(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2014 년 1 월 3 일 (03.01.2014)

WIPO | PCT

(10) 국제공개번호
WO 2014/003516 A1

(51) 국제특허분류:
G06F 15/16 (2006.01) *H04L 9/32* (2006.01)
G06F 21/14 (2013.01)

(21) 국제출원번호: PCT/KR2013/005822

(22) 국제출원일: 2013 년 7 월 1 일 (01.07.2013)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2012-0071147 2012 년 6 월 29 일 (29.06.2012) KR

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

(72) 발명자: **허의남 (HUH, Eui Nam)**; 446-582 경기도 용인시 기흥구 보라동 570 현대 모닝 사이드 아파트 316 동 1802 호, Gyeonggi-do (KR). **나상호 (NA, Sang Ho)**; 446-906 경기도 용인시 기흥구 서천동 1 번지 전자 정보 대학 322 호, Gyeonggi-do (KR).

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

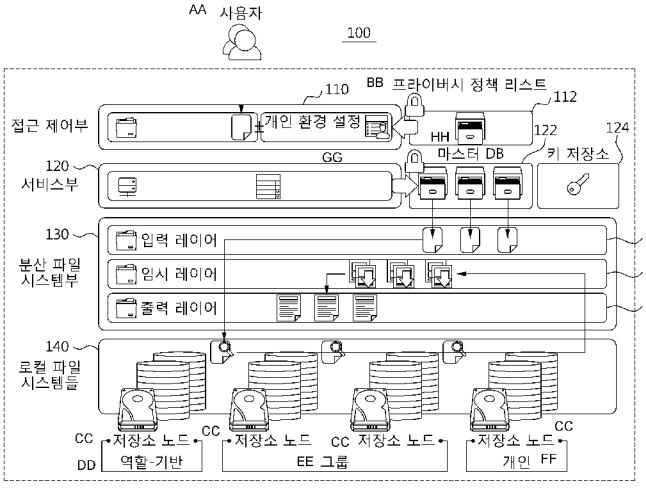
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA,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

공개:
— 국제조사보고서와 함께 (조약 제 21 조(3))

(54) **Title**: METHOD AND APPARATUS FOR PROVIDING DATA SHARING

(54) **발명의 명칭** : 데이터 공유 제공 방법 및 장치



AA ... User
BB ... Privacy policy list
CC ... Storage node
DD ... Role-based
EE ... Group
FF ... Individual
GG ... Individual environment setup
HH ... DB Master DB
132 ... Input layer
134 ... Temporary layer
136 ... Output layer
110 ... Access control unit
120 ... Service unit
124 ... Key storage
130 ... Distributed file system unit
140 ... Local file systems

(57) **Abstract**: Provided are a method and apparatus for data sharing based on an individual environment setup. An access control unit authenticates the user having requested a data object, and extracts the individual environment setup of the user. The individual environment setup includes a list of data objects possessed by the user and access information on each data object in the list. A service unit acquires the data object requested from a distributed file system unit using the individual environment setup, and provides the requested data object to the user.

(57) **요약서**: 개인 환경 설정에 기반한 데이터 공유 방법 및 장치가 제공된다. 접근 제어부는 데이터 객체를 요청한 사용자를 인증하고, 사용자의 개인 환경 설정을 추출한다. 개인 환경 설정은 상기 사용자가 소유한 데이터 객체들의 목록 및 목록 내의 각 데이터 객체에 대한 접근 정보를 포함한다. 서비스부는 개인 환경 설정을 사용하여 분산 파일 시스템부로부터 요청된 데이터 객체를 획득하고, 요청된 데이터 객체를 사용자에게 제공한다.

WO 2014/003516 A1

명세서

발명의 명칭: 데이터 공유 제공 방법 및 장치

기술분야

[1] 아래의 실시예들은 데이터 공유 제공 방법 및 장치에 관한 것으로, 보다 상세히는 개인 환경 설정에 기반한 데이터 공유 방법 및 장치가 제공된다.

배경기술

[2] 최근 클라우드 서비스(cloud service)와 같이 아웃소싱(outsourcing) 형태의 컴퓨팅 자원을 활용한 다양한 서비스가 제공되고 있다. 아웃소싱 형태의 컴퓨팅 자원은 플랫폼, 인프라 및 어플리케이션 등을 의미할 수 있다. 이러한 아웃소싱 형태는 인터넷 상의 일반 사용자들에게 서비스를 제공하고, 기업의 정보통신 인프라 비용을 절감하고, 비용 대비 자원 효율성을 향상시키기 위해 도입되고 있다.

[3] 종래의 단순한 접근 제어 리스트(Access Control List; ACL)에 기반한 접근 제어 방식은 기본적인 사용자 인증만을 제공할 뿐, 사용자가 허가되지 않은 데이터에 접근할 경우에 있어서의 접근 제어 또는 기업에서 요구되는 계층화된 접근 제어에 대한 요구를 충족시키지 못한다. 또한, 종래의 접근 제어 방식은 사용자들 간의 또는 그룹들 간의 데이터 공유 형태만을 제공할 뿐, 하나의 파일에 다수의 공유 사용자 및 공유 그룹들이 존재하는 복잡한 형태의 데이터 공유를 제공하기 어렵니다.

[4] 하기에서, 분산 컴퓨팅 환경 혹은 분산 파일 시스템 환경의 서비스에서 사용자에게 다양한 접근 제어를 제공하면서도 안전한 파일 공유를 제공하는 방법 및 장치가 개시된다.

발명의 상세한 설명

기술적 과제

[5] 일 실시예는 클라우드 서비스와 같은 분산 컴퓨팅 혹은 분산 파일 시스템을 사용하는 서비스에서 다수의 사용자들 간에 프라이버시를 보호하면서 다양한 형태의 공유 및 접근 제어를 수행하는 방법 및 장치를 제공할 수 있다.

과제 해결 수단

[6] 일 측에 따르면, 접근 제어부가 데이터 객체를 요청한 사용자를 인증하는 단계, 접근 제어부가 상기 사용자의 개인 환경 설정을 추출하는 단계 - 상기 개인 환경 설정은 상기 사용자가 소유한 데이터 객체들의 목록 및 상기 목록 내의 각 데이터 객체에 대한 접근 정보를 포함함 -, 서비스부가 상기 개인 환경 설정을 사용하여 분산 파일 시스템부로부터 상기 요청된 데이터 객체를 획득하는 단계 및 서비스부가 요청된 데이터 객체를 제공하는 단계를 포함하는, 데이터 제공 방법이 제공될 수 있다.

[7] 상기 접근 정보는 상기 데이터 객체에 대해 접근이 허가된 개인에 대한 정보,

상기 데이터 객체에 대하여 접근이 허가된 그룹에 대한 정보 및 상기 개인 또는 상기 그룹의 역할에 대한 정보를 포함할 수 있다.

[8] 상기 역할은 상기 데이터 객체를 제공하는 시스템 내에서 설정된 계층화된 직책을 나타낼 수 있다.

[9] 상기 요청된 데이터 객체를 제공하는 단계는, 서비스부가 마스터 데이터베이스에게 요청된 데이터 객체에 대한 정보를 제공하는 단계, 상기 마스터 데이터베이스가 상기 분산 파일 시스템부에게 데이터 객체의 데이터 블록들에 대한 정보를 제공하는 단계, 상기 분산 파일 시스템부가 상기 데이터 블록들에 대한 정보에 기반하여 하나 이상의 저장소 노드들로부터 상기 데이터 블록들 각각을 획득하는 단계, 상기 분산 파일 시스템부가 상기 획득된 데이터 블록들을 하나로 합침으로써 상기 요청된 데이터 객체를 생성하는 단계 및 상기 분산 파일 시스템부가 상기 요청된 데이터 객체를 상기 서비스부로 전달하는 단계를 포함할 수 있다.

[10] 상기 데이터 블록들 각각은 암호화되어 상기 하나 이상의 저장소 노드들 내에 저장되어 있을 수 있다.

[11] 상기 분산 파일 시스템부는 상기 획득된 데이터 블록들 각각을 복호화한 후 상기 복호화된 데이터 블록들을 상기 하나의 데이터로 합칠 수 있다.

[12] 상기 데이터 블록들은 상기 데이터 객체가 기 정의된 크기로 나뉘어진 블록들일 수 있다.

[13] 상기 기 정해진 크기는 하나의 데이터 블록만으로는 상기 데이터 객체의 내용이 확인될 수 없게 하는 크기일 수 있다.

[14] 상기 기 정해진 크기는 상기 데이터 객체의 종류에 따라 상이할 수 있다.

[15] 다른 일 측에 따르면, 데이터 객체를 요청한 사용자를 인증하고, 상기 사용자의 개인 환경 설정을 추출하는 접근 제어부 - 상기 개인 환경 설정은 상기 사용자가 소유한 데이터 객체들의 목록 및 상기 목록 내의 각 데이터 객체에 대한 접근 정보를 포함함 - 및 상기 개인 환경 설정을 사용하여 분산 파일 시스템부로부터 상기 요청된 데이터 객체를 획득하고, 상기 요청된 데이터 객체를 제공하는 서비스부를 포함하는, 데이터 제공 시스템이 제공될 수 있다.

[16] 상기 데이터 제공 시스템은, 상기 서비스로부터 요청된 데이터 객체에 대한 정보를 제공받는 마스터 데이터베이스 및 상기 마스터 데이터베이스로부터 상기 대이터 객체의 데이터 블록들에 대한 정보를 제공받고, 상기 데이터 블록들에 대한 정보에 기반하여 복수 개의 로컬 파일 시스템들로부터 상기 데이터 블록들 각각을 획득하고, 상기 획득된 데이터 블록들을 하나의 데이터로 합침으로써 상기 요청된 데이터 객체를 생성하고, 상기 요청된 데이터 객체를 상기 서비스부로 전달하는 분산 파일 시스템을 더 포함할 수 있다.

발명의 효과

[17] 분산 파일 시스템 환경에서 기업이 요구하는 데이터에 대한 접근 제어를

만족시키고, 보안 문제를 해결하는 방법 및 장치가 제공된다.

[18] 개인의 키로 암호화 되어 저장되는 파일 리스트를 통해 클라우드 서비스로서의 인프라스트럭처(Infrastructure as a Service; IaaS)의 개인 정보 보호, 데이터에 대한 비밀성 및 데이터에 대한 무결성 요구를 충족시키는 방법 및 장치가 제공된다.

[19] 역할-기반 키를 사용하여 다양한 레벨 및 범위에서의 데이터 공유 요구를 충족시키는 방법 및 장치가 제공된다.

[20] 분산 파일 시스템에 데이터 객체가 저장될 -, 데이터 객체의 중요도 및 공유 범위 등을 기반으로 저장소 노드를 분류 및 관리하는 방법 및 장치가 제공된다.

[21] 클라우드 서비스 상의 데이터의 동기화 및 공유, 그리고 개인 정보 문제를 해결하는 방법 및 장치가 제공된다.

도면의 간단한 설명

[22] 도 1은 일 실시예에 따른 데이터 제공 시스템의 구조도이다.

[23] 도 2는 본 발명의 일 실시예에 따른 데이터 제공 방법의 흐름도이다.

[24] 도 3은 일 예에 따른 개인 환경 설정의 구성을 나타낸다.

[25] 도 4는 일 예에 따른 데이터 객체 요청 메시지를 설명한다.

[26] 도 5는 일 예에 따른 마스터 DB 및 데이터 블록들의 구성을 설명한다.

[27] 도 6은 일 예에 따른 키를 사용한 암호화 방법을 설명한다.

발명의 실시를 위한 최선의 형태

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

[29] 하기에서, 데이터 객체는 데이터를 나타내는 객체를 의미할 수 있다. 데이터 객체는 데이터 제공 시스템에 의해 제공되는 전체 데이터 중 특정한 일부를 나타낼 수 있다. 따라서, 용어 "데이터 객체"는 용어 "데이터", "객체", "미디어", "콘텐츠", "문서" 또는 "파일" 등과 교체되어 사용될 수 있다.

[30]

[31] 도 1은 일 실시예에 따른 데이터 제공 시스템의 구조도이다.

[32] 데이터 제공 시스템(100)은 접근 제어부(110), 서비스부(120), 분산 파일 시스템부(130) 및 로컬 파일 시스템들(140)을 포함할 수 있다. 또한, 데이터 제공 시스템(100)은 프라이버시 정책 리스트(112), 마스터 데이터베이스(database; DB)(122) 및 키 저장소(124)를 더 포함할 수 있다.

[33] 분산 파일 시스템부(130)는 입력 레이어(152), 임시 레이어(134), 출력 레이어(136)를 포함할 수 있다.

[34] 로컬 파일 시스템들은 하나 이상의 저장소 노드들을 포함할 수 있다. 하나 이상의 저장소 노드들은 각각 역할-기반 저장소 노드, 그룹 저장소 노드 또는 개인 저장소 노드일 수 있다.

[35] 데이터 제공 시스템(100)은 단일한 컴퓨터, 서버 또는 전자 장치일 수 있다. 데이터 제공 시스템(100)이 단일한 컴퓨터, 서버 또는 전자 장치인 경우,

서비스부(120), 분산 파일 시스템부(130), 로컬 파일 시스템들(140) - 프라이버시 정책 리스트(112), 마스터 DB(122) 및 키 저장소(124)는 각각 단일(single) 또는 복수(multi) 칩(chip), 프로세서(processor) 또는 코어(core)를 나타낼 수 있으며, 프로세서에서 수행되는 함수(function), 라이브러리(library), 서비스(service), 프로세스(process), 쓰레드(thread), 모듈(module) 또는 레이어(layer)를 나타낼 수 있다.

[36] 데이터 제공 시스템(100)은 복수 개의 컴퓨터들, 서버들 또는 전자 장치들일 수 있다. 데이터 제공 시스템(100)이 단일한 컴퓨터, 서버 또는 전자 장치인 경우, 서비스부(120), 분산 파일 시스템부(130), 로컬 파일 시스템들(140) - 프라이버시 정책 리스트(112), 마스터 DB(122) 및 키 저장소(124)는 각각 네트워크로 상호 간에 연결된 컴퓨터, 서버, 데이터베이스 또는 전자 장치일 수 있다.

[37] 특히, 프라이버시 정책 리스트(112) 및 키 저장소(124)는 각각 데이터 제공 시스템(100) 내의 데이터 또는 자료 구조일 수 있다. 마스터 DB는 데이터 제공 시스템(100)에서 운영되는 DB일 수 있다.

[38] 구성 요소들 각각의 구체적인 기능에 대해 하기에서 도 2를 참조하여 상세히 설명된다.

[39]

[40] 도 2는 본 발명의 일 실시예에 따른 데이터 제공 방법의 흐름도이다.

[41] 데이터 제공 방법은 특정한 데이터 객체를 요청한 사용자에게 사용자의 권한에 따라 요청된 데이터 객체를 제공하는 방법일 수 있다. 상기의 요청은 사용자의 단말을 통해 데이터 제공 시스템(100)으로 전송될 수 있다.

[42] 단계(210)에서, 접근 제어부(110)는 데이터 객체를 요청한 사용자를 인증할 수 있다.

[43] 단계(220)에서, 접근 제어부(110)는 프라이버시 정책 리스트(112)로부터 인증된 사용자의 개인 환경 설정을 추출할 수 있다.

[44] 프라이버시 정책 리스트(112)는 시스템에 등록된 사용자들 각각의 개인 환경 설정을 저장할 수 있으며, 접근 제어부(110)의 요청에 따라 인증된 사용자의 개인 환경 설정을 제공할 수 있다. 여기서, 개인 환경 설정은 프라이버시 참조(privacy reference)로 명명될 수도 있다.

[45] 개인 환경 설정의 구체적인 구성의 일 예에 대해 하기에서 도 3을 참조하여 상세히 설명된다.

[46] 단계(220)는 사용자의 인증이 성공한 경우 선택적으로 수행될 수 있다.

[47] 단계(230)에서, 서비스부(120)는 추출된 개인 환경 설정을 사용하여 분산 파일 시스템부(130)로부터 요청된 데이터 객체를 획득할 수 있다. 서비스부(120)는 개인 환경 설정 내의 데이터 객체의 리스트에 기반하여 데이터 객체에 대한 서비스를 제공할 수 있다.

[48] 단계(230)는 단계들(240 내지 280)을 포함할 수 있다.

[49] 단계(240)에서, 서비스부(120)는 마스터 DB(122)에게 요청된 데이터 객체에

대한 정보를 제공할 수 있다. 데이터 객체는 복수 개일 수 있으며, 데이터 객체에 대한 정보는 복수 개의 데이터 객체들 각각에 대한 정보일 수 있다. 여기서, 서비스부(120)는 개인 환경 설정을 사용하여 마스터 DB(122)에게 요청된 데이터 객체에 대한 정보를 제공할 수 있다.

[50] 서비스부(120)는 접근이 허가된 역할, 개인 또는 공유자 별로 데이터 객체에 대한 정보를 생성할 수 있다. 서비스부(120)는 데이터 객체 요청 메시지를 사용하여 마스터 DB(122)에게 요청된 데이터 객체에 대한 정보를 제공할 수 있다. 상기의 정보를 제공하기 위해 사용되는 데이터 객체 요청 메시지에 대해 하기에서 도 4를 참조하여 상세히 설명된다.

[51] 단계(250)에서, 마스터 DB(122)는 분산 파일 시스템부(130)에게 요청된 데이터 객체의 데이터 블록들에 대한 정보를 제공할 수 있다.

[52] 데이터 객체는 역할, 그룹 또는 개인에 따라 서로 상이한 형태로 존재할 수 있다. 즉, 데이터 객체는 데이터 객체에 대한 접근 권한을 갖는 하나 이상의 역할들, 그룹들 및 개인들 각각에 대해 서로 상이한 데이터를 제공할 수 있다. 예컨대, 하나의 데이터 객체에 대해 사용자의 역할을 갖는 개체에게 제공되는 파일 및 관리자의 역할을 갖는 개체에게 제공되는 파일이 있을 수 있다.

[53] 따라서, 역할, 그룹 또는 개인에 따라 데이터 객체를 구성하는 데이터 블록들은 서로 상이할 수 있다. 마스터 DB(122)의 구성 및 데이터 객체를 구성하는 데이터 블록들의 구성의 일 예에 대해 하기에서 도 5를 참조하여 상세히 설명된다.

[54] 단계(260)에서, 분산 파일 시스템부(130)는 데이터 블록들에 대한 정보에 기반하여 하나 이상의 저장소 노드들로부터 데이터 블록들 각각을 획득할 수 있다.

[55] 데이터 블록들은 요청된 데이터 객체가 기 정의된 크기로 나뉘어진 블록들일 수 있다. 기 정의된 크기는 하나의 데이터 블록만으로는 데이터 객체의 내용이 확인될 수 없게 하는 크기일 수 있다. 예컨대, 데이터 객체가 음성을 저장한 파일일 경우, 데이터 블록의 기 정의된 크기는 데이터 블록이 재생되어도 사용자가 음절, 음운, 어절 또는 단어를 인식하기 어려울 정도로 작은 크기일 수 있다. 데이터 객체가 동영상을 저장한 파일일 경우, 데이터 블록의 기 정의된 크기는 동영상 내의 하나의 프레임이 저장되기 어려울 정도로 작은 크기일 수 있다. 데이터 객체가 영상을 저장한 파일일 경우, 데이터 블록의 기 정의된 크기는 사용자가 영상 내의 객체가 무엇을 나타내는지 인식하기 어려울 정도로 작은 크기일 수 있다.

[56] 기 정의된 크기는 바이트(byte), 킬로 바이트(kilo byte) 등의 단위를 가질 수 있다.

[57] 획득된 데이터 블록들은 입력 레이어(132) 내에 저장될 수 있다.

[58] 데이터 블록들 각각은 암호화되어 하나 이상의 저장소 노드들 내에 저장되어 있을 수 있다. 따라서, 획득된 데이터 블록들은 각각 암호화된 데이터 블록일 수 있다.

[59] 단계(270)에서, 분산 파일 시스템부(130)는 획득된 데이터 블록들을 하나로 합침으로써 요청된 데이터 객체를 생성할 수 있다.

[60] 획득된 데이터 블록들이 암호화된 데이터 블록들인 경우, 분산 파일 시스템부(130)는 획득된 데이터 블록들 각각을 복호화한 후 복호화된 데이터 블록들을 하나의 데이터로 합칠 수 있다.

[61] 생성된 데이터 객체는 임시 레이어(134) 내에 저장될 수 있다.

[62] 단계(280)에서, 분산 파일 시스템부(130)는 요청된 데이터 객체를 서비스부(120)로 전달할 수 있다.

[63] 분산 파일 시스템부(130)로 전달되는 객체는 출력 레이어(136) 내에 저장될 수 있다.

[64] 단계(290)에서, 서비스부(120)는 요청된 객체를 사용자 또는 사용자의 단말에게 제공할 수 있다.

[65]

[66] 도 3은 일 에에 따른 개인 환경 설정의 구성을 나타낸다.

[67] 개인 환경 설정은 "파일 ID, "파일 명칭", "역할", "그룹" 및 "개인" 필드를 포함할 수 있다.

[68] 개인 환경 설정은 사용자가 소유한 데이터 객체의 리스트일 수 있다. 프라이버시 정책 리스트(112)는 데이터 제공 시스템(100)에 등록된 사용자들 각각의 개인 환경 설정을 저장 및 제공할 수 있다.

[69] 개인 환경 설정은 데이터 객체의 리스트의 각 엔트리(entry)에 대해, 접근이 허가된 그룹, 접근이 허가된 개인 및 역할에 대한 정보를 포함할 수 있다. 즉, 개인 환경 설정은 데이터 객체의 리스트 내의 객체들 각각에 대해, 데이터 객체에 대해 접근이 허가된 개인에 대한 정보, 데이터 객체에 대해 접근이 허가된 그룹에 대한 정보 및 상기의 개인 또는 그룹의 역할에 대한 정보를 포함할 수 있다.

[70] 역할은 데이터 객체를 제공하는 데이터 제공 시스템(100) 내에서 설정된 계층화된 직책을 나타낼 수 있다. 직책은 읽기, 쓰기, 갱신 및 삭제 등 데이터 객체에 대한 접근의 타입(type)들 중 허용된 타입들에 의해 구분될 수 있다. 계층화된 직책이란, 상위 직책에게 허용된 접근의 타입들이 하위 직책에게 허용된 접근의 타입들을 포함한다는 것을 의미할 수 있다. 즉, 높은 계층의 직책일수록 데이터 객체에 대한 더 포괄적인 접근 권한을 부여받을 수 있다. 직책은, 서비스의 운용자의 측면에서는 "사용자" 또는 "관리자" 등으로 명명될 수 있고, 기업의 측면에서는 각 기업에서의 보안 등급 또는 직책 명칭 등으로 명명될 수 있다.

[71] 예컨대, 역할이 "사용자" 또는 "스텝"일 -, 상기의 역할이 부여된 개체는 데이터 객체를 단지 읽을 수 있다. 반면, 역할이 "관리자" 또는 "부서장"일 -, 상기의 역할이 부여된 개체는 데이터 객체에 대한 모든 타입의 접근을 수행할 수 있다. 여기서, 개체란 개인 또는 그룹일 수 있다.

[72] 데이터 객체는, 데이터 제공 시스템(100) 내부적으로는 파일로서 관리될 수 있다. 따라서, 필드 "파일 ID"는 데이터 객체를 나타내는 파일의 식별자(identifier; ID)를 나타낼 수 있다. 필드 "파일 명칭"은 상기의 파일의 이름을 나타낼 수 있다. 필드 "역할"은 상기의 파일에 가할 수 있는 역할에 대한 정보를 나타낼 수 있다. 필드 "그룹"은 상기의 파일에 대해 상기의 역할을 할 수 있는 그룹을 나타낼 수 있다. 그룹은 데이터 제공 시스템(100) 내에서 명명된 사용자들의 집단일 수 있으며, 기업의 부서, 데이터 제공 서버스 내의 커뮤니티의 명칭 등이 그룹으로서 구성될 수 있다. 필드 "개인"은 상기의 파일에 대해 상기의 역할을 할 수 있는 개인을 나타낼 수 있다.

[73] 개인 환경 설정 중 제1 데이터 객체에 대한 정보는, 제1 데이터 객체의 사용자 또는 제1 데이터 객체의 소유자에 의해 제1 데이터 객체가 데이터 제공 시스템(100)으로 업로드(upload)될 때 생성될 수 있다. 또는, 제1 데이터 객체에 대한 정보는 제1 데이터 객체가 데이터 제공 시스템(100) 내에서 생성될 - 생성될 수 있다.

[74] 상기의 사용자 또는 소유자는 데이터 객체 별로 데이터 객체에 대한 역할, 개인 및 그룹을 설정할 수 있다. 여기서, 개인은 데이터 객체를 공유하거나 데이터 객체에 대한 접근 권한을 갖는 다른 사용자를 의미할 수 있다. 그룹은 데이터 객체를 공유하거나 데이터 객체에 대한 접근 권한을 갖는 사용자들의 그룹을 의미할 수 잇다. 따라서, 개인 환경 설정에 의해 데이터 객체에 대한 접근 권한이 세밀하게 제어될 수 있다.

[75] 상기의 사용자 또는 소유자는 데이터 객체 별로 데이터 객체에 대한 역할, 개인 및 그룹을 갱신할 수 있다. 사용자 또는 소유자에 의해 개인 환경 설정이 갱신될 때, 상기의 갱신은 데이터 제공 시스템(100)에 의해 정해진 절차에 따라 자동으로 수행될 수 있다. 여기서, 정해진 절차는 상기의 갱신에 의해 데이터 객체에 대한 접근 권한에 영향을 받는 다른 사용자 또는 그룹에 의한 상기의 갱신에 대한 동의를 획득하는 것을 포함할 수 있다. 상기의 동의를 획득하는 과정은 데이터 제공 시스템(100)에 의해 자동으로 수행될 수 있다.

[76] 전술된 설정 및 갱신은 사용자의 단말 또는 소유자의 단말을 통한 요청에 따라, 접근 제어부(110)에 의해 수행될 수 있다.

[77]

[78] 도 4는 일 예에 따른 데이터 객체 요청 메시지를 설명한다.

[79] 데이터 객체 요청 메시지는 제1 타입의 데이터 객체 요청 메시지(410), 제2 타입의 데이터 객체 요청 메시지(420) 및 제3 타입의 데이터 객체 요청 메시지(430) 등으로 분류될 수 있다.

[80] 각 타입의 데이터 객체 요청 메시지는 필드 "파일 식별자", 필드 "타입", 필드 "값"을 포함할 수 있다. "파일 식별자"는 데이터 객체 요청 메시지가 어떠한 데이터 객체 또는 파일에 대한 데이터 객체 요청 메시지인지 나타낼 수 있다. "타입"은 데이터 객체 요청 메시지가 어떤 타입의 데이터 객체 요청

메시지인가를 나타낼 수 있다. 즉, "타입"에 의해, 제1 타입(410), 제2 타입(420) 및 제3 타입(430)이 구별될 수 있다. 필드 "값"은 각 타입의 데이터 객체 요청 메시지에 요구되는 값을 나타낼 수 있다.

[81] 제1 타입의 데이터 객체 요청 메시지(410)에서, 필드 "값"은 데이터 객체의 요청이 어떤 역할을 갖는 사용자에 의해 이루어졌는가를 나타낼 수 있다. 제2 타입의 데이터 객체 요청 메시지(420)에서, 필드 "값"은 데이터 객체의 요청이 어떤 그룹에 의해 이루어졌는가를 나타낼 수 있다. 제3 타입의 데이터 객체 요청 메시지(430)에서, 필드 "값"은 데이터 객체의 요청이 어떤 개인에 의해 이루어졌는가를 나타낼 수 있다.

[82] 마스터 DB(122)는 데이터 객체 요청 메시지 내의 필드들을 참조하여 서비스부(120)로 전송해 줄 데이터 객체를 결정할 수 있다.

[83]

[84] 도 5는 일 예에 따른 마스터 DB 및 데이터 블록들의 구성을 설명한다.

[85] 마스터 DB(122)는 기 정의된 규정에 따라 데이터 객체에 대한 정보를 가지고 있다. 여기서, 데이터 객체에 대한 정보는 데이터 객체에 대응하는 파일들의 정보를 포함할 수 있다. 전술된 것처럼, 데이터 객체는 역할, 그룹 또는 개인에 대응하여 서로 상이한 형태로 존재할 수 있다. 즉, 역할, 그룹 또는 개인에 따라 데이터 객체는 하나 이상의 파일들에 대응할 수 있다. 하나 이상의 파일들 각각은 특정한 역할, 그룹 또는 개인에게 제공되는 데이터 객체일 수 있다.

[86] 마스터 DB(122)는 역할, 그룹 및 개인 각각에 대해 별도의 데이터베이스를 관리할 수 있다. 예컨대, 역할에 대한 데이터베이스는, 데이터 객체에 대한 역할에 따라 하나 이상의 파일들 중 하나의 선택된 파일을 데이터 객체로서 사용자에게 제공해 주기 위한 정보를 저장할 수 있다. 하나의 데이터 객체에 대해서, 원본의 데이터 객체에 대한 역할들, 그룹들, 개인들 각각에 대해 나뉘어진 데이터 블록들이 존재할 수 있다.

[87] 마스터 DB(122)가 제공하는 데이터 노드 테이블(500)은 필드 "파일 ID" 및 필드 "데이터 노드"들을 포함할 수 있다. "파일 ID"는 데이터 객체에 대응하는 파일들 각각의 ID를 나타낸다. "데이터 노드"는 데이터 객체에 대응하는 파일의 데이터 노드들을 나타낸다. 예컨대, ID_1로 식별되는 제1 파일은 제1 데이터 노드, 제2 데이터 노드, 제3 데이터 노드 및 제4 데이터 노드 등을 포함하는 반면, ID_2로 식별되는 제1 파일은 제1 데이터 노드, 제4 데이터 노드, 제5 데이터 노드 등을 포함할 수 있다.

[88] 마스터 DB(122)는 각 데이터 노드의 정보를 제공할 수 있다. 여기서, 데이터 노드의 정보는 데이터 노드의 위치에 대한 정보를 포함할 수 있다. 데이터 노드의 위치에 대한 정보는 {DataNodeN(데이터 노드 N), File_ID(파일_식별자), Location(위치), Sequence(시퀀스)}와 같은 형태로 제공될 수 있다.

[89] 여기서, DataNodeN은 하나 이상의 저장소 노드들 중 데이터 노드가 실제로 저장된 데이터 노드를 가리키는 식별자 또는 번호일 수 있다. File_ID는 데이터

제공 시스템에서 파일을 관리하기 위해 사용하는 ID일 수 있다. Location은 데이터 노드가 저장소 노드 내에서 저장된 위치를 나타내는 정보일 수 있다. 예컨대, Location은 데이터 노드가 저장된 위치를 나타내는 저장소 노드의 주소 또는 데이터 제공 시스템의 주소일 수 있다. Sequence는 데이터 블록의 데이터 객체 내에서의 순서 값 또는 파일 내에서의 순서 값일 수 있다.

[90] 도 2를 참조하여 전술된 단계(250)에서, 분산 파일 시스템부(130)는 전술된 데이터 노드의 위치에 대한 정보를 마스터 DB(122)로부터 입력받을 수 있다. 단계(260)에서, 분산 파일 시스템부(130)는 데이터 노드의 위치에 대한 정보를 사용하여, 상기의 정보가 나타내는 저장소 노드에게 데이터 노드를 요청할 수 있다.

[91]

[92] 저장소 노드는 데이터 블록이 실제로 저장된 저장소일 수 있다. 저장소 노드는 데이터 객체에 대한 소유권 정보, 즉 역할, 그룹 및 개인에 따라 구분될 수 있다. 예컨대, 역할-기반 저장소 노드는 역할 별로 제공되는 데이터 객체 또는 파일의 데이터 블록들을 저장할 수 있다. 그룹 저장소 노드는 그룹 별로 제공되는 데이터 객체 또는 파일의 데이터 블록들을 저장할 수 있다. 개인 저장소 노드는 개인 별로 제공되는 데이터 객체 또는 파일의 데이터 블록들을 저장할 수 있다. 저장소 노드는 분산 파일 시스템부(130)로부터 요청받은 데이터 블록을 분산 파일 시스템부(130)의 임시 레이어(134)로 전송할 수 있다. 상기의 전송에 있어서, 데이터 블록에 대한 암호화 및 복호화는 저장소 노드 또는 분산 파일 시스템부(130)에 의해 수행될 수 있다.

[93]

[94] 전술된 데이터 객체에 대한 접근 권한은 복합적으로 수행될 수 있다. 데이터 객체를 구성하는 데이터 노드들은 데이터 객체에 대한 역할, 그룹 및 개인에 따라 분리될 수 있다. 즉, 데이터 객체에 대해 역할으로서의 접근 권한, 그룹으로서의 접근 권한 및 개인으로서의 접근 권한을 모두 가진 사용자만이 역할 별로 제공되는 데이터 노드, 그룹 별로 제공되는 데이터 노드 및 개인 별로 제공되는 데이터 노드를 모두 접근 및 획득할 수 있고, 이들 데이터 노드들로 구성된 완전한 데이터 객체를 접근하거나 제공 받을 수 있다. 즉, 모든 접근 권한들을 가진 사용자가 아니면, 데이터 객체에 접근할 수 없게 될 수 있다. 또한, 상기의 분리에 의해 일부 데이터 노드 또는 일부 저장소 노드가 악의적인 공격에 노출되더라도, 데이터 객체가 유출되거나 유추되지 않을 수 있다.

[95]

[96] 도 6은 일 예에 따른 키를 사용한 암호화 방법을 설명한다.

[97] 전술된 개인 환경 설정 정보, 데이터 노드 테이블 및 데이터 노드는 외부 공격자에 대한 데이터 안전성을 위해 암호화될 수 있다.

[98] 키 저장소(124)는 암호화 및 복호화를 위한 키를 저장할 수 있다. 키 저장소(124)는 사용자의 키를 저장할 수 있으며, 사용자의 키를 사용하여 암호화

및 복호화가 수행될 수 있다. 키 저장소(124)는 제 3의 서비스 제공자에 의해 제공될 수 있다.

[99] 도 2를 참조하여 전술된 단계(210)에서, 접근 제어부(110)는 사용자의 ID 및 암호 외의 추가적인 정보를 사용함으로써 키 저장소(124)로부터 사용자의 키를 획득할 수 있다. 여기서, 추가적인 정보는, 사용자의 인증서 비밀번호, 일회용 비밀번호 및 모바일 단말에 의해 제공된 임시 비밀번호 등을 포함할 수 있다.

[100] 사용자 키는 속성 정보를 포함할 수 있다. 속성 정보의 일 예로, 제1 속성 정보(510) 및 제2 속성 정보(520)가 도시되었다.

[101] 제1 속성 정보(510)에서, 사용자는 역할 "스텝"으로서의 접근 권한, 그룹 "세일즈"로서의 접근 권한 및 개인 "제1 사용자"로서의 접근 권한을 부여받았다. 따라서, 제1 속성 정보(510) 또한 사용자가 상기의 접근 권한들을 모두 가짐을 나타낼 수 있다.

[102] 사용자가 그룹 "본부"로서의 접근 권한을 더 부여받을 경우, 사용자의 접근 권한이 변경된다. 제2 속성 정보(520)는 사용자의 변경된 접근 권한들을 나타낼 수 있다. 제2 속성 정보(520)는 사용자가 1) 역할 "스텝"으로서의 접근 권한, 2) 그룹 "세일즈" 또는 "본부"로서의 접근 권한 및 3) 개인 "제1 사용자"로서의 접근 권한을 가지고 있음을 나타낼 수 있다.

[103] 사용자는 자신의 접근 권한을 나타내는 키를 사용하여 데이터 객체를 요청할 수 있으며, 서비스부(120)는 사용자의 접근 권한에 맞는 데이터 객체를 사용자에게 제공할 수 있다.

[104]

[105] 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.

[106]

[107] 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.

[108]

[109] 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.

[110]

[111] 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] 접근 제어부가 데이터 객체를 요청한 사용자를 인증하는 단계;
접근 제어부가 상기 사용자의 개인 환경 설정을 추출하는 단계 - 상기 개인 환경 설정은 상기 사용자가 소유한 데이터 객체들의 목록 및 상기 목록 내의 각 데이터 객체에 대한 접근 정보를 포함함 -;
서비스부가 상기 개인 환경 설정을 사용하여 분산 파일 시스템부로부터 상기 요청된 데이터 객체를 획득하는 단계; 및
서비스부가 요청된 데이터 객체를 제공하는 단계
를 포함하는, 데이터 제공 방법.

[청구항 2] 제1항에 있어서,
상기 접근 정보는 상기 데이터 객체에 대해 접근이 허가된 개인에 대한 정보, 상기 데이터 객체에 대하여 접근이 허가된 그룹에 대한 정보 및 상기 개인 또는 상기 그룹의 역할에 대한 정보를 포함하는, 데이터 제공 시스템.

[청구항 3] 제2항에 있어서,
상기 역할은 상기 데이터 객체를 제공하는 시스템 내에서 설정된 계층화된 직책을 나타내는, 데이터 제공 시스템.

[청구항 4] 제1항에 있어서,
상기 요청된 데이터 객체를 제공하는 단계는,
서비스부가 마스터 데이터베이스에게 요청된 데이터 객체에 대한 정보를 제공하는 단계;
상기 마스터 데이터베이스가 상기 분산 파일 시스템부에게 데이터 객체의 데이터 블록들에 대한 정보를 제공하는 단계;
상기 분산 파일 시스템부가 상기 데이터 블록들에 대한 정보에 기반하여 하나 이상의 저장소 노드들로부터 상기 데이터 블록들 각각을 획득하는 단계;
상기 분산 파일 시스템부가 상기 획득된 데이터 블록들을 하나로 합침으로써 상기 요청된 데이터 객체를 생성하는 단계; 및
상기 분산 파일 시스템부가 상기 요청된 데이터 객체를 상기 서비스부로 전달하는 단계
를 포함하는, 데이터 제공 방법.

[청구항 5] 제4항에 있어서,
상기 데이터 블록들 각각은 암호화되어 상기 하나 이상의 저장소 노드들 내에 저장되어 있고,
상기 분산 파일 시스템부는 상기 획득된 데이터 블록들 각각을 복호화한 후 상기 복호화된 데이터 블록들을 상기 하나의

데이터로 합치는, 데이터 제공 방법.

[청구항 6] 제4항에 있어서,
상기 데이터 블록들은 상기 데이터 객체가 기 정의된 크기로 나뉘어진 블록들이며,
상기 기 정해진 크기는 하나의 데이터 블록만으로는 상기 데이터 객체의 내용이 확인될 수 없게 하는 크기인, 데이터 제공 방법.

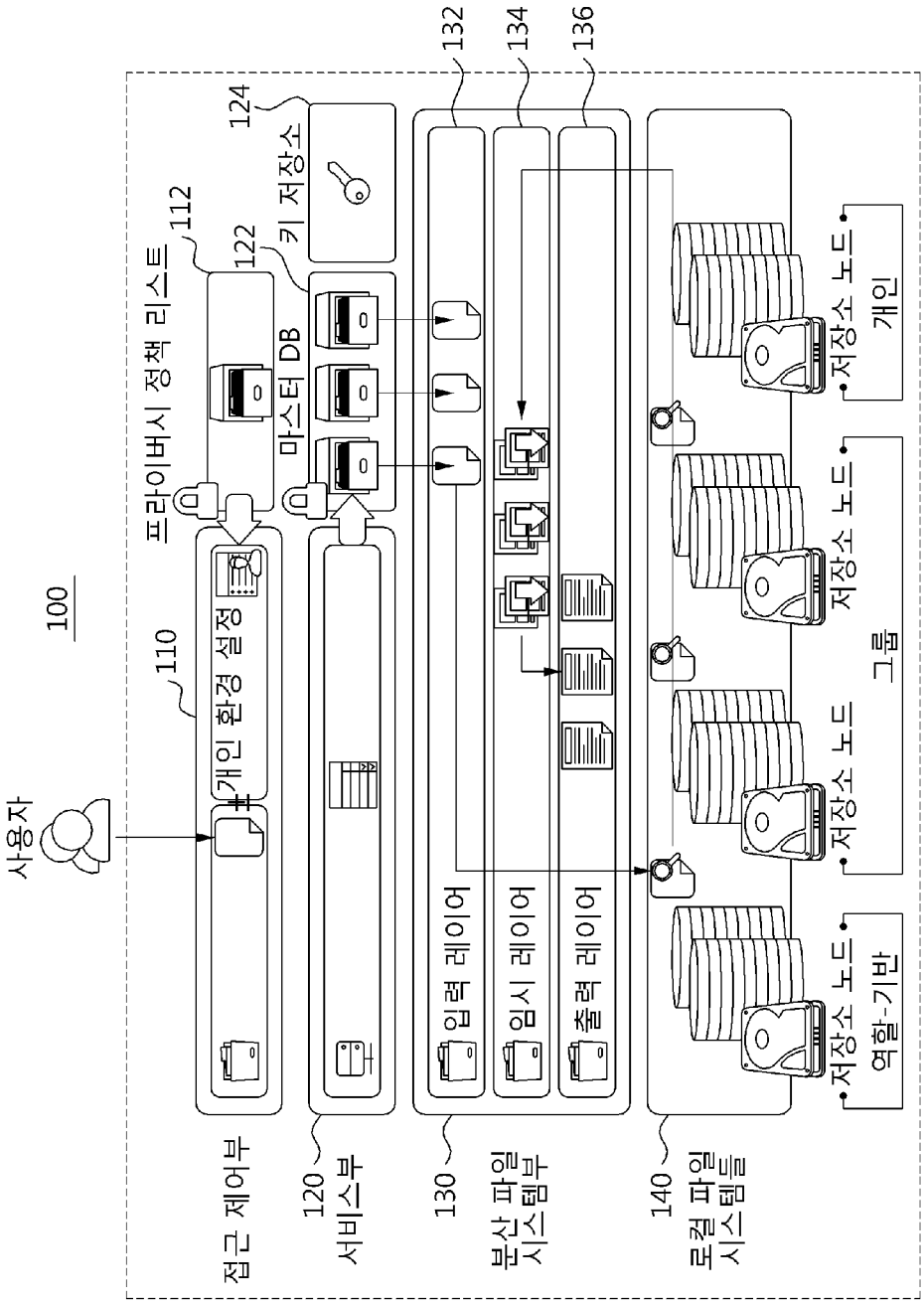
[청구항 7] 제6항에 있어서,
상기 기 정해진 크기는 상기 데이터 객체의 종류에 따라 상이한, 데이터 제공 방법.

[청구항 8] 제1항 내지 제7항 중 어느 한 항의 방법을 수행하는 프로그램을 수록한 컴퓨터 판독 가능 기록 매체.

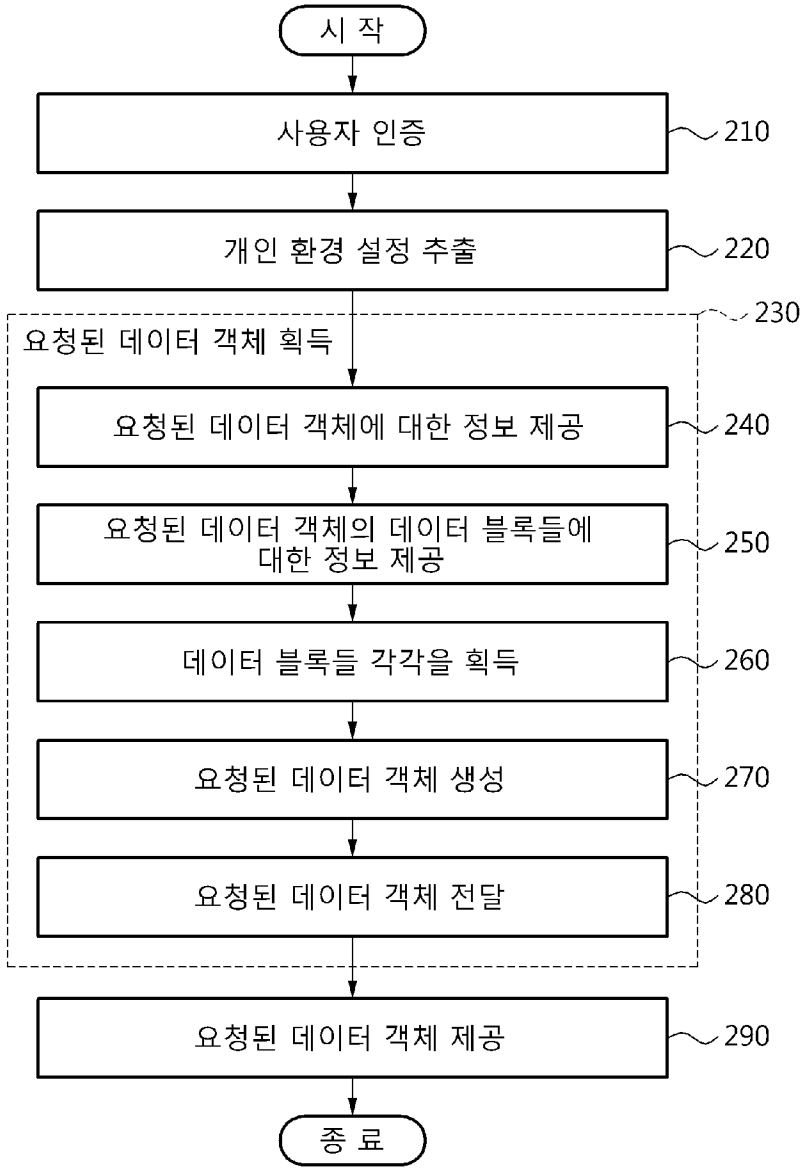
[청구항 9] 데이터 객체를 요청한 사용자를 인증하고, 상기 사용자의 개인 환경 설정을 추출하는 접근 제어부 - 상기 개인 환경 설정은 상기 사용자가 소유한 데이터 객체들의 목록 및 상기 목록 내의 각 데이터 객체에 대한 접근 정보를 포함함 -; 및
상기 개인 환경 설정을 사용하여 분산 파일 시스템부로부터 상기 요청된 데이터 객체를 획득하고, 상기 요청된 데이터 객체를 제공하는 서비스부
를 포함하는, 데이터 제공 시스템.

[청구항 10] 제9항에 있어서,
상기 서비스로부터 요청된 데이터 객체에 대한 정보를 제공받는 마스터 데이터베이스;
상기 마스터 데이터베이스로부터 상기 대이터 객체의 데이터 블록들에 대한 정보를 제공받고, 상기 데이터 블록들에 대한 정보에 기반하여 복수 개의 로컬 파일 시스템들로부터 상기 데이터 블록들 각각을 획득하고, 상기 획득된 데이터 블록들을 하나의 데이터로 합침으로써 상기 요청된 데이터 객체를 생성하고, 상기 요청된 데이터 객체를 상기 서비스부로 전달하는 분산 파일 시스템
을 더 포함하는, 데이터 제공 시스템.

[Fig. 1]


100
사용자
110
개인 환경 설정
프라이버시 정책 리스트
112
122
마스터 DB
124
키 저장소
132
134
136
입력 레이어
임시 레이어
출력 레이어
저장소 노드
개인
저장소 노드
저장소 노드
그룹
저장소 노드
역할-기반
접근 제어부
120
서비스부
130
분산 파일 시스템부
140
로컬 파일 시스템들

[Fig. 2]


시 작
사용자 인증
210
개인 환경 설정 추출
220
230
요청된 데이터 객체 획득
요청된 데이터 객체에 대한 정보 제공
240
요청된 데이터 객체의 데이터 블록들에 대한 정보 제공
250
데이터 블록들 각각을 획득
260
요청된 데이터 객체 생성
270
요청된 데이터 객체 전달
280
요청된 데이터 객체 제공
290
종 료

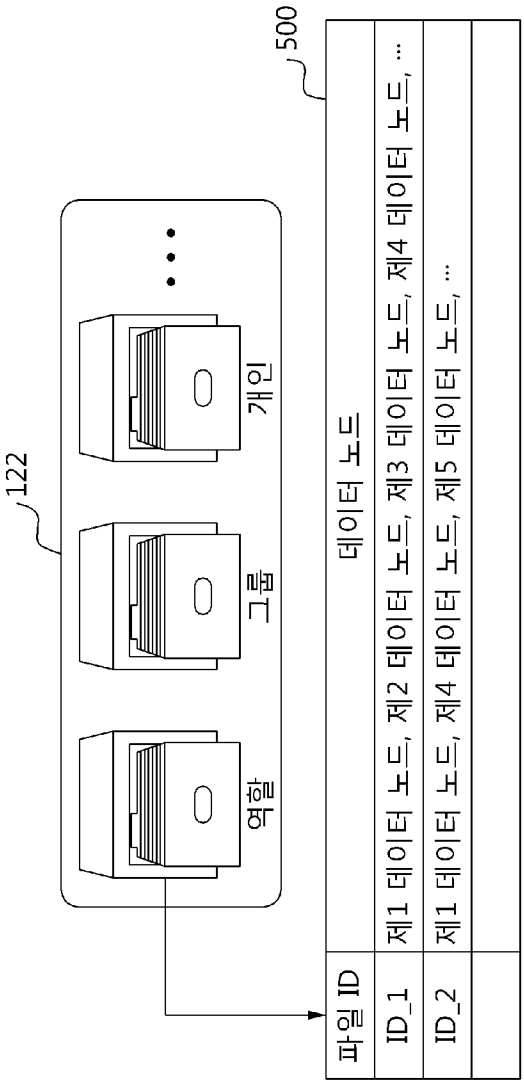
[Fig. 3]

개인 환경 설정

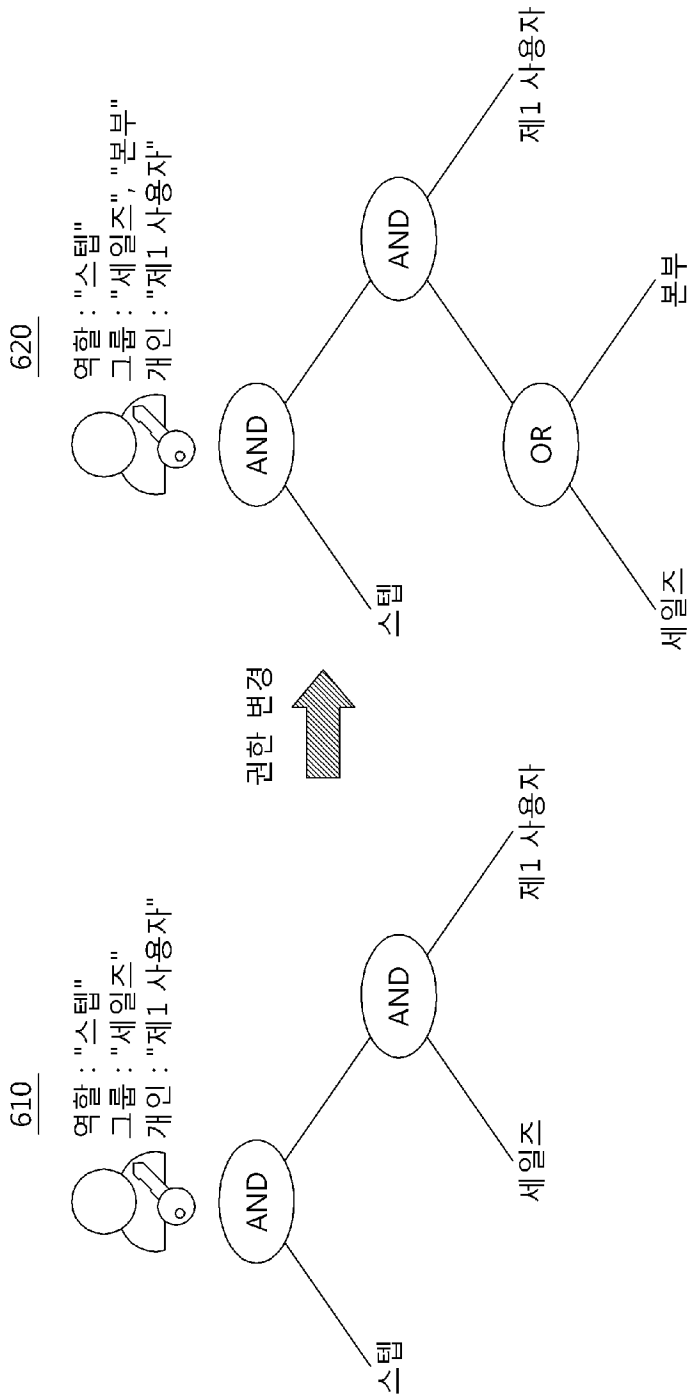
파일 ID	파일 명칭	역할	그룹	개인	• • •	• • •
ID_1	filename1	사용자	제1 그룹	제1 사용자		
		관리자	제2 그룹	제2 사용자		
			• • •	• • •		
ID_2	filename2	스텝	제1 부서	제1 사용자		
		부서장	제2 부서			

[Fig. 4]

[Fig. 5]


500
데이터 노드
파일 ID
ID_1
제1 데이터 노드, 제2 데이터 노드, 제3 데이터 노드, 제4 데이터 노드, ...
ID_2
제1 데이터 노드, 제4 데이터 노드, 제5 데이터 노드, ...
122
역할
그룹
개인

[Fig. 6]


610
역할 : "스텝"
그룹 : "세일즈"
개인 : "제1 사용자"
AND
스텝
AND
세일즈
제1 사용자
권한 변경
620
역할 : "스텝"
그룹 : "세일즈", "본부"
개인 : "제1 사용자"
AND
스텝
AND
OR
세일즈
본부
제1 사용자

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2013/005822

A. CLASSIFICATION OF SUBJECT MATTER

G06F 15/16(2006.01)i, G06F 21/14(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 15/16; G06F 21/20; G06F 17/30; H04L 12/22; G06F 21/14; H04L 9/32

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: dispersion, access control, role

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2012-0065783 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 21 June 2012	1-3,8,9
A	See abstract; paragraphs [8]-[9], [11]-[19]; claims 1-6 and figures 1-5.	4-7,10
Y	KR 10-2012-0013475 A (SK TELECOM CO., LTD. et al.) 15 February 2012	1-3,8,9
A	See abstract; paragraphs [40]-[41], [52]-[53]; claims 1, 6 and 10 and figure 1.	4-7,10
A	SHIM, Won-Bo et al., "An Access Control Model For The Authority Filtering in the Distributed Environment", Journal of the Korea Academia-Industrial Cooperation Society, vol. 8 no. 2, 2007 See abstract, 2. Authority Filtering using Work Concept.	1-10
A	AN, Dong-Chan, "Fine-Grained Access Control Method in XML Data Stream", The Korean Society Of Computer And Information vol. 15 no. 1, June 2007 See abstract, 3.3 Access Control Policy, 4.2 Roll Prime Number Labelling Technique.	1-10

☐ 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
24 SEPTEMBER 2013 (24.09.2013)	**25 SEPTEMBER 2013 (25.09.2013)**

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/KR2013/005822

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2012-0065783 A	21/06/2012	NONE	
KR 10-2012-0013475 A	15/02/2012	NONE	

국 제 조 사 보 고 서

국제출원번호
PCT/KR2013/005822

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 15/16(2006.01)i, G06F 21/14(2013.01)i, H04L 9/32(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 15/16; G06F 21/20; G06F 17/30; H04L 12/22; G06F 21/14; H04L 9/32

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: 분산, 접근제어,역할

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-2012-0065783 A (한국전자통신연구원) 2012.06.21 요약; 단락 [8]-[9], [11]-[19]; 청구항 1-6 및 도면 1-5 참조.	1-3,8,9
A		4-7,10
Y	KR 10-2012-0013475 A (에스케이 텔레콤주식회사 외 2명) 2012.02.15 요약; 단락 [40]-[41], [52]-[53]; 청구항 1, 6, 10 및 도면 1 참조.	1-3,8,9
A		4-7,10
A	심안보 외, `분산환경에서의 권한 필터링을 위한 접근제어 모델`, 한국산학기술학회 논문지, 제8권 제2호, 2007 요약, 2. 워크개념을 이용한 권한 필터링 참조.	1-10
A	안동찬, `XML 데이터 스트림 환경에서 세분화된 접근 제어 방법`, 한국컴퓨터정보학회 제15권 제1호, 2007. 6 요약, 3.3 접근제어 정책, 4.2 롤 프라임 넘버 레이블링 기법 참조.	1-10

☐ 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 09월 24일 (24.09.2013)	2013년 09월 25일 (25.09.2013)

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

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2013/005822

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2012-0065783 A	2012/06/21	없음	
KR 10-2012-0013475 A	2012/02/15	없음	