(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2013 년 5 월 2 일 (02.05.2013)

WIPO | PCT

(10) 국제공개번호
WO 2013/062352 A1

(51) 국제특허분류:
G06F 15/16 (2006.01) *H04L 9/32* (2006.01)

(21) 국제출원번호: PCT/KR2012/008855

(22) 국제출원일: 2012 년 10 월 26 일 (26.10.2012)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2011-0110555 2011 년 10 월 27 일 (27.10.2011) KR

(71) 출원인: **인텔렉추얼디스커버리 주식회사 (INTELLCETUAL DISCOVERY CO., LTD.)** [KR/KR]; 135-090 서울시 강남구 삼성로 511, 10 층, Seoul (KR).

(72) 발명자: **허의남 (HUH, Eui Nam)**; 138-040 서울시 송파구 풍납동 388-7 우성아파트 2 동 708 호, Seoul (KR). **나상호 (NA, Sang Ho)**; 446-906 경기도 용인시 기흥구 서천동 1 번지 전자정보대학 322 호, Gyeonggi-do (KR). **박준영 (PARK, Jun Young)**; 446-906 경기도 용인시 기흥구 서천동 1 번지 전자정보대학 322 호, Gyeonggi-do (KR). **김진택 (KIM, Jin Taek)**; 100-454 서울시 중구 신당4 동 신당삼성아파트 113 동 1404 호, Seoul (KR).

(74) 대리인: **특허법인 무한 (MUHANN PATENT & LAW FIRM)**; 135-814 서울시 강남구 논현동 51-8 명림빌딩 2, 5, 6 층, Seoul (KR).

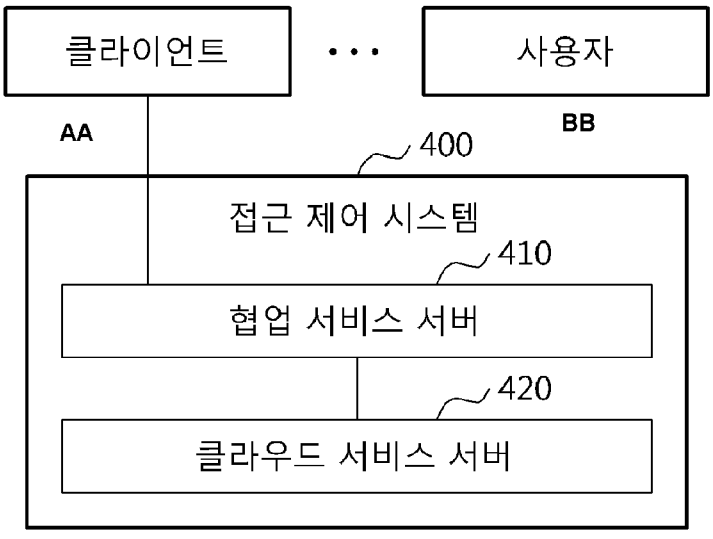
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY,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

[다음 쪽 계속]

(54) **Title**: METHOD AND SYSTEM FOR ACCESS CONTROL IN CLOUD COMPUTING SERVICE

(54) **발명의 명칭** : 클라우드 컴퓨팅 서비스에서의 접근제어 방법 및 시스템



AA ... Client
BB ... User
400 ... Access control system
410 ... Cooperative service server
420 ... Cloud service server

(57) **Abstract**: The present invention relates to a method and system for granting an authority suitable for a user through an access control on the basis of a security policy in a computing service. A cooperative service server authenticates the user through a cloud service server, and issues an access token including user authentication information and user authority information. The cloud service server compares access token information and an access control list, and determines whether to approve a user's access to a service on the basis of the compared result.

(57) **요약서**: 컴퓨팅 서비스에서 보안 정책에 기반한 접근 제어를 통해 사용자에게 적합한 권한을 부여하는 방법 및 시스템이 제공된다. 협업 서비스 서버는 클라우드 서비스 서버를 통해 사용자를 인증하며, 사용자 인증 정보 및 사용자 권한 정보를 포함하는 접근 토큰을 발행한다. 클라우드 서비스 서버는 접근 토큰의 정보 및 접근 제어 리스트를 비교하고, 비교의 결과에 기반하여 사용자의 서비스 접근의 승인 여부를 결정한다.

WO 2013/062352 A1

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: 클라우드 컴퓨팅 서비스에서의 접근제어 방법 및 시스템

기술분야

[1] 본 발명은 클라우드 컴퓨팅 시스템에 관한 것으로, 더욱 상세하게는 클라우드 컴퓨팅 서비스에서 보안 정책에 기반한 접근 제어를 통해 사용자에게 적합한 권한을 부여하는 방법 및 시스템에 관한 것이다.

배경기술

[2] 클라우드 컴퓨팅은 가상화(visualization) 기술 및 분산 처리(distributed processing) 기술을 활용함으로써 대규모의 IT 자원을 제공하는 기술이다. 클라우드 컴퓨팅 서비스에 의해 사용자는 인터넷을 통해 컴퓨팅 자원에 대한 서비스를 제공받을 수 있다. 여기서, 컴퓨팅 자원은 메모리(memory) 자원, 중앙 처리 장치(Central Processing Unit; CPU) 자원, 네트워크 자원 및 스토리지(storage) 자원 등을 포함할 수 있다. 사용자는 자신이 사용한 컴퓨팅 자원에 상응하는 요금을 클라우드 컴퓨팅 서비스의 운영 주체에게 지불할 수 있다.

[3] 말하자면, 클라우드 컴퓨팅은 서로 상이한 물리적인 위치에 존재하는 컴퓨팅 자원들을 가상화 기술을 통해 하나의 컴퓨팅 자원으로 통합하고, 통합된 컴퓨팅 자원을 사용자들에게 제공하는 기술이다. 즉, 클라우딩 컴퓨팅은 '인터넷에 기반한 사용자 중심의 주문형 아웃소싱 서비스 기술'로 간주될 수 있다.

[4] 사용자는, 인터넷이 제공된다면, 클라우드 컴퓨팅 서비스를 통해 자신만의 컴퓨팅 환경을 시간 및 장소에 무관하게 사용할 수 있다. 클라우딩 컴퓨팅 서비스는 사용자에게 상기의 사용자가 사용한 자원만큼의 요금을 부과한다. 또한, 사용자는 클라우드 컴퓨팅 서비스의 컴퓨팅 환경을 통해, 하드웨어 서비스, 소프트웨어 서비스 및 사후 서비스 등과 같은 모든 서비스를 제공받을 수 있다. 따라서, 시스템의 유지 및 보수의 비용이 절감될 수 있고, 하드웨어 및 소프트웨어의 구매 비용이 절감될 수 있고, 컴퓨팅 처리를 위해 사용되는 에너지가 절감될 수 있다.

[5] 클라우드 컴퓨팅 서비스가 주목을 받음에 따라, IT 대기업들의 주도 하에 클라우드 컴퓨팅 서비스가 널리 보급되고 있다. 클라우드 컴퓨팅 서비스에 있어서, 퍼블릭 클라우드(public cloud), 프라이빗 클라우드(private cloud) 등과 같은 4가지의 클라우드 컴퓨팅 서비스 타입이 존재한다.

[6] 퍼블릭 클라우드 서비스는, 불특정된 다수의 사용자들에게 인터넷을 통해 클라우드 서비스를 제공한다. 퍼블릭 클라우드 서비스는 무상의 서비스 제공을 의미하는 것은 아니며, 서비스에 관련된 데이터 및 소스의 공개(open)을 의미하는 것 또한 아니다. 퍼블릭 클라우드 서비스에서도, 사용자 접근

제어(access control) 및 과금 등과 같은 서비스가 제공될 수 있다. 퍼블릭 클라우드 서비스 하에서는, 서비스의 제공자가 사용자의 정보를 관리하고, 모든 클라우드 컴퓨팅 서비스의 리소스들이 공유된다. 따라서, 퍼블릭 클라우드 서비스는 사용자의 개인 정보의 보호에 있어서, 취약점을 갖는다.

[7] 프라이빗 클라우드 서비스는 퍼블릭 클라우드 서비스에서와 같은 컴퓨팅 환경을 제공한다. 프라이빗 클라우드 서비스는 특정한 기업 또는 기관에서 클라우드 컴퓨팅 서비스, 데이터 및 프로세스를 직접 관리하는 클라우드 서비스를 의미한다. 말하자면, 프라이빗 클라우드 서비스는 보안을 위해서 외부로부터의 접근을 회피하고, 인증된 사용자들만의 접근을 허용하는 폐쇄적인 클라우드 서비스 타입이다.

[8] 커뮤니케이션 클라우드 서비스는 특정한 사용자들의 집단을 위한 클라우드 컴퓨팅 서비스이다. 커뮤니케이션 클라우드 서비스는 특정한 집단의 구성원들에게만 접근 권한을 부여한다. 집단의 구성원들은 커뮤니케이션 클라우드 서비스를 통해 서로 간에 데이터 및 어플리케이션 등을 공유한다.

[9] 하이브리드 클라우드 서비스는 퍼블릭 클라우드 서비스 및 프라이빗 클라우드 서비스가 결합된 서비스이다. 하이브리드 클라우드 서비스는 기본적으로 퍼블릭 클라우드 서비스를 제공하며 사용자가 공유를 원치 않는 데이터 및 서비스에 대해서는 프라이빗 클라우드 서비스의 정책을 따른다.

[10] 클라우드 컴퓨팅 서비스의 구조는 인프라형 서비스 구조, 플랫폼형 서비스 구조 및 소프트웨어 서비스 구조로 분류될 수 있다. 인프라형 서비스 구조는 사용자의 요구에 맞춰 사용자 만의 컴퓨팅 환경을 제공한다. 플랫폼형 서비스 구조는 사용자의 컴퓨팅 목적에 맞게 사용자가 플랫폼을 선택하고, 선택된 플랫폼을 사용할 수 있는 환경을 제공한다. 소프트웨어 서비스 구조는 사용자가 사용 목적에 맞는 소프트웨어를 선택하여 사용할 수 있는 환경을 제공한다.

[11] 클라우드 컴퓨팅 서비스에서는, 강력하고 체계적인 접근 제어 정책 및 권한 부여 정책이 요구된다. 또한, 퍼스널 클라우드 서비스는 서로 상이한 서비스 제공자들 간의 협업을 통해 서비스가 제공된다. 따라서, 퍼스널 클라우드 서비스에 대하여, 상기의 퍼스널 클라우드 서비스의 특징에 맞는 접근 제어 방법이 요구되며, 접근 제어에 대한 권한위임(delegation) 및 권한부여(authorization) 정책(policy)의 제공이 요구된다. 또한, 기존의 접근 제어 방법에 비해 퍼스널 클라우드 서비스에 특화된 접근 제어 방법이 요구된다.

발명의 상세한 설명

기술적 과제

[12] 일 실시예는 퍼스널 클라우드 서비스를 위한 접근 제어 방법 및 시스템을 제공할 수 있다.

[13] 일 실시예는 서로 상이한 서비스 제공자들 간의 협업을 통해 서비스를 제공하는 퍼스널 클라우드 서비스의 특징에 맞는 접근 제어에 관련된 방법 및

시스템을 제공할 수 있으며, 권한위임 및 권한부여 정책에 관련된 방법 및 시스템을 제공할 수 있다.

과제 해결 수단

[14] 일 측에 따르면, 사용자가 가입한 서비스와 관련된 상기 사용자의 권한 정보 및 상기 서비스에 대한 보안 정책 정보를 저장하는 사용자 서비스 리스트 데이터베이스 및 사용자의 서비스 접근 요청, 사용자 인증 및 서비스 권한에 기반하여 상기 서비스의 접근 토큰을 발행하는 접근 토큰 발행부를 포함하는, 클라우드 컴퓨팅 서비스의 협업 서비스 서버가 제공될 수 있다.

[15] 상기 협업 서비스 서버는 클라우드 서비스 서버를 통해 상기 사용자 인증을 수행할 수 있다.

[16] 상기 접근 토큰 발행부는 상기 클라우드 서비스 서버로부터 제공된 상기 사용자 인증의 결과에 기반하여 상기 접근 토큰을 발행할 수 있다.

[17] 상기 사용자 서비스 리스트 데이터베이스는 상기 클라우드 서비스 서버에게 상기 권한 정보 및 상기 보안 정책 정보를 제공할 수 있다.

[18] 상기 접근 토큰은 상기 사용자 인증의 정보 및 상기 권한 정보를 포함할 수 있다.

[19] 상기 사용자 서비스 리스트 데이터베이스는 상기 권한 정보 및 상기 보안 정책 정보를 주기적으로 업데이트할 수 있다.

[20] 상기 사용자 서비스 리스트 데이터베이스는 상기 사용자가 새로운 서비스를 요청할 때 상기 사용자가 가입한 서비스와 관련된 상기 권한 정보 및 상기 보안 정책 정보를 업데이트할 수 있다.

[21] 다른 일 측에 따르면, 사용자가 접근하는 서비스에 관련된 보안 정책을 저장하고, 상기 서비스에 대한 사용자 권한 정보를 저장하는 정책 정보부 및 접근 토큰의 정보를 접근 제어 목록, 보안 정책 및 사용자의 권한 정보와 비교하고, 상기 비교의 결과로 상기 접근 제어 목록 및 상기 보안 정책 및 상기 사용자 권한 정보에 부합하면, 상기 사용자의 상기 서비스에 대한 접근을 승인하는 정책 결정부를 포함하는, 클라우드 서비스 서버가 제공될 수 있다.

[22] 상기 클라우드 서비스 서버는 상기 사용자의 권한, 서비스 정책 및 역할을 설정 또는 수정하는 정책 관리부를 더 포함할 수 있다.

[23] 상기 정책 관리부는 상기 사용자의 권한, 상기 서비스 정책 또는 상기 역할의 설정 또는 수정이 발생한 경우, 설정 또는 수정된 상기 사용자의 권한의 정보, 상기 서비스 정책의 정보 또는 상기 역할의 정보를 상기 협업 서비스 서버로 전송할 수 있다.

[24] 또 다른 일 측에 따르면, 사용자 서비스 리스트 데이터베이스가 사용자가 가입한 서비스와 관련된 상기 사용자의 권한 정보 및 상기 서비스에 대한 보안 정책 정보를 저장하는 단계 및 접근 토큰 발행부가 사용자의 서비스 접근 요청, 사용자 인증 및 서비스 권한에 기반하여 상기 서비스의 접근 토큰을 발행하는

단계를 포함하는, 클라우드 컴퓨팅 서비스에서의 협업 서비스 제공 방법이 제공될 수 있다.

[25] 상기 클라우드 컴퓨팅 서비스에서의 협업 서비스 제공 방법은, 상기 클라우드 서비스 서버를 통해 상기 사용자 인증을 수행하는 단계를 더 포함할 수 있다.

[26] 상기 발행하는 단계는 상기 클라우드 서비스 서버로부터 제공된 상기 사용자 인증의 결과에 기반하여 상기 접근 토큰을 발행할 수 있다.

[27] 상기 저장하는 단계는 상기 클라우드 서비스 서버에게 상기 권한 정보 및 상기 보안 정책 정보를 제공할 수 있다.

[28] 또 다른 일 측에 따르면, 정책 정보부가 사용자가 접근하는 서비스에 관련된 보안 정책을 저장하고, 상기 서비스에 대한 사용자 권한 정보를 저장하는 단계 및 정책 결정부가 접근 토큰의 정보를 접근 제어 목록, 보안 정책 및 사용자의 권한 정보와 비교하고, 상기 비교의 결과로 상기 접근 제어 목록 및 상기 보안 정책 및 상기 사용자 권한 정보에 부합하면, 상기 사용자의 상기 서비스에 대한 접근을 승인하는 단계를 포함하는, 클라우드 서비스 제공 방법이 제공될 수 있다.

[29] 상기 클라우드 서비스 제공 방법은, 정책 관리부가 사용자의 권한, 서비스 정책 및 역할을 설정 또는 수정하는 단계를 더 포함할 수 있다.

[30] 상기 클라우드 서비스 제공 방법은, 상기 정책 관리부가 상기 사용자의 권한, 상기 서비스 정책 또는 상기 역할의 설정 또는 수정이 발생한 경우, 설정 또는 수정된 상기 사용자의 권한의 정보, 상기 서비스 정책의 정보 또는 상기 역할의 정보를 상기 협업 서비스 서버로 전송하는 단계를 더 포함할 수 있다.

발명의 효과

[31] 서로 상이한 서비스 제공자들 간의 협업을 통해 서비스를 제공하는 퍼스널 클라우드 서비스의 특징에 맞는 접근 제어에 관련된 방법 및 시스템이 제공된다.

[32] 퍼스널 클라우드 서비스의 특징에 맞는 권한위임 및 권한부여 정책에 관련된 방법 및 시스템이 제공된다.

도면의 간단한 설명

[33] 도 1은 XACML에서의 데이터 흐름을 나타낸다.

[34] 도 2는 애져 접근 제어 서비스의 프레임 워크를 나타낸다.

[35] 도 3은 역할 기반 접근 제어 워크플로우를 나태낸다.

[36] 도 4는 일 실시예에 따른 클라우드 컴퓨팅 서비스에서의 접근 제어 시스템이다.

[37] 도 5 는 일 실시예에 따른 협업 서비스 서버의 블록도이다.

[38] 도 6 은 일 실시예에 따른 클라우드 서비스 서버의 블록도이다.

[39] 도 7은 일 실시예에 따른 본 발명의 또 다른 일 실시 예에 따른 다중 클라우드 서비스 서버의 접근 제어 시스템이다.

[40] 도 8은 일 실시예에 따른 단일 클라우드 서비스 서버의 접근 제어 방법의 흐름도이다.

발명의 실시를 위한 형태

[41] 이하에서, 첨부된 도면을 참조하여 실시예들을 상세하게 설명한다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[42] 도 1은 XACML에서의 데이터 흐름을 나타낸다.

[43] 확장가능한 접근 제어 마크업 언어(eXtensible Access Control Markup Language; XACML)는 웹 환경 하에서 인증 정보 및 권한 정보 등과 같은 보안 정보를 전달하기 위한 데이터 구조를 정의하는 표준일 수 있다.

[44] 접근 제어는 요구된 자원 접근의 허용 여부에 대한 판단을 위한 정보 및 접근 결정의 시행(execution)을 위한 정보를 포함할 수 있다. 접근 제어 정책은 접근 제어 결정을 위한 기준이 될 수 있다.

[45] XACML의 핵심 규격은 인가 정책을 평가하기 위한 문법 및 규칙에 의해 정의된다. XACML은 대규모 환경에서 동작할 수 있다. XACML은 접근 제어를 위해 이용되는 정보가 자동화된 주체에 의해 관리되는 응용을 위해 효율적으로 동작할 수 있도록 설계될 수 있다.

[46] XACML와 관련하여, 속성(attribute)은 서브젝트(subject), 자원(resource), 액션(action), 술어(predicate) 또는 목표(target)가 참조할 수 있는 환경의 특징을 의미할 수 있다.

[47] 정책 관리 지점(Policy Administration Point; PAP))은 정책 또는 정책 집합을 생성하는 시스템 요소일 수 있다.

[48] 정책 결정 지점(Policy Decision Point; PDP)는 적용 가능한 정책을 평가하고, 권한 부여 결정을 생성하는 시스템 요소일 수 있다.

[49] 정책 집행 지점(정책 수행부(PEP: Policy Enforcement Point))은 결정 요청을 생성하고, 권한 부여 결정을 시행함으로써 접근 제어를 수행하는 시스템 요소일 수 있다.

[50] 정책 정보 지점(Policy Information Point; PIP)은 속성 값의 근원지의 역할을 하는 시스템 요소일 수 있다.

[51] 하기에서, 도 1을 참조하여 XACML의 데이터 흐름이 설명된다.

[52] 단계(105)에서, PAP들은 정책들 및 정책 집합(set)들을 작성(write)할 수 있다. PAP들은 PDP가 작성된 정책들 및 정책 집합들을 이용할 수 있게하기 위해, 정책들 및 정책 집합들을 PDP에게 제공할 수 있다. 정책들 및 정책 집합들은 특정한(specified) 목표(target)에 대한 완전한(complete) 정책을 나타낼(represent) 수 있다.

[53] 단계(110)에서, 접근 요청자는 접근에 대한 요청을 PEP로 전송할 수 있다.

[54] 단계(115)에서, PEP는 접근에 대한 요청을 상기의 접근 요청의 원 요청 포맷(native request format)으로 문맥 처리기(context handler)로 전송할 수 있다. 선택적으로, 접근에 대한 요청은 서브젝트들, 자원, 액션 및 환경(environment) 및 다른 카테고리들의 속성을 포함할 수 있다.

[55] 단계(120)에서, 문맥 처리기는 XACML 요청 문맥을 구축(construct)할 수 있고, 생성된 XACML 요청 문맥을 PDP로 전송할 수 있다.

[56] 단계(125)에서, PDP는 추가적인 서브젝트, 자원, 액션, 환경 및 다른 카테고리들의 속성들을 문맥 처리기에게 요청할 수 있다.

[57] 단계(130)에서, 문맥 처리기는 PIP에게 속성들을 요청할 수 있다.

[58] 단계(135)에서, PIP는 요청된 속성들을 획득할 수 있다. 요청된 속성들은 서브젝트 속성, 환경 속성 및 자원 속성을 포함할 수 있다.

[59] 단계(140)에서, PIP는 요청된 속성들을 문맥 처리기에게 반환할 수 있다.

[60] 선택적으로, 단계(145)에서, 문맥 처리기는 문맥에 자원을 포함(include)시킬 수 있다.

[61] 단계(150)에서, 문맥 처리기는 요청된 속성들을 PDP로 전송할 수 있다. 선택적으로, 문맥 처리기는 자원들을 PDP로 전송할 수 있다.

[62] PDP는 정책을 평가(evaluate)할 수 있다.

[63] 단계(155)에서, PDP는 응답 문맥을 문맥 처리기로 전송할 수 있다. 응답 문맥은 권한부여 결정(authorization decision)을 포함할 수 있다.

[64] 단계(160)에서, 문맥 처리기는 응답 문맥을 PEP의 원 요청 포멧으로 전환(translate)할 수 있다. 문맥 처리기는 응답을 PEP로 반환할 수 있다.

[65] 단계(165)에서, PEP는 의무(obligation)들을 이행(fulfill)할 수 있다.

[66] 만약, 접근이 허가(permit)되면, PEP는 자원으로의 접근을 허가할 수 있다. 그렇지 않으면, PEP는 접근을 거부(deny)할 수 있다.

[67] 도 2는 애져 접근 제어 서비스의 프레임 워크를 나타낸다.

[68] 애져 접근 제어 서비스(azure access control service)는 클라우드 내에서 표준 기반의 토큰을 발행할 수 있다. 토큰은 호스트 또는 모든 앱패브릭(AppFabric)의 계정을 사용할 수 있는 멀티-테넌트(multi-tenant)일 수 있다. 토큰은 보안 토큰일 수 있다.

[69] 닷넷(.NET)의 접근 제어 서비스는, 인증 서비스 및 권한부여 서비스가 외부의 보안 전문가에 의해 관리될 수 있게하는 기능을 제공할 수 있다.

[70] 애져의 보안 전문가는 인증 및 토큰 발행(issue)을 제어할 수 있다. 따라서, 어플리케이션은 인증 절차를 토큰 확인으로 대신할 수 있다.

[71] 애저 플랫폼 상에서 수행되는 앱패브릭 접근 컨트롤(control)은 어플리케이션 또는 사용자로부터 벨리드 클레임(valid claim)을 수신할 수 있다. 앱패브릭 접근 컨트롤은 데이터 어플리케이션으로부터 허가 요청을 수신할 수 있다. 앱패브릭 접근 컨트롤은 어플리케이션 또는 사용자로 보안 토큰을 전송할 수 있다.

[72] 도 3은 역할 기반 접근 제어 워크플로우를 나타낸다.

[73] 역할-기반 접근 제어(Role-Based Access Control; RBAC)는 퍼스널 클라우드 서비스에서의 접근 제어에 있어서 기본 개념이 될 수 있다. 도 3에서, 사용자들 각각은 하나 이상의 역할들에 대응한다. 역할들 각각은 하나 이상의 허가들에 대응한다. 예컨대, 각 사용자는 특정한 역할들을 부여받을 수 있으며, 각 역할은

특정한 허가들을 부여받을 수 있다.

[74] 종래의(legacy) 접근 제어 방식에서는, 특정한 데이터 또는 자원에는, 상기의 데이터 또는 자원에 대한 권한을 보유하는 사용자만이 접근할 수 있다.

[75] RBAC을 따르는 모델은 헬스케어 분야 등에서 사용될 수 있다. 예컨대, 일반적인 병원에서는 사용자 별로 역할이 분명하게 구분될 수 있다. 여기서, 사용자는 의사, 간호사 및 환자를 포함할 수 있다.

[76] 사용자의 역할에 따른 권한부여는, 시스템 관리자를 대신하여, 역할-기반 접근 제어에 의해 결정될 수 있다.

[77] 개별적인 사용자들은 사용자의 직무에 따라 뚜렷하게 구분될 수 있다. 직무 상의 역할에 따라, 각 사용자에 대한 서비스 사용의 승인 여부가 서로 상이할 수 있다.

[78] 사용자의 역할 및 역할의 권한은 다-대-다 관계로 구성될 수 있다.

[79] 역할-기반 접근 제어는 다양한 자격증명을 제공할 수 있고, 그룹 별 권한부여를 제공할 수 있다. 반면, 역할-기반 접근 제어는 사용자 권한을 고려하는 서비스 접근 및 데이터 접근을 충족시키지 못할 수 있다. 또한, 역할-기반 접근 제어는 정책 및 사용자 프로파일 정보의 권한의 식별을 충족시키지 못할 수 있다. 따라서, 클라우드 환경을 고려하는 새로운 접근 제어 방법 및 시스템이 요구될 수 있다.

[80] 도 4는 일 실시예에 따른 클라우드 컴퓨팅 서비스에서의 접근 제어 시스템이다.

[81] 접근 제어 시스템(400)은 협업 서비스 서버(410) 및 클라우드 서비스 서버(420)을 포함할 수 있다. 접근 제어 시스템(400)은 단일한 클라우드 서비스 제공자에 의해 제공될 수 있다. 물론, 상술된 구성 외에 다른 구성이 접근 제어 시스템(400)에 포함될 수 있음은 자명하다.

[82] 클라이언트는 사용자가 사용하는 단말을 나타낼 수 있다.

[83] 클라우드 서비스 서버(420)는 사용자를 인증할 수 있다. 사용자는 클라우드 컴퓨팅 서비스를 이용하기 위해서 사용자에게 클라우드 컴퓨팅 서비스를 제공하는 클라우드 서비스 서버(420)에 회원 가입을 할 수 있다. 사용자는 클라우드 서비스 서버(420)에 자신이 사용할 사용자 식별자(identifier; ID), 사용자 패스워드 및 사용자 개인 정보를 입력할 수 있다. 클라우드 서비스 서버(430)는 사용자 인증 후 사용자에게 사용자가 원하는 ID를 발급해 줄 수 있다.

[84] 사용자는 사용자 인증 요청을 협업 서비스 서버(410)로 전송할 수 있다. 협업 서비스 서버(410)는 사용자 인증 요청의 리다이렉션(redirection)을 통해 클라우드 서비스 서버(420)에서 사용자 인증이 수행되게 할 수 있다. 클라우드 서비스 서버(420)는 사용자 개인 정보를 암호화할 수 있고, 암호화된 사용자 개인 정보를 저장할 수 있다. 클라우드 서비스 서버(420)는 상기의 암호화 및 저장을 통해 사용자 개인 정보가 클라우드 서비스 서버(420) 내에 남지 않게 할 수 있다.

[85] 협업 서비스 서버(410)는 사용자의 개인 정보가 클라우드 서비스 서버(420)

내에 남지 않게 하기 위해, 리다이렉션을 통해 클라우드 서비스 서버(420)에게 사용자 인증의 수행을 요청할 수 있다.

[86] 사용자가 인증된 경우, 협업 서비스 서버(410)는 클라우드 서비스 서버(420)의 보안 정책에 기반하여 사용자의 서비스 접근을 위한 접근 토큰을 발행할 수 있다. 접근 토큰은 사용자 인증 정보 및 사용자 권한 정보를 포함할 수 있다.

[87] 사용자가 요청한 서비스가 사용자 서비스 리스트 데이터베이스(530)에 등록되지 않은 경우, 클라우드 서비스 서버(420)는 정책 관리부(630)에게 서비스를 요청할 수 있다. 사용자 서비스 리스트 데이터베이스(530) 및 정책 관리부(630)에 대해 도 5 및 도 6을 참조하여 하기에서 상세히 설명된다.

[88] 클라우드 서비스 서버(420)는 접근 토큰의 사용자 인증 정보 및 사용자 권한 정보를 클라우드 서비스 서버(420)의 접근 제어 목록, 정책 정보부(620)의 보안 정책 및 정책 정보부(620)의 사용자 역할 정보와 비교할 수 있다. 여기서, 사용자 역할 정보는 사용자 권한 정보일 수 있다. 클라우드 서비스 서버(420)는 상기의 비교의 결과에 기반하여 사용자가 원하는 서비스로의 접근을 승인할 수 있다. 정책 정보부(620)에 대해 도 6을 참조하여 하기에서 상세히 설명된다.

[89] 도 5 는 일 실시예에 따른 협업 서비스 서버의 블록도이다.

[90] 협업 서비스 서버(410)는 정책 수행부(510)를 포함할 수 있다. 정책 수행부(510)는 도 1을 참조하여 전술된 PEP일 수 있다.

[91] 정책 수행부(510)는 접근 토큰 발행부(520) 및 사용자 서비스 리스트 데이터베이스(User Service List Database; USLD)(530)를 포함할 수 있다.

[92] USLD(530)는 사용자가 가입한 서비스, 상기의 서비스와 관련된 사용자의 권한 정보 및 상기의 서비스에 대한 보안 정책 정보를 저장할 수 있다.

[93] USLD(530)는 사용자가 가입한 서비스와 관련된 사용자의 권한 정보 및 보안 정책 정보를 주기적으로 업데이트할 수 있다. USLD(530)는 사용자가 새로운 서비스를 요청할 때 사용자가 가입한 서비스와 관련된 사용자의 권한 정보 및 보안 정책 정보를 업데이트할 수 있다.

[94] 접근 토큰 발행부(520)는 면허 확인(Credential Verification; CV)를 수행할 수 있다.

[95] 접근 토큰 발행부(520)는 사용자의 서비스 접근 요청, 사용자 인증 및 서비스 권한에 기반하여 서비스 접근 토큰을 발행할 수 있다. 접근 토큰은 사용자 인증의 정보 및 사용자의 권한 정보를 포함할 수 있다. 접근 토큰 발행부(520)는 사용자에 의해 서비스 접근이 요청될 때 클라우드 서비스 서버(420)로부터 제공된 사용자 인증의 결과에 기반하여 접근 토큰을 발행할 수 있다. 클라우드 서비스 서버(420)는 USLD(530)로부터 사용자가 가입한 서비스와 관련된 권한 정보 및 상기의 서비스와 관련된 보안 정책 정보를 제공 받을 수 있고, 접근 토큰을 발행하기 위해 상기의 권한 정보 및 보안 정책 정보를 이용할 수 있다.

[96] 도 6 은 일 실시예에 따른 클라우드 서비스 서버의 블록도이다.

[97] 클라우드 서비스 서버(420)는 정책 결정부(610), 정책 정보부(620) 및 정책

관리부(630)를 포함할 수 있다. 정책 결정부(610)는 도 1을 참조하여 전술된 PDP일 수 있다. 정책 관리부(630)는 도 1을 참조하여 전술된 PAP일 수 있다.

[98] 정책 결정부(610)는 접근 토큰의 정보를 접근 제어 목록, 정책 정보부(620)의 보안 정책 및 정책 정보부(620)의 사용자 권한 정보와 비교할 수 있다. 정책 결정부(610)는, 상기의 비교의 결과로 접근 토큰의 정보가 접근 제어 목록, 정책 정보부(620)의 보안 정책 및 정책 정보부(620)의 사용자 권한 정보에 부합 또는 일치하면, 사용자의 서비스에 대한 접근을 승인할 수 있다.

[99] 정책 정보부(620)는 서비스에 관련된 보안 정책을 저장할 수 있다. 정책 정보부(620)는 각 서비스에 대한 사용자 권한 정보를 저장할 수 있다. 정책 정보부(422)는 정책 결정부(610)에서 보안 정책 또는 사용자 권한 정보 등과 같은 정보를 요청한 경우, 요청된 정보를 정책 결정부(610)에게 제공할 수 있다.

[100] 정책 관리부(630)는, 사용자의 서비스 요청에 따라, 적합한 사용자의 권한, 서비스 정책 및 역할(role)의 설정 및 수정을 수행할 수 있다. 정책 관리부(630)는 사용자의 권한, 서비스 정책 또는 역할의 설정 또는 수정이 발생한 경우, 설정 또는 수정된 사용자의 권한의 정보, 서비스 정책의 정보 또는 역할의 정보를 협업 서비스 서버(410)의 USLD(530)로 전송할 수 있다.

[101] 정책 관리부(630)는 서비스에 대한 사용자 권한 정보, 서비스 정책 정보 및 역할 정보를 정책 결정부(610)에게 제공할 수 있다.

[102] 서비스 제공자들 각각은 사용자의 권한, 서비스 정책 및 역할을 관리할 수 있다. 서비스 제공자들 각각은 새로운 정보의 생성 또는 변경이 발생한 경우, 상기의 정보를 정책 정보부(620)에 전송할 수 있다. 여기서, 새로운 정보는 사용자의 권한, 서비스 정책 및 역할을 포함할 수 있다. 정책 정보부(620)는 생성 또는 변경된 정보에 기반하여 사용자의 권한, 서비스 정책 또는 역할을 업데이트할 수 있다.

[103] 도 7은 일 실시예에 따른 본 발명의 또 다른 일 실시 예에 따른 다중 클라우드 서비스 서버들의 접근 제어 시스템이다.

[104] 다중 클라우드 서비스 서버들은 클라우드 컴퓨팅 서비스를 제공할 수 있다.

[105] 도 4를 참조하여 전술된 접근 제어 시스템(400)은 복수 개의 클라우드 서비스 서버들을 포함할 수 있다. 예컨대, 클라우드 서비스 서버(420)는 복수 개일 수 있다. 상술한 구성 외에 다른 구성이 접근 제어 시스템(400)에 포함될 수 있다.

[106] 복수 개의 클라우드 서비스 서버들은 각각 서로 상이한 클라우드 서비스 제공자에 의해 제공 또는 운영될 수 있다.

[107] 복수 개의 클라우드 서비스 서버들로서, 제1 클라우드 서비스 서버(710) 및 제2 클라우드 서비스 서버(720)가 도시되었다.

[108] 제1 클라우드 서비스 서버(710) 및 제2 클라우드 서비스 서버(720)는 각각 도 4 내지 도 6을 참조하여 전술된 클라우드 서비스 서버(420)의 기능을 수행할 수 있다.

[109] 앞서 도 1 내지 도 6을 참조하여 설명된 기술적 내용들이 그대로 적용될 수

있으므로, 보다 상세한 설명은 이하 생략하기로 한다.

[110] 도 8은 일 실시예에 따른 단일 클라우드 서비스 서버의 접근 제어 방법의 흐름도이다.

[111] 단계(810)에서, 사용자는 클라우드 컴퓨팅 서비스를 이용하기 위해서 클라우드 서비스 서버(420)에 회원 가입을 할 수 있다.

[112] 사용자는 클라우드 서비스 서버(420)에 자신이 사용할 사용자 식별자(identifier; ID), 사용자 패스워드 및 사용자 개인 정보를 입력할 수 있다. 클라우드 서비스 서버(420)는 클라이언트로부터 사용자 식별자, 사용자 패스워드 및 사용자 개인 정보를 수신하고, 수신한 사용자 식별자, 사용자 패스워드 및 사용자 개인 정보를 사용하여 사용자를 등록할 수 있다. 클라우드 서비스 서버(430)는 사용자 인증 후 사용자에게 사용자가 원하는 ID를 발급해 줄 수 있다.

[113] 단계(820)에서, 사용자는 인증 요청을 협업 서비스 서버(410)로 전송할 수 있다. 협업 서비스 서버(410)는 사용자가 사용하는 클라이언트로부터 인증 요청을 수신할 수 있다.

[114] 단계(825)에서, 협업 서비스 서버(410)는 사용자 인증 요청의 리다이렉션(redirection)을 통해 클라우드 서비스 서버(420)에서 사용자 인증이 수행되게 할 수 있다. 협업 서비스 서버(410)는 사용자 인증 요청을 클라우드 서비스 서버(420)로 리다이렉트할 수 있다.

[115] 단계(830)에서, 리다이렉션에 의해 사용자 인증 요청을 수신한 클라우드 서비스 서버(420)는 사용자 인증을 수행할 수 있다.

[116] 클라우드 서비스 서버(420)는 사용자 개인 정보를 암호화할 수 있고, 암호화된 사용자 개인 정보를 저장할 수 있다. 클라우드 서비스 서버(420)는 상기의 암호화 및 저장을 통해 사용자 개인 정보가 클라우드 서비스 서버(420) 내에 남지 않게 할 수 있다.

[117] 사용자 인증 후, 단계(840)에서, 사용자는 이용을 원하는 서비스에 대한 서비스 요청을 협업 서비스 서버(410)로 전송할 수 있다. 협업 서비스 서버(410)는 사용자의 클라이언트로부터 서비스 요청을 수신할 수 있다.

[118] 단계(850)에서, 협업 서비스 서버(410)는 사용자가 요청한 서비스가 새로운 서비스인지 여부를 판단할 수 있다. 협업 서비스 서버(410)는 사용자가 새로운 서비스를 이용하는지 여부를 판단할 수 있다.

[119] 협업 서비스 서버(410)는, 사용자가 요청한 서비스가 USLD(530)에 등록되지 않은 경우, 사용자가 요청한 서비스를 새로운 서비스로 판단할 수 있다. USLD(530)는 사용자 인증 정보를 포함할 수 있으며, 사용자 ID 및 사용자가 요청한 서비스의 정보를 포함할 수 있다.

[120] 사용자가 새로운 서비스를 이용하는 경우, 단계(860)가 수행될 수 있다. 사용자가 기존의 서비스를 이용하는 경우, 단계(870)가 수행될 수 있다.

[121] 단계(860)에서, 협업 서비스 서버(410)의 접근 토큰 발행부(520)는 클라우드 서비스 서버(420)의 정책 관리부(630)에게 새로운 서비스를 요청할 수 있다. 정책

관리부(630)는 접근 토큰 발행부(520)로부터 새로운 서비스의 요청을 수신할 수 있다.

[122] 단계(862)에서, 정책 관리부(630)는 사용자 인증 정보에 기반하여 새로운 서비스를 설정할 수 있다. 여기서, 새로운 서비스의 설정은 새로운 서비스에 대한 서비스 이용 권한, 서비스 범위, 서비스 보안 정책 및 서비스 역할 중 하나 이상의 설정을 포함할 수 있다.

[123] 단계(864)에서, 정책 관리부(630)는 정책 정보부(620) 내에 새로운 서비스의 설정을 저장할 수 있다.

[124] 정책 정보부(620)에 등록된 권한 정보 및 보안 정책 정보는 USLD(530)에 저장될 수 있다.

[125] 단계(866)에서, 접근 토큰 발행부(520)는 사용자의 서비스 접근 요청, 사용자 인증 및 서비스 권한에 기반하여 상기 서비스의 접근 토큰을 생성할 수 있다. 접근 토큰 발행부(520)는 사용자 인증의 정보, 권한 정보 및 보안 정책 정보에 기반하여 접근 토큰을 생성할 수 있다. 권한 정보 및 보안 정보는 USLD(530)에 의해 제공될 수 있다.

[126] 접근 토큰 발행부(520)는 생성된 접근 토큰을 사용자의 클라이언트에게 전송할 수 있다.

[127] 사용자가 기존의 서비스를 이용하는 경우, 단계(870)에서, 협업 서비스 서버(410)는 사용자가 원하는 서비스에 대한 권한 정보를 USLD(530)에서 검색한다. 기존의 서비스가 이용될 경우, 기존의 서비스에 대한 기존의 권한 정보 및 보안 정책 정보가 활용될 수 있다. 예컨대, 기존의 서비스가 이용될 경우, 권한 정책 및 보안 정책이 변동되지 않으므로, 기존의 권한 정보 및 보안 정책 정보가 활용될 수 있다.

[128] 단계(875)에서, 접근 토큰 발행부(520)는 사용자의 서비스 접근 요청, 사용자 인증 및 서비스 권한에 기반하여 상기 서비스의 접근 토큰을 생성할 수 있다. 접근 토큰 발행부(520)는 사용자 인증의 정보, 권한 정보 및 보안 정책 정보에 기반하여 접근 토큰을 생성할 수 있다. 권한 정보 및 보안 정보는 USLD(530)에 의해 제공될 수 있다.

[129] 접근 토큰 발행부(520)는 생성된 접근 토큰을 사용자의 클라이언트에게 전송할 수 있다.

[130] 단계(880)에서, 사용자의 클라이언트는 접근 토큰을 사용하여 클라우드 서비스 서버(420)에게 서비스 접근을 요청할 수 있다. 클라우드 서비스 서버(420)는 사용자의 클라이언트로부터 서비스 접근 요청을 수신할 수 있다. 서비스 접근 요청은 접근 토큰을 포함할 수 있다. 서비스 접근 요청은 접근 토큰을 사용함에 의해 수행될 수 있다.

[131] 단계(885)에서, 클라우드 서비스 서버(420)의 정책 결정부(610)는 정책 정보부(620)에 의해 제공된 권한 정보, 정책 정보부(620)에 의해 제공된 보안 정책 정보 및 접근 제어 목록의 사용자 접근 제어 목록을 접근 토큰의 사용자

인증 정보, 접근 토큰의 권한 정보 및 접근 토큰의 보안 정책 정보와 비교할 수 있다. 정책 결정부(610)는 상기의 비교의 결과 정책 정보부(620)에 의해 제공된 권한 정보, 정책 정보부(620)에 의해 제공된 보안 정책 정보 및 접근 제어 목록의 사용자 접근 제어 목록이 접근 토큰의 사용자 인증 정보, 접근 토큰의 권한 정보 및 접근 토큰의 보안 정책 정보에 부합하면, 사용자가 서비스 접근을 요청한 서비스를 승인할 수 있다.

[132] 상기의 승인 후, 사용자는 서비스를 호출할 수 있고, 협업 서비스 환경에서 서비스를 이용할 수 있다.

[133] 단계(890)에서, 사용자가 서비스를 이용하는 중, 사용자는 다른 서비스 또는 다른 클라우드 서비스 제공자에 의해 제공되는 서비스를 이용하는 것을 원할 수 있다. 협업 서비스 서버(410)는 사용자의 클라이언트로부터 다른 서비스 요청을 수신할 수 있다.

[134] 협업 서비스 서버(410)의 접근 토큰 발행부(520)는 다른 서비스를 제공하는 클라우드 서비스 서버(420)의 정책 관리부(630)에게 상기의 다른 서비스의 이용의 요청을 할 수 있다. 즉, 다른 서비스에 대한 요청은 협업 서비스 서버(410)의 접근 토큰 발행부(520)를 통해 클라우드 서비스 서버(420)의 정책 관리부(630)로 전송된다.

[135] 다른 서비스의 이용 요청이 발생한 경우, 다른 서비스에 대응하는 클라우드 서비스 서버(420)의 접근 토큰에 새로운 권한 정보 및 보안 정책 정보가 업데이트들 수 있다. 새로운 권한 정보 및 보안 정책 정보가 업데이트된 접근 토큰을 사용함으로싸 사용자는 다른 서비스를 이용할 수 있다.

[136] 앞서 도 1 내지 도 7을 참조하여 설명된 기술적 내용들이 그대로 적용될 수 있으므로, 보다 상세한 설명은 이하 생략하기로 한다.

[137] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPA(field programmable array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬

프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[138] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[139] 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.

[140] 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.

[141] 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.

청구범위

[청구항 1] 사용자가 가입한 서비스와 관련된 상기 사용자의 권한 정보 및 상기 서비스에 대한 보안 정책 정보를 저장하는 사용자 서비스 리스트 데이터베이스; 및
사용자의 서비스 접근 요청, 사용자 인증 및 서비스 권한에 기반하여 상기 서비스의 접근 토큰을 발행하는 접근 토큰 발행부를 포함하는, 클라우드 컴퓨팅 서비스의 협업 서비스 서버.

[청구항 2] 제1항에 있어서,
상기 협업 서비스 서버는 클라우드 서비스 서버를 통해 상기 사용자 인증을 수행하는, 클라우드 컴퓨팅 서비스의 협업 서비스 서버.

[청구항 3] 제2항에 있어서,
상기 접근 토큰 발행부는 상기 클라우드 서비스 서버로부터 제공된 상기 사용자 인증의 결과에 기반하여 상기 접근 토큰을 발행하는, 클라우드 컴퓨팅 서비스의 협업 서비스 서버.

[청구항 4] 제1항에 있어서,
상기 사용자 서비스 리스트 데이터베이스는 상기 클라우드 서비스 서버에게 상기 권한 정보 및 상기 보안 정책 정보를 제공하는, 클라우드 컴퓨팅 서비스의 협업 서비스 서버.

[청구항 5] 제1항에 있어서,
상기 접근 토큰은 상기 사용자 인증의 정보 및 상기 권한 정보를 포함하는, 클라우드 컴퓨팅 서비스의 협업 서비스 서버.

[청구항 6] 제1항에 있어서,
상기 사용자 서비스 리스트 데이터베이스는 상기 권한 정보 및 상기 보안 정책 정보를 주기적으로 업데이트하는, 클라우드 컴퓨팅 서비스의 협업 서비스 서버.

[청구항 7] 제1항에 있어서,
상기 사용자 서비스 리스트 데이터베이스는 상기 사용자가 새로운 서비스를 요청할 때 상기 사용자가 가입한 서비스와 관련된 상기 권한 정보 및 상기 보안 정책 정보를 업데이트하는, 클라우드 컴퓨팅 서비스의 협업 서비스 서버.

[청구항 8] 사용자가 접근하는 서비스에 관련된 보안 정책을 저장하고, 상기 서비스에 대한 사용자 권한 정보를 저장하는 정책 정보부; 및
접근 토큰의 정보를 접근 제어 목록, 보안 정책 및 사용자의 권한 정보와 비교하고, 상기 비교의 결과로 상기 접근 제어 목록 및 상기 보안 정책 및 상기 사용자 권한 정보에 부합하면, 상기 사용자의 상기 서비스에 대한 접근을 승인하는 정책 결정부

를 포함하는, 클라우드 서비스 서버.

[청구항 9] 제8항에 있어서,
상기 사용자의 권한, 서비스 정책 및 역할을 설정 또는 수정하는 정책 관리부
를 더 포함하는, 클라우드 서비스 서버.

[청구항 10] 제9항에 있어서,
상기 정책 관리부는 상기 사용자의 권한, 상기 서비스 정책 또는 상기 역할의 설정 또는 수정이 발생한 경우, 설정 또는 수정된 상기 사용자의 권한의 정보, 상기 서비스 정책의 정보 또는 상기 역할의 정보를 상기 협업 서비스 서버로 전송하는, 클라우드 서비스 서버.

[청구항 11] 사용자 서비스 리스트 데이터베이스가 사용자가 가입한 서비스와 관련된 상기 사용자의 권한 정보 및 상기 서비스에 대한 보안 정책 정보를 저장하는 단계; 및
접근 토큰 발행부가 사용자의 서비스 접근 요청, 사용자 인증 및 서비스 권한에 기반하여 상기 서비스의 접근 토큰을 발행하는 단계
를 포함하는, 클라우드 컴퓨팅 서비스에서의 협업 서비스 제공 방법.

[청구항 12] 제11항에 있어서,
클라우드 서비스 서버를 통해 상기 사용자 인증을 수행하는 단계
를 더 포함하는, 클라우드 컴퓨팅 서비스에서의 협업 서비스 제공 방법.

[청구항 13] 제12항에 있어서,
상기 발행하는 단계는 상기 클라우드 서비스 서버로부터 제공된 상기 사용자 인증의 결과에 기반하여 상기 접근 토큰을 발행하는, 클라우드 컴퓨팅 서비스에서의 협업 서비스 제공 방법.

[청구항 14] 제11항에 있어서,
상기 저장하는 단계는 상기 클라우드 서비스 서버에게 상기 권한 정보 및 상기 보안 정책 정보를 제공하는, 클라우드 컴퓨팅 서비스에서의 협업 서비스 제공 방법.

[청구항 15] 제11항에 있어서,
상기 접근 토큰은 상기 사용자 인증의 정보 및 상기 권한 정보를 포함하는, 클라우드 컴퓨팅 서비스에서의 협업 서비스 제공 방법.

[청구항 16] 제11항에 있어서,
상기 사용자 서비스 리스트 데이터베이스는 상기 권한 정보 및 상기 보안 정책 정보를 주기적으로 업데이트하는, 클라우드 컴퓨팅 서비스에서의 협업 서비스 제공 방법.

[청구항 17] 제11항에 있어서,

상기 사용자 서비스 리스트 데이터베이스는 상기 사용자가 새로운 서비스를 요청할 때 상기 사용자가 가입한 서비스와 관련된 상기 권한 정보 및 상기 보안 정책 정보를 업데이트하는, 클라우드 컴퓨팅 서비스에서의 협업 서비스 제공 방법.

[청구항 18] 정책 정보부가 사용자가 접근하는 서비스에 관련된 보안 정책을 저장하고, 상기 서비스에 대한 사용자 권한 정보를 저장하는 단계; 및

정책 결정부가 접근 토큰의 정보를 접근 제어 목록, 보안 정책 및 사용자의 권한 정보와 비교하고, 상기 비교의 결과로 상기 접근 제어 목록 및 상기 보안 정책 및 상기 사용자 권한 정보에 부합하면, 상기 사용자의 상기 서비스에 대한 접근을 승인하는 단계

를 포함하는, 클라우드 서비스 제공 방법.

[청구항 19] 제18항에 있어서,

정책 관리부가 사용자의 권한, 서비스 정책 및 역할을 설정 또는 수정하는 단계

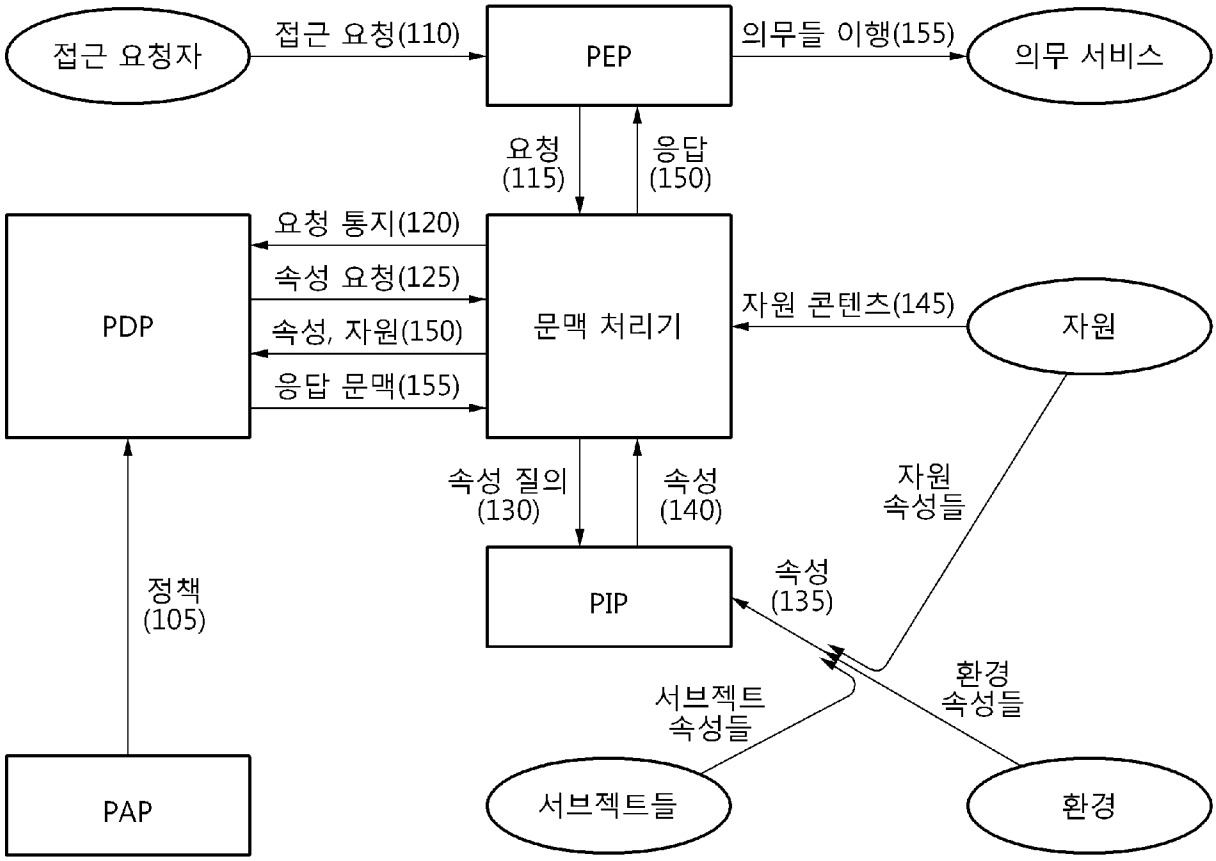
를 더 포함하는, 클라우드 서비스 제공 방법.

[청구항 20] 제19항에 있어서,

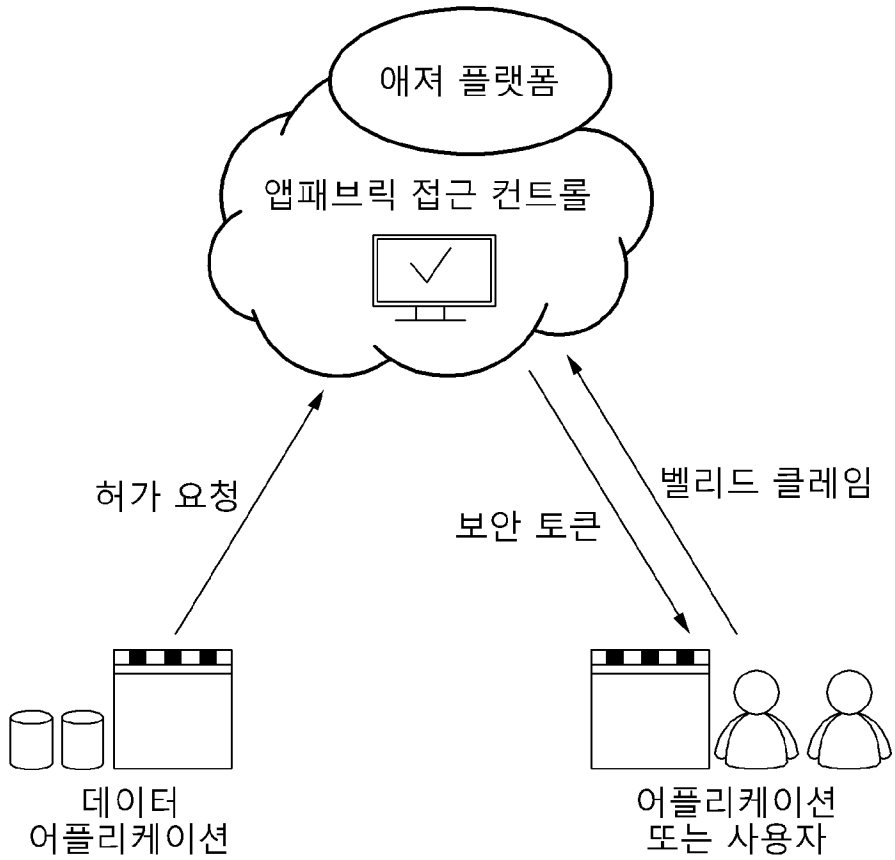
상기 정책 관리부가 상기 사용자의 권한, 상기 서비스 정책 또는 상기 역할의 설정 또는 수정이 발생한 경우, 설정 또는 수정된 상기 사용자의 권한의 정보, 상기 서비스 정책의 정보 또는 상기 역할의 정보를 상기 협업 서비스 서버로 전송하는 단계

를 더 포함하는, 클라우드 서비스 공 방법.

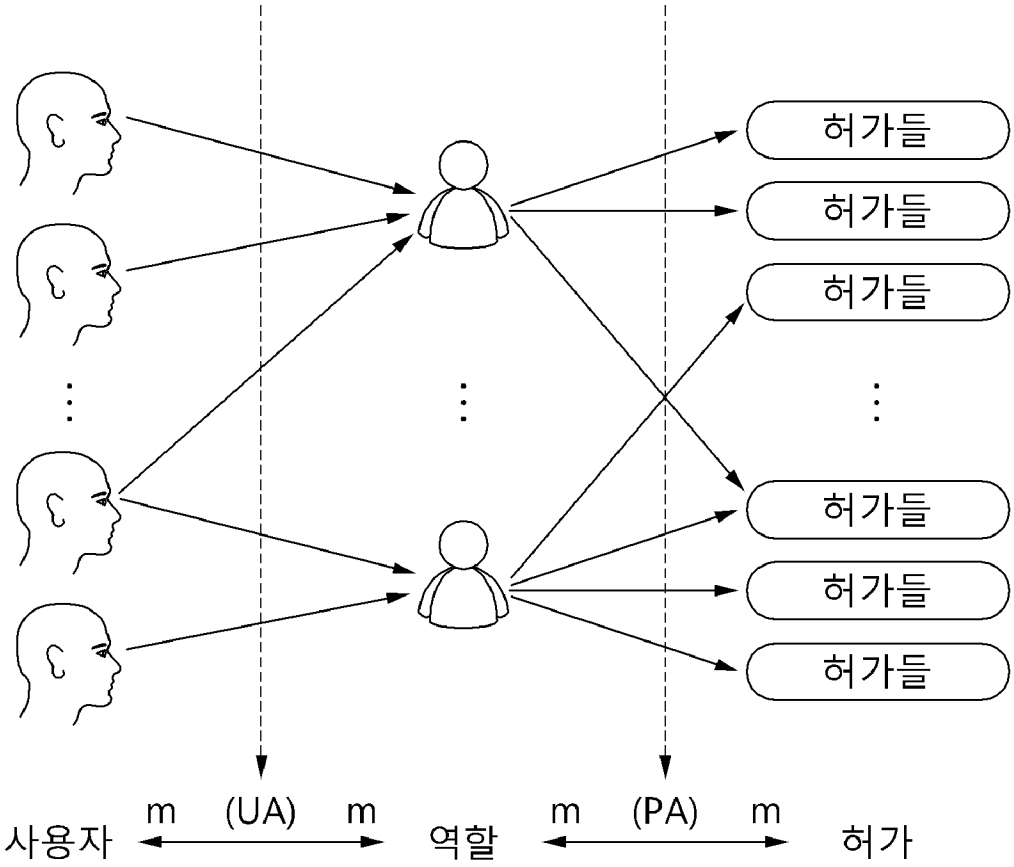
[Fig. 1]


접근 요청자
접근 요청(110)
PEP
의무들 이행(155)
의무 서비스
요청
(115)
응답
(150)
요청 통지(120)
속성 요청(125)
속성, 자원(150)
응답 문맥(155)
PDP
문맥 처리기
자원 콘텐츠(145)
자원
속성 질의
(130)
속성
(140)
자원
속성들
정책
(105)
PIP
속성
(135)
환경
속성들
서브젝트
속성들
PAP
서브젝트들
환경

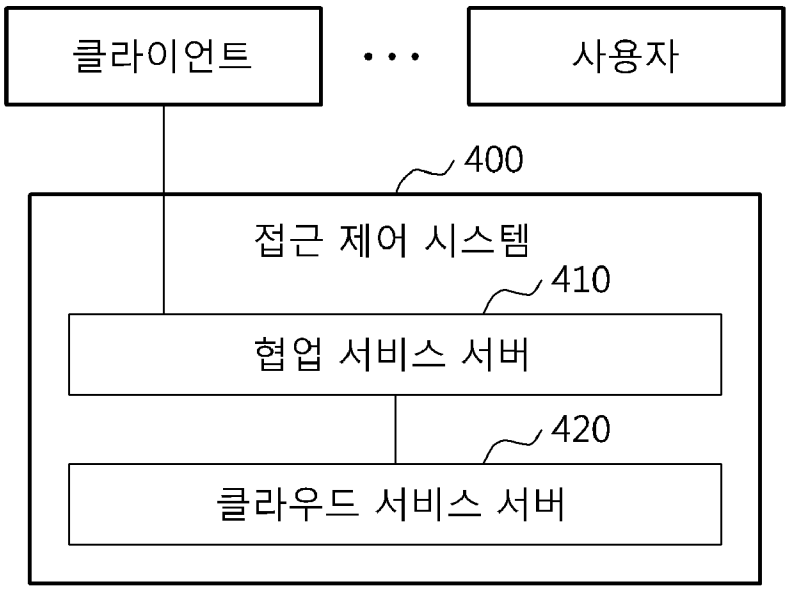
[Fig. 2]


애져 플랫폼
앱패브릭 접근 컨트롤
허가 요청
보안 토큰
벨리드 클레임
데이터
어플리케이션
어플리케이션
또는 사용자

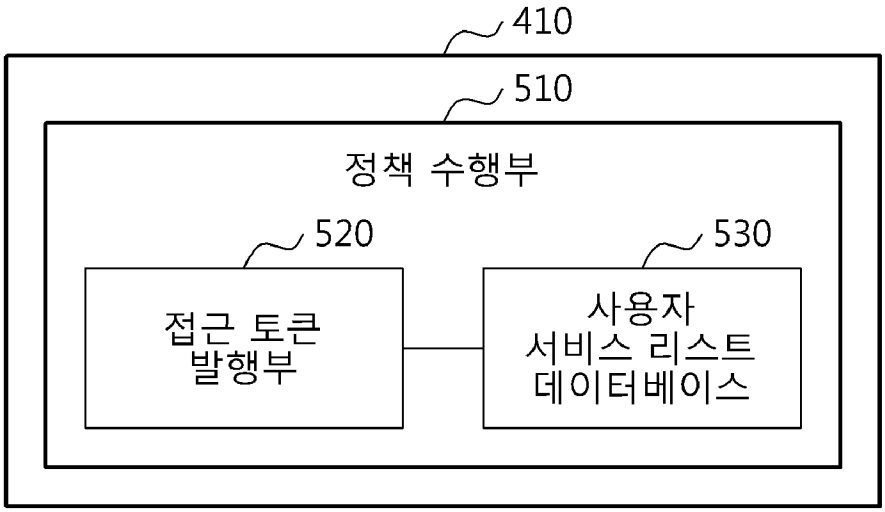
[Fig. 3]


허가들
허가들
허가들
허가들
허가들
허가들
사용자
m
(UA)
m
역할
m
(PA)
m
허가

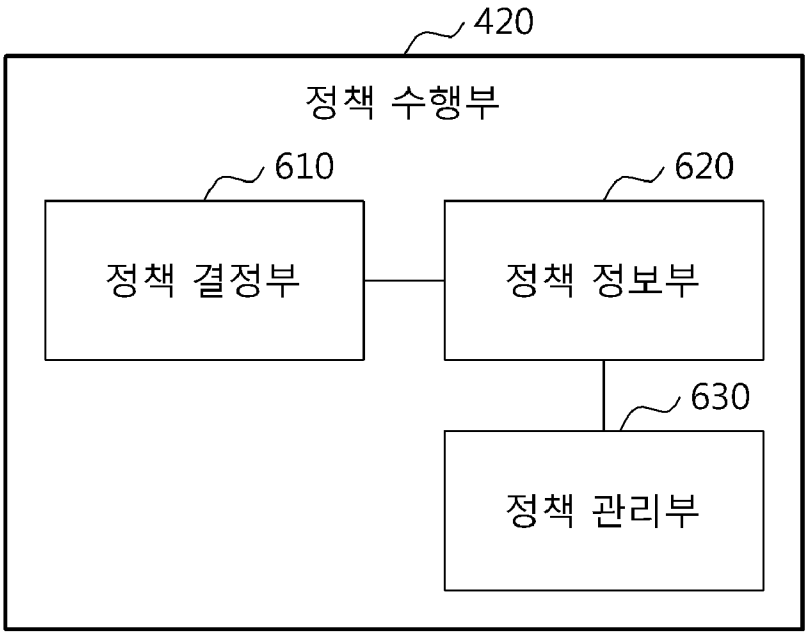
[Fig. 4]


클라이언트
• • •
사용자
400
접근 제어 시스템
410
협업 서비스 서버
420
클라우드 서비스 서버

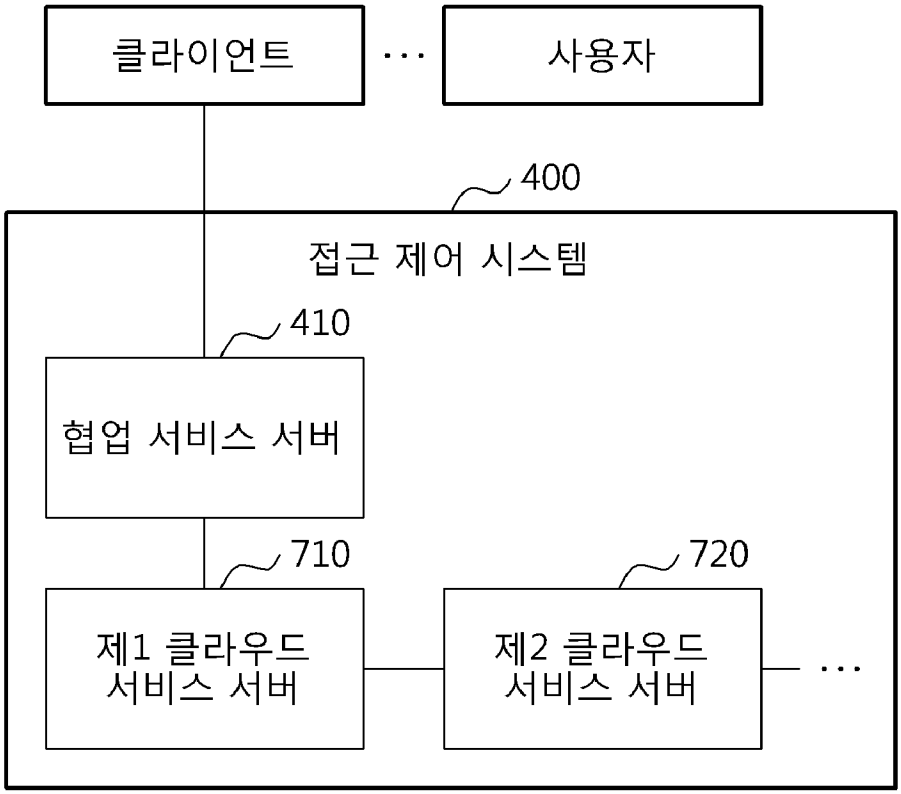
[Fig. 5]


410
510
정책 수행부
520
530
접근 토큰
발행부
사용자
서비스 리스트
데이터베이스

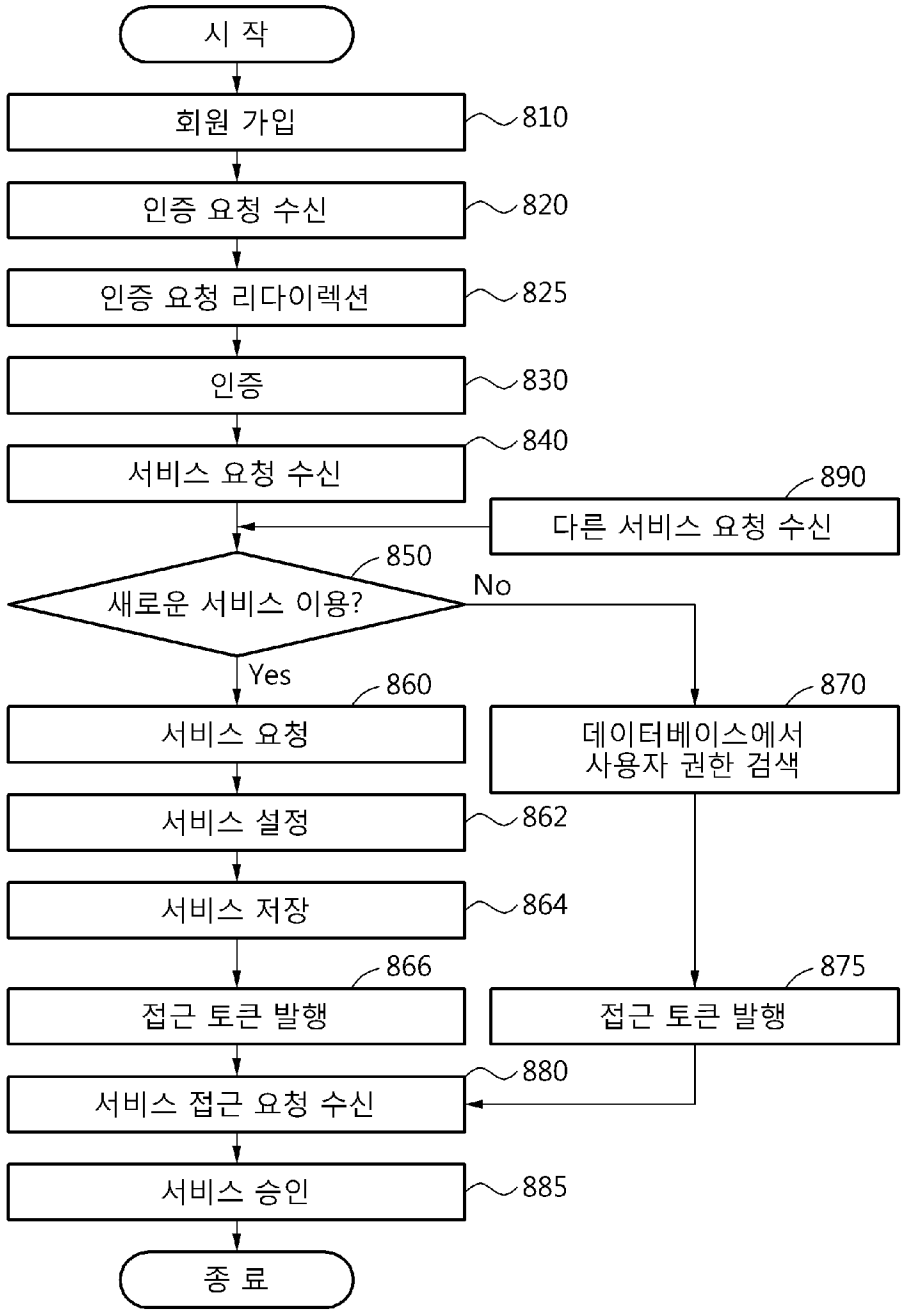
[Fig. 6]


420
정책 수행부
610
620
정책 결정부
정책 정보부
630
정책 관리부

[Fig. 7]


클라이언트
...
사용자
400
접근 제어 시스템
410
협업 서비스 서버
710
720
제1 클라우드 서비스 서버
제2 클라우드 서비스 서버
...

[Fig. 8]


시 작
회원 가입
810
인증 요청 수신
820
인증 요청 리다이렉션
825
인증
830
서비스 요청 수신
840
890
다른 서비스 요청 수신
850
새로운 서비스 이용?
No
Yes
860
서비스 요청
870
데이터베이스에서
사용자 권한 검색
서비스 설정
862
서비스 저장
864
866
접근 토큰 발행
875
접근 토큰 발행
880
서비스 접근 요청 수신
서비스 승인
885
종 료

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2012/008855

A. CLASSIFICATION OF SUBJECT MATTER

G06F 15/16(2006.01)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 15/16; G06F 15/00; G06F 17/00; H04N 5/76; G06F 9/06; H04L 9/32; H04W 12/08; 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: cloud computing, access right, authentication, security

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2011-0045598 A (SAMSUNG SDS CO.,LTD.) 04 May 2011 See abstract, paragraphs [24], [29]-[33], [44], claims 1-7 and figures 1, 2.	1-20
Y A	KR 10-2008-0002290 A (POSCO ICT COMPANY LTD) 04 January 2008 See abstract, paragraphs [39]-[42], [53]-[60], claim 1.	1-7,11-17 8-10,18-20
Y A	KR 10-2008-0009898 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE et al.) 30 January 2008 See abstract, paragraphs [20]-[33], [38]-[42], claims 1-10 and figures 1-3.	6-10,16-20 1-5,11-15
A	KR 10-0651751 B1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 01 December 2006 See paragraphs [27]-[35], [39], claims 4-6 and figure 2.	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 FEBRUARY 2013 (26.02.2013)	**27 FEBRUARY 2013 (27.02.2013)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2012/008855

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2011-0045598 A	04.05.2011	NONE	
KR 10-2008-0002290 A	04.01.2008	CN 101461178 A	17.06.2009
		JP 2009-539172 A	12.11.2009
		US 2009-0313477 A1	17.12.2009
		WO 2008-002102 A1	03.01.2008
KR 10-2008-0009898 A	30.01.2008	NONE	
KR 10-0651751 B1	01.12.2006	US 2007-0089162 A1	19.04.2007

국 제 조 사 보 고 서

국제출원번호
PCT/KR2012/008855

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 15/16(2006.01)i, H04L 9/32(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
G06F 15/16; G06F 15/00; G06F 17/00; H04N 5/76; G06F 9/06; H04L 9/32; H04W 12/08; 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: 클라우드 컴퓨팅, 접근 권한, 인증, 보안

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-2011-0045598 A (삼성에스디에스 주식회사) 2011.05.04 요약, 단락 [24], [29]-[33], [44], 청구항 1-7 및 도면 1, 2 참조.	1-20
Y A	KR 10-2008-0002290 A (포스데이타 주식회사) 2008.01.04 요약, 단락 [39]-[42], [53]-[60], 청구항 1 참조.	1-7,11-17 8-10,18-20
Y A	KR 10-2008-0009898 A (한국전자통신연구원 외 1명) 2008.01.30 요약, 단락 [20]-[33], [38]-[42], 청구항 1-10 및 도면 1-3 참조.	6-10,16-20 1-5,11-15
A	KR 10-0651751 B1 (한국전자통신연구원) 2006.12.01 단락 [27]-[35], [39], 청구항 4-6 및 도면 2 참조.	1-20

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

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

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

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

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

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

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

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

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

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2013년 02월 26일 (26.02.2013)	**2013년 02월 27일 (27.02.2013)**

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 82-42-472-7140

심사관
홍경아
전화번호 82-42-481-5668

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2012/008855

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2011-0045598 A	2011.05.04	없음	
KR 10-2008-0002290 A	2008.01.04	CN 101461178 A	2009.06.17
		JP 2009-539172 A	2009.11.12
		US 2009-0313477 A1	2009.12.17
		WO 2008-002102 A1	2008.01.03
KR 10-2008-0009898 A	2008.01.30	없음	
KR 10-0651751 B1	2006.12.01	US 2007-0089162 A1	2007.04.19