



- (51) 국제특허분류:
G06F 21/34 (2013.01) H04L 9/32 (2006.01)
- (21) 국제출원번호: PCT/KR2013/012157
- (22) 국제출원일: 2013년 12월 26일 (26.12.2013)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2013-0064495 2013년 6월 5일 (05.06.2013) KR
10-2013-0065364 2013년 6월 7일 (07.06.2013) KR
- (71) 출원인: 에스케이플래닛 주식회사 (SK PLANET CO., LTD.) [KR/KR]; 463-400 경기도 성남시 분당구 판교로 264 (삼평동), Gyeonggi-do (KR).
- (72) 발명자: 고경완 (KO, Kyungwan); 143-758 서울시 광진구 아차산로 262, 더샵스타시티아파트 A 동 3503호 (자양동), Seoul (KR). 엄봉수 (UM, Bongsu); 133-724 서울시 성동구 상원길 80, 동아그린아파트 101 동 708호 (성수동 1가), Seoul (KR).
- (74) 대리인: 박종한 (PARK, Chonghan); 152-740 서울시 구로구 디지털로 26길 5, 319 (구로동, 에이스하이엔드타워), 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, LT, 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.

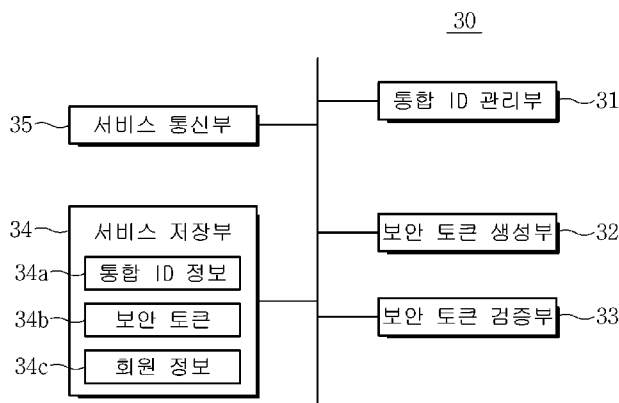
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, 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))

(54) Title: AUTHENTICATION METHOD USING SECURITY TOKEN, AND SYSTEM AND APPARATUS FOR SAME

(54) 발명의 명칭: 보안토큰을 이용한 인증 방법, 이를 위한 시스템 및 장치



- 31 ... Integrated ID management unit
32 ... Security token generation unit
33 ... Security token verification unit
34 ... Service storage unit
34a ... Integrated ID information
34b ... Security token
34c ... Membership information
35 ... Service communication unit

(57) Abstract: The present invention relates to an authentication method using a security token, and a system and an apparatus for the same. In particular, in the present invention, at the time of authentication using a security token, a disposable security token is used in verification, and at the time of re-login for use of a service on a web, authentication is performed through verification of a security token to which bidirectional encryption is applied, so that it is possible to improve security against hacking (cookie hijacking) from the outside. Further, since an authentication value constituting a security token can be changed by applying various calculation schemes, a stability of an authentication procedure is ensured. Furthermore, using a disposable security token instead of security or authentication information exposed in an authentication process of a cookie scheme, a token length, data loss, and data use amount can be reduced, and data transmission and movement speed can be improved.

(57) 요약서: 본 발명은 보안토큰을 이용한 인증 방법, 이를 위한 시스템 및 장치에 관한 것으로서, 특히, 보안토큰을

[다음 쪽 계속]



이용한 인증 시 일회용 보안토큰을 이용하여 검증을 수행하고, 웹 상에서 서비스 이용을 위한 재 로그인 시 양방향 암호화가 적용된 보안토큰의 검증을 통해 인증을 수행함으로써, 외부의 해킹(cookie hijacking)으로부터 보안성을 높일 수 있다. 또한, 보안토큰을 구성하는 인증 값을 다양한 연산 방식을 적용하여 변경할 수 있기 때문에, 인증 절차 상의 안정성이 보장된다. 또한, 쿠키 방식의 인증 과정에서 노출되는 보안 또는 인증 정보를 일회용 보안토큰을 활용하여 토큰 길이, 데이터 손실 및 사용량을 줄일 수 있고, 데이터 전송 및 이동 속도를 향상시킬 수 있다.

명세서

발명의 명칭: 보안토큰을 이용한 인증 방법, 이를 위한 시스템 및 장치

기술분야

- [1] 본 발명은 보안토큰을 이용한 인증 방법, 이를 위한 시스템 및 장치에 관한 것으로서, 더욱 상세하게는 로직 처리장치 접속 시 일회용 보안토큰을 이용하여 인증을 위한 검증을 수행하고, 웹 상에서 서비스 이용을 위한 재 로그인 시 양방향 암호화가 적용된 로그인 유지 보안토큰의 검증을 통해 인증을 수행하는 보안토큰을 이용한 인증 방법, 이를 위한 시스템 및 장치에 관한 것이다.

배경기술

- [2] 이동통신망의 발달과 통신 기술의 발달에 따라서, 유무선 통신망을 기반으로 다양한 서비스들이 제공되고 있으나, 다양한 서비스 별로 사용자 ID 체계가 분산 관리되고 있기 때문에, 고객의 편의성 저하, 정보 보안 및 법규 준수의 어려움, 신규 서비스의 도입과 서비스간 연계 저해 등의 문제가 발생하고, 다양한 서비스의 사용자 ID에 대한 통합의 필요성이 대두되고 있으며, 이에 하나의 통합된 ID를 관리하는 통합 ID 관리 시스템(가칭)에 대한 개발이 이루어지고 있다.
- [3] 이러한, 통합 ID 관리 시스템의 구축에 있어서, 사용자 ID 통합은 서비스 별로 다양한 회원 정책(회원 자격/범위, 회원 확인 방식 등)을 수용할 수 있는 융통성, 운영 안정성, 서비스 유지 가능성, 및 향후 확장성 등이 고려되어야 한다.
- [4] 특히, 여러 웹 서비스 혹은 여러 어플리케이션에서의 인증(Authentication)을 통합하여 한번의 인증으로 다수의 웹 서비스나 여러 어플리케이션을 이용할 수 있도록 하기 위하여, 별도의 통합 인증 서버를 구축하여 서로 다른 여러 서비스 혹은 어플리케이션의 인증을 통합 서버를 통해 수행하거나, 단일 인증(SSO: Single Sign on) 기술을 통해서 특정 어플리케이션 또는 서비스에서의 인증 정보를 다른 서비스 혹은 인증 서버로 전달하여, 사용자가 다시 로그인할 필요가 없도록 한다. 이와 관련된 기술은 인증 정보를 전달하는 방식에 따라서, 쿠키, 세션, 인증 토큰, 티켓 등을 이용하는 방식으로 구분 가능하며, 통합 대상에 따라서, 웹 서비스간의 단일 인증, 어플리케이션 간의 단일 인증, 네트워크 접속과 서비스 간 단일 인증 등으로 구분될 수 있다.
- [5] 하지만, 이러한 웹 상(HTTP 환경)의 인증 과정에서 사용되는 인증 정보는 해커들에 의해 복사되거나 중간에 모니터링 되어 악용될 수 있으며, 이럴 경우 사용자의 개인정보가 외부에 노출되는 문제가 발생한다.

발명의 상세한 설명

기술적 과제

- [6] 이러한 종래의 문제점을 해결하기 위하여, 본 발명의 목적은 로직 처리장치

접속 시 일회용 보안토큰을 이용하여 검증을 수행하여 외부의 해킹(cookie hijacking)으로부터 안정성을 유지할 수 있는 보안토큰을 이용한 인증 방법, 이를 위한 시스템 및 장치를 제공하고자 한다.

- [7] 또한, 본 발명의 다른 목적은 서비스 이용을 위한 재 로그인 시 양방향 암호화가 적용된 보안토큰의 검증을 통해 인증을 수행하여 외부의 해킹으로부터 안정성을 유지할 수 있는 보안토큰을 이용한 인증 방법, 이를 위한 시스템 및 장치를 제공하고자 한다.

과제 해결 수단

- [8] 상술한 바와 같은 목적을 달성하기 위한 본 발명의 실시 예에 따른 인증장치는 적어도 하나의 단말기 및 서비스를 제공하는 로직 처리장치와 연결되고, 인증 보안토큰을 이용하여 인증을 수행하고, 로그인 유지 보안토큰을 이용하여 로그인 유지를 하기 위한 데이터를 송수신하는 서비스통신부와, 단말기의 요청에 따라 로그인 인증을 수행하는 통합 ID 관리부와, 로그인에 성공한 경우, 인증 보안토큰을 발행하고, 인증 보안토큰을 메시지에 포함하여 단말기로 전송하는 보안토큰 생성부 및 로직 처리장치로부터 인증 보안토큰에 대한 검증을 요청 받으면, 인증 보안토큰에 대한 검증을 수행하고, 인증 보안토큰이 검증된 경우, 회원정보 조회 키 값을 적용하여 로직 처리장치로 회원정보를 제공하는 보안토큰 검증부를 포함하는 것을 특징으로 한다.
- [9] 또한, 본 발명에 따른 인증장치에 있어서, 인증 보안토큰은 보안토큰 생성부를 통해 발행되고, 로직 처리장치의 최초 검증 요청 시에만 유효하도록 설정된 일회용 보안토큰인 것을 특징으로 한다.
- [10] 또한, 본 발명에 따른 인증장치에 있어서, 로그인 유지 보안토큰은 아이디 인증 시마다 재발급되는 제1 인증 값과, 특정 아이디로 로그인 인증을 수행하기 위한 사용자 프로파일에 대한 정보를 포함하는 제2 인증 값으로 구성되는 것을 특징으로 한다.
- [11] 또한, 본 발명에 따른 인증장치에 있어서, 보안토큰 생성부는 로그인에 성공하면 로그인 유지 보안토큰을 발행하여 단말기로 전송하고, 재 로그인 인증 요청에 따라 로그인 유지 보안토큰의 인증 값을 변경하여 단말기로 전송하는 것을 특징으로 한다.
- [12] 또한, 본 발명에 따른 인증장치에 있어서, 보안토큰 검증부는 단말기로부터 로직 처리장치의 재 로그인 인증을 위한 로그인 유지 보안토큰에 대한 검증이 요청되면, 로그인 유지 보안토큰에 대한 검증을 수행하는 것을 특징으로 한다.
- [13] 또한, 본 발명에 따른 인증장치에 있어서, 보안토큰 검증부는 로직 처리장치로부터 수신된 인증 보안토큰에 대한 최초 검증 요청 여부를 확인하고, 인증 보안토큰이 최초 검증 요청된 보안토큰인 경우, 단말기와 연관된 회원정보 조회 키 값을 생성하여 로직 처리장치로 제공하는 것을 특징으로 한다.
- [14] 본 발명의 실시 예에 따른 단말기는 서비스를 제공하는 로직 처리장치 및

인증장치와 통신하고, 인증 보안토큰을 이용하여 인증을 수행하고, 로그인 유지 보안토큰을 이용하여 로그인 유지를 수행하기 위한 데이터를 송수신하는 통신부 및 로직 처리장치에 접속하여 로그인 인증을 수행하고, 로그인에 성공한 경우, 인증장치로부터 인증 보안토큰을 포함하는 메시지를 수신하고, 수신된 메시지를 분석하여 확인되는 인증 보안토큰을 로직 처리장치로 전송하고, 인증 보안토큰의 검증 결과에 따라 로직 처리장치로부터 제공되는 다수의 서비스를 이용하도록 제어하는 제어부를 포함하는 것을 특징으로 한다.

[15] 또한, 본 발명에 따른 단말기에 있어서, 인증장치로부터 수신된 메시지를 분석하여 확인되는 인증 보안토큰 및 재 로그인을 위하여 인증장치로부터 수신되거나, 인증장치로부터 수신된 메시지를 분석하여 확인된 로그인 유지 보안토큰을 저장하는 저장부를 더 포함하는 것을 특징으로 한다.

[16] 또한, 본 발명에 따른 단말기에 있어서, 제어부는 재 로그인 인증을 위한 로그인 유지 보안토큰의 유무를 확인하고, 로그인 유지 보안토큰이 존재하는 경우, 인증장치로 로그인 유지 보안토큰에 대한 검증을 요청하고, 로그인 유지 보안토큰의 검증이 완료되면, 로그인 유지 보안토큰을 기반으로 재 로그인 인증을 수행하고, 재 로그인 인증에 상응하여 인증장치로부터 변경된 인증 값을 가지는 로그인 유지 보안토큰을 수신하는 것을 특징으로 한다.

[17] 본 발명의 실시 예에 따른 보안토큰을 이용한 인증 시스템은 로직 처리장치에 접속하여 로그인 인증을 수행하고, 로그인에 성공한 경우, 인증장치로부터 인증 보안토큰을 포함하는 메시지를 수신하고, 수신된 메시지를 분석하여 확인되는 보안토큰을 로직 처리장치로 전송하고, 인증 보안토큰의 검증 결과에 따라 로직 처리장치로부터 제공되는 다수의 서비스를 이용하는 단말기 및 단말기의 요청에 따라 로직 처리장치에 접속하기 위한 로그인 인증을 수행하고, 로그인에 성공한 경우, 인증 보안토큰을 발행한 후에 보안토큰을 메시지에 포함하여 단말기로 전송하고, 로직 처리장치로부터 인증 보안토큰에 대한 검증을 요청 받으면, 인증 보안토큰에 대한 검증을 수행하고, 인증 보안토큰이 검증된 경우, 회원정보 조회 키 값을 적용하여 로직 처리장치로 회원정보를 제공하는 인증장치를 포함하는 것을 특징으로 한다.

[18] 또한, 본 발명에 따른 보안토큰을 이용한 인증 시스템에 있어서, 단말기는 재 로그인 인증을 위한 로그인 유지 보안토큰의 유무를 확인하고, 로그인 유지 보안토큰이 존재하는 경우, 인증장치로 로그인 유지 보안토큰에 대한 검증을 요청하고, 로그인 유지 보안토큰의 검증이 완료되면, 로그인 유지 보안토큰을 기반으로 재 로그인 인증을 수행하고, 재 로그인 인증에 상응하여 인증장치로부터 변경된 인증 값을 가지는 로그인 유지 보안토큰을 수신하는 것을 특징으로 한다.

[19] 또한, 본 발명에 따른 보안토큰을 이용한 인증 시스템에 있어서, 인증장치는 단말기의 요청에 따라 로그인 인증을 수행하고, 로그인에 성공한 경우, 로그인 유지 보안토큰을 발행하고, 단말기로부터 재 로그인 인증을 위한 로그인 유지

보안토큰에 대한 검증이 요청되면, 로그인 유지 보안토큰에 대한 검증을 수행하고, 로그인 유지 보안토큰의 검증이 완료되면, 로그인 유지 보안토큰의 인증 값을 변경하고, 변경된 인증 값을 가지는 로그인 유지 보안토큰을 단말기로 전송하는 것을 특징으로 한다.

- [20] 또한, 본 발명에 따른 보안토큰을 이용한 인증 시스템에 있어서, 단말기의 요청에 따라 인증 보안토큰에 대한 검증을 인증장치로 요청하고, 인증장치의 검증 결과에 따라 단말기와 연관된 회원정보를 조회하는 로직 처리장치를 더 포함하는 것을 특징으로 한다.
- [21] 본 발명의 실시 예에 따른 보안토큰을 이용한 인증 방법은 단말기가 재 로그인 인증을 위한 로그인 유지 보안토큰의 유무를 확인하는 단계와, 로그인 유지 보안토큰이 존재하는 경우, 단말기가 인증장치로 로그인 유지 보안토큰에 대한 검증을 요청하는 단계와, 로그인 유지 보안토큰의 검증이 완료되면, 단말기가 로그인 유지 보안토큰을 기반으로 재 로그인 인증을 수행하는 단계 및 단말기가 재 로그인 인증에 상응하여 인증장치로부터 변경된 인증 값을 가지는 로그인 유지 보안토큰을 수신하는 단계를 포함하는 것을 특징으로 한다.
- [22] 또한, 본 발명에 따른 보안토큰을 이용한 인증 방법에 있어서, 확인하는 단계 이전에, 단말기가 로직 처리장치에 접속하여 로그인 인증을 수행하는 단계와, 로그인에 성공한 경우, 단말기가 인증장치로부터 로그인 유지 보안토큰을 수신하는 단계 및 단말기가 수신된 로그인 유지 보안토큰을 저장하는 단계를 더 포함하는 것을 특징으로 한다.
- [23] 또한, 본 발명에 따른 보안토큰을 이용한 인증 방법에 있어서, 확인하는 단계는 로그인 유지 보안토큰이 존재하지 않으면, 단말기가 아이디와 비밀번호를 이용하여 로그인 인증을 수행하기 위한 입력화면을 출력하는 단계를 더 포함하는 것을 특징으로 한다.
- [24] 또한, 본 발명에 따른 보안토큰을 이용한 인증 방법에 있어서, 수신하는 단계 이후에, 단말기가 특정 인증 값이 변경된 로그인 유지 보안토큰을 기존의 로그인 유지 보안토큰을 대체하여 저장하는 단계를 더 포함하는 것을 특징으로 한다.
- [25] 본 발명의 실시 예에 따른 보안토큰을 이용한 인증 방법은 인증장치가 적어도 하나의 단말기의 요청에 따라 서비스를 제공하는 로직 처리장치에 접속하기 위한 로그인 인증을 수행하는 단계와, 로그인에 성공한 경우, 인증장치가 로그인 유지 보안토큰을 발행하는 단계와, 단말기로부터 서비스를 제공하는 로직 처리장치로의 재 로그인 인증을 위한 로그인 유지 보안토큰에 대한 검증이 요청되면, 인증장치가 로그인 유지 보안토큰에 대한 검증을 수행하는 단계와, 로그인 유지 보안토큰의 검증이 완료되면, 인증장치가 로그인 유지 보안토큰의 인증 값을 변경하는 단계 및 인증장치가 변경된 인증 값을 가지는 로그인 유지 보안토큰을 단말기로 전송하는 단계를 포함하는 것을 특징으로 한다.
- [26] 또한, 본 발명에 따른 보안토큰을 이용한 인증 방법에 있어서, 로그인 인증을 수행하는 단계는 인증장치가 아이디와 비밀번호의 입력 화면을 제공하는 단계

및 인증장치가 단말기로부터 아이디와 비밀번호를 수신하고, 수신된 아이디와 비밀번호를 확인하는 단계를 포함하는 것을 특징으로 한다.

[27] 또한, 본 발명에 따른 보안토큰을 이용한 인증 방법에 있어서, 보안토큰에 대한 검증을 수행하는 단계는 인증장치가 단말기 별로 기 발행된 로그인 유지 보안토큰과 특정 단말기로부터 검증이 요청된 로그인 유지 보안토큰의 일치 여부를 확인하는 것을 특징으로 한다.

[28] 또한, 본 발명에 따른 보안토큰을 이용한 인증 방법에 있어서, 보안토큰에 대한 검증을 수행하는 단계는 로그인 유지 보안토큰에 대한 검증에 실패한 경우, 인증장치가 단말기로 경고 메시지를 전송하는 단계를 더 포함하는 것을 특징으로 한다.

[29] 또한, 본 발명에 따른 보안토큰을 이용한 인증 방법에 있어서, 변경하는 단계는 인증장치가 로그인 유지 보안토큰을 구성하는 제1 인증 값과 제2 인증 값 중에서 제1 인증 값을 적어도 하나의 연산 방식을 적용하여 변경하는 것을 특징으로 한다.

[30] 본 발명의 실시 예에 따른 보안토큰을 이용한 인증 방법에 있어서, 단말기가 특정 로직 처리장치에 접속하여 로그인 인증을 수행하는 단계와, 단말기가 로그인에 성공한 경우, 인증장치로부터 인증 보안토큰을 포함하는 메시지를 수신하는 단계와, 단말기가 수신된 메시지를 분석하여 인증 보안토큰을 확인하는 단계와, 단말기가 인증 보안토큰을 로직 처리장치로 전송하는 단계 및 단말기가 인증 보안토큰의 검증 결과에 따라 로직 처리장치로부터 제공되는 다수의 서비스를 이용하는 단계를 포함하는 것을 특징으로 한다.

[31] 또한, 본 발명에 따른 보안토큰을 이용한 인증 방법에 있어서, 확인하는 단계는 단말기가 인증장치로부터 수신된 메시지에 포함된 서비스 제공 사이트 코드 정보, 인증 보안토큰이 전송될 URL 정보, 국내 또는 외국 사이트 구분 코드 정보, 인증 보안토큰 중 하나 이상에 해당하는 정보를 확인하는 것을 특징으로 한다.

[32] 또한, 본 발명에 따른 보안토큰을 이용한 인증 방법에 있어서, 확인하는 단계 이후에, 단말기가 메시지에 포함된 보안토큰을 저장하는 단계를 더 포함하는 것을 특징으로 한다.

[33] 본 발명의 실시 예에 따른 보안토큰을 이용한 인증 방법은 인증장치가 적어도 하나의 단말기의 요청에 따라 특정 로직 처리장치에 접속하기 위한 로그인 인증을 수행하는 단계와, 로그인에 성공한 경우, 인증장치가 인증 보안토큰을 발행하는 단계와, 인증장치가 인증 보안토큰을 메시지에 포함하여 단말기로 전송하는 단계와, 인증장치가 로직 처리장치로부터 인증 보안토큰에 대한 검증을 요청 받으면, 인증 보안토큰에 대한 검증을 수행하는 단계 및 인증 보안토큰이 검증된 경우, 인증장치가 회원정보 조회 키 값을 적용하여 로직 처리장치로 회원정보를 제공하는 단계를 포함하는 것을 특징으로 한다.

[34] 또한, 본 발명에 따른 보안토큰을 이용한 인증 방법에 있어서, 로그인 인증을 수행하는 단계는 인증장치가 로직 처리장치로의 접속 요청에 따라 아이디와

비밀번호의 입력 화면을 제공하는 단계 및 인증장치가 단말기로부터 아이디와 비밀번호를 수신하고, 수신된 아이디와 비밀번호를 확인하는 단계를 포함하는 것을 특징으로 한다.

- [35] 또한, 본 발명에 따른 보안토큰을 이용한 인증 방법에 있어서, 보안토큰에 대한 검증을 수행하는 단계는 인증장치가 로직 처리장치로부터 수신된 인증 보안토큰에 대한 최초 검증 요청 여부를 확인하는 단계와, 인증 보안토큰이 최초 검증 요청된 보안토큰인 경우, 인증장치가 단말기와 연관된 회원정보 조회 키 값을 생성하는 단계를 포함하는 것을 특징으로 한다.
- [36] 또한, 본 발명에 따른 보안토큰을 이용한 인증 방법에 있어서, 인증 보안토큰에 대한 검증을 수행하는 단계는 인증 보안토큰이 최초 검증 요청된 인증 보안토큰이 아닌 경우, 인증장치가 로직 처리장치로 경고 메시지를 전송하는 단계를 더 포함하는 것을 특징으로 한다.
- [37] 또한, 본 발명에 따른 보안토큰을 이용한 인증 방법에 있어서, 제공하는 단계는 인증장치가 로직 처리장치로부터 회원정보 조회 키 값과 관련된 회원정보의 조회를 요청 받는 단계와, 인증장치가 요청에 따라 회원정보를 조회하는 단계 및 인증장치가 조회된 결과를 로직 처리장치로 전송하는 단계를 포함하는 것을 특징으로 한다.
- [38] 본 발명의 과제 해결을 위한 또 다른 수단으로서, 재 로그인 인증을 위한 로그인 유지 보안토큰의 유무를 확인하는 단계와, 보안토큰이 존재하는 경우, 인증장치로 로그인 유지 보안토큰에 대한 검증을 요청하는 단계와, 로그인 유지 보안토큰의 검증이 완료되면, 로그인 유지 보안토큰을 기반으로 재 로그인 인증을 수행하는 단계 및 재 로그인 인증에 상응하여 인증장치로부터 변경된 인증 값을 가지는 로그인 유지 보안토큰을 수신하는 단계를 실행하는 프로그램을 기록한 컴퓨터 판독 가능한 기록매체를 제공한다.
- [39] 본 발명의 과제 해결을 위한 또 다른 수단으로서, 적어도 하나의 단말기의 요청에 따라 서비스를 제공하는 로직 처리장치에 접속하기 위한 로그인 인증을 수행하는 단계와, 로그인에 성공한 경우, 로그인 유지 보안토큰을 발행하는 단계와, 단말기로부터 로직 처리장치로의 재 로그인 인증을 위한 로그인 유지 보안토큰에 대한 검증이 요청되면, 로그인 유지 보안토큰에 대한 검증을 수행하는 단계와, 로그인 유지 보안토큰의 검증이 완료되면, 로그인 유지 보안토큰의 인증 값을 변경하는 단계 및 변경된 인증 값을 가지는 로그인 유지 보안토큰을 단말기로 전송하는 단계를 실행하는 프로그램을 기록한 컴퓨터 판독 가능한 기록매체를 제공한다.
- [40] 본 발명의 과제 해결을 위한 또 다른 수단으로서, 특정 로직 처리장치에 접속하여 로그인 인증을 수행하는 단계와, 로그인에 성공한 경우, 인증장치로부터 인증 보안토큰을 포함하는 메시지를 수신하는 단계와, 수신된 메시지를 분석하여 인증 보안토큰을 확인하는 단계와, 보안토큰을 로직 처리장치로 전송하는 단계 및 인증 보안토큰의 검증 결과에 따라 로직

처리장치로부터 제공되는 다수의 서비스를 이용하는 단계를 실행하는 프로그램을 기록한 컴퓨터 판독 가능한 기록매체를 제공한다.

- [41] 본 발명의 과제 해결을 위한 또 다른 수단으로서, 적어도 하나의 단말기의 요청에 따라 특정 로직 처리장치에 접속하기 위한 로그인 인증을 수행하는 단계와, 로그인에 성공한 경우, 인증 보안토큰을 발행하는 단계와, 인증 보안토큰을 메시지에 포함하여 단말기로 전송하는 단계와, 로직 처리장치로부터 인증 보안토큰에 대한 검증을 요청 받으면, 인증 보안토큰에 대한 검증을 수행하는 단계 및 인증 보안토큰이 검증된 경우, 회원정보 조회 값을 적용하여 로직 처리장치로 회원정보를 제공하는 단계를 실행하는 프로그램을 기록한 컴퓨터 판독 가능한 기록매체를 제공한다.

발명의 효과

- [42] 본 발명에 따르면, 서비스 이용을 위한 재 로그인 시 양방향 암호화가 적용된 보안토큰의 검증을 통해 인증을 수행함으로써, 외부의 해킹(cookie hijacking)으로부터 보안성을 높일 수 있다.
- [43] 또한, 보안토큰을 구하는 인증 값을 다양한 연산 방식을 적용하여 변경할 수 있기 때문에, 인증 절차 상의 안정성이 보장된다.
- [44] 또한, 쿠키 방식의 인증 과정에서 노출되는 보안 또는 인증 정보를 일회용 보안토큰을 활용하여 토큰 길이, 데이터 손실 및 사용량을 줄일 수 있고, 데이터 전송 및 이동 속도를 향상시킬 수 있다.
- [45] 또한, 일회용 보안토큰을 이용하여 인증을 수행함으로써, 외부의 해킹 으로부터 보안성을 높일 수 있다.

도면의 간단한 설명

- [46] 도 1은 본 발명의 실시 예에 따른 보안토큰을 이용한 인증 시스템을 나타내는 도면이다.
- [47] 도 2는 본 발명에 따른 단말기의 구성을 나타내는 블록도 이다.
- [48] 도 3은 본 발명에 따른 인증장치의 구성을 나타내는 블록도 이다.
- [49] 도 4는 본 발명의 실시 예에 따른 보안토큰을 이용한 인증 과정을 설명하기 위한 데이터 흐름도이다.
- [50] 도 5는 본 발명의 실시 예에 따른 단말기의 동작 방법을 설명하기 위한 흐름도이다.
- [51] 도 6 및 도 7은 본 발명의 실시 예에 따른 인증장치의 동작 방법을 설명하기 위한 흐름도이다.
- [52] 도 8은 본 발명의 다른 실시 예에 따른 로그인 유지 시 보안토큰을 이용한 인증 과정을 설명하기 위한 데이터 흐름도이다.
- [53] 도 9는 본 발명의 다른 실시 예에 따른 단말기의 동작 방법을 설명하기 위한 흐름도이다.
- [54] 도 10은 본 발명의 다른 실시 예에 따른 인증장치의 동작 방법을 설명하기 위한

흐름도이다.

발명의 실시를 위한 형태

- [55] 이하 본 발명의 바람직한 실시 예를 첨부한 도면을 참조하여 상세히 설명한다. 다만, 하기의 설명 및 첨부된 도면에서 본 발명의 요지를 흐릴 수 있는 공지 기능 또는 구성에 대한 상세한 설명은 생략한다. 또한, 도면 전체에 걸쳐 동일한 구성 요소들은 가능한 한 동일한 도면 부호로 나타내고 있음에 유의하여야 한다.
- [56] 이하에서 설명되는 본 명세서 및 청구범위에 사용된 용어나 단어는 통상적이거나 사전적인 의미로 한정해서 해석되어서는 아니 되며, 발명자는 그 자신의 발명을 가장 최선의 방법으로 설명하기 위한 용어의 개념으로 적절하게 정의할 수 있다는 원칙에 입각하여 본 발명의 기술적 사상에 부합하는 의미와 개념으로 해석되어야만 한다. 따라서 본 명세서에 기재된 실시 예와 도면에 도시된 구성은 본 발명의 가장 바람직한 일 실시 예에 불과할 뿐이고, 본 발명의 기술적 사상을 모두 대변하는 것은 아니므로, 본 출원시점에 있어서 이들을 대체할 수 있는 다양한 균등물과 변형 예들이 있을 수 있음을 이해하여야 한다.
- [57] 이하에서는 본 발명의 실시 예에 따른 단말기는 통신망에 연결되어 일회용 보안토큰을 이용하여 인증을 수행하거나, 서비스 이용을 위한 재 로그인 시 보안토큰을 이용하여 인증을 수행할 수 있는 이동통신단말기를 대표적인 예로서 설명하지만 단말기는 이동통신단말기에 한정된 것이 아니고, 모든 정보통신기기, 멀티미디어 단말기, 유선/무선 단말기, 고정형 단말기 및 IP(Internet Protocol) 단말기 등의 다양한 단말기에 적용될 수 있다. 특히, 운영체제로는 iOS, 안드로이드(Android), 심비안(Symbian), 바다(Bada) 등의 모바일 운영체제가 포함될 수 있고, 이러한 조건들을 합쳐서 모바일 환경이 형성될 수 있다. 또한, 단말기는 휴대폰, PMP(Portable Multimedia Player), MID(Mobile Internet Device), 스마트폰(Smart Phone), 데스크톱(Desktop), 태블릿컴퓨터(Tablet PC), 노트북(Note book), 넷북(Net book), 서버(Server) 및 정보통신 기기 등과 같은 다양한 이동통신 사양을 갖는 모바일(Mobile) 단말기일 때 유리하게 활용될 수 있다.
- [58] 도 1은 본 발명의 실시 예에 따른 보안토큰을 이용한 인증 시스템을 나타내는 도면이다.
- [59] 도 1을 참조하면, 본 발명에 따른 보안토큰을 이용한 인증 시스템(100)은 단말기(10), 로직 처리장치(20), 인증장치(30) 및 통신망(40)으로 구성된다.
- [60] 통신망(40)은 단말기(10), 로직 처리장치(20) 및 인증장치(30) 사이의 데이터 전송 및 정보 교환을 위한 일련의 데이터 송수신 동작을 수행한다. 특히, 통신망(40)은 다양한 형태의 통신망이 이용될 수 있으며, 예컨대, 무선랜(WLAN, Wireless LAN), 와이파이(Wi-Fi), 와이브로(Wibro), 와이맥스(Wimax), 고속하향패킷접속(HSDPA, High Speed Downlink Packet Access) 등의 무선 통신방식 또는 이더넷(Ethernet), xDSL(ADSL, VDSL), HFC(Hybrid Fiber Coax),

FTTC(Fiber to The Curb), FTTH(Fiber To The Home) 등의 유선 통신방식이 이용될 수 있다. 한편, 통신망(40)은 상기에 제시된 통신방식에 한정되는 것은 아니며, 상술한 통신 방식 이외에도 기타 널리 공지되었거나 향후 개발될 모든 형태의 통신 방식을 포함할 수 있다.

- [61] 단말기(10)는 통신망(40)을 통해 로직 처리장치(20) 및 인증장치(30)와 연결되어 인증 보안토큰을 이용하여 인증을 수행하기 위한 모든 데이터를 송수신한다. 특히, 본 발명의 실시 예에 따른 단말기(10)는 서비스 URL을 이용하여 로직 처리장치(20)에 접속하여 로그인 인증을 수행한다. 로그인에 성공한 경우, 단말기(10)는 인증장치(30)로부터 인증 보안토큰을 포함하는 메시지를 수신하고, 수신된 메시지를 분석하여 확인되는 인증 보안토큰을 로직 처리장치(20)로 전송한다. 그리고, 단말기(10)는 인증 보안토큰의 검증 결과에 따라 로직 처리장치(20)로부터 제공되는 다수의 서비스를 이용한다.
- [62] 또한, 본 발명의 다른 실시 예에 따른 단말기(10)는 통신망(40)을 통해 로직 처리장치(20) 및 인증장치(30)와 연결되어 로그인 유지 보안토큰을 이용하여 인증을 수행하기 위한 모든 데이터를 송수신한다. 특히, 본 발명의 실시 예에 따른 단말기(10)는 서비스 이용을 위해 인증장치(30)에 접속하여 로그인 인증을 수행한다.
- [63] 단말기(10)는 서비스 이용을 위해 재 로그인 요청 시, 재 로그인 인증을 위한 로그인 유지 보안토큰의 유무를 확인한다. 로그인 유지 보안토큰이 존재하는 경우, 단말기(10)는 인증장치(30)로 로그인 유지 보안토큰에 대한 검증을 요청한다. 그리고, 단말기(10)는 로그인 유지 보안토큰의 검증이 완료되면, 로그인 유지 보안토큰을 기반으로 재 로그인 인증을 수행한다. 이때, 단말기(10)는 재 로그인 인증에 상응하여 인증장치(30)로부터 변경된 인증 값을 가지는 로그인 유지 보안토큰을 수신한다. 여기서, 로그인 유지 보안토큰은 아이디 인증 시마다 재발급되는 제1 인증 값과, 특정 아이디로 로그인 인증을 수행하기 위한 사용자 프로파일에 대한 정보를 포함하는 제2 인증 값으로 구성된다.
- [64] 인증장치(30)는 통신망(40)을 통해 단말기(10) 및 로직 처리장치(20)와 연결되어 인증 보안토큰을 이용하여 인증을 수행하기 위한 모든 데이터를 송수신한다. 특히, 본 발명의 실시 예에 따른 인증장치(30)는 단말기(10)의 요청에 따라 로직 처리장치(20)에 접속하기 위한 로그인 인증을 수행한다. 로그인에 성공한 경우, 인증장치(30)는 인증 보안토큰을 발행한 후, 인증 보안토큰을 메시지에 포함하여 단말기(10)로 전송한다.
- [65] 인증장치(30)는 로직 처리장치(20)로부터 인증 보안토큰에 대한 검증을 요청 받으면, 인증 보안토큰에 대한 검증을 수행한다. 그리고, 인증장치(30)는 인증 보안토큰이 검증된 경우, 회원정보 조회 키 값을 적용하여 로직 처리장치(20)로 회원정보를 제공한다.
- [66] 또한, 본 발명의 다른 실시 예에 따른 인증장치(30)는 통신망(40)을 통해

단말기(10) 및 로직 처리장치(20)와 연결되어 로그인 유지 보안토큰을 이용하여 인증을 수행하기 위한 모든 데이터를 송수신한다. 특히, 본 발명의 실시 예에 따른 인증장치(30)는 단말기(10)의 요청에 따라 로직 처리장치(20)에 접속하기 위한 로그인 인증을 수행한다. 로그인에 성공한 경우, 인증장치(30)는 로그인 유지 보안토큰을 발행한 후, 로그인 유지 보안토큰을 단말기(10)로 전송한다.

[67] 인증장치(30)는 단말기(10)로부터 재 로그인 인증을 위한 로그인 유지 보안토큰에 대한 검증이 요청되면, 로그인 유지 보안토큰에 대한 검증을 수행한다. 그리고, 인증장치(30)는 로그인 유지 보안토큰의 검증이 완료되면, 로그인 유지 보안토큰의 인증 값을 변경한다. 이때, 인증장치(30)는 로그인 유지 보안토큰을 구성하는 제1 인증 값과 제2 인증 값 중에서 제1 인증 값을 다양한 연산 방식을 적용하여 변경할 수 있다. 이후, 인증장치(30)는 변경된 인증 값을 가지는 로그인 유지 보안토큰을 단말기(10)로 전송한다.

[68] 로직 처리장치(20)는 통신망(40)을 통해 단말기(10) 및 인증장치(30)와 연결되어 인증 보안토큰을 이용하여 인증을 수행하기 위한 모든 데이터를 송수신한다. 특히, 본 발명의 실시 예에 따른 로직 처리장치(20)는 단말기(10)의 요청에 따라 인증 보안토큰에 대한 검증을 인증장치(30)로 요청한다. 그리고, 로직 처리장치(20)는 인증장치(30)의 검증 결과에 따라 단말기(10)와 연관된 회원정보를 조회한다.

[69] 또한, 본 발명의 다른 실시 예에 따른 로직 처리장치(20)는 통신망(40)을 통해 단말기(10) 및 인증장치(30)와 연결되어 로그인 유지 보안토큰을 이용하여 인증을 수행하기 위한 모든 데이터를 송수신한다. 특히, 본 발명의 실시 예에 따른 로직 처리장치(20)는 인증장치(30)의 검증 결과에 따라 단말기(10)로 서비스를 제공한다.

[70] 이를 통해, 본 발명은 서비스 이용을 위해 재 로그인 시 양방향 암호화가 적용된 보안토큰의 검증을 통해 인증을 수행함으로써, 외부의 해킹(cookie hijacking)으로부터 보안성을 높일 수 있다. 또한, 일회용 보안토큰을 이용하여 인증을 수행함으로써, 외부의 해킹으로부터 보안성을 높일 수 있다. 또한, 보안토큰을 구성하는 인증 값을 다양한 연산 방식을 적용하여 변경할 수 있기 때문에, 인증 절차 상의 안정성이 보장된다. 또한, 쿠키 방식의 인증 과정에서 노출되는 보안 또는 인증 정보를 일회용 보안토큰을 활용하여 토큰 길이, 데이터 손실 및 사용량을 줄일 수 있고, 데이터 전송 및 이동 속도를 향상시킬 수 있다.

[71] 본 발명에 따르면, 로직 처리장치(20)에 접속하여 서비스를 이용하기 위한 인증 방식으로는 SSO 인증 방식이 적용될 수 있다. 여기서, SSO(Single Sign On) 인증방식은 기본 인증방식, ID 연합(Federation) 인증방식, Assertion 인증방식으로 구분된다. 첫째로, 기본 인증방식은 주로 신규로 시스템을 구축하는 경우나, 사용자 정보를 통합하는 경우에 많이 사용된다. 따라서, 통합 인증 정보 및 통합 로그인 페이지를 중앙 인증 서버에 포함한다. 둘째로, ID 연합 인증방식은 서비스 제공자들 별로 인증정보 관리서버가 존재하여 기존

사용중인 사용자 정보를 그대로 이용하기 위해 사용된다. 따라서, 통합 인증정보 관리서버에는 통합 인증정보가 존재하기 않으며, 다만, 로그인 여부를 중앙 관리하기 위하여 로그인 여부를 알 수 있는 인증 정보를 가지고 있다. 셋째로, Assertion 인증 방식은 기존 서비스 제공자에 사용중인 인증정보와 통합 인증정보를 같이 사용할 경우에 적합한 방식으로, 로그인 페이지를 서비스 제공자가 가지고 있으며, 서비스 제공자에서 로그인 처리 후에 중앙 인증 서버로 강제 로그인 처리를 한다. 이때, 인증 정보가 공존하므로, 인증정보 동기화 작업도 필요하다.

- [72] 또한, 본 발명에 따른 단말기(10)나 인증장치(30)에 탑재되는 프로세서는 본 발명에 따른 방법을 실행하기 위한 프로그램 명령을 처리할 수 있다. 일 구현 예에서, 이 프로세서는 싱글 스레드(Single-threaded) 프로세서일 수 있으며, 다른 구현 예에서 본 프로세서는 멀티 스레드(Multi-threaded) 프로세서일 수 있다. 나아가 본 프로세서는 메모리 혹은 저장 장치 상에 저장된 명령을 처리하는 것이 가능하다.
- [73] 도 2는 본 발명에 따른 단말기의 구성을 나타내는 블록도 이다.
- [74] 도 2를 참조하면, 본 발명에 따른 단말기(10)는 제어부(11), 입력부(12), 표시부(13), 저장부(14) 및 통신부(15)를 포함한다. 여기서, 제어부(11)는 서비스 URL 접속 모듈(11a)을 포함하고, 저장부(14)는 보안토큰(14a)을 포함한다.
- [75] 입력부(12)는 숫자 및 문자 정보 등의 다양한 정보를 입력 받고, 각종 기능을 설정 및 단말기(10)의 기능 제어와 관련하여 입력되는 신호를 제어부(11)로 전달한다. 또한, 입력부(12)는 사용자의 터치 또는 조작에 따른 입력 신호를 발생하는 키패드와 터치패드 중 적어도 하나를 포함하여 구성될 수 있다. 이때, 입력부(12)는 표시부(13)와 함께 하나의 터치패널(또는 터치스크린(touch screen))의 형태로 구성되어 입력과 표시 기능을 동시에 수행할 수 있다. 또한, 입력부(12)는 키보드, 키패드, 마우스, 조이스틱 등과 같은 입력 장치 외에도 향후 개발될 수 있는 모든 형태의 입력 수단이 사용될 수 있다. 특히, 본 발명의 실시 예에 따른 입력부(12)는 로직 처리장치(20) 접속을 위한 아이디(ID)와 비밀번호(PW)를 입력 받아 제어부(11)로 전달한다.
- [76] 표시부(13)는 단말기(10)의 기능 수행 중에 발생하는 일련의 동작상태 및 동작결과 등에 대한 정보를 표시한다. 또한, 표시부(13)는 단말기(10)의 메뉴 및 사용자가 입력한 사용자 데이터 등을 표시할 수 있다. 여기서, 표시부(13)는 액정표시장치(LCD, Liquid Crystal Display), 초박막 액정표시장치(TFT-LCD, Thin Film Transistor LCD), 발광다이오드(LED, Light Emitting Diode), 유기 발광다이오드(OLED, Organic LED), 능동형 유기발광다이오드(AMOLED, Active Matrix OLED), 레티나 디스플레이(Retina Display), 플렉시블 디스플레이(Flexible display) 및 3차원(3 Dimension) 디스플레이 등으로 구성될 수 있다. 이때, 표시부(13)가 터치스크린(Touch screen) 형태로 구성된 경우, 표시부(13)는 입력부(12)의 기능 중 일부 또는 전부를 수행할 수 있다. 본 발명의 실시 예에

따른 표시부(13)는 로직 처리장치(20) 접속을 위해 아이디와 비밀번호를 입력할 수 있는 입력 화면을 출력한다.

- [77] 저장부(14)는 데이터를 저장하기 위한 장치로, 주 기억 장치 및 보조 기억 장치를 포함하고, 단말기(10)의 기능 동작에 필요한 응용 프로그램을 저장한다. 이러한 저장부(14)는 크게 프로그램 영역과 데이터 영역을 포함할 수 있다. 여기서, 단말기(10)는 사용자의 요청에 상응하여 각 기능을 활성화하는 경우, 제어부(11)의 제어 하에 해당 응용 프로그램들을 실행하여 각 기능을 제공하게 된다. 특히, 본 발명에 따른 저장부(14)는 단말기(10)를 부팅시키는 운영체제, 인증장치(30)로부터 제공되는 보안토큰을 확인하는 프로그램, 서비스 이용을 위해 재 로그인을 요청하는 프로그램, 로직 처리장치(20)에 접속하는 프로그램, 인증장치(30)로부터 제공되는 보안토큰이 포함된 메시지를 파싱하는 프로그램 등을 저장한다. 또한, 저장부(14)는 인증장치(30)로부터 제공되는 보안토큰(14a)을 저장한다. 여기서, 보안토큰(14a)은 아이디 인증 시마다 재발급되는 제1 인증 값(Random Value)과, 특정 아이디로 로그인 인증을 수행하기 위한 사용자 프로파일에 대한 정보를 포함하는 제2 인증 값(Unique Value)으로 구성된다. 예를 들어, 보안토큰은 "010abc"로 구성되며, 제2 인증 값이 "0101"이고, 제1 인증 값이 "abc"를 포함할 수 있는데, 이때, 제1 인증 값은 서비스 이용을 위한 재 로그인 시마다 변경될 수 있다. 즉, 첫번째 로그인 시에는 로그인 유지 보안토큰이 "0101abc"로 이용되고, 두번째 로그인 시에는 로그인 유지 보안토큰이 "0101efg"로 이용되고, 세번째 로그인 시에는 로그인 유지 보안토큰이 "0101hij"로 변경될 수 있다.

- [78] 통신부(15)는 로직 처리장치(20) 및 인증장치(30)와 통신망(40)을 통해 데이터를 송수신하기 위한 기능을 수행한다. 여기서, 통신부(15)는 송신되는 신호의 주파수를 상승 변환 및 증폭하는 RF 송신 수단과 수신되는 신호를 저잡음 증폭하고 주파수를 하강 변환하는 RF 수신 수단 등을 포함한다. 이러한 통신부(15)는 무선통신 모듈(미도시) 및 유선통신 모듈(미도시) 중 적어도 하나를 포함할 수 있다. 그리고, 무선통신 모듈은 무선 통신 방법에 따라 데이터를 송수신하기 위한 구성이며, 단말기(10)가 무선 통신을 이용하는 경우, 무선망 통신 모듈, 무선랜 통신 모듈 및 무선랜 통신 모듈 중 어느 하나를 이용하여 데이터를 인증장치(30)로 송수신할 수 있다. 또한, 유선통신 모듈은 유선으로 데이터를 송수신하기 위한 것이다. 유선통신 모듈은 유선을 통해 통신망(40)에 접속하여, 인증장치(30)로 데이터를 송수신할 수 있다. 즉, 단말기(10)는 무선통신 모듈 또는 유선통신 모듈을 이용하여 통신망(40)에 접속하며, 통신망(40)을 통해 인증장치(30)와 데이터를 송수신할 수 있다. 특히, 본 발명의 실시 예에 따른 통신부(15)는 로직 처리장치(20) 및 인증장치(30)와 통신하고, 인증 보안 토큰 또는 로그인 유지 보안토큰을 이용하여 인증을 수행하기 위한 데이터를 송수신한다.

- [79] 제어부(11)는 운영 체제(OS, Operation System) 및 각 구성을 구동시키는

프로세스 장치가 될 수 있다. 특히, 본 발명에 따른 제어부(11)는 서비스 URL을 이용하여 로직 처리장치(20)에 접속하고, 로그인 인증을 수행한다. 로그인에 성공한 경우, 제어부(11)는 인증장치(30)로부터 인증 보안토큰을 포함하는 메시지를 수신한다.

- [80] 제어부(11)는 수신된 메시지를 분석하여 인증 보안토큰을 확인한다. 이때, 제어부(11)는 인증장치(30)로부터 수신된 메시지에 포함된 서비스 제공 사이트 코드 정보, 인증 보안토큰이 전송될 URL 정보, 국내 또는 외국 사이트 구분 코드 정보, 인증 보안토큰 등의 정보를 확인한다. 여기서, 인증 보안토큰은 인증장치(30)를 통해 발행되고, 로직 처리장치(20)의 최초 검증 요청 시에만 유효하도록 설정된 일회용 보안토큰이 된다. 그리고 나서, 제어부(11)는 메시지에 포함된 인증 보안토큰을 저장하여 관리한다.
- [81] 제어부(11)는 인증 보안토큰을 로직 처리장치(20)로 전송한다. 그리고, 제어부(11)는 인증 보안토큰의 검증 결과에 따라 로직 처리장치(20)로부터 제공되는 다수의 서비스를 이용한다.
- [82] 또한, 본 발명의 다른 실시 예에 따른 제어부(11)는 서비스를 제공하는 로직 처리장치(20)에 접속하여 로그인 인증을 수행한다. 로그인에 성공한 경우, 제어부(11)는 인증장치(30)로부터 로그인 유지 보안토큰을 수신한다. 여기서, 로그인 유지 보안토큰은 아이디 인증 시마다 재발급되는 제1 인증 값(Random Value)과, 특정 아이디로 로그인 인증을 수행하기 위한 사용자 프로파일에 대한 정보를 포함하는 제2 인증 값(Unique Value)으로 구성된다. 그리고, 제어부(11)는 인증장치(30)로부터 수신된 로그인 유지 보안토큰을 저장한다.
- [83] 제어부(11)는 재 로그인 인증을 위한 로그인 유지 보안토큰의 유무를 확인한다. 로그인 유지 보안토큰이 존재하는 경우, 제어부(11)는 인증장치(30)로 로그인 유지 보안토큰에 대한 검증을 요청한다. 한편, 로그인 유지 보안토큰이 존재하지 않으면, 제어부(11)는 아이디와 비밀번호를 이용하여 로그인 인증을 수행하기 위한 입력화면을 출력한다.
- [84] 로그인 유지 보안토큰의 검증이 완료되면, 제어부(11)는 로그인 유지 보안토큰을 기반으로 재 로그인 인증을 수행한다. 그리고, 제어부(11)는 재 로그인 인증에 상응하여 인증장치(30)로부터 변경된 인증 값을 가지는 로그인 유지 보안토큰을 수신한다. 이후, 제어부(11)는 특정 인증 값이 변경된 로그인 유지 보안토큰을 기존의 보안토큰을 대체하여 저장한다.
- [85] 이와 같은 단말기(10)의 기능을 보다 효과적으로 수행하기 위하여, 제어부(11)는 서비스 URL 접속 모듈(11a)을 포함한다. 특히, 서비스 URL 접속 모듈(11a)은 로직 처리장치(20) 및 인증장치(30)를 통해 제공되는 보안토큰을 이용하여 인증을 수행하기 위한 기능을 지원한다.
- [86] 도 3은 본 발명에 따른 인증장치의 구성을 나타내는 블록도 이다.
- [87] 도 3을 참조하면, 본 발명에 따른 인증장치(30)는 통합 ID 관리부(31), 보안토큰 발행부(32), 보안토큰 검증부(33), 서비스저장부(34) 및 서비스통신부(35)로

구성된다. 여기서, 서비스저장부(22)는 통합 ID 정보(34a), 보안토큰(34b) 및 회원 정보(34c)를 포함한다.

- [88] 서비스통신부(35)는 단말기(10) 및 로직 처리장치(20)와 연결되고, 보안토큰을 이용하여 인증을 수행하기 위한 데이터를 송수신한다.
- [89] 서비스저장부(34)는 인증장치(30)의 기능을 수행하기 위한 프로그램 및 데이터가 저장된다. 특히, 서비스저장부(34)는 단말기(10)의 아이디와 비밀번호를 이용하여 로그인을 수행하기 위한 통합 ID 정보(34a), 단말기(10)의 인증을 수행하기 위한 보안토큰(34b) 및 단말기(10)의 사용자에 대한 회원정보(34c) 등을 저장한다.
- [90] 통합 ID 관리부(31)는 단말기(10)의 요청에 따라 로직 처리장치(20)에 접속하기 위한 로그인 인증을 수행한다. 여기서, 통합 ID 관리부(31)는 로직 처리장치(20)로의 접속 요청에 따라 아이디와 비밀번호의 입력 화면을 제공하고, 단말기(10)로부터 아이디와 비밀번호를 수신하면, 수신된 아이디와 비밀번호를 확인한다.
- [91] 보안토큰 생성부(32)는 단말기(10)의 아이디와 비밀번호를 인증하여 로그인에 성공한 경우, 인증 보안토큰을 발행하고, 인증 보안토큰을 메시지에 포함하여 단말기(10)로 전송한다. 여기서, 인증 보안토큰은 로직 처리장치(20)의 최초 검증 요청 시에만 유효하도록 설정된 일회용 보안토큰이 된다.
- [92] 보안토큰 생성부(32)는 단말기(10)의 아이디와 비밀번호를 인증하여 로그인에 성공한 경우, 로그인 유지 보안토큰을 발행하고, 로그인 유지 보안토큰을 단말기(10)로 전송한다. 여기서, 로그인 유지 보안토큰은 아이디 인증 시마다 재발급되는 제1 인증 값(Random Value)과, 특정 아이디로 로그인 인증을 수행하기 위한 사용자 프로파일에 대한 정보를 포함하는 제2 인증 값(Unique Value)으로 구성된다.
- [93] 보안토큰 생성부(32)는 단말기(10)로부터 수신되는 서비스 이용을 위한 재 로그인 인증 요청에 따라 재 로그인 인증이 완료되면, 로그인 유지 보안토큰의 인증 값을 변경하여 단말기(10)로 전송한다. 여기서, 보안토큰 생성부(32)는 로그인 유지 보안토큰을 구성하는 제1 인증 값과 제2 인증 값 중에서 제1 인증 값을 연산 방식을 적용하여 변경할 수 있으며, 연산 방식으로는 +, -, 시프트 등의 다양한 방식이 적용될 수 있다.
- [94] 보안토큰 검증부(33)는 로직 처리장치(20)로부터 수신된 인증 보안토큰에 대한 최초 검증 요청 여부를 확인하고, 인증 보안토큰이 최초 검증 요청된 인증 보안토큰인 경우, 단말기(10)와 연관된 회원정보 조회 키 값을 생성한다. 한편, 보안토큰 검증부(33)는 인증 보안토큰이 최초 검증 요청된 인증 보안토큰이 아닌 경우, 로직 처리장치(20)로 경고 메시지를 전송한다.
- [95] 보안토큰 검증부(33)는 인증 보안토큰이 검증된 경우, 회원정보 조회 키 값을 적용하여 로직 처리장치(20)로 회원정보를 제공한다. 즉, 보안토큰 검증부(33)는 로직 처리장치(20)로부터 회원정보 조회 키 값과 관련된 회원정보의 조회를 요청

받는다. 그리고, 보안토큰 검증부(33)는 요청에 따라 회원정보를 조회하고, 조회된 결과를 로직 처리장치(20)로 전송한다.

- [96] 보안토큰 검증부(33)는 단말기(10)로부터 로그인 유지 보안토큰에 대한 검증을 요청 받으면, 로그인 유지 보안토큰에 대한 검증을 수행한다. 즉, 로그인 유지 보안토큰 검증부(33)는 단말기 별로 기 발행된 로그인 유지 보안토큰과 특정 단말기로부터 검증이 요청된 로그인 유지 보안토큰의 일치 여부를 확인한다. 한편, 보안토큰 검증부(33)는 로그인 유지 보안토큰의 검증에 실패한 경우, 로직 처리장치(20)로 경고 메시지를 전송한다.
- [97] 또한, 상술한 바와 같이 구성되는 인증장치(30)는 서버 기반 컴퓨팅 기반 방식 또는 클라우드 방식으로 동작하는 하나 이상의 서버로 구현될 수 있다. 특히, 클라우드 컴퓨팅 장치를 이용하며, 보안토큰을 적용하여 인증을 수행하기 위한 데이터는 인터넷 상의 클라우드 컴퓨팅 장치에 영구적으로 저장될 수 있는 클라우드 컴퓨팅(Cloud Computing) 기능을 통해 제공될 수 있다. 여기서, 클라우드 컴퓨팅은 데스크톱, 태블릿 컴퓨터, 노트북, 넷북 및 스마트폰 등의 디지털 단말기에 인터넷 기술을 활용하여 가상화된 IT(Information Technology) 자원, 예를 들어, 하드웨어(서버, 스토리지, 네트워크 등), 소프트웨어(데이터베이스, 보안, 웹 서버 등), 서비스, 데이터 등을 온 디맨드(On demand) 방식으로 서비스하는 기술을 의미한다.
- [98] 도 4는 본 발명의 실시 예에 따른 보안토큰을 이용한 인증 과정을 설명하기 위한 데이터 흐름도이다.
- [99] 도 4를 참조하면, 본 발명에 따른 보안토큰을 이용한 인증 과정 상의 데이터 흐름은 먼저, 단말기(10)는 S101 단계에서 서비스 URL을 이용하여 로직 처리장치(20)로 접속한다. URL을 입력하면, 인증장치(30)는 S103 단계에서 해당되는 로직 처리장치(20)와 관련된 아이디 및 비밀번호 입력 화면에 대한 이미지를 단말기(10)로 제공한다. 이후, 단말기(10)는 S105 단계에서 사용자 입력에 따라 입력 화면에 아이디와 비밀번호를 입력 받고, S107 단계에서 이에 대한 정보를 인증장치(30)로 전송한다.
- [100] 인증장치(30)는 단계에서 단말기(10)로부터 수신된 아이디와 비밀번호의 매칭 여부를 확인하여 인증 성공 여부를 판단한다(S109 내지 S111). 그리고, 인증장치(30)는 로그인 인증에 성공한 경우, S113 단계에서 인증 보안토큰을 발행한다. 이때, 인증 보안토큰은 로직 처리장치(20)의 최초 검증 요청 시에만 유효하도록 설정된 일회용 보안토큰이 된다. 이후, 인증장치(30)는 S115 단계에서 인증 보안토큰을 포함하는 메시지를 생성한다. 즉, 메시지는 서비스 제공 사이트 코드 정보, 인증 보안토큰이 전송될 URL 정보, 국내 또는 외국 사이트 구분 코드 정보, 인증 보안토큰 등에 대한 정보를 포함한다.
- [101] 인증장치(30)는 S117 단계에서 생성된 메시지를 단말기(10)로 전송한다. 한편, 인증장치(30)는 아이디와 비밀번호를 이용한 로그인 인증 과정에서 입력된 아이디와 비밀번호가 매칭되지 않는 경우, 로그인 재 요청을 수행할 수 있다.

- [102] 단말기(10)는 S119 단계에서 메시지를 확인한다. 이때, 단말기(10)는 인증장치(30)로부터 수신된 메시지에 포함된 서비스 제공 사이트 코드 정보, 인증 보안토큰이 전송될 URL 정보, 국내 또는 외국 사이트 구분 코드 정보, 인증 보안토큰 등에 대한 정보를 확인한다. 그리고, 단말기(10)는 S121 단계에서 확인된 인증 보안토큰을 저장한다.
- [103] 단말기(10)는 S123 단계에서 로직 처리장치(20)로 인증 보안토큰을 전송한다. 즉, 단말기(10)는 최초 로직 처리장치 접속 시에는 로직 처리장치(20)의 주소정보만을 알고 있으며, 인증장치(30)를 통해 제공되는 인증 보안토큰을 통한 인증을 이용하여 로직 처리장치(20)에 대한 로직 아이피를 확인할 수 있다.
- [104] 인증 보안토큰에 대한 검증이 요청되면, 로직 처리장치(20)는 S125 단계에서 인증 보안토큰에 대한 검증을 인증장치(30)로 요청한다.
- [105] 인증장치(30)는 S127 단계에서 인증 보안토큰을 확인한다. 이때, 인증장치(30)는 S129 단계에서 로직 처리장치(20)로부터 수신된 인증 보안토큰에 대한 최초 검증 요청 여부를 확인한다. 인증 보안토큰이 최초 검증 요청된 인증 보안토큰인 경우, 인증장치(30)는 S131 단계에서 단말기(10)와 연관된 회원정보 조회 키 값을 생성한다. 한편, 최초 검증이 요청된 인증 보안토큰이 아닌 경우, 인증장치(30)는 A단계에서 로직 처리장치(20)로 경고 메시지를 전송할 수 있다.
- [106] 인증장치(30)는 S133 단계에서 회원정보 조회 키 값을 로직 처리장치(20)로 전송한다. 그리고, 로직 처리장치(20)는 S135 단계에서 인증장치(30)로부터 수신된 회원정보 조회 키 값을 저장한다. 여기서, 회원정보 조회 키 값은 일정한 형식에 한정되는 것이 아니고, 다양한 형태의 숫자, 문자, 등의 조합으로 구성될 수 있으며, 회원정보 조회 또는 사용자 프로파일 등의 정보 조회를 요청하는 경우에 이용될 수 있다.
- [107] 로직 처리장치(20)는 S137 단계에서 인증장치(30)로 단말기(10) 사용자에 대한 회원정보 조회를 요청한다. 이때, 로직 처리장치(20)는 인증장치(30)로부터 제공된 회원정보 조회 키 값을 이용하여 회원정보 조회를 요청할 수 있다.
- [108] 회원정보 조회가 요청되면, 인증장치(30)는 S139 단계에서 해당되는 회원의 회원정보를 조회한다. 여기서, 회원정보는 단말기(10) 사용자의 개인정보, 로직 처리장치 이용 정보, 과거 로그인 정보 등의 정보를 포함한다. 그리고, 인증장치(30)는 S141 단계에서 조회된 회원정보를 로직 처리장치(20)로 전송한다.
- [109] 로직 처리장치(20)는 S143 단계에서 인증장치(30)로부터 수신된 회원정보를 확인한다. 이때, 로직 처리장치(20)는 수시로 인증장치(30)에 접속하여 회원정보를 이용할 수 있다.
- [110] 로직 처리장치(20)는 S145 단계에서 단말기(10)로 서비스를 제공한다. 이후, 단말기(10)는 S147 단계에서 로직 처리장치(20)로부터 제공되는 서비스를 이용한다.

- [111] 이를 통해, 본 발명은 일회용 보안토큰을 이용하여 인증을 수행함으로써, 외부의 해킹(cookie hijacking)으로부터 보안성을 높일 수 있다. 또한, 쿠키 방식의 인증 과정에서 노출되는 보안 또는 인증 정보를 일회용 보안토큰을 활용하여 토큰 길이, 데이터 손실 및 사용량을 줄일 수 있고, 데이터 전송 및 이동 속도를 향상시킬 수 있다.
- [112] 도 5는 본 발명의 실시 예에 따른 단말기의 동작 방법을 설명하기 위한 흐름도이다.
- [113] 도 5를 참조하면, 본 발명에 따른 단말기(10)는 S151 단계에서 서비스 URL을 이용하여 로직 처리장치(20)에 접속한다. 그리고, 단말기(10)는 S153 단계에서 URL 접속에 따라 인증장치(30)로부터 해당되는 로직 처리장치(20)와 관련된 아이디 및 비밀번호 입력 화면에 대한 이미지를 수신하고, 수신된 입력 화면을 표시한다. 이후, 단말기(10)는 S155 단계에서 사용자 입력에 따라 입력 화면에 아이디와 비밀번호를 입력 받고, 이에 대한 정보를 인증장치(30)로 전송한다.
- [114] 단말기(10)는 S157 단계에서 아이디 및 비밀번호의 매칭 여부에 따른 로그인 성공 여부를 확인한다. 로그인에 성공한 경우, 단말기(10)는 S159 단계에서 인증장치(30)로부터 인증 보안토큰을 포함하는 메시지를 수신한다. 이때, 인증 보안토큰은 로직 처리장치(20)의 최초 검증 요청 시에만 유효하도록 설정된 일회용 보안토큰이 된다. 또한, 메시지는 서비스 제공 사이트 코드 정보, 인증 보안토큰이 전송될 URL 정보, 국내 또는 외국 사이트 구분 코드 정보, 인증 보안토큰 등에 대한 정보를 포함한다.
- [115] 한편, 단말기(10)는 아이디와 비밀번호를 이용한 로그인 인증 과정에서 입력된 아이디와 비밀번호가 매칭되지 않는 경우, 로그인 재 요청을 위한 입력 화면을 출력한다.
- [116] 단말기(10)는 S161 단계에서 인증장치(30)로부터 수신된 메시지를 확인한다. 단말기(10)는 인증장치(30)로부터 수신된 메시지에 포함된 서비스 제공 사이트 코드 정보, 인증 보안토큰이 전송될 URL 정보, 국내 또는 외국 사이트 구분 코드 정보, 인증 보안토큰 등에 대한 정보를 확인한다. 그리고, 단말기(10)는 S163 단계에서 인증 보안토큰을 저장한다.
- [117] 단말기(10)는 S165 단계에서 로직 처리장치(20)로 인증 보안토큰을 전송한다. 즉, 단말기(10)는 최초 로직 처리장치 접속 시에는 로직 처리장치의 주소정보만을 알고 있으며, 인증장치(30)를 통해 제공되는 인증 보안토큰을 통한 인증을 이용하여 로직 처리장치(20)에 대한 로직 아이피를 확인할 수 있다.
- [118] 단말기(10)는 S167 단계에서 인증 보안토큰 검증에 성공 여부를 확인한다. 즉, 단말기(10)는 인증 보안토큰의 검증이 최초 검증을 요청한 경우에 해당하면, 로직 처리장치(20)와 연결되어 서비스를 이용할 수 있다(S169).
- [119] 도 6 및 도 7은 본 발명의 실시 예에 따른 인증장치의 동작 방법을 설명하기 위한 흐름도이다.
- [120] 도 6 및 도 7을 참조하면, 본 발명에 따른 인증장치(20)는 S181 단계에서

단말기(10)의 특정 사이트 접속 요청에 따라 해당되는 로직 처리장치(20)와 관련된 아이디 및 비밀번호 입력 화면에 대한 이미지를 단말기(10)로 제공한다. 이후, 인증장치(30)는 S183 단계에서 단말기(10)로부터 아이디와 비밀번호를 수신한다.

- [121] 인증장치(30)는 S185 단계에서 단말기(10)로부터 수신된 아이디와 비밀번호의 매칭 여부를 확인하여 인증 성공 여부를 판단한다. 인증에 성공한 경우, 인증장치(30)는 S187 단계에서 인증 보안토큰을 발행한다. 이때, 인증 보안토큰은 로직 처리장치(20)의 최초 검증 요청 시에만 유효하도록 설정된 일회용 보안토큰이 된다. 이후, 인증장치(30)는 S189 단계에서 인증 보안토큰을 포함하는 메시지를 생성한다. 즉, 메시지는 서비스 제공 사이트 코드 정보, 보안토큰이 전송될 URL 정보, 국내 또는 외국 사이트 구분 코드 정보, 보안토큰 등에 대한 정보를 포함한다.
- [122] 인증장치(30)는 S191 단계에서 생성된 메시지를 단말기(10)로 전송한다. 한편, 인증장치(30)는 아이디와 비밀번호를 이용한 로그인 인증 과정에서 입력된 아이디와 비밀번호가 매칭되지 않는 경우, 로그인 재 요청을 수행할 수 있다.
- [123] 인증장치(30)는 S193 단계에서 로직 처리장치(20)로부터 인증 보안토큰에 대한 검증이 요청되는지 확인한다. 인증 보안토큰에 대한 검증이 요청되면, 인증장치(30)는 S195 단계에서 보안토큰을 확인한다.
- [124] 즉, 인증장치(30)는 S197 단계에서 로직 처리장치(20)로부터 수신된 인증 보안토큰에 대한 최초 검증 요청 여부를 판단한다. 인증 보안토큰이 최초 검증 요청된 인증 보안토큰인 경우, 인증장치(30)는 S119 단계에서 단말기(10)와 연관된 회원정보 조회 키 값을 생성하고, 생성된 회원정보 조회 키 값을 로직 처리장치(20)로 전송한다. 여기서, 회원정보 조회 키 값은 일정한 형식에 한정되는 것이 아니고, 다양한 형태의 숫자, 문자, 등의 조합으로 구성될 수 있으며, 회원정보 조회 또는 사용자 프로파일 등의 정보 조회를 요청하는 경우에 이용될 수 있다. 한편, 최초 검증이 요청된 보안토큰이 아닌 경우, 인증장치(30)는 S201 단계에서 로직 처리장치(20)로 경고 메시지를 전송할 수 있다.
- [125] 인증장치(30)는 S203 단계에서 로직 처리장치(20)로부터 단말기(10) 사용자에게 회원정보 조회가 요청되는지 확인한다. 회원정보 조회가 요청되면, 인증장치(30)는 S205 단계에서 해당되는 회원의 회원정보를 조회한다. 여기서, 회원정보는 단말기(10) 사용자의 개인정보, 로직 처리장치 이용 정보, 과거 로그인 정보 등의 정보를 포함한다. 그리고, 인증장치(30)는 S207 단계에서 조회된 회원정보를 로직 처리장치(20)로 전송한다.
- [126] 도 8은 본 발명의 다른 실시 예에 따른 로그인 유지 시 보안토큰을 이용한 인증 과정을 설명하기 위한 데이터 흐름도이다.
- [127] 도 8을 참조하면, 본 발명에 따른 보안토큰을 이용한 인증 과정 상의 데이터 흐름은 먼저, 단말기(10)는 S11 단계에서 서비스를 이용하기 위한 서비스 URL을 접속한다. 서비스 URL을 입력하면, 인증장치(30)는 S13 단계에서 아이디 및

비밀번호 입력 화면에 대한 이미지를 단말기(10)로 제공한다. 이후, 단말기(10)는 S15 단계에서 사용자 입력에 따라 입력 화면에 아이디와 비밀번호를 입력 받고, S17 단계에서 이에 대한 정보를 인증장치(30)로 전송한다.

- [128] 인증장치(30)는 단계에서 단말기(10)로부터 수신된 아이디와 비밀번호의 매칭 여부를 확인하여 인증 성공 여부를 판단한다(S19 내지 S21). 그리고, 인증장치(30)는 로그인 인증에 성공한 경우, 로그인 유지 보안토큰을 발행하고, 로그인 유지 보안토큰을 단말기(10)로 전송한다(S23 내지 S25). 이때, 로그인 유지 보안토큰은 아이디 인증 시마다 재발급되는 제1 인증 값과, 특정 아이디로 로그인 인증을 수행하기 위한 사용자 프로파일에 대한 정보를 포함하는 제2 인증 값으로 구성된다.
- [129] 단말기(10)는 S27 단계에서 인증장치(30)로부터 수신된 로그인 유지 보안토큰을 저장한다.
- [130] 단말기(10)는 서비스를 이용하기 위한 재 로그인 요청 시, 재 로그인 인증을 위한 로그인 유지 보안토큰의 유무를 확인한다. 로그인 유지 보안토큰이 존재하는 경우, 단말기(10)는 S31 단계에서 인증장치(30)로 로그인 유지 보안토큰에 대한 검증을 요청한다.
- [131] 인증장치(30)는 S33 단계에서 단말기(10)로부터 재 로그인 인증을 위한 로그인 유지 보안토큰에 대한 검증이 요청되면, 로그인 유지 보안토큰에 대한 검증을 수행한다. 그리고, 인증장치(30)는 S35 단계에서 검증 성공 여부를 확인한다. 검증에 성공하면, 인증장치(30)는 S37 단계에서 로그인 유지 보안토큰의 인증 값을 변경한다. 이때, 인증장치(30)는 로그인 유지 보안토큰을 구성하는 제1 인증 값과 제2 인증 값 중에서 제1 인증 값을 다양한 연산 방식을 적용하여 변경할 수 있다. 이후, 인증장치(30)는 S39 단계에서 변경된 인증 값을 가지는 로그인 유지 보안토큰을 단말기(10)로 전송한다.
- [132] 한편, 로그인 유지 보안토큰의 검증이 성공하지 않으면, 인증장치(30)는 단말기(10)로 경고 메시지를 전송할 수 있다.
- [133] 단말기(10)는 S41 단계에서 로그인 유지 보안토큰 검증 완료에 따라 재 수신되는 보안토큰을 저장한다. 여기서, 인증장치(30)로부터 수신되는 로그인 유지 보안토큰은 단말기(10)의 재 로그인 인증 요청에 상응하여 인증장치(30)로부터 변경된 인증 값을 가지는 로그인 유지 보안토큰이 되며, 단말기(10)는 특정 인증 값이 변경된 로그인 유지 보안토큰을 기존의 로그인 유지 보안토큰을 대체하여 저장한다. 그리고, 단말기(10)는 S43 단계에서 서비스를 이용한다.
- [134] 이를 통해, 본 발명은 서비스 이용을 위한 재 로그인 시 양방향 암호화가 적용된 보안토큰의 검증을 통해 인증을 수행함으로써, 외부의 해킹(cookie hijacking)으로부터 보안성을 높일 수 있다. 또한, 보안토큰을 구성하는 인증 값을 다양한 연산 방식을 적용하여 변경할 수 있기 때문에, 인증 절차 상의 안정성이 보장된다. 또한, 쿠키 방식의 인증 과정에서 노출되는 보안 또는 인증 정보를

일회용 보안토큰을 활용하여 토큰 길이, 데이터 손실 및 사용량을 줄일 수 있고, 데이터 전송 및 이동 속도를 향상시킬 수 있다.

[135] 도 9는 본 발명의 다른 실시 예에 따른 단말기의 동작 방법을 설명하기 위한 흐름도이다.

[136] 도 9를 참조하면, 본 발명에 따른 단말기(10)는 서비스를 제공하는 로직 처리장치(20)에 접속하여 로그인 인증을 수행한다(S51 내지 S55). 즉, 단말기(10)는 서비스 URL을 접속하고, 서비스 URL 접속에 따라 인증장치(30)로부터 아이디 및 비밀번호 입력 화면에 대한 이미지를 수신하고, 수신된 입력 화면을 표시한다. 이후, 단말기(10)는 사용자 입력에 따라 입력 화면에 아이디와 비밀번호를 입력 받고, 이에 대한 정보를 인증장치(30)로 전송한다.

[137] 단말기(10)는 S57 단계에서 아이디 및 비밀번호의 매칭 여부에 따른 로그인 성공 여부를 확인한다. 로그인에 성공한 경우, 단말기(10)는 S58 단계에서 인증장치(30)로부터 로그인 유지 보안토큰을 수신한다. 여기서, 로그인 유지 보안토큰은 아이디 인증 시마다 재발급되는 제1 인증 값(Random Value)과, 특정 아이디로 로그인 인증을 수행하기 위한 사용자 프로파일에 대한 정보를 포함하는 제2 인증 값(Unique Value)으로 구성된다. 그리고, 단말기(10)는 S59 단계에서 인증장치(30)로부터 수신된 보안토큰을 저장한다.

[138] 단말기(10)는 S61 단계에서 서비스 이용을 위한 재 로그인이 요청되는지 확인한다. 재 로그인이 요청되면, 단말기(10)는 S63 단계에서 인증장치(30)로 로그인 유지 보안토큰 검증을 요청한다. 즉, 단말기(10)는 재 로그인 인증을 위한 보안토큰의 유무를 확인한다. 로그인 유지 보안토큰이 존재하는 경우, 단말기(10)는 인증장치(30)로 로그인 유지 보안토큰에 대한 검증을 요청한다. 한편, 로그인 유지 보안토큰이 존재하지 않으면, 단말기(10)는 아이디와 비밀번호를 이용하여 로그인 인증을 수행하기 위한 입력화면을 출력한다.

[139] 단말기(10)는 S65 단계에서 로그인 유지 보안토큰에 대한 검증 성공 여부를 확인한다. 로그인 유지 보안토큰의 검증이 완료되면, 단말기(10)는 로그인 유지 보안토큰을 기반으로 재 로그인 인증을 수행한다. 즉, 단말기(10)는 S67 단계에서 재 로그인 인증에 상응하여 인증장치(30)로부터 변경된 인증 값을 가지는 로그인 유지 보안토큰을 수신한다. 이후, 단말기(10)는 S69 단계에서 특정 인증 값이 변경된 로그인 유지 보안토큰을 기존의 로그인 유지 보안토큰을 대체하여 저장한다. 그리고, 단말기(10)는 S71 단계에서 서비스를 이용한다.

[140] 도 10은 본 발명의 다른 실시 예에 따른 인증장치의 동작 방법을 설명하기 위한 흐름도이다.

[141] 도 10을 참조하면, 본 발명에 따른 인증장치(30)는 S81 단계에서 단말기(10)의 서비스 URL 접속 요청에 따라 해당되는 로직 처리장치(20)와 관련된 아이디 및 비밀번호 입력 화면에 대한 이미지를 단말기(10)로 제공한다. 이후, 인증장치(30)는 S83 단계에서 단말기(10)로부터 아이디와 비밀번호를 수신한다.

- [142] 인증장치(30)는 S85 단계에서 단말기(10)로부터 수신된 아이디와 비밀번호의 매칭 여부를 확인하여 인증 성공 여부를 판단한다. 인증에 성공한 경우, 인증장치(30)는 S87 단계에서 로그인 유지 보안토큰을 발행하고, 로그인 유지 보안토큰을 단말기(10)로 전송한다. 이때, 로그인 유지 보안토큰은 아이디 인증 시마다 재발급되는 제1 인증 값과, 특정 아이디로 로그인 인증을 수행하기 위한 사용자 프로파일에 대한 정보를 포함하는 제2 인증 값으로 구성된다.
- [143] 인증장치(30)는 S89 단계에서 단말기(10)로부터 로그인 유지 보안토큰에 대한 검증이 요청되는지 확인한다. 단말기(10)로부터 재 로그인 인증을 위한 로그인 유지 보안토큰에 대한 검증이 요청되면, 인증장치(30)는 S91 단계에서 로그인 유지 보안토큰에 대한 검증을 수행한다. 그리고, 인증장치(30)는 S93 단계에서 검증 성공 여부를 확인한다. 검증에 성공하면, 인증장치(30)는 S95 단계에서 로그인 유지 보안토큰의 인증 값을 변경한다. 이때, 인증장치(30)는 로그인 유지 보안토큰을 구성하는 제1 인증 값과 제2 인증 값 중에서 제1 인증 값을 다양한 연산 방식을 적용하여 변경할 수 있다. 예를 들어, 보안토큰은 "0101abc"로 구성되며, 제2 인증 값이 "0101"이고, 제1 인증 값이 "abc"를 포함할 수 있는데, 이때, 제1 인증 값은 로직 처리장치(20)로의 재 로그인 시마다 변경될 수 있다. 즉, 첫번째 로그인 시에는 로그인 유지 보안토큰이 "0101abc"로 이용되고, 두번째 로그인 시에는 로그인 유지 보안토큰이 "0101efg"로 이용되고, 세번째 로그인 시에는 로그인 유지 보안토큰이 "0101hij"로 이용될 수 있다. 여기서, 인증장치(30)는 로그인 유지 보안토큰을 구성하는 제1 인증 값과 제2 인증 값 중에서 제1 인증 값을 연산 방식을 적용하여 변경할 수 있으며, 연산 방식으로는 +, -, 시프트 등의 다양한 방식이 적용될 수 있다.
- [144] 이후, 인증장치(30)는 S97 단계에서 변경된 인증 값을 가지는 로그인 유지 보안토큰을 단말기(10)로 전송한다.
- [145] 한편, 로그인 유지 보안토큰의 검증이 성공하지 않으면, 인증장치(30)는 S99 단계에서 단말기(10)로 경고 메시지를 전송할 수 있다.
- [146] 한편, 단말기(10)나 인증장치(30)에 탑재되는 메모리는 그 장치 내에서 정보를 저장한다. 일 구현예의 경우, 메모리는 컴퓨터로 판독 가능한 매체이다. 일 구현예에서, 메모리는 휘발성 메모리 유닛 일 수 있으며, 다른 구현예의 경우, 메모리는 비휘발성 메모리 유닛 일 수도 있다. 일 구현예의 경우, 저장장치는 컴퓨터로 판독 가능한 매체이다. 다양한 서로 다른 구현예에서, 저장장치는 예컨대 하드디스크 장치, 광학디스크 장치, 혹은 어떤 다른 대용량 저장장치를 포함할 수도 있다.
- [147] 비록 본 명세서와 도면에서는 예시적인 장치 구성을 기술하고 있지만, 본 명세서에서 설명하는 기능적인 동작과 주제의 구현물들은 다른 유형의 디지털 전자 회로로 구현되거나, 본 명세서에서 개시하는 구조 및 그 구조적인 등가물들을 포함하는 컴퓨터 소프트웨어, 펌웨어 혹은 하드웨어로 구현되거나, 이들 중 하나 이상의 결합으로 구현 가능하다. 본 명세서에서 설명하는 주제의

구현물들은 하나 이상의 컴퓨터 프로그램 제품, 다시 말해 본 발명에 따른 장치의 동작을 제어하기 위하여 혹은 이것에 의한 실행을 위하여 유형의 프로그램 저장매체 상에 인코딩된 컴퓨터 프로그램 명령에 관한 하나 이상의 모듈로서 구현될 수 있다. 컴퓨터로 판독 가능한 매체는 기계로 판독 가능한 저장 장치, 기계로 판독 가능한 저장 기판, 메모리 장치, 기계로 판독 가능한 전파형 신호에 영향을 미치는 물질의 조성물 혹은 이들 중 하나 이상의 조합일 수 있다.

- [148] 컴퓨터 프로그램 명령어와 데이터를 저장하기에 적합한 컴퓨터로 판독 가능한 매체는, 예컨대 기록매체는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM(Compact Disk Read Only Memory), DVD(Digital Video Disk)와 같은 광 기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media), 및 롬(ROM, Read Only Memory), 램(RAM, Random Access Memory), 플래시 메모리, EPROM(Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM)과 같은 반도체 메모리를 포함한다. 프로세서와 메모리는 특수 목적의 논리 회로에 의해 보충되거나, 그것에 통합될 수 있다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다. 이러한 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

- [149] 본 명세서는 다수의 특정한 구현물의 세부사항들을 포함하지만, 이들은 어떠한 발명이나 청구 가능한 것의 범위에 대해서도 제한적인 것으로서 이해되어서는 안되며, 오히려 특정한 발명의 특정한 실시형태에 특유할 수 있는 특징들에 대한 설명으로서 이해되어야 한다. 개별적인 실시형태의 문맥에서 본 명세서에 기술된 특정한 특징들은 단일 실시형태에서 조합하여 구현될 수도 있다. 반대로, 단일 실시형태의 문맥에서 기술한 다양한 특징들 역시 개별적으로 혹은 어떠한 적절한 하위 조합으로도 복수의 실시형태에서 구현 가능하다. 나아가, 특징들이 특정한 조합으로 동작하고 초기에 그와 같이 청구된 바와 같이 묘사될 수 있지만, 청구된 조합으로부터의 하나 이상의 특징들은 일부 경우에 그 조합으로부터 배제될 수 있으며, 그 청구된 조합은 하위 조합이나 하위 조합의 변형물로 변경될 수 있다.

- [150] 마찬가지로, 특정한 순서로 도면에서 동작들을 묘사하고 있지만, 이는 바람직한 결과를 얻기 위하여 도시된 그 특정한 순서나 순차적인 순서대로 그러한 동작들을 수행하여야 한다거나 모든 도시된 동작들이 수행되어야 하는 것으로 이해되어서는 안 된다. 특정한 경우, 멀티태스킹과 병렬 프로세싱이 유리할 수 있다. 또한, 상술한 실시형태의 다양한 시스템 컴포넌트의 분리는 그러한 분리를 모든 실시형태에서 요구하는 것으로 이해되어서는 안되며,

설명한 프로그램 컴포넌트와 시스템들은 일반적으로 단일의 소프트웨어 제품으로 함께 통합되거나 다중 소프트웨어 제품에 패키징 될 수 있다는 점을 이해하여야 한다.

- [151] 한편, 본 명세서와 도면에 개시된 본 발명의 실시 예들은 이해를 돕기 위해 특정 예를 제시한 것에 지나지 않으며, 본 발명의 범위를 한정하고자 하는 것은 아니다. 여기에 개시된 실시 예들 이외에도 본 발명의 기술적 사상에 바탕을 둔 다른 변형 예들이 실시 가능하다는 것은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 자명한 것이다.

산업상 이용가능성

- [152] 본 발명은 로직 처리장치 접속 시 일회용 보안토큰을 이용하여 검증을 수행하고, 웹 상에서 서비스 이용을 위한 재 로그인 시 양방향 암호화가 적용된 보안토큰의 검증을 통해 인증을 수행함으로써, 외부의 해킹으로부터 보안성을 높일 수 있다. 또한, 보안토큰을 구성하는 인증 값을 다양한 연산 방식을 적용하여 변경할 수 있기 때문에, 인증 절차 상의 안정성이 보장된다. 또한, 쿠키 방식의 인증 과정에서 노출되는 보안 또는 인증 정보를 일회용 보안토큰을 활용하여 토큰 길이, 데이터 손실 및 사용량을 줄일 수 있고, 데이터 전송 및 이동 속도를 향상시킬 수 있다. 이는 시판 또는 영업의 가능성이 충분할 뿐만 아니라 현실적으로 명백하게 실시할 수 있는 정도이므로 산업상 이용가능성이 있다.

청구범위

- [청구항 1] 적어도 하나의 단말기 및 서비스를 제공하는 로직 처리장치와 연결되고, 인증 보안토큰을 이용하여 인증을 수행하고, 로그인 유지 보안토큰을 이용하여 로그인 유지를 하기 위한 데이터를 송수신하는 서비스통신부;
상기 단말기의 요청에 따라 로그인 인증을 수행하는 통합 ID 관리부;
상기 로그인에 성공한 경우, 인증 보안토큰을 발행하고, 상기 인증 보안토큰을 메시지에 포함하여 상기 단말기로 전송하는 보안토큰 생성부; 및
상기 로직 처리장치로부터 인증 보안토큰에 대한 검증을 요청 받으면, 상기 인증 보안토큰에 대한 검증을 수행하고, 상기 인증 보안토큰이 검증된 경우, 회원정보 조회 키 값을 적용하여 상기 로직 처리장치로 회원정보를 제공하는 보안토큰 검증부;
를 포함하는 것을 특징으로 하는 인증장치.
- [청구항 2] 제1항에 있어서, 상기 인증 보안토큰은
상기 보안토큰 생성부를 통해 발행되고, 상기 로직 처리장치의 최초 검증 요청 시에만 유효하도록 설정된 일회용 보안토큰인 것을 특징으로 하는 인증장치.
- [청구항 3] 제1항에 있어서, 상기 로그인 유지 보안토큰은
아이디 인증 시마다 재발급되는 제1 인증 값과, 특정 아이디로 로그인 인증을 수행하기 위한 사용자 프로파일에 대한 정보를 포함하는 제2 인증 값으로 구성되는 것을 특징으로 하는 인증장치.
- [청구항 4] 제1항에 있어서, 상기 보안토큰 검증부는
상기 로직 처리장치로부터 수신된 인증 보안토큰에 대한 최초 검증 요청 여부를 확인하고, 상기 인증 보안토큰이 최초 검증 요청된 보안토큰인 경우, 상기 단말기와 연관된 회원정보 조회 키 값을 생성하여 상기 로직 처리장치로 제공하는 것을 특징으로 하는 인증장치.
- [청구항 5] 제1항에 있어서, 상기 보안토큰 생성부는
상기 로그인에 성공하면 로그인 유지 보안토큰을 발행하여 단말기로 전송하고, 재 로그인 인증 요청에 따라 상기 로그인 유지 보안토큰의 인증 값을 변경하여 단말기로 전송하는 것을 특징으로 하는 인증장치.
- [청구항 6] 제1항에 있어서, 상기 보안토큰 검증부는
상기 단말기로부터 상기 로직 처리장치의 재 로그인 인증을 위한 로그인 유지 보안토큰에 대한 검증이 요청되면, 상기 로그인 유지

[청구항 7]

보안토큰에 대한 검증을 수행하는 것을 특징으로 하는 인증장치.
서비스를 제공하는 로직 처리장치 및 인증장치와 통신하고, 인증
보안토큰을 이용하여 인증을 수행하고, 로그인 유지 보안토큰을
이용하여 로그인 유지를 수행하기 위한 데이터를 송수신하는
통신부; 및

상기 로직 처리장치에 접속하여 로그인 인증을 수행하고, 상기
로그인에 성공한 경우, 상기 인증장치로부터 인증 보안토큰을
포함하는 메시지를 수신하고, 상기 수신된 메시지를 분석하여
확인되는 인증 보안토큰을 상기 로직 처리장치로 전송하고, 상기
인증 보안토큰의 검증 결과에 따라 상기 로직 처리장치로부터
제공되는 다수의 서비스를 이용하도록 제어하는 제어부;
를 포함하는 것을 특징으로 하는 단말기.

[청구항 8]

제7항에 있어서,
상기 인증장치로부터 수신된 메시지를 분석하여 확인되는 인증
보안토큰 및 재 로그인을 위하여 상기 인증장치로부터
수신되거나, 상기 인증장치로부터 수신된 메시지를 분석하여
확인된 로그인 유지 보안토큰을 저장하는 저장부;
를 더 포함하는 것을 특징으로 하는 단말기.

[청구항 9]

제7항에 있어서, 상기 제어부는
재 로그인 인증을 위한 로그인 유지 보안토큰의 유무를 확인하고,
상기 로그인 유지 보안토큰이 존재하는 경우, 상기 인증장치로
상기 로그인 유지 보안토큰에 대한 검증을 요청하고, 상기 로그인
유지 보안토큰의 검증이 완료되면, 상기 로그인 유지 보안토큰을
기반으로 재 로그인 인증을 수행하고, 상기 재 로그인 인증에
상응하여 상기 인증장치로부터 변경된 인증 값을 가지는 로그인
유지 보안토큰을 수신하는 것을 특징으로 하는 단말기.

[청구항 10]

로직 처리장치에 접속하여 로그인 인증을 수행하고, 상기
로그인에 성공한 경우, 인증장치로부터 인증 보안토큰을 포함하는
메시지를 수신하고, 상기 수신된 메시지를 분석하여 확인되는
보안토큰을 상기 로직 처리장치로 전송하고, 상기 인증
보안토큰의 검증 결과에 따라 상기 로직 처리장치로부터 제공되는
다수의 서비스를 이용하는 단말기; 및

상기 단말기의 요청에 따라 상기 로직 처리장치에 접속하기 위한
로그인 인증을 수행하고, 상기 로그인에 성공한 경우, 상기 인증
보안토큰을 발행한 후에 보안토큰을 메시지에 포함하여 상기
단말기로 전송하고, 상기 로직 처리장치로부터 상기 인증
보안토큰에 대한 검증을 요청 받으면, 상기 인증 보안토큰에 대한
검증을 수행하고, 상기 인증 보안토큰이 검증된 경우, 회원정보

[청구항 11]

조회 키 값을 적용하여 상기 로직 처리장치로 회원정보를 제공하는 상기 인증장치;
 를 포함하는 것을 특징으로 하는 보안토큰을 이용한 인증 시스템.
 제10항에 있어서, 상기 단말기는
 재 로그인 인증을 위한 로그인 유지 보안토큰의 유무를 확인하고,
 상기 로그인 유지 보안토큰이 존재하는 경우, 상기 인증장치로
 상기 로그인 유지 보안토큰에 대한 검증을 요청하고, 상기 로그인
 유지 보안토큰의 검증이 완료되면, 상기 로그인 유지 보안토큰을
 기반으로 재 로그인 인증을 수행하고, 상기 재 로그인 인증에
 상응하여 상기 인증장치로부터 변경된 인증 값을 가지는 로그인
 유지 보안토큰을 수신하는 것을 특징으로 하는 보안토큰을 이용한
 인증 시스템.

[청구항 12]

제10항에 있어서, 상기 인증장치는
 상기 단말기의 요청에 따라 로그인 인증을 수행하고, 상기
 로그인에 성공한 경우, 로그인 유지 보안토큰을 발행하고, 상기
 단말기로부터 재 로그인 인증을 위한 로그인 유지 보안토큰에
 대한 검증이 요청되면, 상기 로그인 유지 보안토큰에 대한 검증을
 수행하고, 상기 로그인 유지 보안토큰의 검증이 완료되면, 상기
 로그인 유지 보안토큰의 인증 값을 변경하고, 상기 변경된 인증
 값을 가지는 로그인 유지 보안토큰을 상기 단말기로 전송하는
 것을 특징으로 하는 보안토큰을 이용한 인증 시스템.

[청구항 13]

제10항에 있어서,
 상기 단말기의 요청에 따라 상기 인증 보안토큰에 대한 검증을
 상기 인증장치로 요청하고, 상기 인증장치의 검증 결과에 따라
 상기 단말기와 연관된 회원정보를 조회하는 로직 처리장치;
 를 더 포함하는 것을 특징으로 하는 보안토큰을 이용한 인증
 시스템.

[청구항 14]

단말기가 특정 로직 처리장치에 접속하여 로그인 인증을 수행하는
 단계;
 상기 단말기가 상기 로그인에 성공한 경우, 인증장치로부터 인증
 보안토큰을 포함하는 메시지를 수신하는 단계;
 상기 단말기가 상기 수신된 메시지를 분석하여 상기 인증
 보안토큰을 확인하는 단계;
 상기 단말기가 상기 인증 보안토큰을 상기 로직 처리장치로
 전송하는 단계; 및
 상기 단말기가 상기 인증 보안토큰의 검증 결과에 따라 상기 로직
 처리장치로부터 제공되는 다수의 서비스를 이용하는 단계;
 를 포함하는 것을 특징으로 하는 보안토큰을 이용한 인증 방법.

- [청구항 15] 제14항에 있어서, 상기 확인하는 단계는
상기 단말기가 상기 인증장치로부터 수신된 메시지에 포함된 서비스 제공 사이트 코드 정보, 인증 보안토큰이 전송될 URL 정보, 국내 또는 외국 사이트 구분 코드 정보, 인증 보안토큰 중 하나 이상에 해당하는 정보를 확인하는 것을 특징으로 하는 보안토큰을 이용한 인증 방법.
- [청구항 16] 제14항에 있어서, 상기 확인하는 단계 이후에,
상기 단말기가 상기 메시지에 포함된 인증 보안토큰을 저장하는 단계;
를 더 포함하는 것을 특징으로 하는 보안토큰을 이용한 인증 방법.
- [청구항 17] 인증장치가 적어도 하나의 단말기의 요청에 따라 특정 로직 처리장치에 접속하기 위한 로그인 인증을 수행하는 단계;
상기 로그인에 성공한 경우, 상기 인증장치가 인증 보안토큰을 발행하는 단계;
상기 인증장치가 상기 인증 보안토큰을 메시지에 포함하여 상기 단말기로 전송하는 단계;
상기 인증장치가 상기 로직 처리장치로부터 상기 인증 보안토큰에 대한 검증을 요청 받으면, 상기 인증 보안토큰에 대한 검증을 수행하는 단계; 및
상기 보안토큰이 검증된 경우, 상기 인증장치가 회원정보 조회 키 값을 적용하여 상기 로직 처리장치로 회원정보를 제공하는 단계;
를 포함하는 것을 특징으로 하는 보안토큰을 이용한 인증 방법.
- [청구항 18] 제17항에 있어서, 상기 로그인 인증을 수행하는 단계는
상기 인증장치가 상기 로직 처리장치로의 접속 요청에 따라 아이디와 비밀번호의 입력 화면을 제공하는 단계; 및
상기 인증장치가 상기 단말기로부터 아이디와 비밀번호를 수신하고, 수신된 아이디와 비밀번호를 확인하는 단계;
를 포함하는 것을 특징으로 하는 보안토큰을 이용한 인증 방법.
- [청구항 19] 제17항에 있어서, 상기 인증 보안토큰에 대한 검증을 수행하는 단계는
상기 인증장치가 상기 로직 처리장치로부터 수신된 인증 보안토큰에 대한 최초 검증 요청 여부를 확인하는 단계;
상기 보안토큰이 최초 검증 요청된 인증 보안토큰인 경우, 상기 인증장치가 상기 단말기와 연관된 회원정보 조회 키 값을 생성하는 단계;
를 포함하는 것을 특징으로 하는 보안토큰을 이용한 인증 방법.
- [청구항 20] 제17항에 있어서, 상기 인증 보안토큰에 대한 검증을 수행하는 단계는

- 상기 보안토큰이 최초 검증 요청된 인증 보안토큰이 아닌 경우,
상기 인증장치가 상기 로직 처리장치로 경고 메시지를 전송하는
단계;
- [청구항 21] 를 더 포함하는 것을 특징으로 하는 보안토큰을 이용한 인증 방법.
제17항에 있어서, 상기 제공하는 단계는
상기 인증장치가 상기 로직 처리장치로부터 상기 회원정보 조회
키 값과 관련된 회원정보의 조회를 요청 받는 단계;
상기 인증장치가 상기 요청에 따라 상기 회원정보를 조회하는
단계; 및
상기 인증장치가 상기 조회된 결과를 상기 로직 처리장치로
전송하는 단계;
를 포함하는 것을 특징으로 하는 보안토큰을 이용한 인증 방법.
- [청구항 22] 단말기가 재 로그인 인증을 위한 로그인 유지 보안토큰의 유무를
확인하는 단계;
상기 로그인 유지 보안토큰이 존재하는 경우, 상기 단말기가 상기
인증장치로 상기 로그인 유지 보안토큰에 대한 검증을 요청하는
단계;
상기 로그인 유지 보안토큰의 검증이 완료되면, 상기 단말기가
상기 로그인 유지 보안토큰을 기반으로 재 로그인 인증을
수행하는 단계; 및
상기 단말기가 상기 재 로그인 인증에 상응하여 상기
인증장치로부터 변경된 인증 값을 가지는 로그인 유지 보안토큰을
수신하는 단계;
를 포함하는 것을 특징으로 하는 보안토큰을 이용한 인증 방법.
- [청구항 23] 제22항에 있어서, 상기 확인하는 단계 이전에,
상기 단말기가 서비스 제공을 위하여 로그인 인증을 수행하는
단계;
상기 로그인에 성공한 경우, 상기 단말기가 인증장치로부터
로그인 유지 보안토큰을 수신하는 단계; 및
상기 단말기가 상기 수신된 로그인 유지 보안토큰을 저장하는
단계;
를 더 포함하는 것을 특징으로 하는 보안토큰을 이용한 인증 방법.
- [청구항 24] 제22항에 있어서, 상기 확인하는 단계는
상기 로그인 유지 보안토큰이 존재하지 않으면, 상기 단말기가
아이디와 비밀번호를 이용하여 로그인 인증을 수행하기 위한
입력화면을 출력하는 단계;
를 더 포함하는 것을 특징으로 하는 보안토큰을 이용한 인증 방법.
- [청구항 25] 제22항에 있어서, 상기 수신하는 단계 이후에,

[청구항 26]

상기 단말기가 특정 인증 값이 변경된 로그인 유지 보안토큰을 기존의 로그인 유지 보안토큰을 대체하여 저장하는 단계;
 를 더 포함하는 것을 특징으로 하는 보안토큰을 이용한 인증 방법.
 인증장치가 적어도 하나의 단말기의 요청에 따라 서비스를 제공하는 로직 처리장치에 접속하기 위한 로그인 인증을 수행하는 단계;

상기 로그인에 성공한 경우, 상기 인증장치가 로그인 유지 보안토큰을 발행하는 단계;

상기 단말기로부터 상기 로직 처리장치로의 재 로그인 인증을 위한 로그인 유지 보안토큰에 대한 검증이 요청되면, 상기 인증장치가 상기 로그인 유지 보안토큰에 대한 검증을 수행하는 단계;

상기 로그인 유지 보안토큰의 검증이 완료되면, 상기 인증장치가 상기 로그인 유지 보안토큰의 인증 값을 변경하는 단계; 및
 상기 인증장치가 상기 변경된 인증 값을 가지는 로그인 유지 보안토큰을 상기 단말기로 전송하는 단계;

[청구항 27]

를 포함하는 것을 특징으로 하는 보안토큰을 이용한 인증 방법.

제26항에 있어서, 상기 로그인 인증을 수행하는 단계는
 상기 인증장치가 아이디와 비밀번호의 입력 화면을 제공하는 단계; 및

상기 인증장치가 상기 단말기로부터 아이디와 비밀번호를 수신하고, 수신된 아이디와 비밀번호를 확인하는 단계;

[청구항 28]

를 포함하는 것을 특징으로 하는 보안토큰을 이용한 인증 방법.

제26항에 있어서, 상기 로그인 유지 보안토큰에 대한 검증을 수행하는 단계는

상기 인증장치가 단말기 별로 기 발행된 로그인 유지 보안토큰과 특정 단말기로부터 검증이 요청된 로그인 유지 보안토큰의 일치 여부를 확인하는 것을 특징으로 하는 보안토큰을 이용한 인증 방법.

[청구항 29]

제26항에 있어서, 상기 보안토큰에 대한 검증을 수행하는 단계는
 상기 로그인 유지 보안토큰에 대한 검증에 실패한 경우, 상기 인증장치가 상기 단말기로 경고 메시지를 전송하는 단계;

[청구항 30]

를 더 포함하는 것을 특징으로 하는 보안토큰을 이용한 인증 방법.

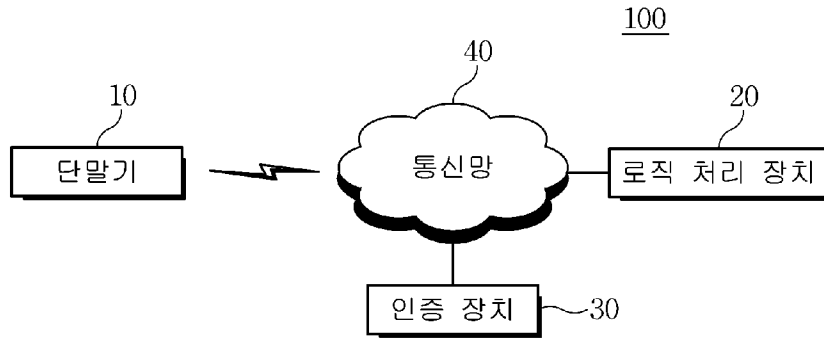
제26항에 있어서, 상기 변경하는 단계는

상기 인증장치가 상기 로그인 유지 보안토큰을 구성하는 제1 인증 값과 제2 인증 값 중에서 제1 인증 값을 적어도 하나의 연산 방식을 적용하여 변경하는 것을 특징으로 하는 보안토큰을 이용한 인증 방법.

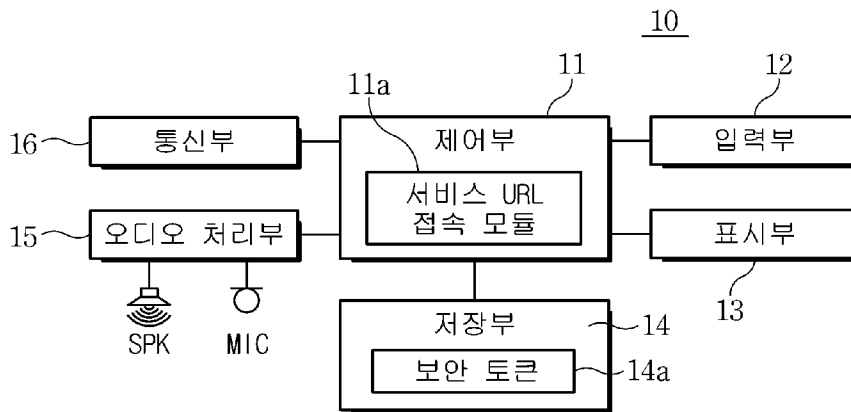
- [청구항 31] 재 로그인 인증을 위한 로그인 유지 보안토큰의 유무를 확인하는 단계;
 상기 로그인 유지 보안토큰이 존재하는 경우, 상기 인증장치로 상기 로그인 유지 보안토큰에 대한 검증을 요청하는 단계;
 상기 로그인 유지 보안토큰의 검증이 완료되면, 상기 로그인 유지 보안토큰을 기반으로 재 로그인 인증을 수행하는 단계; 및
 상기 재 로그인 인증에 상응하여 상기 인증장치로부터 변경된 인증 값을 가지는 로그인 유지 보안토큰을 수신하는 단계를 실행하는 프로그램을 기록한 컴퓨터 판독 가능한 기록매체.
- [청구항 32] 적어도 하나의 단말기의 요청에 따라 서비스를 제공하는 로직 처리장치에 접속하기 위한 로그인 인증을 수행하는 단계;
 상기 로그인에 성공한 경우, 로그인 유지 보안토큰을 발행하는 단계;
 상기 단말기로부터 상기 로직 처리장치로의 재 로그인 인증을 위한 로그인 유지 보안토큰에 대한 검증이 요청되면, 상기 로그인 유지 보안토큰에 대한 검증을 수행하는 단계;
 상기 로그인 유지 보안토큰의 검증이 완료되면, 상기 로그인 유지 보안토큰의 인증 값을 변경하는 단계; 및
 상기 변경된 인증 값을 가지는 로그인 유지 보안토큰을 상기 단말기로 전송하는 단계를 실행하는 프로그램을 기록한 컴퓨터 판독 가능한 기록매체.
- [청구항 33] 특정 로직 처리장치에 접속하여 로그인 인증을 수행하는 단계;
 상기 로그인에 성공한 경우, 인증장치로부터 인증 보안토큰을 포함하는 메시지를 수신하는 단계;
 상기 수신된 메시지를 분석하여 상기 인증 보안토큰을 확인하는 단계;
 상기 인증 보안토큰을 상기 로직 처리장치로 전송하는 단계; 및
 상기 인증 보안토큰의 검증 결과에 따라 상기 로직 처리장치로부터 제공되는 다수의 서비스를 이용하는 단계를 실행하는 프로그램을 기록한 컴퓨터 판독 가능한 기록매체.
- [청구항 34] 적어도 하나의 단말기의 요청에 따라 특정 로직 처리장치에 접속하기 위한 로그인 인증을 수행하는 단계;
 상기 로그인에 성공한 경우, 인증 보안토큰을 발행하는 단계;
 상기 인증 보안토큰을 메시지에 포함하여 상기 단말기로 전송하는 단계;
 상기 로직 처리장치로부터 상기 인증 보안토큰에 대한 검증을 요청 받으면, 상기 인증 보안토큰에 대한 검증을 수행하는 단계; 및
 상기 인증 보안토큰이 검증된 경우, 회원정보 조회 키 값을

적용하여 상기 로직 처리장치로 회원정보를 제공하는 단계를
실행하는 프로그램을 기록한 컴퓨터 판독 가능한 기록매체.

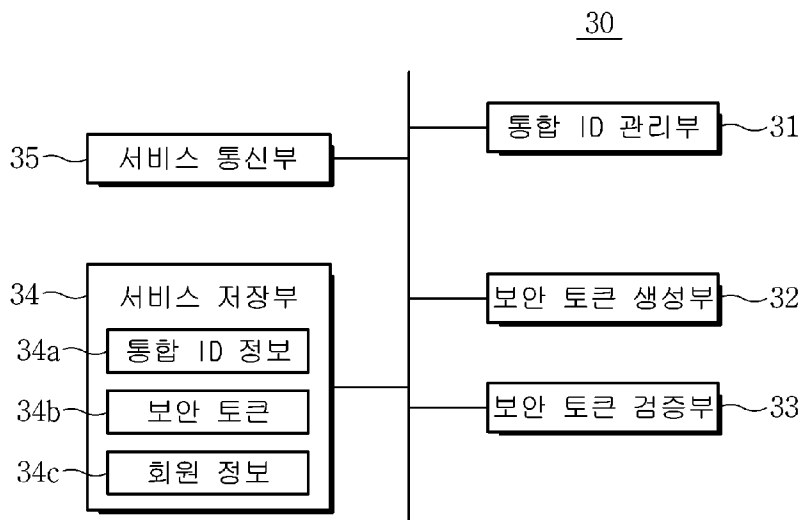
[Fig. 1]



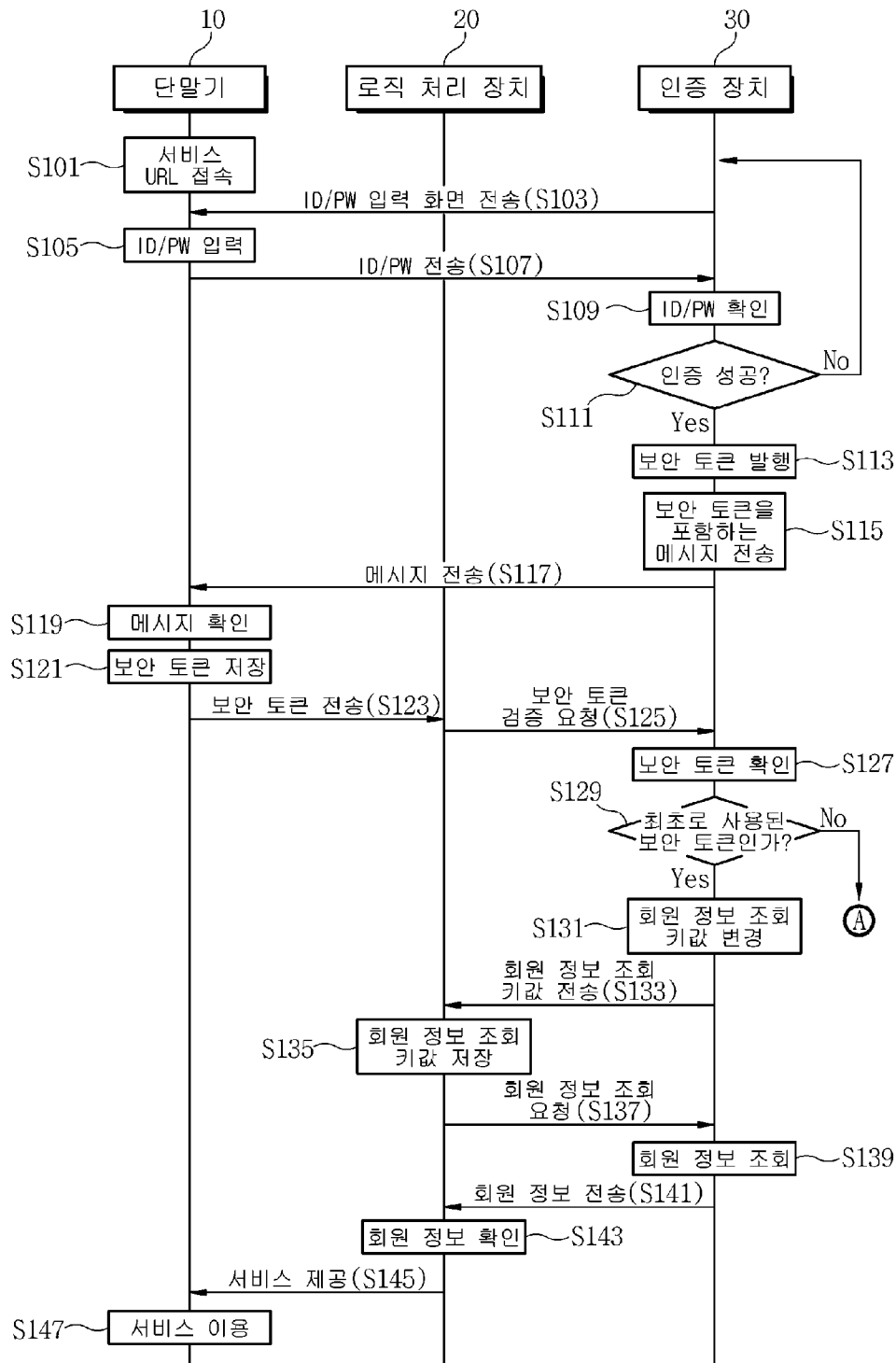
[Fig. 2]



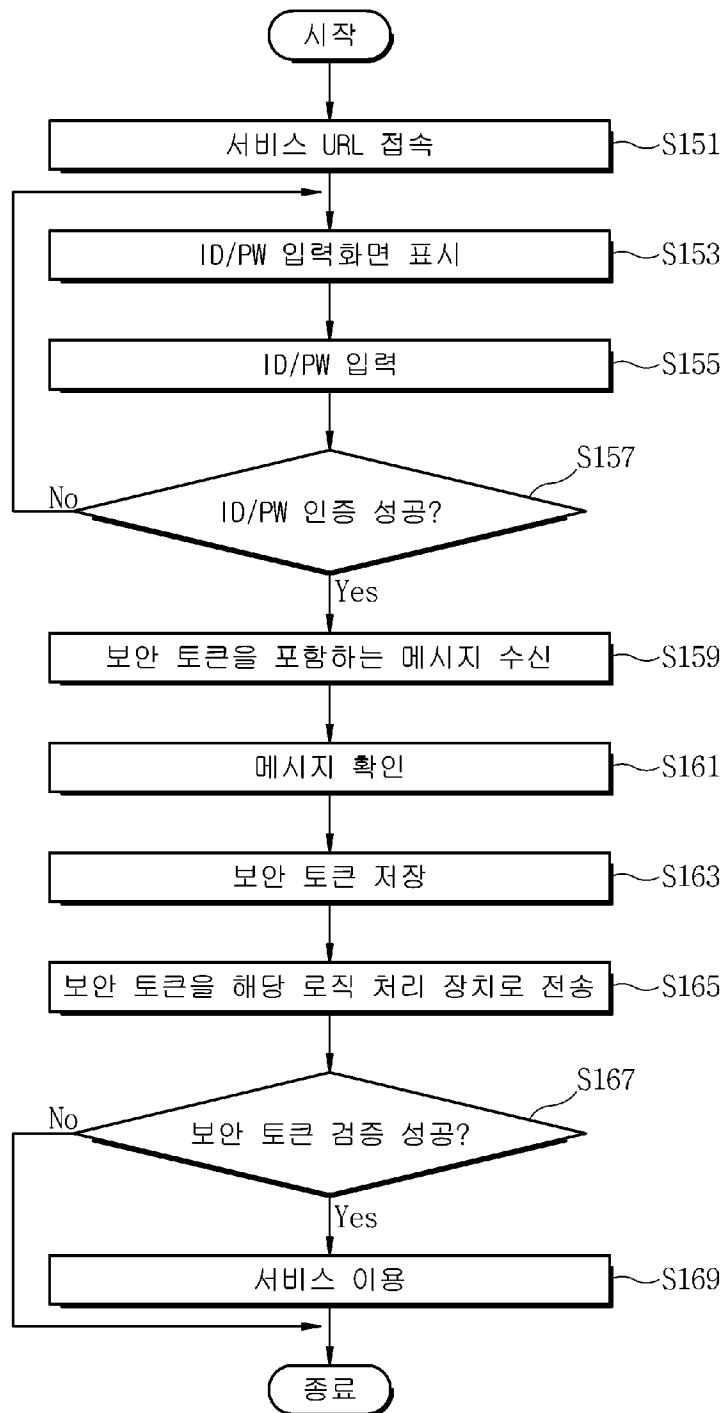
[Fig. 3]



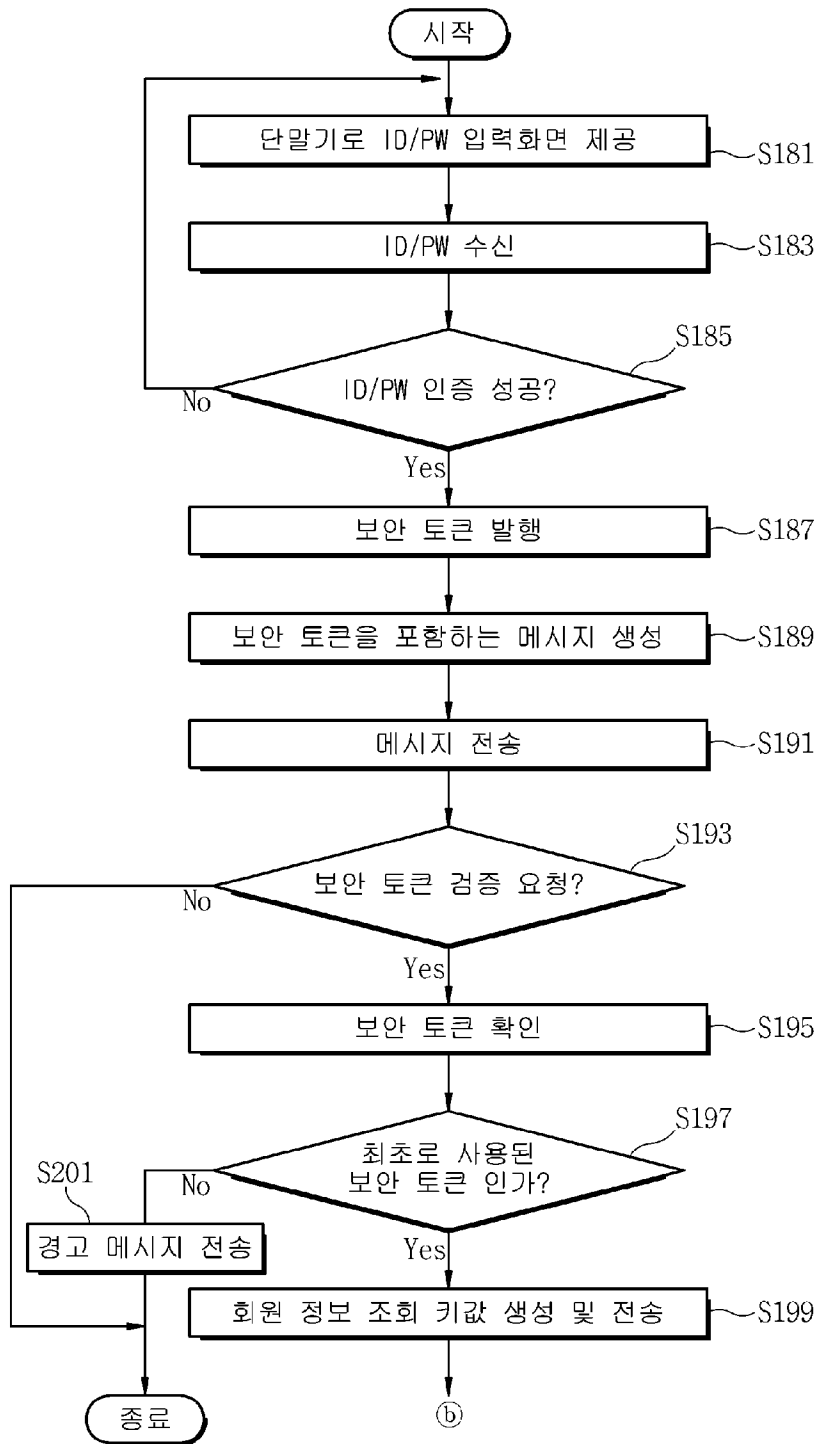
[Fig. 4]



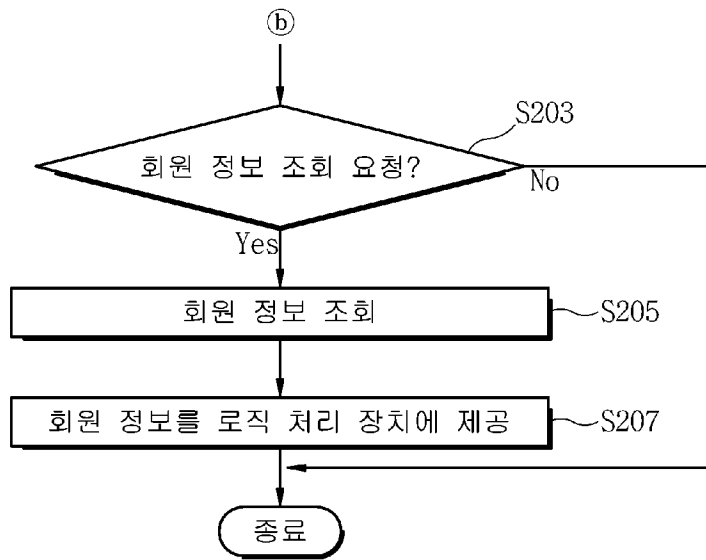
[Fig. 5]



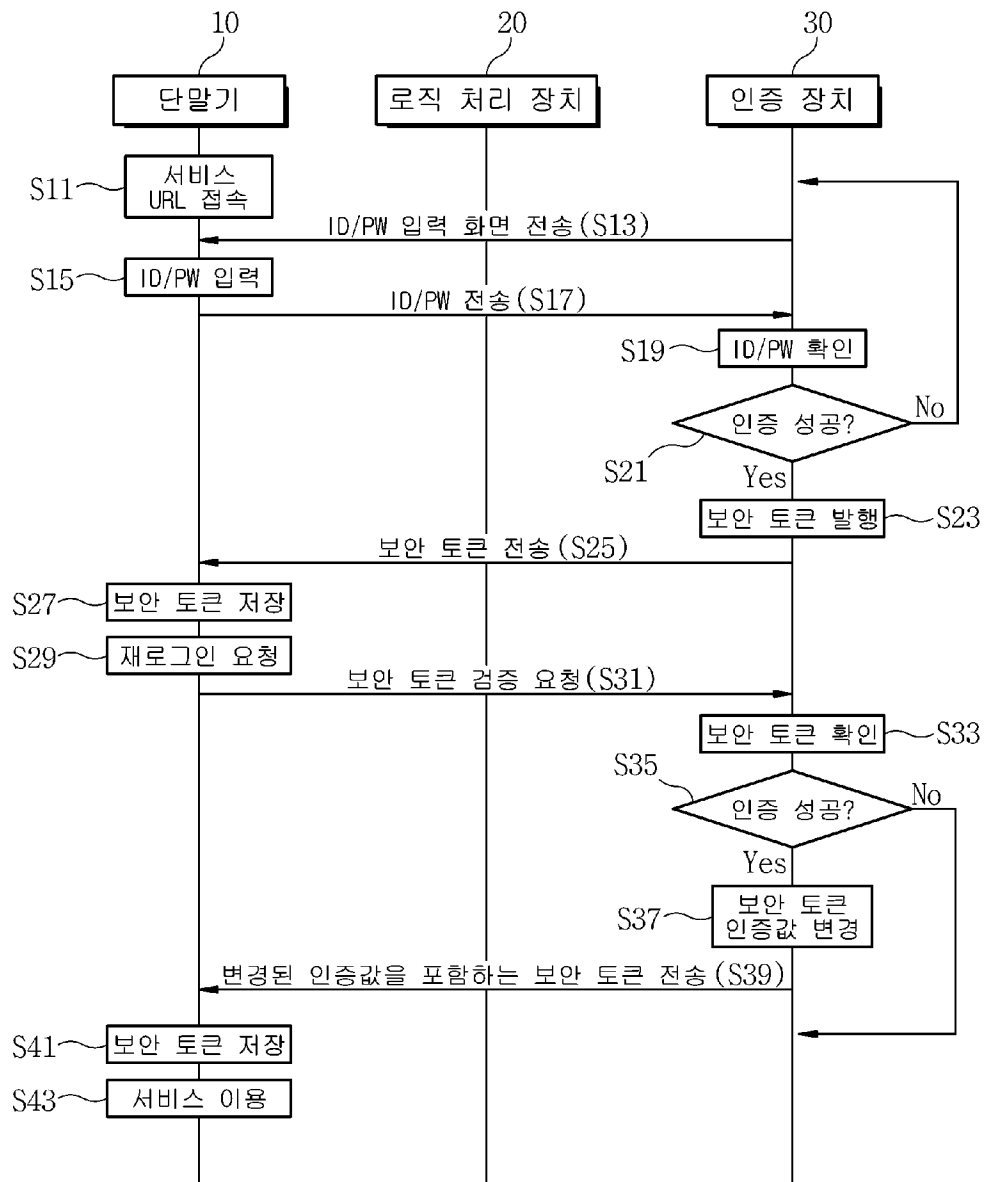
[Fig. 6]



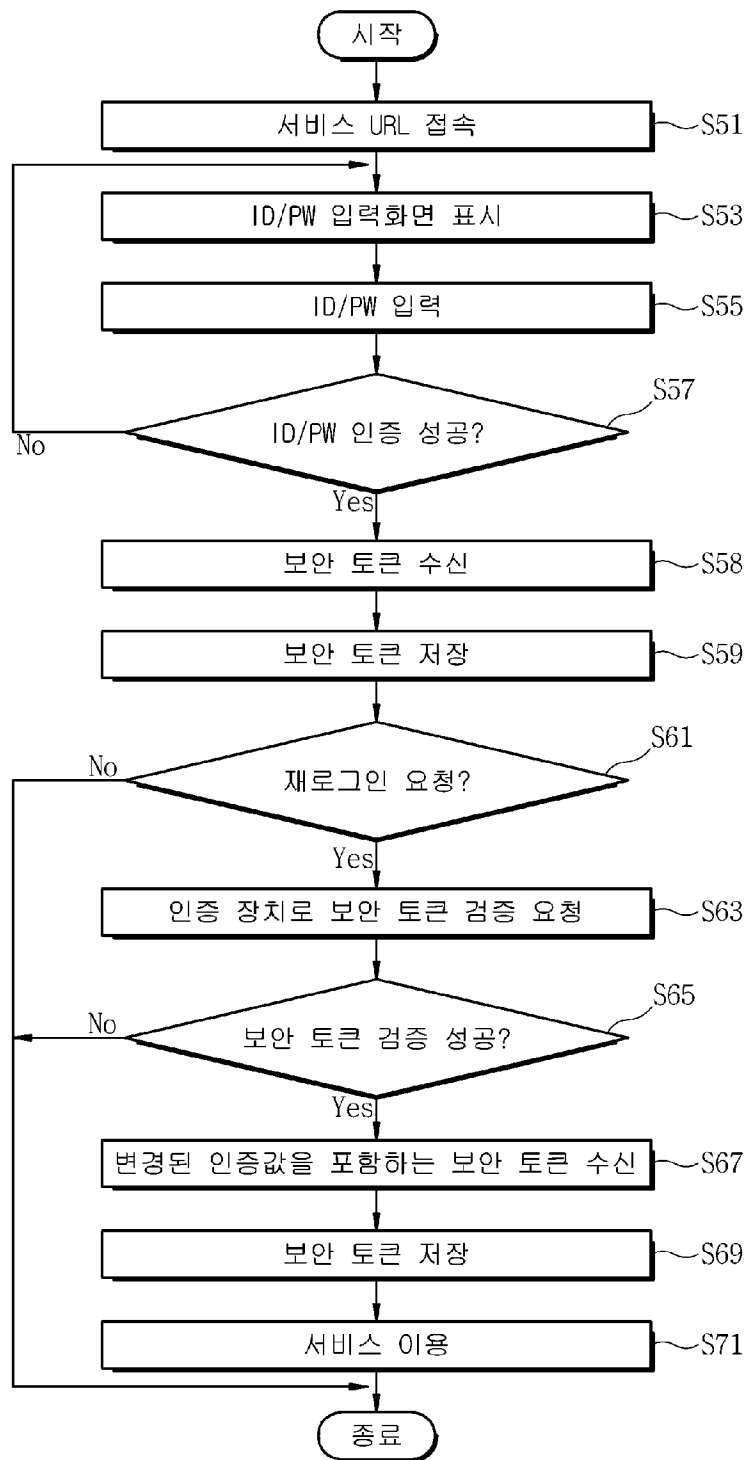
[Fig. 7]



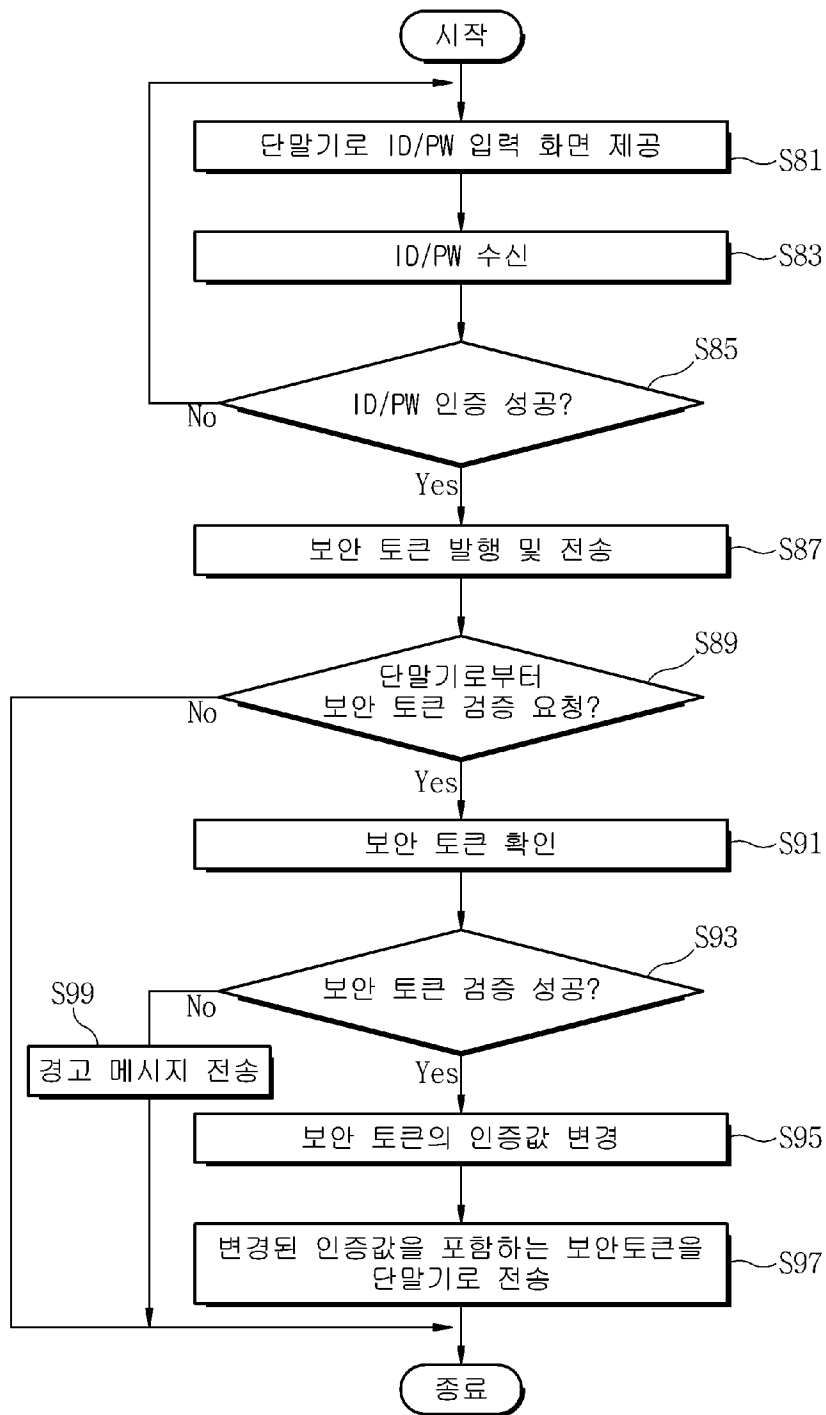
[Fig. 8]



[Fig. 9]



[Fig. 10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2013/012157**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/34(2013.01)i, H04L 9/32(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)

G06F 21/34; G06Q 20/40; G06F 21/20; H04L 9/32; G06Q 40/02; G06F 21/00

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: login, security token, verification, member information, re-login.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2013-0039745 A (SAMSUNG SDS CO.,LTD.) 22 April 2013 See paragraphs [0031]-[0036]; claim 1; and figures 1-2.	1-3,7,10,13-18,21 ,33-34
A		4-6,8-9,11-12 ,19-20,22-32
Y	KR 10-2012-0076594 A (SK PLANET CO., LTD.) 09 July 2012 See claims 1-3; figures 1-3.	1-3,7,10,13-18,21 ,33-34
Y	KR 10-2007-0105479 A (HUH, Kee Nyoung) 31 October 2007 See abstract; claims 1-6; and figure 1.	2-3
A	KR 10-2010-0066907 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 18 June 2010 See paragraphs [0013]-[0032]; claim 1; and figures 1-2.	1-34
A	KR 10-2013-0010097 A (HANA BANK) 25 January 2013 See abstract; claims 1-5; and figures 1-5.	1-34

☐ 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

11 APRIL 2014 (11.04.2014)

Date of mailing of the international search report

15 APRIL 2014 (15.04.2014)

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/KR2013/012157

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2013-0039745 A	22/04/2013	KR 10-2012-0119490 A	31/10/2012
KR 10-2012-0076594 A	09/07/2012	NONE	
KR 10-2007-0105479 A	31/10/2007	NONE	
KR 10-2010-0066907 A	18/06/2010	NONE	
KR 10-2013-0010097 A	25/01/2013	NONE	

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/34(2013.01)i, H04L 9/32(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 21/34; G06Q 20/40; G06F 21/20; H04L 9/32; G06Q 40/02; G06F 21/00

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: 로그인, 보안토큰, 검증, 회원정보, 재로그인.

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y A	KR 10-2013-0039745 A (삼성에스디에스 주식회사) 2013.04.22 단락 [0031]-[0036]; 청구항 1; 및 도면 1-2 참조.	1-3, 7, 10, 13-18, 21, 33-34 4-6, 8-9, 11-12, 19-20, 22-32
Y	KR 10-2012-0076594 A (에스케이플래닛 주식회사) 2012.07.09 청구항 1-3; 도면 1-3 참조.	1-3, 7, 10, 13-18, 21, 33-34
Y	KR 10-2007-0105479 A (허기녕) 2007.10.31 요약; 청구항 1-6; 및 도면 1 참조.	2-3
A	KR 10-2010-0066907 A (한국전자통신연구원) 2010.06.18 단락 [0013]-[0032]; 청구항 1; 및 도면 1-2 참조.	1-34
A	KR 10-2013-0010097 A (주식회사 하나은행) 2013.01.25 요약; 청구항 1-5; 및 도면 1-5 참조.	1-34



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

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

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

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

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

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

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

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2014년 04월 11일 (11.04.2014)

국제조사보고서 발송일

2014년 04월 15일 (15.04.2014)

ISA/KR의 명칭 및 우편주소

대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-472-7140

심사관

안정환

전화번호 +82-42-481-8440



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2013-0039745 A	2013/04/22	KR 10-2012-0119490 A	2012/10/31
KR 10-2012-0076594 A	2012/07/09	없음	
KR 10-2007-0105479 A	2007/10/31	없음	
KR 10-2010-0066907 A	2010/06/18	없음	
KR 10-2013-0010097 A	2013/01/25	없음	