, 로그인 발생, 로그아웃, 이중 로그인 여부, 로그인 세션의 정상 종료 여부 등)를, 사용자가 해당 웹 사이트에서 운영되는 로그인 상태 제어를 위한 설정 메뉴에 일일이 접근할 필요 없이, 휴대가 용이한 모바일 기기에서 동작하는 제어 어플리케이션(제어 앱)을 통해 용이하게 모니터링 가능하게 할 수 있다.

[26] 또한, 본 발명의 일실시예에 따르면, 이중 로그인 모니터링 요청이 발생 함에 따라, 관리대상서버에 로그인하는 클라이언트 단말에 대한 로그인 정보(로그인 아이디, IP 주소, 로그인 시간, 국가코드 등)를, 이전 로그인 정보와 비교하여 산출한 상기 로그인에 대한 속도값에 기초하여, 상기 클라이언트 단말에 대해 이중 로그인 여부를 간단하게 판단하여 탐지할 수 있다.

[27] 또한, 본 발명의 일실시예에 따르면, 이중 로그인으로 판단되는 클라이언트 단말에 대한 로그인 정보를, 제어 어플리케이션을 통해 화면 상에 표시하여, 사용자에게 이중 로그인에 대해 용이하게 알람할 수 있다.

[28] 또한, 본 발명의 실시예는 이중 로그인으로 판단되는 클라이언트 단말을 로그아웃 처리하여, 관리대상서버에 대한 클라이언트 단말의 이중 로그인을 자동 차단 함으로써, 부정한 로그인에 따른 피해를 최소화 할 수 있다.

[29] 또한, 본 발명의 실시예는 클라이언트 단말이 관리대상서버에 로그인 함에

따라 생성되는 로그인 정보가, 선정된 블록 조건(예, 로그인 지역, 로그인 시간)을 만족하는 경우, 해당 클라이언트 단말을 자동으로 로그아웃 처리(차단)할 수 있다.

[30] 또한, 본 발명의 실시예는 관리대상서버에서 로그인 세션이 정상적으로 종료되지 않은 클라이언트 단말을 모니터링하여, 제어 어플리케이션을 통해 사용자에게 알람하고, 사용자의 선택(예컨대, 로그인 차단)에 따라 해당 클라이언트 단말을 로그아웃 처리하여, 개인 정보 유출에 따른 피해를 방지할 수 있다.

[31] 또한, 본 발명의 실시예는 로그인 모니터링 요청이 발생 함에 연동하여 관리대상서버에 로그인하는 클라이언트 단말에 대한 로그인 정보를 제어 어플리케이션을 통해 화면 상에 표시하여, 관리대상서버에 로그인하는 클라이언트 단말을 손쉽게 모니터링할 수 있게 하고, 사용자의 선택에 따라 부정 로그인으로 의심되는 클라이언트 단말을 로그아웃 처리할 수 있다.

도면의 간단한 설명

[32] 도 1은 종래의 일실시예에 따른 사용자 로그인 상태 제어 절차를 도시한 도면이다.

[33] 도 2는 본 발명의 일실시예에 따른 이중 로그인 탐지 시스템과, 클라이언트 단말에 의한 이중 로그인을 탐지하려는 관리대상서버 간의 전체적인 연결 관계를 도시한 도면이다.

[34] 도 3은 본 발명의 일실시예에 따른 이중 로그인 탐지 시스템의 내부 구성을 도시한 블록도이다.

[35] 도 4는 본 발명의 일실시예에 따른 이중 로그인 탐지 시스템에서, 관리대상서버에 로그인하는 클라이언트 단말에 대해 이중 로그인으로 판단하는 과정을 설명하기 위한 도면이다.

[36] 도 5는 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템의 내부 구성을 도시한 블록도이다.

[37] 도 6은 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템에서, 로그인 상태 제어 절차의 일례를 도시한 도면이다.

[38] 도 7은 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템에서, 제어 어플리케이션에서의 사용자 로그인 절차의 일례를 도시한 도면이다.

[39] 도 8은 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템에서, 사용자 로그인 시 관리대상서버와 제어 어플리케이션 간의 상호 동작의 일례를 도시한 도면이다.

[40] 도 9는 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템에서, 사용자 로그아웃 시 관리대상서버와 제어 어플리케이션 간의 상호 동작의 일례를 도시한 도면이다.

[41] 도 10은 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템에서, 사용자

로그아웃 시 관리대상서버와 제어 어플리케이션 간의 상호 동작의 다른 일례를 도시한 도면이다.

[42] 도 11은 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템에서, 로그인 차단 절차의 일례를 도시한 도면이다.

[43] 도 12는 본 발명의 일실시예에 따른 이중 로그인 탐지 방법의 순서를 도시한 흐름도이다.

발명의 실시를 위한 최선의 형태

[44] 이하, 첨부된 도면들을 참조하여 본 발명의 일실시예에 따른 응용프로그램 업데이트 장치 및 방법에 대해 상세히 설명한다. 그러나, 본 발명이 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[45] 도 2는 본 발명의 일실시예에 따른 이중 로그인 탐지 시스템과, 클라이언트 단말에 의한 이중 로그인을 탐지하려는 관리대상서버 간의 전체적인 연결 관계를 도시한 도면이다.

[46] 도 2를 참조하면, 본 발명의 일실시예에 따른 이중 로그인 탐지 시스템(200)은, 사용자의 모바일 기기(예컨대, 스마트 폰, 태블릿 피시 등)에 설치된 제어 어플리케이션에 의해 구현될 수 있다.

[47] 즉, 이중 로그인 탐지 시스템(200)은, 상기 제어 어플리케이션을 통해, 사전에 등록된 적어도 하나의 관리대상서버에 로그인하는 클라이언트 단말을 모니터링하여, 해당 로그인이 이중 로그인인지를 탐지하고, 이중 로그인으로 탐지되는 클라이언트 단말을 자동으로 로그아웃 처리할 수 있다.

[48] 일례로, 이중 로그인 탐지 시스템(200)은, 관리대상서버에 로그인 함에 따라 생성되는 클라이언트 단말에 대한 로그인 정보를 획득하고, 상기 클라이언트 단말에 관한 이전 로그인 정보를 상기 관리대상서버로부터 수집하고, 상기 로그인 정보와 상기 이전 로그인 정보와의 비교를 통해, 상기 로그인과 관련한 속도값을 연산하고, 상기 연산한 속도값이 지정된 임계치를 초과하는 경우 클라이언트 단말을 이중 로그인으로 판단할 수 있다.

[49] 여기서, 상기 이전 로그인 정보는, 상기 로그인 정보 내 로그인 아이디(예, 'sky01')와 동일한 로그인 아이디를 포함하면서, 현재 로그인을 기준으로 가장 최근에 정상 로그인으로 판단된 로그인 정보일 수 있다.

[50] 즉, 이중 로그인 탐지 시스템(200)은 동일한 로그인 아이디를 사용하여 시간 차를 두고 발생하는 관리대상서버(예컨대, 웹 사이트 'www.sky.com'의 운영 서버)로의 로그인에 대해, 상기 로그인과 관련한 속도값에 기초하여, 동일한 사용자에 의한 정상 로그인인지, 또는 다른 사용자에 의한 부정 로그인(이중 로그인)인지를 판단할 수 있다.

[51] 이중 로그인 탐지 시스템(200)은 예컨대, 위도와 경도 값을 이용한 절대 거리(이격 거리)와 로그인 시간의 차를 이용하여 연산한 속도값에 따라, 이중

로그인을 탐지 및 자동 차단할 수 있다.

[52] 구체적으로, 이중 로그인 탐지 시스템(200)은 클라이언트 단말이 관리대상서버에 로그인을 시도하면, 현재 로그인한 제1 지역과 이전에 로그인한 제2 지역의 위도좌표값과 경도좌표값을 비교하여 제1, 제2 지역 간 거리 차를 계산하고, 상기 거리 차와 로그인 시간 차를 이용하여 이전 로그인에 대한 현재 로그인의 속도값을 연산할 수 있다. 이중 로그인 탐지 시스템(200)은 상기 속도값이 지정된 속도보다 빠른 경우, 현재 로그인에 대해 이중 로그인으로 탐지하고, 클라이언트 단말을 자동으로 로그아웃 할 수 있다.

[53] 한편, '부산역'으로부터 '일본 키타큐슈 공항'까지의 거리 차는 221.04km이고, '부산역'으로부터 '서울 남산'까지의 거리 차는 322.45km로서, 거리 상으로는 '부산역'에서 '일본 키타큐슈 공항'이 더 가깝지만, 현실적으로 '부산역'에서 '서울 남산'으로 이동하는 것이 더 빠를 수 있다. 즉, 거리가 가까워도 국가가 상이하면 실제로 사용자가 이동하기 어려우므로 이중 로그인일 가능성이 높다. 따라서, 단순히 제1, 제2 지역 간 거리 차와 시간 차에 의한 속도값 비교를 통해서는 정확한 결과를 획득하기 어려울 수 있다.

[54] 따라서, 이중 로그인 탐지 시스템(200)은 단순히 제1, 제2 지역 간 거리 차와 시간 차에 의한 속도값 비교를 통해서는 정확한 결과를 획득하기 어려울 수 있기 때문에, 로그인 정보와 이전 로그인 정보 내 국가코드를 추가적으로 비교하여, 이중 로그인 탐지의 정밀도를 높일 수 있다.

[55] 이중 로그인 탐지 시스템(200)은 현재 로그인한 제1 지역과 이전에 로그인한 제2 지역의 국가코드가 같은 경우와, 국가코드가 상이한 경우에, 연산된 속도값과 비교할 속도, 임계치를 다르게 지정할 수 있다. 일례로, 이중 로그인 탐지 시스템(200)은 제1 지역과 제2 지역의 국가코드가 상이한 경우, 국가코드가 같은 경우에 상기 연산된 속도값과 비교할 임계치(속도)를, 거리 차에 비례하여 증가시켜 변경할 수 있다.

[56] 다시 말해, 이중 로그인 탐지 시스템(200)은 두 지역 간 국가가 상이한 경우 임계치를 증가시키는 조정을 통해, 거리가 가까워도 국가가 상이하면 이중 로그인으로 판단할 가능성을 높여, 이중 로그인 탐지의 정밀도를 높일 수 있다.

[57] 도 3은 본 발명의 일실시예에 따른 이중 로그인 탐지 시스템의 내부 구성을 도시한 블록도이다.

[58] 도 3을 참조하면, 본 발명의 일실시예에 따른 이중 로그인 탐지 시스템(300)은, 획득부(310), 연산부(320), 판단부(330) 및 처리부(340)를 포함하여 구성할 수 있다. 또한, 실시예에 따라, 이중 로그인 탐지 시스템(300)은 변경부(350), 알람부(360), 접속부(370) 및 메모리부(380)를 각각 추가하여 구성할 수 있다.

[59] 획득부(310)는 이중 로그인 모니터링 요청이 발생 함에 연동하여, 관리대상서버에 로그인하는 클라이언트 단말에 관한 로그인 정보를 획득한다.

[60] 본 발명의 일실시예에 따른 이중 로그인 탐지 시스템(300)은 모바일 기기에 설치된 제어 어플리케이션을 통해 구현될 수 있다. 모바일 기기에서 구동되는

제어 어플리케이션에서, '이중 로그인 탐지'에 관한 메뉴가 선택되면, 이중 로그인 모니터링 요청이 발생할 수 있다.

[61] 획득부(310)는 상기 이중 로그인 모니터링 요청의 발생에 따라, 관리대상서버에 대한 접속 정보(예, 관리대상서버에 의해 운영되는 웹 사이트의 주소)가 메모리부(380)에 등록되어 있는 적어도 하나의 관리대상서버를 식별하고, 식별한 관리대상서버에 로그인하는 클라이언트 단말(예, 'PC', '모바일 기기' 등)에 관한 로그인 정보를, 상기 관리대상서버로부터 획득할 수 있다.

[62] 여기서, 상기 로그인 정보는 상기 관리대상서버에 로그인 함에 따라 생성되는 클라이언트 단말에 대한 IP 주소, 로그인 시간, 로그인 아이디, 세션(통신채널) 값 및 국가코드 중 적어도 하나를 포함할 수 있다.

[63] 획득부(310)는 후술하는 알람부(360)를 통해, 상기 획득한 로그인 정보를 제어 어플리케이션을 통해 화면에 표시할 수도 있다.

[64] 실시예에 따라, 이중 로그인 탐지 시스템(300)은 접속부(370)를 더 포함할 수 있다.

[65] 접속부(370)는 상기 이중 로그인 모니터링 요청의 발생에 따라, 메모리부(380)로부터 식별한 관리대상서버에 대한 접속 정보를 이용하여 상기 관리대상서버에 접속할 수 있다. 획득부(310)는 상기 접속된 관리대상서버로부터, 상기 클라이언트 단말에 대한 IP 주소, 로그인 시간, 로그인 아이디, 세션 값 및 국가코드 중 적어도 하나의 로그인 정보를 획득할 수도 있다.

[66] 이때, 접속부(370)는 일정 시간 간격(예, '5분')으로 상기 관리대상서버에 접속하여, 상기 관리대상서버와의 접속을 유지하고, 획득부(310)는 상기 관리대상서버와의 접속을 유지한 상태에서, 상기 로그인 정보를 획득할 수도 있다.

[67] 이때, 상기 관리대상서버가 복수일 경우, 접속부(370)는 상기 각 관리대상서버에 대한 접속 정보를 이용하여, 상기 각각의 관리대상서버에 교대로 접속하고, 획득부(310)는 상기 각 관리대상서버에 로그인하는 클라이언트 단말에 관한 로그인 정보를 획득할 수도 있다. 예를 들어, 접속부(370)는 관리대상서버(A, B, C)가 세 개일 경우, 각 관리대상서버의 접속 정보를 식별하여, 관리대상서버 A에 접속하고, 5분 경과 후에 관리대상서버 B에 접속하고, 5분 경과 후에 관리대상서버 C에 접속하는 과정을 반복하여 수행할 수 있다.

[68] 연산부(320)는 상기 로그인 정보를, 상기 관리대상서버로부터 수집된 상기 클라이언트 단말에 관한 이전 로그인 정보와 비교하여, 상기 로그인과 관련한 속도값을 연산한다.

[69] 여기서, 상기 이전 로그인 정보는, 상기 로그인 정보 내 로그인 아이디(예, 'sky01')와 동일한 로그인 아이디를 포함하면서, 현재 로그인을 기준으로 가장 최근에 정상 로그인으로 판단된 로그인 정보일 수 있다.

[70] 일례로, 연산부(320)는 상기 이전 로그인 정보에 의해 식별되는 제1 지역 및

상기 로그인 정보에 의해 식별되는 제2 지역 간 거리 차를 구하고, 상기 이전 로그인 정보 내 로그인 시간과, 상기 로그인 정보 내 로그인 시간을 이용하여, 시간 차를 구하고, 상기 거리 차 및 상기 시간 차를 이용하여, 상기 클라이언트 단말의 로그인과 관련한 속도값을 연산할 수 있다.

[71] 이때, 연산부(320)는 상기 이전 로그인 정보 내 IP 주소에 의해 식별되는 제1 지역에 대한 위도좌표값 및 경도좌표값과, 상기 로그인 정보 내 IP 주소에 의해 식별되는 제2 지역에 대한 위도좌표값 및 경도좌표값을 추출하고, 상기 추출한 위도좌표값과 경도좌표값을 이용하여, 상기 제1 지역 및 제2 지역 간 거리 차를 구할 수 있다.

[72] 예를 들어, 도 4의 (i)에 도시된 로그인 정보와, 도 4의 (ii)에 도시된 이전 로그인 정보 A를 참조하면, 연산부(320)는 상기 이전 로그인 정보 A 내 IP 주소 '175.176.139.138'에 의해 식별되는 제1 지역 '서울 남산'에 대한 위도 및 경도로 이루어진 좌표값 '(37.558, 126.985)'을 추출하고, 상기 로그인 정보 내 IP 주소 '123.99.113.81'에 의해 식별되는 제2 지역 '부산역'에 대한 위도 및 경도로 이루어진 좌표값 '(35.114, 129.041)'을 추출하고, 추출한 좌표값을 이용하여, 제1 지역과 제2 지역 간 거리 차 예컨대, '322.45km'를 구할 수 있다.

[73] 또한, 연산부(320)는 상기 이전 로그인 정보 A 내 로그인 시간 '2015-09-16 13:24:09'와, 상기 로그인 정보 내 로그인 시간 '2015-09-16 10:20:01' 간의 시간 차 '3시간 4분 8초'를 구할 수 있다.

[74] 즉, 연산부(320)는 상기 거리 차를 상기 시간 차로 나누는 연산을 통해, 제2 지역 '부산역'에서 로그인하는 클라이언트 단말의 속도값 '104.7 km/h'을 연산할 수 있다.

[75] 일례로, 연산부(320)는 다양한 Open API(예컨대, Whois Open API, Geolocation Open API, IP-API 등)을 선택적으로 사용하여, 상기 이전 로그인 정보 A 내 IP 주소로부터 이전에 로그인한 제1 지역 '서울 남산'에 대한 위도좌표값과 경도좌표값 '(37.558, 126.985)'을 추출할 수 있다. 마찬가지로, 연산부(320)는 3가지 기법(Whois, Geolocation, IP-API)을 선택적으로 사용하여, 상기 로그인 정보 내 IP 주소로부터 현재 로그인한 제2 지역 '부산역'에 대한 위도좌표값과 경도좌표값 '(35.114, 129.041)'을 추출할 수 있다.

[76] 여기서, Whois Open API를 이용할 경우 위치 탐지의 정확도는 매우 높은 장점이 있으나, 구글 맵스 API와 연동해야 위도좌표값과 경도좌표값을 얻을 수 있고, 해외 IP의 경우에는 위도좌표값과, 경도좌표값을 제외한 국가 코드만 출력해주므로 해외 IP로 접속하는 경우에는 탐지가 어렵다는 단점을 가질 수 있다.

[77] 또한, Geolocation API를 이용할 경우 비교적 높은 정확도를 가지지만 웹 사이트에 접속할 때마다 사용자에게 위치 정보 제공 여부를 확인해야 하므로 사용자가 불편을 느낄 수 있다.

[78] 마지막으로, IP-API를 이용할 경우 Whois Open API와 Geolocation API보다

정확도는 떨어지지만, 사용자에게 위치 정보 제공 여부를 확인할 필요가 없고, 위도좌표값 및 경도좌표값을 바로 얻을 수 있으며, 해외 IP의 위도좌표값 및 경도좌표값도 얻을 수 있다는 장점을 가질 수 있다.

[79] 따라서, 연산부(320)는 이러한 여러 가지 Open API가 가지는 장단점을 고려하여 Open API를 선택적으로 사용하여, IP 주소로부터 위도좌표값과, 경도좌표값을 용이하게 추출할 수 있다.

[80] 판단부(330)는 상기 연산한 속도값이, 지정된 임계치를 초과 함에 따라, 상기 클라이언트 단말에 대해 이중 로그인으로 판단한다.

[81] 즉, 판단부(330)는 동일한 로그인 아이디를 사용하여 시간 차를 두고 발생하는 관리대상서버(예컨대, 웹 사이트 'www.sky.com'의 운영 서버)로의 로그인에 대해, 상기 로그인과 관련한 속도값에 기초하여, 동일한 사용자에 의한 정상 로그인인지, 또는 다른 사용자에 의한 부정 로그인(이중 로그인)인지를 판단할 수 있다.

[82] 일례로, 판단부(330)는 상기 속도값이 지정된 임계치(예컨대, '100km/h') 보다 크면(속도가 빠르면), 현재 제2 지역에서 관리대상서버에 로그인하는 클라이언트 단말을 이중 로그인으로 판단하고, 상기 속도값이 지정된 임계치보다 작으면(속도가 느리면), 현재 제2 지역에서 관리대상서버에 로그인하는 클라이언트 단말을 정상 로그인으로 판단할 수 있다.

[83] 여기서, 상기 임계치는 이전 로그인 정보와 로그인 정보 내 국가코드가 동일한 경우에 이중 로그인을 판단하기 위한 비교 속도(예컨대, '100km/h')로 지정될 수 있다.

[84] 예를 들어, 판단부(330)는 상기 속도값 '104.7 km/h'이 임계치 '100km/h'를 초과함에 따라, 제2 지역에서 현재 로그인한 클라이언트 단말에 대해 이중 로그인으로 판단할 수 있다. 즉, 판단부(330)는 상기 속도값이 지정된 속도보다 빠른 경우, 현재 로그인에 대해 이중 로그인으로 탐지할 수 있다.

[85] 또한, 판단부(330)는 로그인과 관련해 연산한 속도값 '98.7 km/h'이 상기 임계치 '100km/h'를 초과하지 않을 경우, 상기 클라이언트 단말에 대해 정상 로그인으로 판단할 수 있다. 즉, 판단부(330)는 상기 속도값이 지정된 속도보다 느린 경우, 현재 로그인에 대해 정상 로그인으로 판단할 수 있다.

[86] 이 경우, 판단부(330)는 상기 관리대상서버에서, 상기 클라이언트 단말에 관한 이전 로그인 정보를, 상기 로그인 정보로 갱신하도록 함으로써, 이후의 이중 로그인 판단 시 이전 로그인 정보로서 사용되도록 할 수 있다.

[87] 이와 같이, 판단부(330)는 동일한 로그인 아이디를 사용하여 시간 차를 두고 관리대상서버에 로그인하는 클라이언트 단말에 대해, 로그인 정보와 이전 로그인 정보와의 비교를 통해 산출한 로그인에 관한 속도값에 기초하여 이중 로그인 여부를 용이하게 탐지할 수 있게 된다.

[88] 실시예에 따라, 판단부(330)는 상기 이전 로그인 정보 내 로그인 시간과, 상기 로그인 정보 내 로그인 시간 간의 시간 차가, 정해진 시간격(예컨대, '1초')

이내이면, 상기 속도값에 무관하게, 상기 클라이언트 단말에 대해 이중 로그인으로 판단할 수도 있다.

[89] 즉, 판단부(330)는 동일한 로그인 아이디를 사용하여 로그인하는 클라이언트 단말에 대한 로그인 정보와 이전 로그인 정보에서, 로그인 시간에 따른 시간 차가 거의 없어 상기 속도값을 산출하지 못하는 경우, 현재 로그인 한 클라이언트 단말에 대해 이중 로그인으로 판단할 수 있다.

[90] 처리부(340)는 상기 이중 로그인으로 판단된 클라이언트 단말을, 로그아웃 처리한다.

[91] 일례로, 처리부(340)는 상기 클라이언트 단말이 이중 로그인으로 판단 됨에 따라, 상기 관리대상서버에 이중 로그인에 관한 메시지를 전송하여, 상기 관리대상서버로부터, 상기 로그인 정보가 삭제되도록 하여, 상기 로그아웃 처리할 수 있다.

[92] 또한, 처리부(340)는 상기 로그인 정보로부터 식별되는 세션 값을 이용하여, 상기 클라이언트 단말과 상기 관리대상서버와의 연결을 해제하여, 상기 로그아웃 처리할 수도 있다.

[93] 이와 같이, 처리부(340)는 이중 로그인으로 판단되는 클라이언트 단말을 로그아웃 처리하여, 관리대상서버에 대한 클라이언트 단말의 이중 로그인을 자동 차단 함으로써, 부정한 로그인에 따른 피해를 최소화 할 수 있다.

[94] 또한, 실시예에 따라, 처리부(340)는 상기 클라이언트 단말에 부여된 등급을 확인하고, 상기 확인된 등급에 기초하여, 상기 클라이언트 단말에게 로그인 허용시간을 할당하고, 상기 로그인 허용시간이 도과하면, 상기 속도값이 상기 임계치를 초과하는지의 여부와 무관하게, 상기 클라이언트 단말을 로그아웃 처리할 수도 있다.

[95] 예를 들어, 처리부(340)는 클라이언트 단말에 부여된 등급이 'A등급'으로 가장 높은 등급으로 확인되면, 상기 속도값이 지정된 임계치를 초과하여 이중 로그인으로 판단되는 경우에도, 상기 등급에 상응하는 로그인 허용시간 '1시간' 동안에 한해, 클라이언트 단말이 관리대상서버에 로그인 하도록 허용할 수 있다. 처리부(340)는 로그인 허용시간 '1시간'이 경과하면, 클라이언트 단말을 자동으로 로그아웃 처리하여, 클라이언트 단말을 등급 별로 지정된 시간 동안에 한해 로그인 하도록 할 수 있다.

[96] 한편, '부산역'으로부터 '일본 키타큐슈 공항'까지의 거리 차는 221.04km이고, '부산역'으로부터 '서울 남산'까지의 거리 차는 322.45km로서, 거리 상으로는 '부산역'에서 '일본 키타큐슈 공항'이 더 가깝지만, 현실적으로 '부산역'에서 '서울 남산'으로 이동하는 것이 더 빠를 수 있다. 즉, 거리가 가까워도 국가가 상이하면 실제로 사용자가 이동하기 어려우므로 이중 로그인일 가능성이 높다. 따라서, 단순히 제1, 제2 지역 간 거리 차와 시간 차에 의한 속도값 비교를 통해서는 정확한 결과를 획득하기 어려울 수 있다.

[97] 이에 따라, 이중 로그인 탐지 시스템(300)은 로그인 정보와 이전 로그인 정보 내

국가코드를 추가적으로 비교하고, 국가코드가 상이한 경우에, 연산된 속도값과 비교할 속도, 즉 임계치를 다르게 지정하여 이중 로그인 탐지의 정밀도를 높이기 위해, 변경부(350)를 더 포함할 수 있다.

[98] 변경부(350)는 상기 이전 로그인 정보 내 국가코드와, 상기 로그인 정보 내 국가코드를 비교하고, 상기 비교 결과, 국가코드가 상이하면, 상기 이전 로그인 정보에 의해 식별되는 제1 지역 및 상기 로그인 정보에 의해 식별되는 제2 지역 간의 거리 차에 비례하여, 상기 임계치를 변경한다.

[99] 일례로, 변경부(350)는 제1 지역과 제2 지역의 국가코드가 상이한 경우, 국가코드가 같은 경우에 연산된 속도값과 비교하는 임계치를, 제1 지역과 제2 지역 간 거리 차에 비례하여, 증가시켜 변경할 수 있다.

[100] 다시 말해, 변경부(350)는 두 지역 간 국가가 상이한 경우, 임계치를 증가시키는 조정을 통해, 거리가 가까워도 국가가 상이하면 이중 로그인으로 판단할 가능성을 높일 수 있고, 이에 따라 이중 로그인 탐지의 정밀도를 높일 수 있다.

[101] 예를 들어, 도 4의 (i)에 도시된 로그인 정보와, 도 4의 (iii)에 도시된 이전 로그인 정보 B를 참조하면, 연산부(320)는 상기 이전 로그인 정보 B 내 IP 주소 '220.108.196.157'에 의해 식별되는 제1 지역 '일본 키타큐슈 공항'에 대한 위도 및 경도로 이루어진 좌표값 '(33.888, 130.873)'을 추출하고, 상기 로그인 정보 내 IP 주소 '123.99.113.81'에 의해 식별되는 제2 지역 '부산역'에 대한 위도 및 경도로 이루어진 좌표값 '(35.114, 129.041)'을 추출하고, 추출한 좌표값을 이용하여, 제1 지역과 제2 지역 간 거리 차 예컨대, '221.04km'를 구할 수 있다.

[102] 또한, 연산부(320)는 상기 이전 로그인 정보 B 내 로그인 시간 '2015-09-16 11:15:06'과, 상기 로그인 정보 내 로그인 시간 '2015-09-16 10:20:01' 간의 시간 차 '55분 5초'를 구할 수 있다.

[103] 즉, 연산부(320)는 상기 거리 차를 상기 시간 차로 나누는 연산을 통해, 제2 지역 '부산역'에서 로그인하는 클라이언트 단말의 속도값 '240.3 km/h'을 연산할 수 있다.

[104] 이때, 변경부(350)는 이전 로그인 정보 B 내 국가코드 '1010'과, 로그인 정보 내 국가코드 '1111'을 비교하고, 국가코드가 상이하므로, 국가코드가 같은 경우에 연산된 속도값과 비교하기 위해 지정된 임계치 '100km/h'를, 제1 지역과 제2 지역 간 거리 차 '221.04km'에 비례하여, 2.21배 증가시켜 변경할 수 있다.

[105] 판단부(330)는 상기 속도값 '240.3 km/h'이, 변경된 임계치 '221km/h' 보다 크므로, 현재 제2 지역 '부산역'에서 관리대상서버에 로그인하는 클라이언트 단말을 이중 로그인으로 판단할 수 있다. 처리부(340)는 상기 로그인 정보로부터 식별되는 세션 값을 이용하여, 이중 로그인으로 판단된 클라이언트 단말과 관리대상서버와의 연결을 해제하여, 자동으로 로그아웃 처리할 수 있다.

[106] 또한, 실시예에 따라, 변경부(350)는 상기 비교 결과, 국가코드가 동일하면, 상기 임계치를 유지하되, 상기 거리 차가, 정해진 거리간격을 넘음에 따라 상기 거리 차에 비례하여, 상기 임계치를 감소시켜 변경할 수도 있다.

[107] 예를 들어, 국가코드가 제1, 제2 지역 모두 '1111'로 동일한 경우, 지정된 임계치 '100 km/h'를 유지하되, 제1, 제2 지역 간 거리 차 '322.45km'가 정해진 거리간격(예컨대, 현재 로그인 하는 제2 지역 '부산역'이 속한 도시 '부산'의 반경 '100km')을 넘으면, 상기 거리 차 '322.45km'에 비례하여 상기 임계치를 3.22배 감소시켜 변경할 수도 있다. 이 경우, 판단부(330)는 상기 속도값 '240.3 km/h'이, 변경된 임계치 '31.05km/h'보다 작으므로, 정상 로그인으로 판단할 수 있다.

[108] 실시예에 따라, 이중 로그인 탐지 시스템(300)은 알람부(360)를 더 포함할 수 있다.

[109] 알람부(360)는 상기 클라이언트 단말이 이중 로그인으로 판단 됨에 따라, 상기 획득한 로그인 정보 내, 상기 클라이언트 단말의 IP 주소, 로그인 시간 및 국가코드 중 적어도 하나를, 화면 상에 표시하여, 사용자에게 이중 로그인에 대해 알람한다.

[110] 즉, 본 발명에 따르면, 이중 로그인으로 판단되는 클라이언트 단말에 대한 로그인 정보를, 제어 어플리케이션을 통해 화면 상에 표시하여, 관리대상서버로의 이중 로그인을 사용자에게 용이하게 알람할 수 있다.

[111] 이와 같이, 본 발명의 일실시예에 따르면, 관리대상서버에 의해 운영되는 웹 사이트에 대한 클라이언트 단말의 로그인 상태(예컨대, 로그인 발생, 로그아웃, 이중 로그인 여부, 로그인 세션의 정상 종료 여부 등)를, 사용자가 해당 웹 사이트에서 운영되는 로그인 상태 제어를 위한 설정 메뉴에 일일이 접근할 필요 없이, 휴대가 용이한 모바일 기기에서 동작하는 제어 어플리케이션(제어 앱)을 통해 용이하게 모니터링 할 수 있도록 할 수 있다.

[112] 또한, 본 발명의 일실시예에 따르면, 이중 로그인 모니터링 요청이 발생 함에 따라, 관리대상서버에 로그인하는 클라이언트 단말에 대한 로그인 정보(로그인 아이디, IP 주소, 로그인 시간, 국가코드 등)를, 이전 로그인 정보와 비교하여 산출한 상기 로그인에 대한 속도값에 기초하여, 상기 클라이언트 단말에 대해 이중 로그인 여부를 간단하게 판단하여 탐지할 수 있도록 할 수 있다.

[113] 또한, 본 발명의 실시예는 이중 로그인으로 판단되는 클라이언트 단말을 로그아웃 처리하여, 관리대상서버에 대한 클라이언트 단말의 이중 로그인을 자동 차단 함으로써, 부정한 로그인에 따른 피해를 최소화 할 수 있다.

[114] 도 4는 본 발명의 일실시예에 따른 이중 로그인 탐지 시스템에서, 관리대상서버에 로그인하는 클라이언트 단말에 대해 이중 로그인으로 판단하는 과정을 설명하기 위한 도면이다.

[115] 도 4를 참조하면, 본 발명의 일실시예에 따른 이중 로그인 탐지 시스템은, 도 4의 (i)에 도시된 로그인 정보와, 도 4의 (ii)에 도시된 이전 로그인 정보 A를 비교하여, 클라이언트 단말이 관리대상서버에 로그인하는 속도값 '104.7 km/h'을 연산할 수 있다.

[116] 구체적으로, 이중 로그인 탐지 시스템은 상기 이전 로그인 정보 A 내 IP 주소 '175.176.139.138'에 의해 식별되는 제1 지역 '서울 남산'에 대한 위도 및 경도로

이루어진 좌표값 '(37.558, 126.985)'을 추출하고, 상기 로그인 정보 내 IP 주소 '123.99.113.81'에 의해 식별되는 제2 지역 '부산역'에 대한 위도 및 경도로 이루어진 좌표값 '(35.114, 129.041)'을 추출하고, 추출한 좌표값을 이용하여, 제1 지역과 제2 지역 간 거리 차 예컨대, '322.45km'를 구할 수 있다.

[117] 이중 로그인 탐지 시스템은 상기 이전 로그인 정보 A 내 로그인 시간 '2015-09-16 13:24:09'와, 상기 로그인 정보 내 로그인 시간 '2015-09-16 10:20:01' 간의 시간 차 '3시간 4분 8초'를 구하고, 상기 거리 차를 상기 시간 차로 나누는 연산을 통해, 제2 지역 '부산역'에서 로그인하는 클라이언트 단말의 속도값 '104.7 km/h'을 연산할 수 있다.

[118] 이중 로그인 탐지 시스템은 상기 속도값 '104.7 km/h'이 임계치 '100km/h'를 초과함에 따라, 제2 지역에서 현재 로그인한 클라이언트 단말에 대해 이중 로그인으로 판단하고, 해당 클라이언트 단말을 자동으로 로그아웃 처리할 수 있다.

[119] 또한, 이중 로그인 탐지 시스템은, 도 4의 (ⅰ)에 도시된 로그인 정보와, 도 4의 (ⅲ)에 도시된 이전 로그인 정보 B를 비교하여, 클라이언트 단말이 관리대상서버에 로그인하는 속도값 '240.3 km/h'을 연산할 수 있다.

[120] 구체적으로, 이중 로그인 탐지 시스템은 상기 이전 로그인 정보 B 내 IP 주소 '220.108.196.157'에 의해 식별되는 제1 지역 '일본 키타큐슈 공항'에 대한 위도 및 경도로 이루어진 좌표값 '(33.888, 130.873)'을 추출하고, 상기 로그인 정보 내 IP 주소 '123.99.113.81'에 의해 식별되는 제2 지역 '부산역'에 대한 위도 및 경도로 이루어진 좌표값 '(35.114, 129.041)'을 추출하고, 추출한 좌표값을 이용하여, 제1 지역과 제2 지역 간 거리 차 예컨대, '221.04km'를 구할 수 있다.

[121] 이중 로그인 탐지 시스템은 상기 이전 로그인 정보 B 내 로그인 시간 '2015-09-16 11:15:06'과, 상기 로그인 정보 내 로그인 시간 '2015-09-16 10:20:01' 간의 시간 차 '55분 5초'를 구하고, 상기 거리 차를 상기 시간 차로 나누는 연산을 통해, 제2 지역 '부산역'에서 로그인하는 클라이언트 단말의 속도값 '240.3 km/h'을 연산할 수 있다.

[122] 이때, 이중 로그인 탐지 시스템은 상기 이전 로그인 정보 B 내 국가코드 '1010'과, 로그인 정보 내 국가코드 '1111'을 비교하고, 국가코드가 상이하므로, 지정된 임계치 '100km/h'를, 제1 지역과 제2 지역 간 거리 차 '221.04km'에 비례하여, 2.21배 증가시켜 변경할 수 있다.

[123] 이중 로그인 탐지 시스템은 상기 속도값 '240.3 km/h'이, 변경된 임계치 '221km/h' 보다 크므로, 현재 제2 지역 '부산역'에서 관리대상서버에 로그인하는 클라이언트 단말을 이중 로그인으로 판단하고, 상기 로그인 정보로부터 식별되는 세션 값을 이용하여, 이중 로그인으로 판단된 클라이언트 단말과 관리대상서버와의 연결을 해제하여, 자동으로 로그아웃 처리할 수 있다.

[124] 도 5는 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템의 내부 구성을

도시한 블록도이다.

[125] 도 5를 참조하면, 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템(500)은 접속부(510), 획득부(520), 판단부(530) 및 처리부(540)를 포함하여 구성할 수 있다. 또한, 실시예에 따라, 이중 로그인 탐지 시스템(500)은 알람부(550), 입력부(560) 및 메모리 공간(570)을 각각 추가하여 구성할 수 있다.

[126] 접속부(510)는 로그인 모니터링 요청이 발생 함에 연동하여, 접속 정보를 이용하여 관리대상서버에 접속한다.

[127] 모바일 기기에서 제어 어플리케이션이 구동 됨에 따라 로그인 모니터링 요청이 발생할 수 있다. 접속부(510)는 상기 로그인 모니터링 요청의 발생에 따라, 메모리 공간(570)에 유지된 상기 관리대상서버에 대한 접속 아이디 및 패스워드를 포함하는 상기 접속 정보를 식별하고, 식별한 접속 정보를 관리대상서버에 전송하여 접속을 요청할 수 있다.

[128] 실시예에 따라, 이중 로그인 탐지 시스템(500)은 입력부(560)를 더 포함할 수 있다. 입력부(560)는 사용자로부터 적어도 하나의 관리대상서버와, 상기 관리대상서버에 의해 운영되는 웹 사이트로의 접속 아이디 및 패스워드를 포함하는 접속 정보를 입력 받는다. 메모리 공간(570)은 사용자에 의해 입력된 접속 아이디와 패스워드를, 관리대상서버에 연관시켜 유지할 수 있다.

[129] 예를 들어, 접속부(510)는 로그인 모니터링 요청의 발생에 연동하여, 관리대상서버 A에 의해 운영되는 웹 사이트 'www.abc.co.kr'에 대한 접속 아이디 'sky01' 및 패스워드 '****'를 메모리 공간(570)으로부터 식별하고, 식별한 접속 아이디 및 패스워드를 이용하여 관리대상서버에 접속할 수 있다.

[130] 획득부(520)는 상기 접속된 관리대상서버로부터, 클라이언트 단말이 상기 관리대상서버에 로그인 함에 따라 생성되는 로그인 정보를 획득한다. 여기서, 클라이언트 단말은 상기 접속 정보 내 접속 아이디(예, 'sky01')와 동일한 로그인 아이디(예, 'sky01')를 사용하여 관리대상서버에 로그인 한 모바일 기기와 같은 클라이언트 단말일 수 있다.

[131] 즉, 획득부(520)는 상기 접속 정보 내 접속 아이디와 일치하는 로그인 아이디로 상기 관리대상서버에 로그인하는 상기 클라이언트 단말에 대한 IP 주소(예, 210.180.65.62), 로그인 시간(예, 2014.12.31.21:10), 로그인 아이디(예, 'sky01') 및 세션 값 중 적어도 하나의 로그인 정보를 획득할 수 있다. 여기서, 상기 세션 값은 관리대상서버에 로그인 한 클라이언트 단말과 상기 관리대상서버 간의 통신 채널을 지칭하는 값일 수 있다.

[132] 획득부(520)는 상기 관리대상서버와의 접속을 유지한 상태에서, 상기 로그인 정보를 획득할 수 있다. 이를 위해, 접속부(510)는 일정 시간 간격(예, '5분')으로 상기 관리대상서버에 접속하여, 상기 관리대상서버와의 접속을 유지할 수 있다.

[133] 이때, 상기 관리대상서버가 복수일 경우, 접속부(510)는 상기 각 관리대상서버에 대한 접속 정보를 이용하여, 상기 각각의 관리대상서버에 교대로 접속할 수 있다. 예를 들어, 접속부(510)는 관리대상서버(A, B, C)가 세

개일 경우, 각 관리대상서버의 접속 정보를 식별하여, 관리대상서버 A에 접속하고, 5분 경과 후에 관리대상서버 B에 접속하고, 5분 경과 후에 관리대상서버 C에 접속하는 과정을 반복하여 수행할 수 있다.

[134] 또한, 획득부(520)는 상기 복수의 관리대상서버 중, 상기 로그인 정보를 획득하지 못한 관리대상서버로부터 로그인 관리 페이지를 제공받아, 상기 로그인 관리 페이지에서 상기 로그인 정보를 파싱(parsing)하여 획득할 수 있다.

[135] 클라이언트 단말에서 관리대상서버에 로그인 함에 따라, 관리대상서버는 상기 클라이언트 단말에 대한 로그인 정보(로그인 아이디, IP 주소, 로그인 시간, 로그인 아이디)를 포함하는 로그인 관리 페이지를 운영하여, 로그인 한 클라이언트 단말을 관리할 수 있다. 획득부(520)는 관리대상서버로부터 수신한 상기 로그인 관리 페이지로부터, 상기 클라이언트 단말에 관한 로그인 정보를 획득할 수도 있다.

[136] 실시예에 따라, 이중 로그인 탐지 시스템(500)은 알람부(550)를 더 포함할 수 있다.

[137] 알람부(550)는 상기 획득한 로그인 정보를 화면 상에 표시하여, 사용자에게 알람한다. 구체적으로, 알람부(550)는 상기 획득한 로그인 정보 내 상기 클라이언트 단말의 IP 주소, 로그인 시간 및 로그인 아이디 중 적어도 하나를 화면 상에 표시하거나, 효과음 등을 이용해 음성 출력 함으로써, 사용자에게 클라이언트 단말로부터의 관리대상서버로의 로그인 발생에 대해 알람할 수 있다.

[138] 다른 일례로, 입력부(560)는 관리대상서버를 복수 개 입력 받을 수 있으며, 클라이언트 단말의 각 관리대상서버로의 로그인을 모니터링하려는 접속 시간을 관리대상서버 각각으로 할당 받을 수 있다.

[139] 구체적으로, 입력부(560)는 사용자에 의해 복수 개의 관리대상서버(A, B, C)가 입력되는 경우, 각 관리대상서버에 대한 접속 시간을, 예컨대, 관리대상서버 A에 대한 접속 시간 '22시~6시', 관리대상서버 B에 대한 접속 시간 '0시~8시', 및 관리대상서버 C에 대한 접속 시간 '23시~9시'와 같이 할당 받을 수 있다.

[140] 알람부(550)는 상기 복수의 관리대상서버 별로 할당되는 접속 시간에, 상기 관리대상서버 각각으로 획득되는 로그인 정보를 화면 상에 표시하여, 사용자에게 알람할 수 있다. 알람부(550)는 알람하려는 로그인 정보를, 해당 관리대상서버와 연관시켜 화면 상에 표시할 수 있다.

[141] 예를 들어, 알람부(550)는 접속 시간 '22시~6시' 동안 관리대상서버 A로부터 클라이언트 단말의 로그인 발생에 따른 로그인 정보가 획득되는 경우, 상기 로그인 정보를 화면 상에 표시하여 알람할 수 있다. 또한, 알람부(550)는 '0시~8시' 동안 관리대상서버 B로부터 클라이언트 단말의 로그인 발생에 따른 로그인 정보가 획득되는 경우, 상기 로그인 정보를 화면 상에 표시하여 알람할 수 있다. 또한, 알람부(550)는 관리대상서버 C로부터 클라이언트 단말의 로그인 발생에 따른 로그인 정보가 획득되는 경우, 상기 로그인 정보를 화면 상에

표시하여 알람할 수 있다.

[142] 이와 같이, 본 발명의 일실시예에 따르면, 로그인 모니터링 요청이 발생 함에 연동하여, 접속 정보를 이용하여 관리대상서버와 접속을 유지하고, 클라이언트 단말이 상기 접속 정보를 이용하여 상기 관리대상서버에 로그인 함에 따라 생성되는 로그인 정보를, 관리대상서버로부터 획득하여 화면 상에 표시 함으로써, 사용자에게 클라이언트 단말에서의 관리대상서버로의 비정상적인 로그인 발생(또는 로그인 세션이 정상적으로 종료되지 않음)을 용이하게 알람할 수 있다.

[143] 판단부(530)는 상기 로그인 정보에 대해, 선정된 블록 조건을 만족하는지 판단한다. 처리부(540)는 블록 조건을 만족하는 경우, 상기 클라이언트 단말을 로그아웃 처리한다.

[144] 여기서, 상기 블록 조건은, 로그인을 차단하려는 지역(예를 들면, '해외 지역', '사용자의 집과 사무실 제외한 모든 지역' 등) 또는 로그인 시간(예를 들면, 심야 시간 '0시~6시' 등)이 선정될 수 있다.

[145] 일례로, 판단부(530)는 상기 로그인 정보 내 상기 클라이언트 단말의 IP 주소에 의해 식별되는 지역, 및 상기 로그인 정보 내 상기 클라이언트 단말의 로그인 시간 중 적어도 하나가, 상기 블록 조건에 포함되면, 상기 블록 조건을 만족하는 것으로 판단할 수 있다.

[146] 예를 들어, 판단부(530)는 상기 로그인 정보 내 상기 클라이언트 단말의 IP 주소 '210.180.65.62'에 의해 식별되는 지역 '강남구 논현동'이, 블록 조건 '사용자의 집과 사무실 제외한 모든 지역'에 포함되는 경우, 즉 상기 식별된 지역이 사용자의 집이나 사무실이 아닌 경우, 블록 조건을 만족하는 것으로 판단할 수 있다.

[147] 이에 따라, 처리부(540)는 상기 클라이언트 단말을 로그아웃 처리할 수 있다. 처리부(540)는 상기 로그인 정보로부터 식별되는 세션 값을 이용하여, 상기 클라이언트 단말과 상기 관리대상서버와의 연결을 해제 함으로써, 상기 클라이언트 단말을 자동으로 로그아웃 처리할 수 있다.

[148] 또한, 알람부(550)는 상기 획득한 로그인 정보 내, 상기 클라이언트 단말의 IP 주소 및 로그인 시간 중 적어도 하나를, 상기 블록 조건의 만족 여부와 함께, 화면 상에 표시하여, 사용자에게 클라이언트 단말에 의한 관리대상서버로의 비정상적인 로그인 발생 차단을 알람할 수 있다.

[149] 실시예에 따라, 처리부(540)는 상기 획득한 로그인 정보에 대해, 사용자에 의해 로그인 허용이 선택되면, 상기 클라이언트 단말의 로그인을 유지하거나, 또는 상기 로그인 허용과 관련한 상기 클라이언트 단말의 IP 주소 또는 로그인 아이디를, 상기 블록 조건으로부터 제거할 수 있다.

[150] 또한, 처리부(540)는 상기 획득한 로그인 정보에 대해, 사용자에 의해 로그인 차단이 선택되면, 상기 클라이언트 단말을 로그아웃 처리하거나, 또는 상기 로그인 차단과 관련한 상기 클라이언트 단말의 IP 주소 또는 로그인 아이디를

상기 블록 조건에 추가할 수 있다.

[151] 이와 같이, 본 발명의 일실시예에 따르면, 사용자가 항상 휴대 가능한 모바일 기기에서 동작하는 제어 어플리케이션을 사용하여, 관리대상서버(웹 사이트)에 대한 로그인 상태 정보를 관리 함으로써, 도용된 인증 수단을 통한 로그인 발생을 모니터링하여 사용자에게 알려 개인 정보 유출 사고 및 피해를 방지할 수 있다.

[152] 도 6은 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템에서, 로그인 상태 제어 절차의 일례를 도시한 도면이다.

[153] 도 6을 참조하면, 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템은, 로그인 제어 서비스를 제공하기 위한 로그인 상태 제어 어플리케이션(600) 형태로 모바일 기기에 설치되어 구현될 수 있다.

[154] 로그인 상태 제어 어플리케이션(600)은, 관리대상서버에 의해 운영되는 웹 사이트와 별도의 연결을 설정하여, 모바일 기기에서 여러 웹 사이트에 대한 클라이언트 단말의 로그인 상태를 일괄적으로 제어할 수 있다.

[155] 모바일 기기의 사용자는 로그인 상태 제어 어플리케이션(600)을 이용하여 접속 아이디 및 패스워드를 입력하고, 유무선통신(예, 소켓 통신)을 통해 웹 사이트에 로그인 한다(단계 (1)). 이때, 접속 아이디, 접속 시간, 세션 값 등이 인증 서버의 데이터베이스에 저장된다.

[156] 클라이언트 단말(미도시함)에서 상기 웹 사이트에 로그인을 시도하면, 해당 웹 사이트 운영 서버(관리대상서버)에 로그인 요청 정보가 전달되고, 로그인 제어 서비스에 따라 클라이언트 단말은 해당 웹 사이트에 로그인 한다(단계 (2)).

[157] 단계 (2)에서 로그인이 성공하면 로그인 정보는 인증 서버의 데이터베이스에 저장되고(단계 (3)), 데이터베이스에 저장된 로그인 정보는 유무선통신(소켓 통신)을 통해 모바일 기기의 로그인 상태 제어 어플리케이션(600)으로 전송된다(단계 (4)).

[158] 로그인 정보를 수신한 로그인 상태 제어 어플리케이션(600)은 해당 로그인 정보를 모바일 기기의 데이터베이스에 저장하여 해당 클라이언트 단말의 로그인 상태를 모니터링하고, 로그인 세션이 정상적으로 종료되지 않은 클라이언트 단말에 대해 로그아웃 처리하거나, 부정 로그인으로 의심되는 클라이언트 단말의 IP 주소를 블록 조건에 추가하여 해당 클라이언트 단말을 차단한다(단계 (5)).

[159] 도 7은 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템에서, 제어 어플리케이션에서의 사용자 로그인 절차의 일례를 도시한 도면이다.

[160] 도 7을 참조하면, 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템은, 로그인 제어 서비스를 제공하기 위한 제어 어플리케이션 형태로 모바일 기기에 설치되어 구현될 수 있다.

[161] 모바일 기기에서 실행되는 제어 어플리케이션에서, 사용자의 접속 정보(접속 아이디 및 패스워드)를 메모리 공간으로부터 식별하여 대표적인 유무선통신

방식인 소켓 통신을 통해 관리대상서버(웹 사이트)에 접속하는 절차가 도 7에 도시되어 있다.

[162] 이중 로그인 탐지 시스템은, 제어 어플리케이션을 통해 관리대상서버에 접속하여 사용자 로그인을 수행하고(단계 701), 연결 요청 메시지(예컨대, 'connect.msg')를 전송한다(단계 702).

[163] 관리대상서버는 소켓을 통해 데이터베이스에 질의 메시지(예컨대, 'userCountCheck.msg')를 전송하여(단계 703), 접속한 사용자 ID의 수(예컨대, '1')를 확인하고, 이후 관리대상서버에 로그인하는 사용자 ID를 관리한다.

[164] 관리대상서버는 소켓을 통해 모바일 기기에서 상기 제어 어플리케이션이 종료할 때까지 접속한 사용자 ID 수의 변경(증가 혹은 감소)을 대기하여 로그인 상태를 감지한다(단계 704).

[165] 도 8은 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템에서, 사용자 로그인 시 관리대상서버와 제어 어플리케이션 간의 상호 동작의 일례를 도시한 도면이다.

[166] 도 8을 참조하면, 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템은, 로그인 제어 서비스를 제공하기 위한 제어 어플리케이션 형태로 모바일 기기에 설치되어 구현될 수 있다.

[167] 관리대상서버는 소켓을 통해 접속한 사용자 ID의 수가 변할 때까지 대기한다(단계 801).

[168] 사용자가 브라우저를 활성화하고(단계 802), 브라우저를 통해 로그인 요청 메시지(예컨대, 'browserLogin.msg')를 관리대상서버로 전송한다(단계 803).

[169] 로그인 제어 서비스에 의해 로그인이 성공하면, 데이터베이스는 로그인 정보(로그인 아이디, IP 주소, 로그인 시간, 세션 값 등)를 등록하고, 접속한 사용자 ID 수가 증가 함에 따라 대기 중이던 소켓에게 접속한 사용자 ID 수가 증가한 사실을 통보하는 메시지(예컨대, 'userChange.msg')를 전송한다(단계 804).

[170] 소켓은 접속한 사용자 ID 수의 변경을 통보 받음에 따라, 대기 상태를 종료하고(단계 805), 데이터베이스는 제어 어플리케이션 사용자의 브라우저를 통한 로그인 정보(로그인 아이디, IP 주소, 로그인 시간, 세션 값 등)를 소켓으로 전송한다(단계 806).

[171] 소켓은 데이터베이스로부터 수신되는 접속한 모든 사용자 ID의 로그인 정보(예컨대, 'userData.msg')를 모바일 기기의 제어 어플리케이션으로 전송하고(단계 807), 제어 어플리케이션은 수신한 로그인 정보를 모바일 기기의 데이터베이스에 저장하고, 화면을 통해 출력한다. 이때, 제어 어플리케이션은 사용자의 로그인 상태를 실시간 통보하는 알람을 발생시킨다(단계 808).

[172] 도 9는 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템에서, 사용자 로그아웃 시 관리대상서버와 제어 어플리케이션 간의 상호 동작의 일례를 도시한 도면이다.

[173] 도 9를 참조하면, 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템은,

로그인 제어 서비스를 제공하기 위한 제어 어플리케이션 형태로 모바일 기기에 설치되어 구현될 수 있다.

[174] 모바일 기기에 설치된 브라우저를 통해 사용자가 로그인한 후 로그아웃 하는 절차가 도 9에 도시되어 있다.

[175] 관리대상서버는 소켓을 이용하여, 접속한 사용자의 ID 수가 변할 때까지 대기한다(단계 901).

[176] 모바일 기기에서 실행되는 브라우저는 관리대상서버에 접속한 사용자가 로그인 상태임을 확인한다(단계 902).

[177] 브라우저는 사용자에 의해 로그아웃 버튼이 선택되면 관리대상서버에서의 로그아웃 처리를 위한 메시지(예컨대, 'browserLogout.msg')를 관리대상서버로 전송하고, 로그인 제어 서비스는 상기 메시지를 수신한다(단계 903).

[178] 데이터베이스는 로그인 제어 서비스에 의해 로그아웃된 사용자 ID를 삭제하고 접속한 사용자 ID 수를 감소시킨 후, 대기 중이던 소켓에게 접속한 사용자 ID 수가 감소한 사실을 통보하는 메시지(예컨대, 'userChange.msg')를 전송한다(단계 904).

[179] 관리대상서버는 소켓을 통해, 접속한 사용자 ID 수의 변경을 통보 받음에 따라, 대기 상태를 종료하고(단계 905), 데이터베이스로부터 수신한 로그인 정보(예컨대, 'userData.msg')를 모바일 기기의 제어 어플리케이션으로 전송한다(단계 906).

[180] 제어 어플리케이션은 수신한 로그인 정보를 통해 로그아웃한 로그인 정보를 모바일 기기의 데이터베이스에서 제거하고, 현재 로그인한 사용자의 로그인 정보를 화면에 출력한다(단계 907).

[181] 도 10은 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템에서, 사용자 로그아웃 시 관리대상서버와 제어 어플리케이션 간의 상호 동작의 다른 일례를 도시한 도면이다.

[182] 도 10을 참조하면, 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템은, 로그인 제어 서비스를 제공하기 위한 제어 어플리케이션 형태로 모바일 기기에 설치되어 구현될 수 있다.

[183] 도 10에 도시된 바와 같이, 제어 어플리케이션은 현재 관리대상서버에 접속 중인 사용자들의 로그인 상태 정보를 확인하고, 특정 사용자의 로그인 상태를 로그아웃 상태로 변경할 수 있다.

[184] 관리대상서버는 소켓을 통해 접속한 사용자의 ID 수가 변할 때까지 대기한다(단계 1001).

[185] 모바일 기기의 브라우저는 관리대상서버에 접속한 사용자가 로그인 상태임을 확인한다(단계 1002).

[186] 모바일 기기의 브라우저는 로그인 상태인 로그인 정보 중 하나를 클릭하여, 관리대상서버에게 로그인 상태를 로그아웃 상태로 변경해 줄 것을 요청하는 로그아웃 정보(예컨대, 'logout.msg')를 송신한다(단계 1003). 이때, 로그아웃

정보는 로그인 ID, IP 주소, 로그인 시간, 세션 값 등을 포함할 수 있다.

[187] 데이터베이스는 로그인 제어 서비스에 의해 로그아웃된 사용자 ID를 삭제하고 접속한 사용자 ID 수를 감소시킨 후, 대기 중이던 소켓에게 접속한 사용자 ID 수가 감소한 사실을 통보하는 메시지(예컨대, 'userChange.msg')를 전송한다(단계 1004).

[188] 관리대상서버는 소켓을 통해, 접속한 사용자 ID 수의 변경을 통보 받음에 따라, 대기 상태를 종료하고(단계 1005), 데이터베이스로부터 수신한 로그인 정보(userData.msg)를 모바일 기기의 제어 어플리케이션으로 전송하여(단계 1006), 제어 어플리케이션의 로그인 상태를 업데이트 한다(단계 1007).

[189] 도 11은 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템에서, 로그인 차단 절차의 일례를 도시한 도면이다.

[190] 도 11을 참조하면, 본 발명의 다른 실시예에 따른 이중 로그인 탐지 시스템은, 로그인 제어 서비스를 제공하기 위한 제어 어플리케이션 형태로 모바일 기기에 설치되어 구현될 수 있다.

[191] 제어 어플리케이션은 차단하려는 IP 주소를 선택하는 기능을 제공하며, 차단한 IP 주소에 의해 식별되는 클라이언트 단말로부터 로그인 시도가 탐지될 경우, 로그아웃 처리한다.

[192] 우선, 제어 어플리케이션은 차단하고자 하는 IP 주소를 설정한다(단계 1101).

[193] 로그인 절차(단계1102)에 따라, 차단한 IP 주소로부터 사용자가 로그인을 시도하면, 제어 어플리케이션은 관리대상서버로부터 수신한 로그인 정보와 차단 설정한 IP 주소를 비교하여 차단한 IP 주소로부터의 로그인 시도를 탐지한다(단계 1103).

[194] 제어 어플리케이션은 차단된 IP 주소를 포함하는 로그인 정보를 관리대상서버의 데이터베이스로부터 삭제하기 위하여, 로그아웃 절차(단계 1104)에 따라 해당 사용자의 ID를 로그아웃 처리한다.

[195] 도 12는 본 발명의 일실시예에 따른 이중 로그인 탐지 방법의 순서를 도시한 흐름도이다.

[196] 본 실시예에 따른 이중 로그인 탐지 방법은 상술한 이중 로그인 탐지 시스템(300)에 의해 수행될 수 있다.

[197] 도 12를 참조하면, 단계(1210)에서, 이중 로그인 탐지 시스템(300)은 이중 로그인 모니터링 요청이 발생하는지 확인한다.

[198] 상기 단계(1210)에서 이중 로그인 모니터링 요청이 발생하는 것으로 확인되는 경우, 단계(1220)에서, 이중 로그인 탐지 시스템(300)은 관리대상서버에 로그인하는 클라이언트 단말에 관한 로그인 정보를 획득한다.

[199] 본 발명의 일실시예에 따른 이중 로그인 탐지 시스템(300)은 모바일 기기에 설치된 제어 어플리케이션을 통해 구현될 수 있다. 모바일 기기에서 구동되는 제어 어플리케이션에서, '이중 로그인 탐지'에 관한 메뉴가 선택되면, 이중 로그인 모니터링 요청이 발생할 수 있다.

[200] 이중 로그인 탐지 시스템(300)은 상기 이중 로그인 모니터링 요청의 발생에 따라, 관리대상서버에 대한 접속 정보(예, 관리대상서버에 의해 운영되는 웹 사이트의 주소)가 메모리부에 등록되어 있는 적어도 하나의 관리대상서버를 식별하고, 식별한 관리대상서버에 로그인하는 클라이언트 단말(예, 'PC', '모바일 기기' 등)에 관한 로그인 정보를, 상기 관리대상서버로부터 획득할 수 있다. 이중 로그인 탐지 시스템(300)은 상기 획득한 로그인 정보를 제어 어플리케이션을 통해 화면에 표시할 수 있다.

[201] 여기서, 상기 로그인 정보는 상기 관리대상서버에 로그인 함에 따라 생성되는 클라이언트 단말에 대한 IP 주소, 로그인 시간, 로그인 아이디, 세션(통신채널) 값 및 국가코드 중 적어도 하나를 포함할 수 있다.

[202] 단계(1230)에서, 이중 로그인 탐지 시스템(300)은 상기 로그인 정보를, 상기 관리대상서버로부터 수집된 상기 클라이언트 단말에 관한 이전 로그인 정보와 비교하여, 상기 로그인과 관련한 속도값을 연산한다.

[203] 여기서, 상기 이전 로그인 정보는, 상기 로그인 정보 내 로그인 아이디(예, 'sky01')와 동일한 로그인 아이디를 포함하면서, 현재 로그인을 기준으로 가장 최근에 정상 로그인으로 판단된 로그인 정보일 수 있다.

[204] 예를 들어, 이중 로그인 탐지 시스템(300)은 상기 이전 로그인 정보 A 내 IP 주소 '175.176.139.138'에 의해 식별되는 제1 지역 '서울 남산'에 대한 위도 및 경도로 이루어진 좌표값 '(37.558, 126.985)'을 추출하고, 상기 로그인 정보 내 IP 주소 '123.99.113.81'에 의해 식별되는 제2 지역 '부산역'에 대한 위도 및 경도로 이루어진 좌표값 '(35.114, 129.041)'을 추출하고, 추출한 좌표값을 이용하여, 제1 지역과 제2 지역 간 거리 차 예컨대, '322.45km'를 구할 수 있다.

[205] 이중 로그인 탐지 시스템(300)은 상기 이전 로그인 정보 A 내 로그인 시간 '2015-09-16 13:24:09'와, 상기 로그인 정보 내 로그인 시간 '2015-09-16 10:20:01' 간의 시간 차 '3시간 4분 8초'를 구하고, 상기 거리 차를 상기 시간 차로 나누는 연산을 통해, 제2 지역 '부산역'에서 로그인하는 클라이언트 단말의 속도값 '104.7 km/h'을 연산할 수 있다.

[206] 단계(1240)에서, 이중 로그인 탐지 시스템(300)은 상기 연산한 속도값이, 지정된 임계치를 초과 함에 따라, 상기 클라이언트 단말에 대해 이중 로그인으로 판단한다.

[207] 즉, 이중 로그인 탐지 시스템(300)은 동일한 로그인 아이디를 사용하여 시간 차를 두고 발생하는 관리대상서버(예컨대, 웹 사이트 'www.sky.com'의 운영 서버)로의 로그인에 대해, 상기 로그인과 관련한 속도값에 기초하여, 동일한 사용자에 의한 정상 로그인인지, 또는 다른 사용자에 의한 부정 로그인(이중 로그인)인지를 판단할 수 있다.

[208] 일례로, 이중 로그인 탐지 시스템(300)은 상기 속도값이 지정된 임계치(예컨대, '100km/h') 보다 크면(속도가 빠르면), 현재 제2 지역에서 관리대상서버에 로그인하는 클라이언트 단말을 이중 로그인으로 판단하고, 상기 속도값이

지정된 임계치보다 작으면(속도가 느리면), 현재 제2 지역에서 관리대상서버에 로그인하는 클라이언트 단말을 정상 로그인으로 판단할 수 있다.

[209] 여기서, 상기 임계치는 이전 로그인 정보와 로그인 정보 내 국가코드가 동일한 경우에 이중 로그인을 판단하기 위한 비교 속도(예컨대, '100km/h')로 지정될 수 있다.

[210] 예를 들어, 이중 로그인 탐지 시스템(300)은 상기 속도값 '104.7 km/h'이 임계치 '100km/h'를 초과 함에 따라, 제2 지역에서 현재 로그인한 클라이언트 단말에 대해 이중 로그인으로 판단할 수 있다. 즉, 이중 로그인 탐지 시스템(300)은 상기 속도값이 지정된 속도보다 빠른 경우, 현재 로그인에 대해 이중 로그인으로 탐지할 수 있다.

[211] 단계(1250)에서, 이중 로그인 탐지 시스템(300)은 상기 이중 로그인으로 판단된 클라이언트 단말을, 로그아웃 처리한다.

[212] 일례로, 이중 로그인 탐지 시스템(300)은 상기 클라이언트 단말이 이중 로그인으로 판단 됨에 따라, 상기 관리대상서버에 이중 로그인에 관한 메시지를 전송하여, 상기 관리대상서버로부터, 상기 로그인 정보가 삭제되도록 하여, 상기 로그아웃 처리할 수 있다.

[213] 또한, 이중 로그인 탐지 시스템(300)은 상기 로그인 정보로부터 식별되는 세션 값을 이용하여, 상기 클라이언트 단말과 상기 관리대상서버와의 연결을 해제하여, 상기 로그아웃 처리할 수도 있다.

[214] 이와 같이, 이중 로그인 탐지 시스템(300)은 이중 로그인으로 판단되는 클라이언트 단말을 로그아웃 처리하여, 관리대상서버에 대한 클라이언트 단말의 이중 로그인을 자동 차단 함으로써, 부정한 로그인에 따른 피해를 최소화 할 수 있다.

[215] 본 발명의 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

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

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

청구범위

[청구항 1] 이중 로그인 모니터링 요청이 발생 함에 연동하여,
관리대상서버에 로그인하는 클라이언트 단말에 관한 로그인 정보를 획득하는 단계;
상기 로그인 정보를, 상기 관리대상서버로부터 수집된 상기 클라이언트 단말에 관한 이전 로그인 정보와 비교하여, 상기 로그인과 관련한 속도값을 연산하는 단계;
상기 연산한 속도값이, 지정된 임계치를 초과 함에 따라, 상기 클라이언트 단말에 대해 이중 로그인으로 판단하는 단계; 및
상기 이중 로그인으로 판단된 클라이언트 단말을, 로그아웃 처리하는 단계
를 포함하는 이중 로그인 탐지 방법.

[청구항 2] 제1항에 있어서,
상기 속도값을 연산하는 단계는,
상기 이전 로그인 정보에 의해 식별되는 제1 지역 및 상기 로그인 정보에 의해 식별되는 제2 지역 간 거리 차를 구하는 단계;
상기 이전 로그인 정보 내 로그인 시간과, 상기 로그인 정보 내 로그인 시간을 이용하여, 시간 차를 구하는 단계; 및
상기 거리 차 및 상기 시간 차를 이용하여, 상기 클라이언트 단말의 로그인과 관련한 속도값을 연산하는 단계
를 포함하는 이중 로그인 탐지 방법.

[청구항 3] 제2항에 있어서,
상기 거리 차를 구하는 단계는,
상기 이전 로그인 정보 내 IP 주소에 의해 식별되는 제1 지역에 대한 위도좌표값 및 경도좌표값과, 상기 로그인 정보 내 IP 주소에 의해 식별되는 제2 지역에 대한 위도좌표값 및 경도좌표값을 추출하는 단계; 및
상기 추출한 위도좌표값과 경도좌표값을 이용하여, 상기 제1 지역 및 제2 지역 간 거리 차를 구하는 단계
를 포함하는 이중 로그인 탐지 방법.

[청구항 4] 제1항에 있어서,
상기 이전 로그인 정보 내 국가코드와, 상기 로그인 정보 내 국가코드를 비교하는 단계; 및
상기 비교 결과, 국가코드가 상이하면, 상기 이전 로그인 정보에 의해 식별되는 제1 지역 및 상기 로그인 정보에 의해 식별되는 제2 지역 간의 거리 차에 비례하여, 상기 임계치를 변경하는 단계
를 더 포함하는 이중 로그인 탐지 방법.

[청구항 5] 제1항에 있어서,
상기 클라이언트 단말에 부여된 등급을 확인하는 단계;
상기 확인된 등급에 기초하여, 상기 클라이언트 단말에게 로그인 허용시간을 할당하는 단계; 및
상기 로그인 허용시간이 도과하면, 상기 속도값이 상기 임계치를 초과하는지의 여부와 무관하게, 상기 클라이언트 단말을 로그아웃 처리하는 단계
를 더 포함하는 이중 로그인 탐지 방법.

[청구항 6] 제1항에 있어서,
상기 이전 로그인 정보 내 로그인 시간과, 상기 로그인 정보 내 로그인 시간 간의 시간 차가, 정해진 시간격 이내이면,
상기 속도값을 연산하는 단계를 생략하고, 상기 클라이언트 단말에 대해 이중 로그인으로 판단하는 단계
를 더 포함하는 이중 로그인 탐지 방법.

[청구항 7] 제1항에 있어서,
상기 클라이언트 단말이 이중 로그인으로 판단 됨에 따라,
상기 획득한 로그인 정보 내, 상기 클라이언트 단말의 IP 주소, 로그인 시간 및 국가코드 중 적어도 하나를, 화면 상에 표시하여, 사용자에게 이중 로그인에 대해 알람하는 단계
를 더 포함하는 이중 로그인 탐지 방법.

[청구항 8] 제1항에 있어서,
상기 로그아웃 처리하는 단계는,
상기 클라이언트 단말이 이중 로그인으로 판단 됨에 따라, 상기 관리대상서버에 이중 로그인에 관한 메시지를 전송하여, 상기 관리대상서버로부터, 상기 로그인 정보가 삭제되도록 하여, 상기 로그아웃 처리하는 단계
를 포함하는 이중 로그인 탐지 방법.

[청구항 9] 제1항에 있어서,
상기 로그아웃 처리하는 단계는,
상기 로그인 정보로부터 식별되는 세션 값을 이용하여, 상기 클라이언트 단말과 상기 관리대상서버와의 연결을 해제하는 단계
를 포함하는 이중 로그인 탐지 방법.

[청구항 10] 제1항에 있어서,
상기 연산한 속도값이 상기 임계치를 초과하지 않을 경우, 상기 클라이언트 단말에 대해 정상 로그인으로 판단하는 단계; 및
상기 관리대상서버에서, 상기 클라이언트 단말에 관한 이전 로그인 정보를, 상기 로그인 정보로 갱신하도록 하는 단계
를 더 포함하는 이중 로그인 탐지 방법.

[청구항 11] 제1항에 있어서,
상기 이중 로그인 모니터링 요청의 발생에 따라, 상기 관리대상서버에 대한 접속 정보를 메모리부로부터 식별하고, 상기 접속 정보를 이용하여 관리대상서버에 접속하는 단계
를 더 포함하고,
상기 로그인 정보를 획득하는 단계는,
상기 접속 정보 내 접속 아이디와 일치하는 로그인 아이디로 상기 관리대상서버에 로그인하는 상기 클라이언트 단말에 대한 IP 주소, 로그인 시간, 로그인 아이디, 세션 값 및 국가코드 중 적어도 하나의 로그인 정보를 획득하는 단계
를 포함하는 이중 로그인 탐지 방법.

[청구항 12] 제1항에 있어서,
일정 시간 간격으로 상기 관리대상서버에 접속하여, 상기 관리대상서버와의 접속을 유지하는 단계; 및
상기 관리대상서버와의 접속을 유지한 상태에서, 상기 로그인 정보를 획득하는 단계
를 더 포함하는 이중 로그인 탐지 방법.

[청구항 13] 제1항에 있어서,
상기 관리대상서버가 복수일 경우,
상기 각 관리대상서버에 대한 접속 정보를 이용하여, 상기 각각의 관리대상서버에 교대로 접속하는 단계;
상기 각 관리대상서버에 로그인하는 클라이언트 단말에 관한 로그인 정보를 획득하는 단계
를 더 포함하는 이중 로그인 탐지 방법.

[청구항 14] 이중 로그인 모니터링 요청이 발생 함에 연동하여,
관리대상서버에 로그인하는 클라이언트 단말에 관한 로그인 정보를 획득하는 획득부;
상기 로그인 정보를, 상기 관리대상서버로부터 수집된 상기 클라이언트 단말에 관한 이전 로그인 정보와 비교하여, 상기 로그인과 관련한 속도값을 연산하는 연산부;
상기 연산한 속도값이, 지정된 임계치를 초과 함에 따라, 상기 클라이언트 단말에 대해 이중 로그인으로 판단하는 판단부; 및
상기 이중 로그인으로 판단된 클라이언트 단말을, 로그아웃 처리하는 처리부
를 포함하는 이중 로그인 탐지 시스템.

[청구항 15] 제14항에 있어서,
상기 연산부는,
상기 이전 로그인 정보에 의해 식별되는 제1 지역 및 상기 로그인 정보에

의해 식별되는 제2 지역 간 거리 차를 구하고,
상기 이전 로그인 정보 내 로그인 시간과, 상기 로그인 정보 내 로그인 시간을 이용하여, 시간 차를 구하고,
상기 거리 차 및 상기 시간 차를 이용하여, 상기 클라이언트 단말의 로그인과 관련한 속도값을 연산하는
이중 로그인 탐지 시스템.

[청구항 16] 제15항에 있어서,
상기 연산부는,
상기 이전 로그인 정보 내 IP 주소에 의해 식별되는 제1 지역에 대한 위도좌표값 및 경도좌표값과, 상기 로그인 정보 내 IP 주소에 의해 식별되는 제2 지역에 대한 위도좌표값 및 경도좌표값을 추출하고, 상기 추출한 위도좌표값과 경도좌표값을 이용하여, 상기 제1 지역 및 제2 지역 간 거리 차를 구하는
이중 로그인 탐지 시스템.

[청구항 17] 제14항에 있어서,
상기 이전 로그인 정보 내 국가코드와, 상기 로그인 정보 내 국가코드를 비교하고, 상기 비교 결과, 국가코드가 상이하면, 상기 이전 로그인 정보에 의해 식별되는 제1 지역 및 상기 로그인 정보에 의해 식별되는 제2 지역 간의 거리 차에 비례하여, 상기 임계치를 변경하는 변경부
를 더 포함하는 이중 로그인 탐지 시스템.

[청구항 18] 제14항에 있어서,
상기 처리부는,
상기 클라이언트 단말에 부여된 등급을 확인하고, 상기 확인된 등급에 기초하여, 상기 클라이언트 단말에게 로그인 허용시간을 할당하고, 상기 로그인 허용시간이 도과하면, 상기 속도값이 상기 임계치를 초과하는지의 여부와 무관하게, 상기 클라이언트 단말을 로그아웃 처리하는
이중 로그인 탐지 시스템.

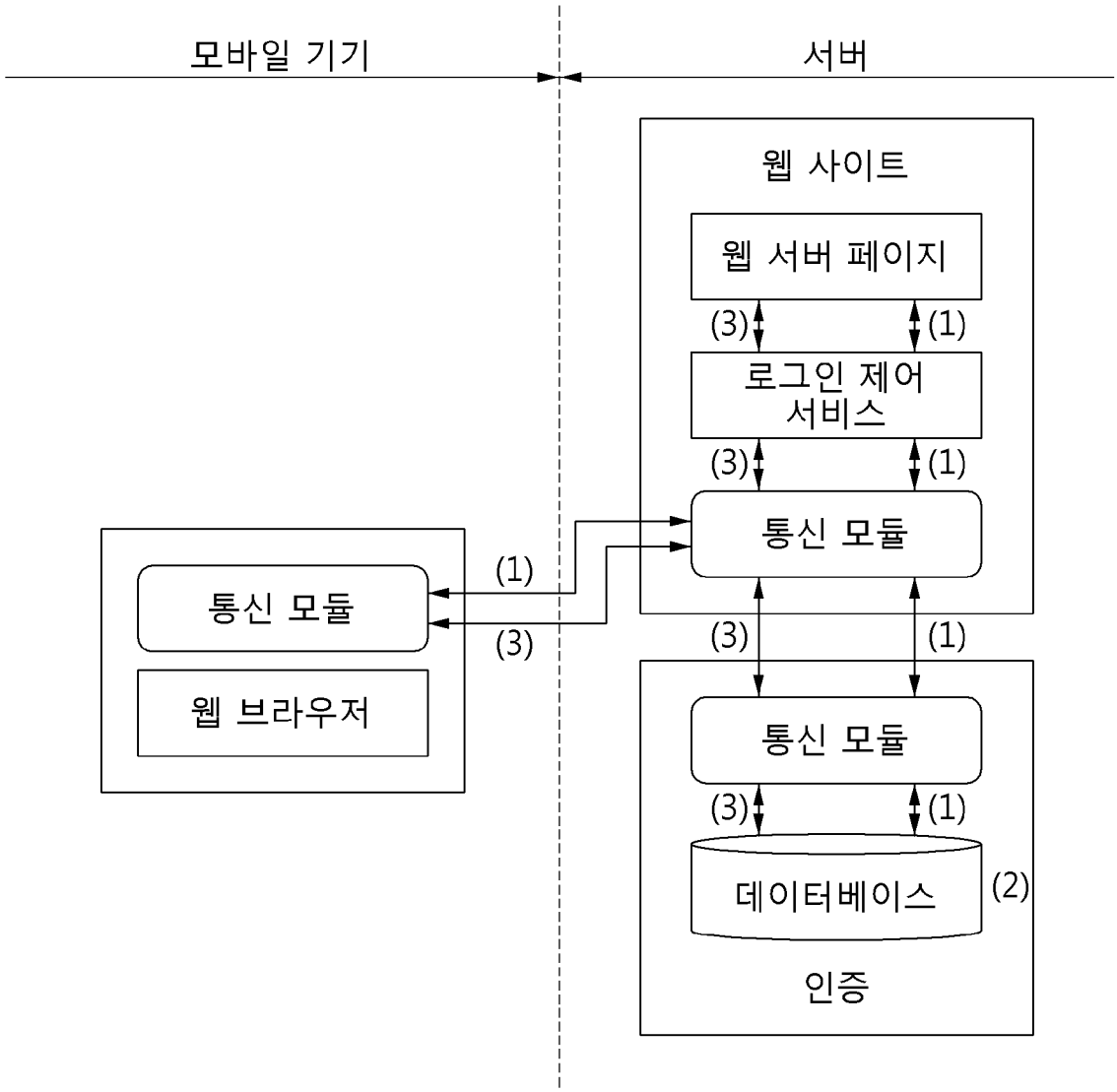
[청구항 19] 제14항에 있어서,
상기 이전 로그인 정보 내 로그인 시간과, 상기 로그인 정보 내 로그인 시간 간의 시간 차가, 정해진 시간격 이내이면,
상기 판단부는,
상기 속도값에 무관하게, 상기 클라이언트 단말에 대해 이중 로그인으로 판단하는
이중 로그인 탐지 시스템.

[청구항 20] 제14항에 있어서,
상기 클라이언트 단말이 이중 로그인으로 판단 됨에 따라,
상기 획득한 로그인 정보 내, 상기 클라이언트 단말의 IP 주소, 로그인

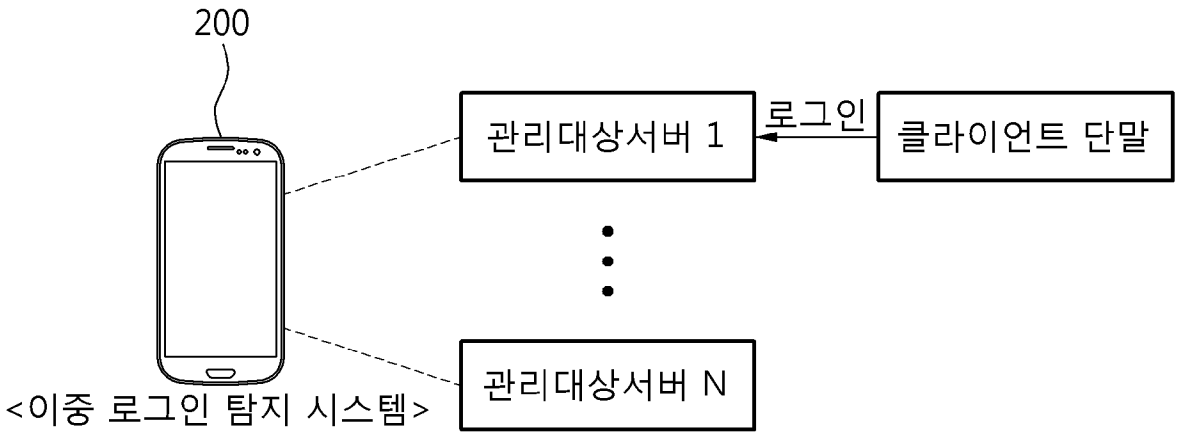
시간 및 국가코드 중 적어도 하나를, 화면 상에 표시하여, 사용자에게 이중 로그인에 대해 알람하는 알람부

를 더 포함하는 이중 로그인 탐지 시스템.

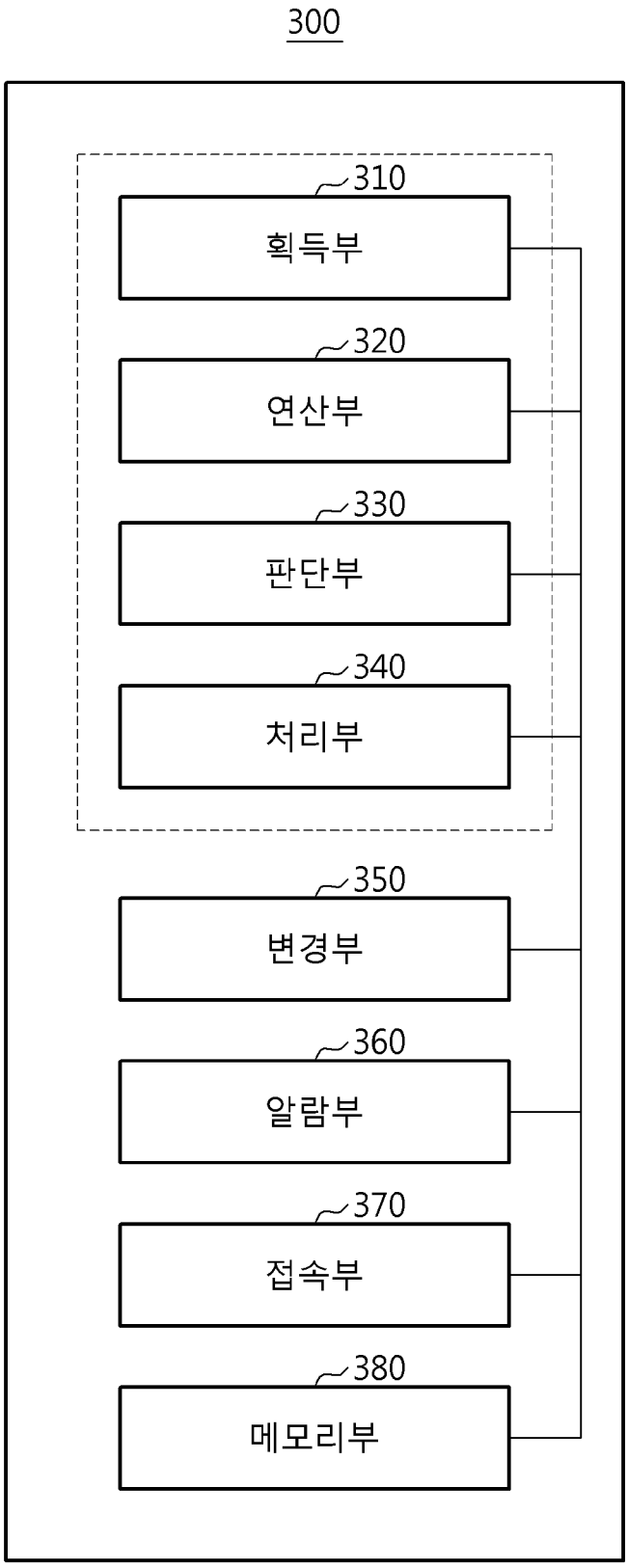
[도1]


모바일 기기
서버
웹 사이트
웹 서버 페이지
(3)
(1)
로그인 제어 서비스
(3)
(1)
통신 모듈
(1)
(3)
통신 모듈
웹 브라우저
(3)
(1)
통신 모듈
(3)
(1)
데이터베이스
(2)
인증

[도2]


200
관리대상서버 1
로그인
클라이언트 단말
관리대상서버 N
<이중 로그인 탐지 시스템>

[도3]


300
310
획득부
320
연산부
330
판단부
340
처리부
350
변경부
360
알람부
370
접속부
380
메모리부

[도4]

i) 로그인 정보

IP 주소	로그인 시간	국가코드
123.99.113.81	2015-09-16 10:20:01	1111

→ (위도, 경도) (35.114, 129.041)

ii) 이전 로그인 정보 A

IP 주소	로그인 시간	국가코드
175.176.139.138	2015-09-16 13:24:09	1111

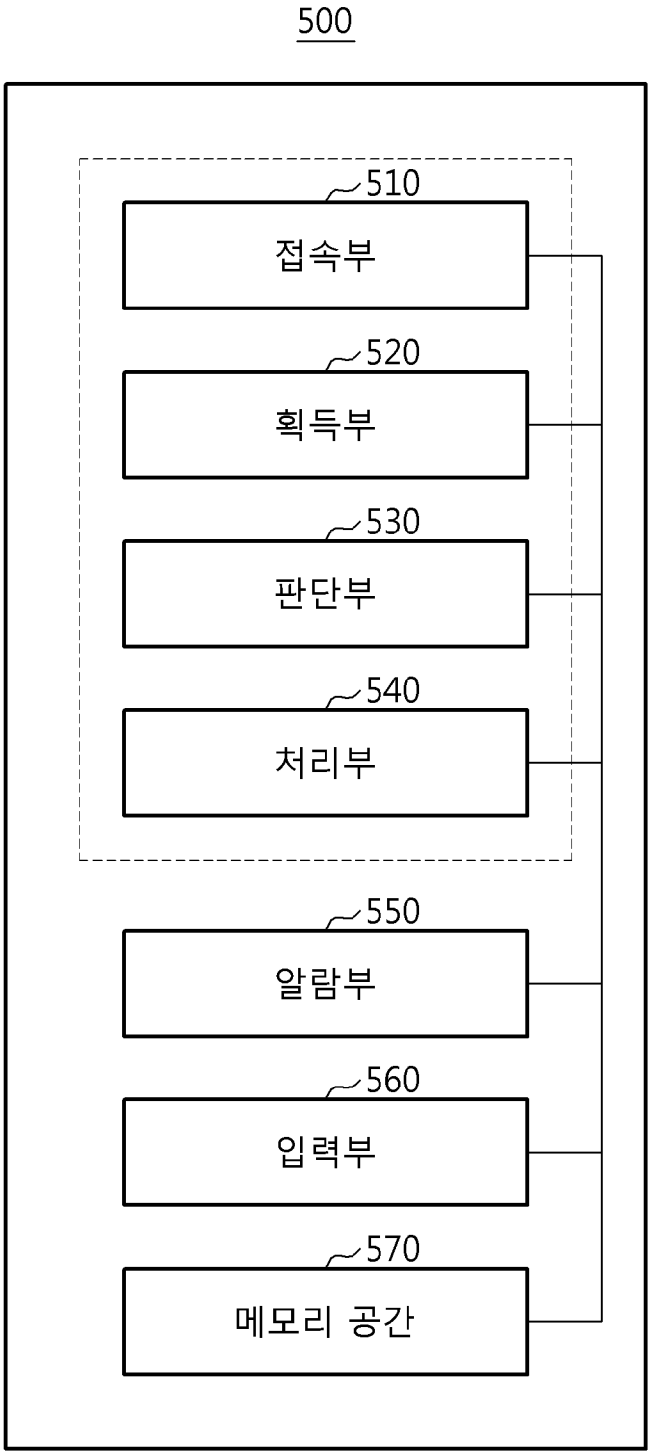
→ (위도, 경도) (37.558, 126.985)

iii) 이전 로그인 정보 B

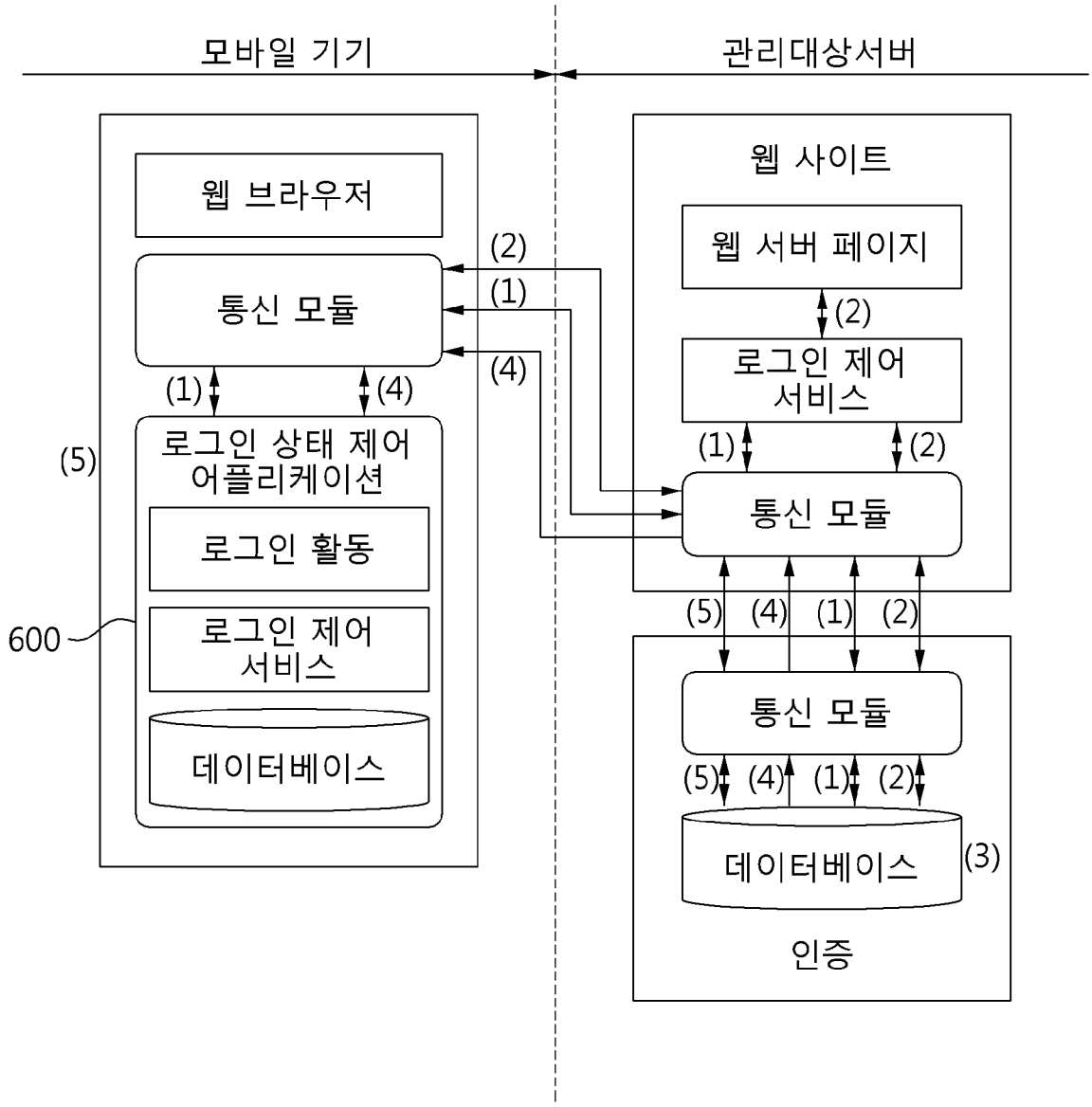
IP 주소	로그인 시간	국가코드
220.108.196.157	2015-09-16 11:15:06	1010

→ (위도, 경도) (33.888, 130.873)

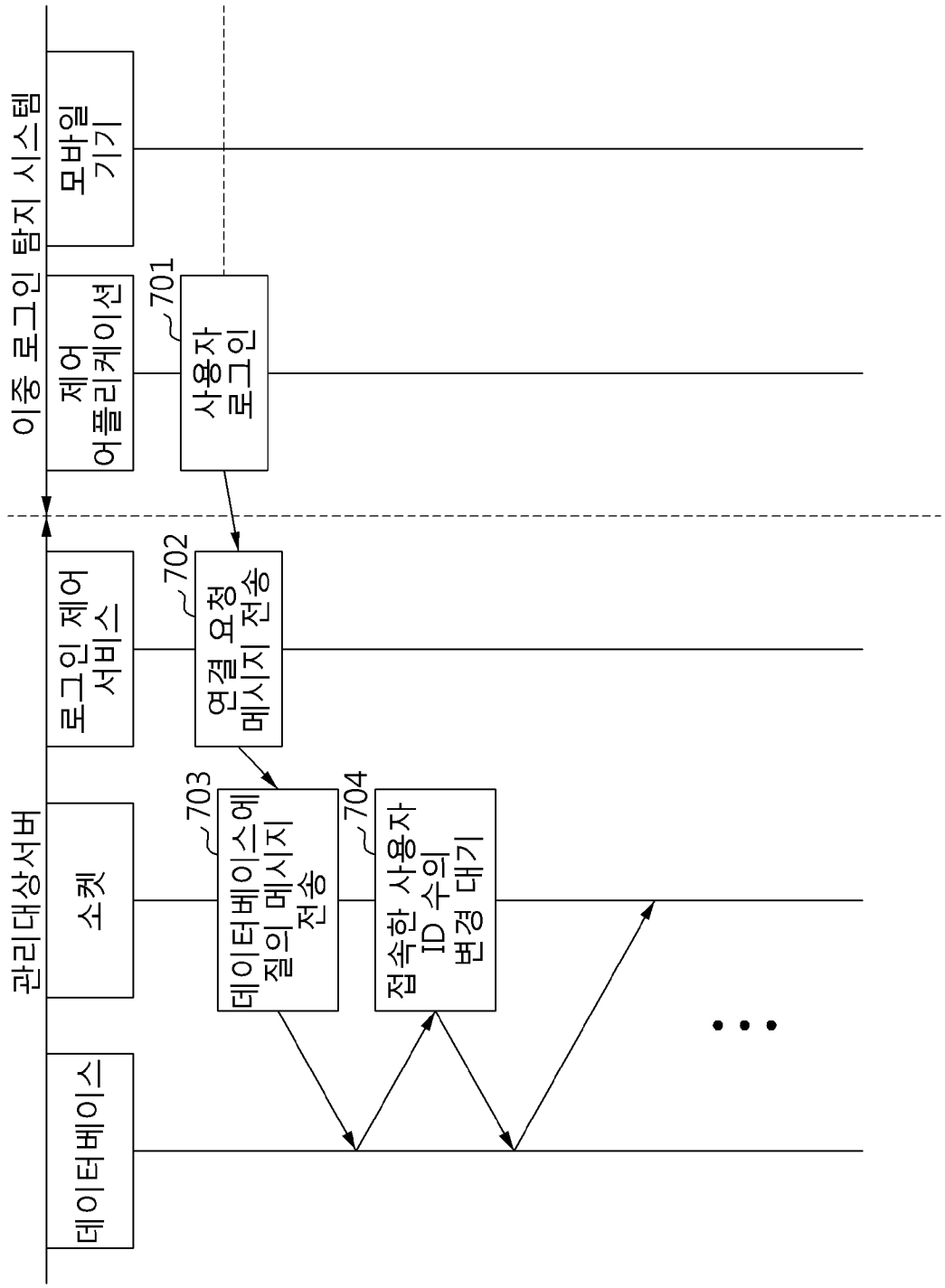
[도5]



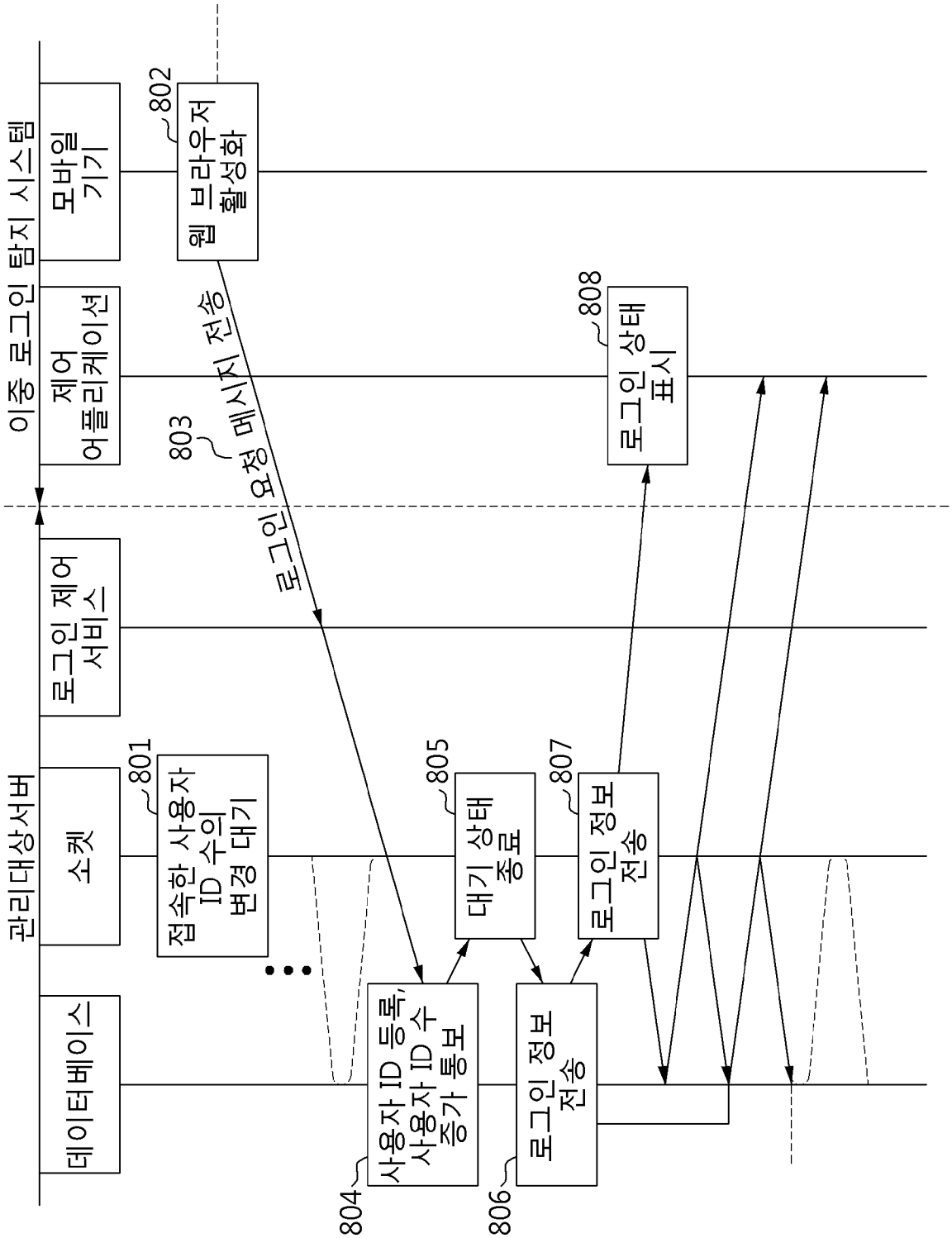
[도6]


모바일 기기
관리대상서버
웹 브라우저
통신 모듈
(1)
(4)
(2)
(1)
(4)
(5)
로그인 상태 제어 어플리케이션
로그인 활동
로그인 제어 서비스
데이터베이스
600
웹 사이트
웹 서버 페이지
(2)
로그인 제어 서비스
(1)
(2)
통신 모듈
(5)
(4)
(1)
(2)
통신 모듈
(5)
(4)
(1)
(2)
데이터베이스
(3)
인증

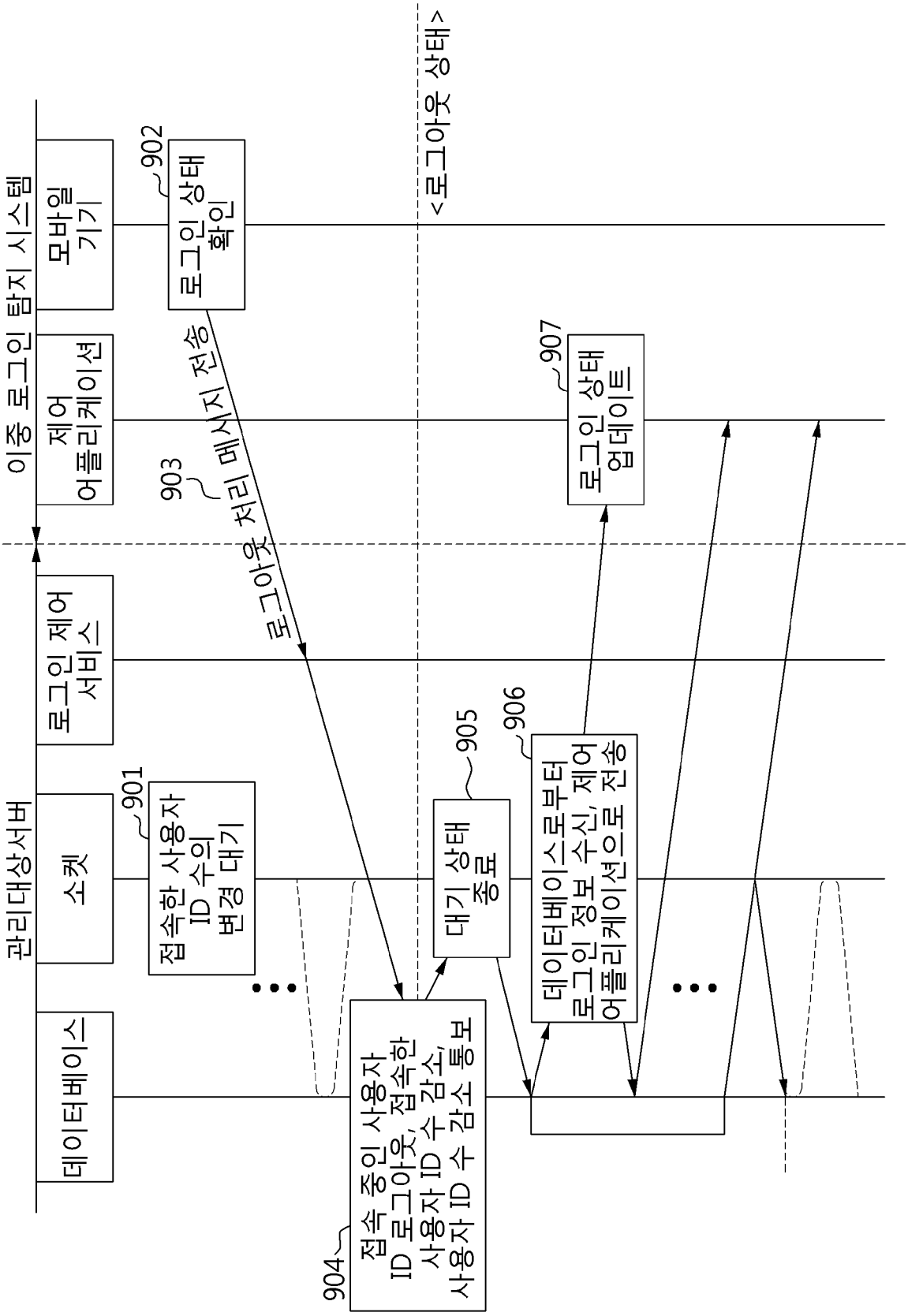
[도7]


이중 로그인 탐지 시스템
관리대상서버
모바일 기기
제어 어플리케이션
701
사용자 로그인
로그인 제어 서비스
702
연결 요청 메시지 전송
소켓
703
데이터베이스에 질의 메시지 전송
704
접속한 사용자 ID 수의 변경 대기
데이터베이스

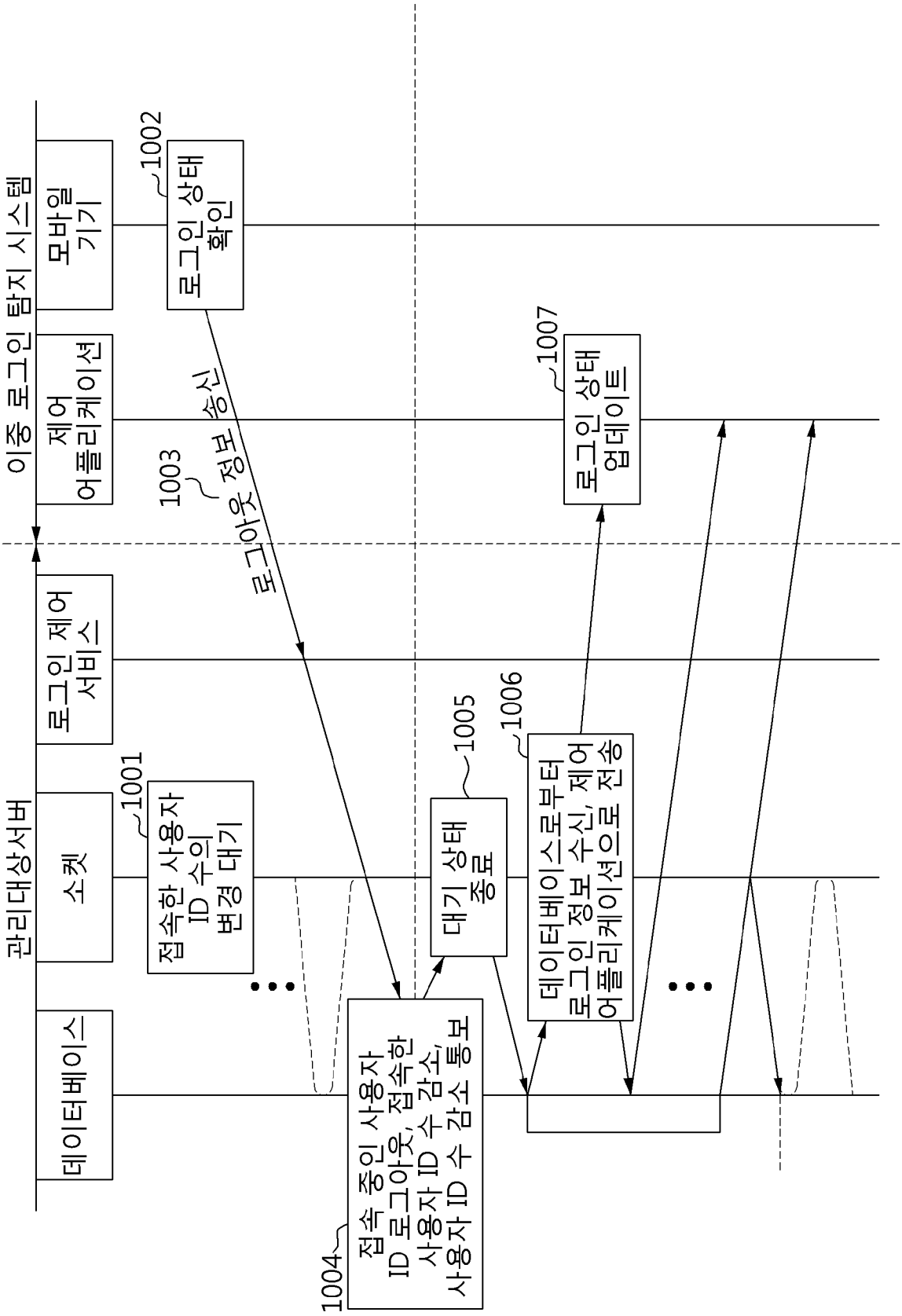
[도8]


이중 로그인 탐지 시스템
관리대상서버
모바일 기기
제어 어플리케이션
로그인 제어 서비스
소켓
데이터베이스
802
웹 브라우저 활성화
803
로그인 요청 메시지 전송
801
접속한 사용자 ID 수의 변경 대기
804
사용자 ID 등록, 사용자 ID 수 증가 통보
805
대기 상태 종료
806
로그인 정보 전송
807
로그인 정보 전송
808
로그인 상태 표시

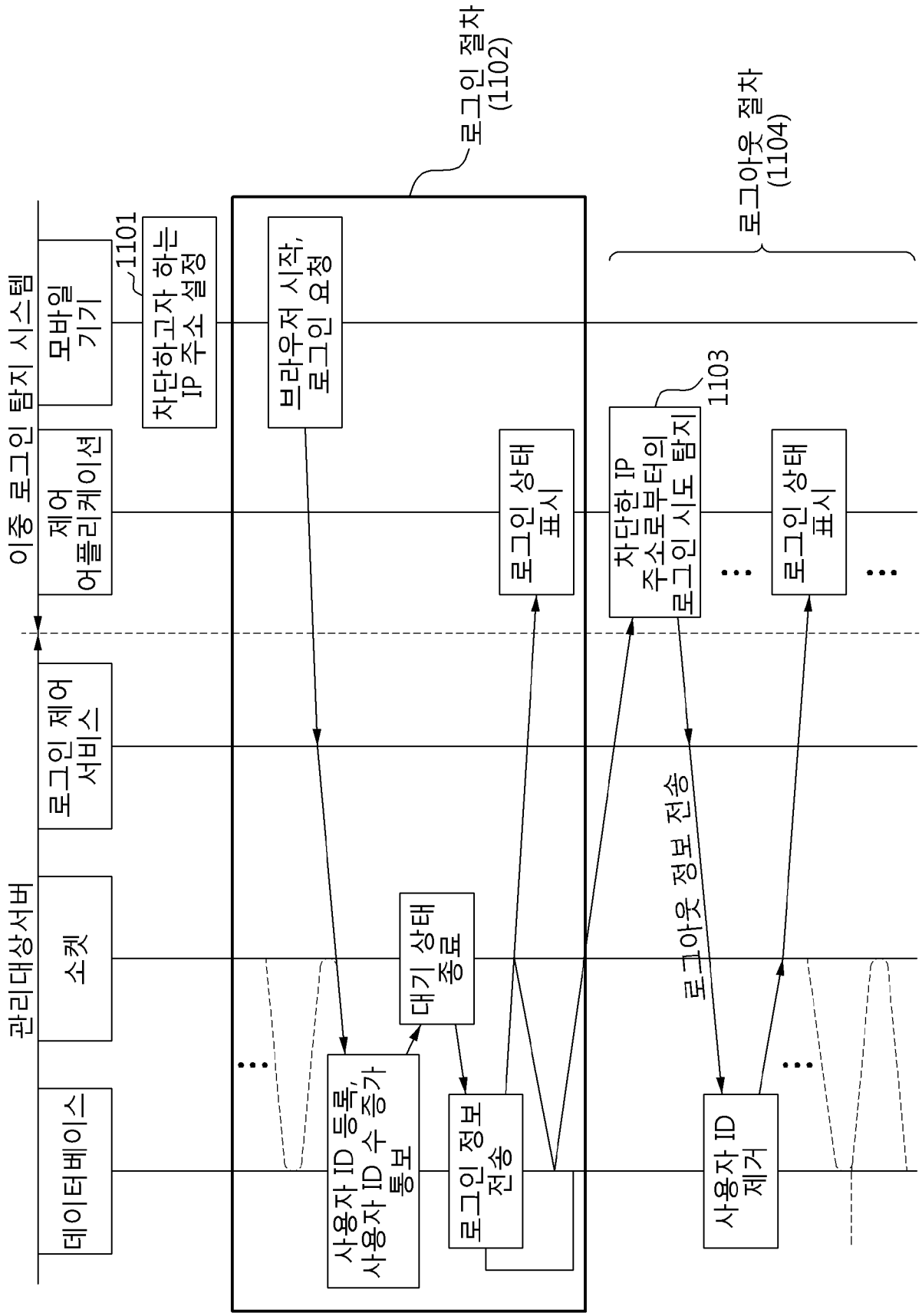
[도9]


이중 로그인 탐지 시스템
관리대상서버
모바일 기기
제어 어플리케이션
로그인 제어 서비스
소켓
데이터베이스
902
로그인 상태 확인
903
로그아웃 처리 메시지 전송
901
접속한 사용자 ID 수의 변경 대기
905
대기 상태 종료
906
데이터베이스로부터 로그인 정보 수신, 제어 어플리케이션으로 전송
907
로그인 상태 업데이트
904
접속 중인 사용자 ID 로그아웃, 접속한 사용자 ID 수 감소, 사용자 ID 수 감소 통보
<로그아웃 상태>

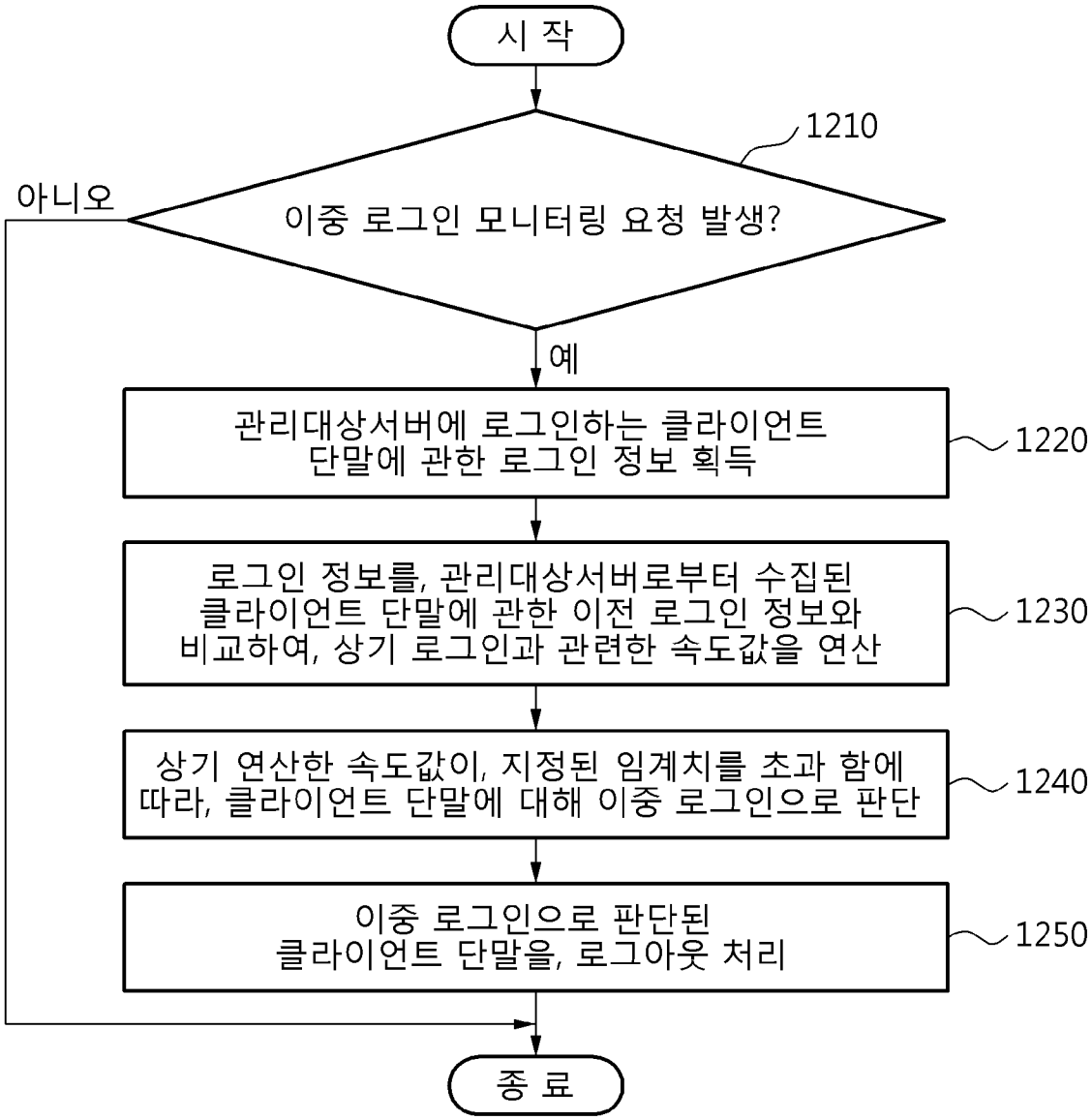
[도10]


이중 로그인 탐지 시스템
관리대상서버
모바일 기기
제어 어플리케이션
로그인 제어 서비스
소켓
데이터베이스
1002
로그인 상태 확인
1003
로그아웃 정보 송신
1007
로그인 상태 업데이트
1001
접속한 사용자 ID 수의 변경 대기
1005
대기 상태 종료
1006
데이터베이스로부터 로그인 정보 수신, 제어 어플리케이션으로 전송
1004
접속 중인 사용자 ID 로그아웃, 접속한 사용자 ID 수 감소, 사용자 ID 수 감소 통보

[도11]


로그인 절차
(1102)
로그아웃 절차
(1104)
1101
1103
이중 로그인 탐지 시스템
관리대상서버
모바일 기기
제어 어플리케이션
로그인 제어 서비스
소켓
데이터베이스
차단하고자 하는 IP 주소 설정
브라우저 시작, 로그인 요청
로그인 상태 표시
차단한 IP 주소로부터의 로그인 시도 탐지
로그인 상태 표시
사용자 ID 등록, 사용자 ID 수 증가 통보
대기 상태 종료
로그인 정보 전송
로그아웃 정보 전송
사용자 ID 제거

[도12]


시 작
1210
이중 로그인 모니터링 요청 발생?
아니오
예
관리대상서버에 로그인하는 클라이언트 단말에 관한 로그인 정보 획득
1220
로그인 정보를, 관리대상서버로부터 수집된 클라이언트 단말에 관한 이전 로그인 정보와 비교하여, 상기 로그인과 관련한 속도값을 연산
1230
상기 연산한 속도값이, 지정된 임계치를 초과 함에 따라, 클라이언트 단말에 대해 이중 로그인으로 판단
1240
이중 로그인으로 판단된 클라이언트 단말을, 로그아웃 처리
1250
종 료

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2016/000318

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/24(2006.01)i, H04L 12/26(2006.01)i, H04L 29/06(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 12/24; G06F 15/00; G06F 21/20; G06F 12/14; H04L 9/32; G06Q 40/02; G06F 13/00; H04L 12/26; H04L 29/06

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: login, speed, distance, time

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2006-0010741 A (ITRACS CORPORATION) 02 February 2006 See claims 1-11; and figures 1, 2.	1-20
Y	US 2013-0110715 A1 (BUCHHOP, Peter) 02 May 2013 See paragraphs [0022], [0033]; claims 1-9; and figure 2.	1-20
Y	KR 10-2012-0100548 A (INCENTRIC) 12 September 2012 See paragraph [0041]; claim 3; and figure 3.	5,18
A	JP 2014-174822 A (RICOH CO., LTD.) 22 September 2014 See paragraphs [0039]-[0042]; claims 1-7; and figure 6.	1-20
A	KR 10-2013-0123329 A (SECUVE) 12 November 2013 See claims 1-8; and figure 1.	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
11 APRIL 2016 (11.04.2016)	**16 MAY 2016 (16.05.2016)**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2016/000318

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2006-0010741 A	02/02/2006	AU 2004-230005 A1	28/10/2004
		CA 2520882 A1	28/10/2004
		CN 1795440 A	28/06/2006
		EP 1611518 A1	04/01/2006
		JP 2006-522420 A	28/09/2006
		US 2007-0162954 A1	12/07/2007
		WO 2004-092961 A1	28/10/2004
US 2013-0110715 A1	02/05/2013	WO 2013-062897 A1	02/05/2013
KR 10-2012-0100548 A	12/09/2012	NONE	
JP 2014-174822 A	22/09/2014	NONE	
KR 10-2013-0123329 A	12/11/2013	KR 10-2013-0123339 A	12/11/2013

국 제 조 사 보 고 서

국제출원번호
PCT/KR2016/000318

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 12/24(2006.01)i, H04L 12/26(2006.01)i, H04L 29/06(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 12/24; G06F 15/00; G06F 21/20; G06F 12/14; H04L 9/32; G06Q 40/02; G06F 13/00; H04L 12/26; H04L 29/06

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: 로그인, 속도, 거리, 시간

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-2006-0010741 A (아이트랙스 코포레이션) 2006.02.02 청구항 1-11; 및 도면 1, 2 참조.	1-20
Y	US 2013-0110715 A1 (PETER BUCHHOP) 2013.05.02 단락 [0022], [0033]; 청구항 1-9; 및 도면 2 참조.	1-20
Y	KR 10-2012-0100548 A (주식회사 인센트릭) 2012.09.12 단락 [0041]; 청구항 3; 및 도면 3 참조.	5,18
A	JP 2014-174822 A (RICOH CO., LTD.) 2014.09.22 단락 [0039]-[0042]; 청구항 1-7; 및 도면 6 참조.	1-20
A	KR 10-2013-0123329 A (주식회사 시큐브) 2013.11.12 청구항 1-8; 및 도면 1 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
2016년 04월 11일 (11.04.2016)	2016년 05월 16일 (16.05.2016)

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

심사관
김성우
전화번호 +82-42-481-3348

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2016/000318

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2006-0010741 A	2006/02/02	AU 2004-230005 A1	2004/10/28
		CA 2520882 A1	2004/10/28
		CN 1795440 A	2006/06/28
		EP 1611518 A1	2006/01/04
		JP 2006-522420 A	2006/09/28
		US 2007-0162954 A1	2007/07/12
		WO 2004-092961 A1	2004/10/28
US 2013-0110715 A1	2013/05/02	WO 2013-062897 A1	2013/05/02
KR 10-2012-0100548 A	2012/09/12	없음	
JP 2014-174822 A	2014/09/22	없음	
KR 10-2013-0123329 A	2013/11/12	KR 10-2013-0123339 A	2013/11/12