(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2016 년 12 월 1 일 (01.12.2016)

WIPO | PCT

(10) 국제공개번호
WO 2016/190476 A1

(51) 국제특허분류:
H04L 9/08 (2006.01)

(21) 국제출원번호: PCT/KR2015/006238

(22) 국제출원일: 2015 년 6 월 19 일 (19.06.2015)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2015-0074302 2015 년 5 월 27 일 (27.05.2015) KR

(71) 출원인: **삼성에스디에스 주식회사 (SAMSUNG SDS CO.,LTD.)** [KR/KR]; 138-240 서울시 송파구 올림픽로 35 길 125 (삼성 SDS 타워, West Campus), Seoul (KR).

(72) 발명자: **유인선 (YOO, In Seon)**; 138-240 서울시 송파구 올림픽로 35 길 125 (삼성 SDS 타워, West Campus), Seoul (KR).

(74) 대리인: **특허법인 가산 (KASAN IP & LAW FIRM)**; 137-867 서울시 서초구 남부순환로 2423 한원빌딩 7 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, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

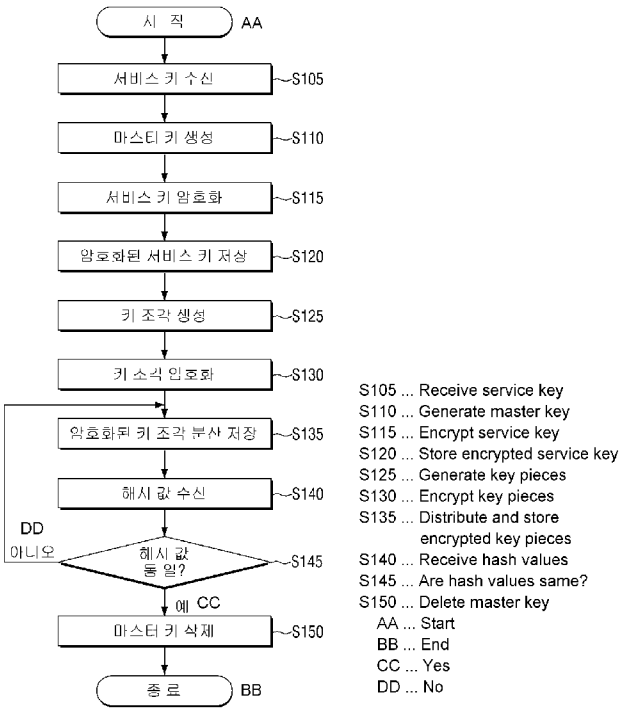
— 국제조사보고서와 함께 (조약 제 21 조(3))

WO 2016/190476 A1

(54) **Title**: METHOD FOR MANAGING ENCRYPTION KEY FOR CLOUD SERVICE AND APPARATUS THEREOF

(54) **발명의 명칭** : 클라우드 서비스를 위한 암호화 키 관리 방법 및 그 장치

[도4]



(57) **Abstract**: A key management method according to embodiments of the present invention may comprise the steps of: encrypting a service key used by an instance of a first user of a cloud service, using a master key; generating two or more key pieces for re-generating the master key; distributing and storing the key pieces in two or more host servers included in a host group for providing the cloud service; receiving a request for provision of the service key from the instance of the first user; receiving the key pieces from the two or more host servers and re-generating the master key on the basis of the received key pieces; and decrypting the encrypted service key using the re-generated master key.

(57) **요약서**: 본 발명의 일 실시예들에 따른 키 관리 방법은, 클라우드 서비스의 제 1 이용자의 인스턴스에 의하여 사용되는 서비스 키를 마스터 키를 이용하여 암호화하는 단계, 상기 마스터 키를 재생성하기 위한 둘 이상의 키 조각을 생성하는 단계, 상기 클라우드 서비스의 제공을 위한 호스트 그룹에 포함된 둘 이상의 호스트 서버에, 상기 키 조각을 분산하여 저장하는 단계, 상기 제 1 이용자의 인스턴스로부터, 상기 서비스 키의 제공 요청을 수신하는 단계, 상기 둘 이상의 호스트 서버로부터 상기 키 조각들을 수신하고, 상기 수신된 키 조각을 기초로 상기 마스터 키를 재생성하는 단계 및 상기 암호화된 서비스 키를 상기 재생성된 마스터 키를 이용하여 복호화하는 단계를 포함할 수 있다.

명세서

발명의 명칭: 클라우드 서비스를 위한 암호화 키 관리 방법 및 그 장치

기술분야

[1] 본 발명은 클라우드 서비스의 데이터 및 중요 자격(credential)들을 암호화하기 위한 서비스 키 및 서비스 키를 암호화하기 위한 마스터 키를 관리하기 위한 방법 및 그 장치에 관한 것이다.

배경기술

[2] 보안이 필요한 수많은 데이터 또는 중요 자격들은 암호화 키(encryption key)를 이용하여 암호화된다. 그러나, 암호화 키가 데이터베이스(database)에 일반적인 텍스트(plain text)로 저장된 경우, 저장된 암호화 키가 데이터베이스 관리자(DataBase Administration, DBA) 또는 내부인에 의하여 유출될 수 있는 위험이 있다. 암호화 키가 하드웨어 보안 모듈(Hardware Security Module, HSM)을 이용하여 암호화된 경우, 암호화 키를 암호화한 마스터 키를 하드웨어 보안 모듈의 제공 업체가 알고 있는 한계가 있다. 또한, 암호화 키가 동형 알고리즘(homomorphic algorithm) 등을 이용하여 암호화된 경우, 암호화 키를 암호화한 마스터 키가 분실되면 더 이상 암호화된 데이터를 복구할 수 없게 되는 문제점이 있다. 따라서, 암호화 키의 비밀성 및 가용성을 동시에 확보할 수 있는 솔루션이 요구되고 있다.

발명의 상세한 설명

기술적 과제

[3] 본 발명이 해결하고자 하는 기술적 과제는, 클라우드 서비스의 데이터 및 중요 자격들을 암복호화할 수 있는 서비스 키를 별도의 마스터 키로 암호화한 후, 특정 조건에서만 마스터 키를 재생성할 수 있는 키 조각을 생성하여 복수 개의 서버에 분산 저장하기 위한 방법 및 그 장치를 제공하기 위한 것이다.

[4] 본 발명의 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해 될 수 있을 것이다.

과제 해결 수단

[5] 상기 기술적 과제를 달성하기 위한 본 발명의 일 태양(Aspect)에 따른 키 관리 방법은, 클라우드 서비스의 제1 이용자의 인스턴스에 의하여 사용되는 서비스 키를 마스터 키를 이용하여 암호화하는 단계, 상기 마스터 키를 재생성하기 위한 둘 이상의 키 조각을 생성하는 단계, 상기 클라우드 서비스의 제공을 위한 호스트 그룹에 포함된 둘 이상의 호스트 서버에, 상기 키 조각을 분산하여 저장하는 단계, 상기 제1 이용자의 인스턴스로부터, 상기 서비스 키의 제공 요청을 수신하는 단계, 상기 둘 이상의 호스트 서버로부터 상기 키 조각들을

수신하고, 상기 수신된 키 조각을 기초로 상기 마스터 키를 재생성하는 단계 및 상기 암호화된 서비스 키를 상기 재생성된 마스터 키를 이용하여 복호화하는 단계를 포함할 수 있다.

[6] 상기 기술적 과제를 달성하기 위한 본 발명의 다른 태양에 따른 키 관리 시스템은, 클라우드 서비스의 제1 이용자의 인스턴스에 의하여 사용되는 서비스 키를 마스터 키를 이용하여 암호화한 후, 상기 마스터 키를 재생성하기 위한 둘 이상의 키 조각을 생성하여 분산 저장하고, 상기 제1 이용자의 인스턴스로부터 서비스 키 제공 요청이 수신되면, 상기 분산 저장된 키 조각을 기초로 마스터 키를 재생성하여 상기 암호화된 서비스 키를 복호화하는 키 액세스 서버 및 상기 키 액세스 서버로부터 상기 키 조각을 수신하여 저장하고, 상기 키 액세스 서버로부터 키 조각 제공 요청이 수신되면 상기 키 조각을 전송하는 호스트 서버를 포함할 수 있다.

[7] 상기 기술적 과제를 달성하기 위한 본 발명의 또 다른 태양에 따르면, 컴퓨팅 장치와 결합하여, 클라우드 서비스의 제1 이용자의 인스턴스에 의하여 사용되는 서비스 키를 마스터 키를 이용하여 암호화하는 단계, 상기 마스터 키를 재생성하기 위한 둘 이상의 키 조각을 생성하는 단계, 상기 클라우드 서비스의 제공을 위한 호스트 그룹에 포함된 둘 이상의 호스트 서버에, 상기 키 조각을 분산하여 저장하는 단계, 상기 제1 이용자의 인스턴스로부터, 서비스 키 제공 요청을 수신하는 단계, 상기 둘 이상의 호스트 서버로부터 상기 키 조각들을 수신하고, 상기 수신된 키 조각을 기초로 상기 마스터 키를 재생성하는 단계 및 상기 암호화된 서비스 키를 상기 재생성된 마스터 키를 이용하여 복호화하는 단계를 실행시키기 위하여, 기록매체에 기록된 컴퓨터 프로그램이 제공될 수 있다.

발명의 효과

[8] 상술한 바와 같은 본 발명에 따르면, 특정 조건에서만 마스터 키를 재생성할 수 있는 키 조각을 생성하여 복수 개의 서버에 분산 저장하고, 어떠한 서버 또는 장치에도 마스터 키를 저장하지 않음으로써, 마스터 키의 비밀성을 확보할 수 있다. 또한, 분산 저장된 키 조각의 일부가 분실되더라도 마스터 키를 재생성할 수 있어, 마스터 키의 가용성을 확보할 수 있다. 나아가, 키 조각이 유출되더라도, 유출된 키 조각만으로는 마스터 키를 재생성할 수 없는 효과가 있다.

도면의 간단한 설명

[9] 도 1 내지 도 3은 본 발명의 몇몇 실시예에 따른 클라우드 서비스 시스템의 개념도이다.

[10] 도 4는 본 발명의 일 실시예에 따른 마스터 키 분산 저장 방법을 설명하기 위한 순서도이다.

[11] 도 5는 본 발명의 일 실시예에 따른 마스터 키 재생성 방법을 설명하기 위한 순서도이다.

[12] 도 6은 본 발명의 다른 실시예에 따른 마스터 키 분산 저장 방법을 설명하기 위한 신호 흐름도이다.

[13] 도 7은 본 발명의 다른 실시예에 따른 마스터 키 재생성 방법을 설명하기 위한 신호 흐름도이다.

[14] 도 8은 본 발명의 일 실시예에 따른 키 액세스 서버의 블록도이다.

[15] 도 9는 본 발명의 일 실시예에 따른 키 액세스 서버의 하드웨어 구성도이다.

발명의 실시를 위한 형태

[16] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하며, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

[17] 본 명세서에 대한 설명에 앞서, 본 명세서에서 사용되는 몇몇 용어들에 대하여 설명하기로 한다.

[18] 클라우드 서비스(Cloud service)는 로컬 컴퓨팅 장치가 각종 데이터를 네트워크에 연결된 외부의 서버에 저장하고, 필요 시 외부의 서버로부터 다운로드하여 이용할 수 있는 서비스이다. 보다 구체적으로, 로컬 컴퓨팅 장치의 인스턴스(instance)는 내부의 저장공간이 아닌, 네트워크에 연결된 외부의 서버에 데이터를 저장할 수 있다. 그리고, 로컬 컴퓨팅 장치의 인스턴스는 외부의 서버에 저장된 데이터가 필요한 경우, 외부의 서버로부터 데이터를 다운로드하여 이용할 수 있다. 특히, 본 발명의 일 실시예에 따른 클라우드 서비스는 로컬 컴퓨팅 장치에 가상화된 인프라 환경을 제공할 수 있는 이아스(Infrastructure as a Service, IaaS) 또는 사아스(Software as a Service)가 될 수 있으나, 이에 한정되는 것은 아니다.

[19] 서비스 키(Service key)는 클라우드 서비스를 통해 실행되는 인스턴스가 데이터를 암복호화하기 위해 사용하는 키이다. 이러한, 서비스 키는 클라우드 서비스의 이용자(Tenant), 클라우드 서비스를 통해 제공되는 서비스 또는 클라우드 서비스를 통해 제공되는 서비스의 애플리케이션 등에 따라 서로 상이한 값을 가지도록 설정될 수 있다. 또한, 서비스 키는 클라우드 서비스의 이용자, 클라우드 서비스를 통해 제공되는 서비스 또는 클라우드 서비스를 통해 제공되는 서비스의 애플리케이션 등에 따라 서로 상이한 크기 또는 타입을 가질 수 있으나, 이에 한정되는 것은 아니다.

[20]

[21] 마스터 키(Master key)는 서비스 키를 암복호화하기 위해 사용되는 키이다.

이러한, 마스터 키는 클라우드 서비스의 이용자, 클라우드 서비스를 통해 제공되는 서비스 또는 클라우드 서비스와 관련된 비즈니스 등에 따라 서로 상이한 값을 가지도록 생성될 수 있으나, 이에 한정되는 것은 아니다.

[22] 이 밖에, 본 명세서에서 사용된 용어들은 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "이루어지다(made of)"는 언급된 구성요소, 단계, 동작 및/또는 소자는 하나 이상의 다른 구성요소, 단계, 동작 및/또는 소자의 존재 또는 추가를 배제하지 않는다.

[23] 이하, 본 발명에 대하여 첨부된 도면에 따라 보다 상세히 설명한다.

[24] 도 1 내지 도 3은 본 발명의 몇몇 실시예에 따른 클라우드 서비스 시스템의 개념도이다. 도 1 내지 도 3에 개시된 클라우드 서비스 시스템의 각각의 구성 요소들은 기능적으로 구분되는 기능 요소들을 나타낸 것으로서, 어느 하나 이상의 구성 요소가 실제 물리적 환경에서는 서로 통합되어 구현될 수 있다.

[25] 도 1을 참조하면, 본 발명의 일 실시예에 따른 클라우드 서비스 시스템은 키 관리 시스템(10) 및 복수 개의 서비스 장치(400)를 포함하여 구성될 수 있다. 그리고, 키 관리 시스템(10)은 키 액세스 서버(100), 복수 개의 호스트 서버(200) 및 키 관리 데이터베이스(300)를 포함하여 구성될 수 있다. 이하, 본 발명의 일 실시예에 따른 클라우드 서비스 시스템의 각각의 구성 요소에 대하여 구체적으로 설명한다.

[26] 키 액세스 서버(100)는 클라우드 서비스의 인스턴스에 의하여 사용되는 서비스 키를 암복호화할 수 있는 마스터 키를 분산하여 관리할 수 있는 서버이다. 특히, 본 발명의 일 실시예에 따른 키 액세스 서버(100)는 마스터 키를 이용하여 서비스 키를 암호화한 후, 특정 조건에서만 마스터 키를 재생성할 수 있는 복수 개의 키 조각을 생성하고, 생성된 키 조각을 복수 개의 호스트 서버(200)에 분산 저장할 수 있다. 또한, 키 액세스 서버(100)는 복수 개의 호스트 서버(200)로부터 수신된 키 조각을 기초로 마스터 키를 재생성하고, 재생성된 마스터 키를 이용하여 서비스 키를 복호화할 수 있다. 이와 같은, 키 액세스 서버(100)에 대해서는, 추후 도 2 내지 도 9를 참조하여 구체적으로 설명할 것이다.

[27] 다음으로, 복수 개의 호스트 서버(200)는 키 액세스 서버(100)로부터 키 조각을 수신하여 저장할 수 있는 서버이다. 보다 구체적으로, 복수 개의 호스트 서버(200)는 클라우드 서비스를 제공하기 위한 동종 또는 이종의 서버 중 키 관리를 위한 에이전트(Key management agent)가 설치된 서버이다. 예를 들어, 복수 개의 호스트 서버(200)에는 키 관리를 위한 에이전트가 설치된, 이용자 관리 서버, 서버 코디네이터 장치, 데이터 분석 서버, 이벤트 관리 서버 또는 빅 데이터 저장 서버 등이 포함될 수 있으나, 이에 한정되지 않고, 키 관리만을 위한 전용 서버가 포함될 수도 있다. 이러한, 복수 개의 호스트 서버(200)는 호스트 그룹(20)을 형성할 수 있다.

[28] 호스트 그룹(20)에 포함된 복수 개의 호스트 서버(200)는 키 액세스 서버(100)로부터 키 조각을 수신하여 저장할 수 있다. 그리고, 복수 개의 호스트 서버(200)는 키 액세스 서버(100)의 요청에 응답하여, 저장된 키 조각을 추출하여 키 액세스 서버(100)에 전송할 수 있다.

[29] 호스트 그룹(20)에 포함된 복수 개의 호스트 서버(200)는 암호화 키(encryption key)를 이용하여 키 조각을 암호화한 후, 암호화된 키 조각을 키 액세스 서버(100)에 전송할 수 있다. 여기서, 암호화 키는 호스트 서버(200)별로 상이하게 프리셋(preset)될 수 있으나, 이에 한정되지 않고, 실시간으로 임시 키(temporary key)를 지정하여 키 액세스 서버(100)와 공유할 수도 있다.

[30] 호스트 그룹(20)에 포함된 복수 개의 호스트 서버(200)는 키 액세스 서버(100)가 공개한 키 조각 검증을 위한 데이터를 이용하여, 키 액세스 서버(100)가 악의적인(malicious)인 서버인지 아닌지 판단할 수 있다.

[31] 호스트 그룹(20)에 포함된 복수 개의 호스트 서버(200)는 키 액세스 서버(100)로부터 키 조각을 수신한 후, 수신된 키 조각의 해시 값(Hash value)를 계산하여 키 액세스 서버(100)에 전송할 수 있다.

[32] 그리고, 호스트 그룹(20)에 포함된 복수 개의 호스트 서버(200)는 키 액세스 서버(100)의 요청에 따라, 무작위적이며 유일한 마스터 키의 생성을 보장하기 위한 랜덤 시드(seed)를 생성하여 키 액세스 서버(100)에 전송할 수 있다.

[33] 다음으로, 키 관리 데이터베이스(300)는 마스터 키를 이용하여 암호화된 서비스 키를 저장할 수 있는 데이터베이스이다. 보다 구체적으로, 키 관리 데이터베이스(300)는 키 액세스 서버(100)로부터 수신된 암호화된 서비스 키를 저장할 수 있다. 또한, 키 관리 데이터베이스(300)는 마스터 키 테이블 및 서비스 키 테이블을 포함하여 저장할 수 있다.

[34] 여기서, 마스터 키 테이블에는 마스터 키의 식별자(identification), 클라우드 서비스의 이용자의 식별자, 서비스 키의 식별자, 마스터 키의 생성일시, 마스터 키의 해시 값 또는 마스터 키의 키 조각이 분산 저장된 호스트 서버(200)의 식별자 등이 포함될 수 있으나, 이에 한정되는 것은 아니다.

[35] 그리고, 서비스 키 테이블에는 서비스 키의 식별자, 클라우드 서비스의 이용자의 식별자, 서비스 키 사용 이력 등이 포함될 수 있으나, 이에 한정되는 것은 아니다.

[36] 이러한, 키 관리 데이터베이스(300)는 키 액세스 서버(100)와 독립된 구성 요소가 될 수 있으나, 이에 한정되지 않고, 키 액세스 서버(100)를 구성하는 하나의 구성 요소가 될 수 있음은 통상의 기술자에게 자명할 것이다. 나아가, 키 관리 데이터베이스(300)는 마스터 키 테이블 및 서비스 키 테이블 등의 사이에 일정한 관계(relation)가 존재하는 관계형 데이터베이스(Relational DataBase, RDB)가 될 수 있으나, 이에 한정되는 것은 아니다.

[37] 다음으로, 서비스 장치(400)는 클라우드 서비스를 제공하는 서버이다. 보다 구체적으로, 서비스 장치(400)는 하이퍼바이저(Hypervisor)를 통하여,

가상화(virtualization)될 수 있다. 여기서, 하이퍼바이저는 서비스 장치(400)의 리소스 및 기타 자원을 할당하고, 자원 관리 및 모니터링을 위한 인터페이스를 제공하는 플랫폼이다. 그리고, 서비스 장치(400)는 가상화된 가상 머신(virtual machine)을 통하여, 클라우드 서비스를 위한 애플리케이션 또는 애플리케이션의 인스턴스를 실행시킬 수 있다.

[38] 서비스 장치(400)의 인스턴스는 서비스 키를 이용하여 클라우드 서비스의 데이터를 암호화할 수 있다. 서비스 장치(400)는 서비스 키를 키 액세스 서버(100)에 전송하여 보호를 요청할 수 있다. 또한, 서비스 장치(400)는 클라우드 서비스의 데이터가 필요한 경우, 키 액세스 서버(100)로부터 서비스 키를 수신한 후, 수신된 서비스 키를 이용하여 클라우드 서비스의 데이터를 복호화할 수 있다.

[39] 그리고, 서비스 장치(400)는 키 관리 상호운용 프로토콜(Key Management Interoperability Protocol, KMIP)을 이용하여, 키 액세스 서버(100)와 데이터를 송수신할 수 있다. 또한, 서비스 장치(400)는 보안 소켓 계층/전송 계층 보안 프로토콜(Secure Sockets Layer/Transport Layer Security Protocol, SSL/TLS Protocol)을 이용하여, 키 액세스 서버(100)와 데이터를 송수신할 수 있다.

[40] 도 2를 참조하면, 본 발명의 다른 실시예에 따른 클라우드 서비스 시스템은 게이트웨이(500) 및 데이터 버스 장치(600)를 더 포함할 수 있다. 이하, 본 발명의 다른 실시예에 따라 클라우드 서비스 시스템에 추가적으로 포함된 구성 요소에 대하여 구체적으로 설명한다.

[41] 게이트웨이(500)는 서비스 장치(400)와 키 관리 시스템(10) 사이의 접근을 제어할 수 있다. 보다 구체적으로, 게이트웨이(500)는 서비스 장치(400)의 키 관리 시스템(10) 내에 포함된 서버에 대한 접근을 제한할 수 있다. 또한, 게이트웨이(500)는 키 관리 시스템(10) 내에 포함된 서버의 서비스 장치(400)에 대한 접근을 제한할 수 있다.

[42] 그리고, 게이트웨이(500)는 서비스 장치(400)에 레스트(REpresentational State Transfer, REST) 아키텍처에 따른 에이피아이(Application Programming Interface, API)를 제공할 수 있다. 또한, 게이트웨이(500)는 서비스 장치(400)로부터 수신된 데이터에 따른 이벤트를 데이터 버스 장치(600)에 전송할 수 있다.

[43] 다음으로, 데이터 버스 장치(600)는 키 관리 시스템(10)에 포함된 서버들 사이의 데이터 전송을 제어할 수 있다. 보다 구체적으로, 데이터 버스 장치(600)는 게이트웨이(500)로부터 수신된 이벤트를 키 액세스 서버(100) 또는 호스트 서버(200) 등에 전송할 수 있다. 또한, 데이터 버스 장치(600)는 키 액세스 서버(100) 또는 호스트 서버(200) 사이의 데이터 전송을 제어할 수 있다.

[44] 다만, 키 관리 시스템(10)에 데이터 버스 장치(600)가 포함되어 있더라도, 키 액세스 서버(100)는 데이터 버스 장치(600)를 이용하지 않고, 호스트 서버(200)와 직접 키 조각을 송수신할 수 있다.

[45] 도 3을 참조하면, 본 발명의 또 다른 실시예에 따른 클라우드 서비스 시스템은

복수 개의 키 액세스 서버(100)가 클러스터링(clustering)되어 구축될 수 있다. 이하, 본 발명의 또 다른 실시예에 따라 클라우드 서비스 시스템에 추가적으로 포함된 구성 요소에 대하여 구체적으로 설명한다.

[46] 메모리 기반 데이터베이스(700)는 키 액세스 서버(100)의 마스터 키에 대한 접근 속도를 향상시키기 위하여, 키 액세스 서버(100)가 반복적으로 이용하는 마스터 키를 메모리에 저장할 수 있다. 보다 구체적으로, 메모리 기반 데이터베이스(700)은 키 액세스 서버(100)에 의하여 재생성된 마스터 키를 수신할 수 있다. 메모리 기반 데이터베이스(700)는 재생성된 마스터 키를 메모리에 저장(in-memory)할 수 있다. 메모리 기반 데이터베이스(700)는 키 액세스 서버(100)로부터 마스터 키 제공 요청을 수신할 수 있다. 메모리 기반 데이터베이스(700)는 마스터 키 제공 요청에 응답하여, 메모리에 저장된 마스터 키를 키 액세스 서버(100)에 전송할 수 있다.

[47] 이하, 본 발명의 일 실시예에 따른 키 액세스 서버(100)의 마스터 키 분산 저장 방법 및 마스터 키 재생성 방법에 대하여 구체적으로 설명한다.

[48] 도 4는 본 발명의 일 실시예에 따른 마스터 키 분산 저장 방법을 설명하기 위한 순서도이다.

[49] 도 4를 참조하면, 키 액세스 서버(100)는 서비스 장치(400)의 인스턴스로부터 서비스 키를 수신한다(S105). 여기서, 서비스 키는 클라우드 서비스 이용자의 인스턴스에 의하여, 데이터를 암복호화하기 위해 사용되는 키이다. 이러한, 서비스 키는 클라우드 서비스의 이용자, 클라우드 서비스를 통해 제공되는 서비스 또는 클라우드 서비스를 통해 제공되는 서비스의 애플리케이션 등에 따라 서로 상이한 크기 또는 타입을 가질 수 있으나, 이에 한정되는 것은 아니다. 또한, 키 액세스 서버(100)는 키 관리 상호운용 프로토콜(KMIP)을 이용하여, 서비스 장치(400)의 인스턴스로부터 서비스 키를 수신할 수 있으나, 이에 한정되는 것은 아니다.

[50] 나아가, 키 액세스 서버(100)는 서비스 장치(400)의 인스턴스로부터 서비스 키를 수신하기 이전에, 서비스 장치(400)의 인스턴스로부터 클라우드 서비스 이용자의 식별자 및 서비스 키의 식별자를 수신하고, 수신된 서비스 이용자의 식별자 및 서비스 키의 식별자를 이용하여 인스턴스를 인증할 수 있으나, 이에 한정되는 것은 아니다.

[51] 다음으로, 키 액세스 서버(100)는 수신된 서비스 키를 암호화하기 위한 마스터 키를 생성한다(S110). 구체적으로, 키 액세스 서버(100)는 호스트 서버(200)에 랜덤 시드(seed)를 요청한다. 키 액세스 서버(100)는 호스트 서버(200)로부터 수신된 랜덤 시드를 기초로, 기 지정된 랜덤 생성 매커니즘에 따라 마스터 키를 생성한다. 따라서, 키 액세스 서버(100)에 의해 생성된 마스터 키는 클라우드 서비스의 이용자(tenant), 클라우드 서비스를 통해 제공되는 서비스 또는 클라우드 서비스와 관련된 비즈니스 등에 따라 무작위적이며 유일한 값을 가질 수 있다. 또한, 키 액세스 서버(100)는 새로운 마스터 키가 필요한 시점에

안정적으로 연결된 호스트 서버(200)들로부터 랜덤 시드를 수신하고, 수신된 랜덤 시드를 기초로 마스터 키를 생성함으로써, 생성된 마스터 키 값의 예측 가능성을 낮출 수 있다.

[52] 다음으로, 키 액세스 서버(100)는 생성된 마스터를 이용하여, 서비스 키를 암호화한다(S115). 그리고, 키 액세스 서버(100)는 암호화된 서비스 키를 키 관리 데이터베이스(300)에 저장한다(S120).

[53] 다음으로, 키 액세스 서버(100)는 마스터 키를 재생성하기 위한 둘 이상의 키 조각을 생성한다(S125). 구체적으로, 키 액세스 서버(100)는 임계 수(threshold) 이상이 존재하는 경우에만, 마스터 키를 재생성할 수 있는 키 조각을 생성할 수 있다. 이하, 키 액세스 서버(100)의 키 조각 생성 방법에 대하여 보다 구체적으로 설명한다.

[54] 키 액세스 서버(100)가 마스터 키를 재생성하기 위해 최소로 필요한 키 조각의 임계 수를 k라 하자. 예를 들어, 임계 수 k는 3이 될 수 있으나, 이에 한정되는 것은 아니다. 키 액세스 서버(100)는 k-1개의 난수(random number)를 생성한다. 키 액세스 서버(100)가 생성한 각각의 난수를 a_{k-1}, a_{k-2}, ..., a_1라 하자. 그리고, 키 액세스 서버(100)는 a_0를 마스터 키로 설정한다.

[55] 키 액세스 서버(100)는 1 내지 k-1차 항의 계수가 a_{k-1}, a_{k-2}, ..., a_1이며, 0차 항의 계수가 a_0인, k차수의 다항식 f(x)을 생성한다. 키 액세스 서버(100)가 생성한 다항식 f(x)는 아래의 수학식 1과 같다.

[56] [수학식 1]

[57] $$f(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1x + a_0$$

[58] 여기서, f(0)는 마스터 키가 된다.

[59] 키 액세스 서버(100)는 키 조각을 분산 저장할 n개의 호스트 서버(200)의 식별자에 대한 다항식 f(0)의 함수 값을 기초로 n개의 키 조각을 생성한다. 여기서, $1 < k <= n$이다.

[60] 따라서, 본 발명의 일 실시예에 따른 키 관리 시스템(10)은 마스터 키와 전혀 상이한 형태의 n개의 키 조각을 생성할 수 있다.

[61] 또한, 키 액세스 서버(100)는 다항식 f(x)의 함수 값을 마스터 키가 가질 수 있는 최대 크기로 나눈 나머지(mod)를 키 조각으로 생성할 수도 있다. 이 경우, 생성된 키 조각의 크기는 모두 동일해질 수 있다.

[62] 따라서, 본 발명의 일 실시예에 따른 키 관리 시스템(10)은 모든 키 조각의 크기가 동일하게 키 조각을 생성함으로써, 만약 키 조각의 일부가 외부 또는 내부에 유출되더라도 유출된 키 조각의 크기를 기초로 마스터 키를 예측하기 곤란하다.

[63] 다음으로, 키 액세스 서버(100)는 호스트 서버(200)별로 상이한 암호화 키를 이용하여, 생성된 n개의 키 조각을 암호화한다(S130). 여기서, 암호화 키는 호스트 서버(200)별로 상이하도록 기 지정되어 있을 수 있다. 이러한, 암호화

키는 호스트 서버(200)에 키 관리를 위한 에이전트가 설치될 당시 키 액세스 서버(100)에 설정될 수 있으나, 이에 한정되지 않고, 실시간으로 지정된 임시 키(temporary key)를 호스트 서버(200)로부터 수신할 수도 있다.

[64] 따라서, 본 발명의 일 실시예에 따른 키 관리 시스템(10)은 호스트 서버(200)별로 상이한 암호화 키를 이용하여 키 조각을 암호화함으로써, 만약 제1 호스트 서버(200)의 암호화된 키 조각이 제2 호스트 서버(200)에 유출되더라도, 제1 호스트 서버(200)의 암호화 키를 알 수 없는 제2 호스트 서버(200)는 암호화된 키 조각을 복호화할 수 없다.

[65] 다음으로, 키 액세스 서버(100)는 n개의 암호화된 키 조각을 n개의 호스트 서버(200)에 분산 저장한다(S135). 보다 구체적으로, 키 액세스 서버(100)는 키 분산 프로토콜(key sharing protocol)을 이용하여, 키 조각을 호스트 서버(200)에 전송할 수 있다. 여기서, 키 분산 프로토콜은 호스트 그룹(20)에 포함된 호스트 서버(200) 사이의 데이터 송수신이 허용되지 않도록 정의된 고유의 프로토콜이다. 또한, 키 분산 프로토콜은 데이터 송수신의 일 측이 키 액세스 서버(100)인 경우에 한하여, 데이터 송수신이 허용되도록 정의된 프로토콜이다.

[66] 또한, 키 액세스 서버(100)는 호스트 그룹(20)에 포함된 호스트 서버(200) 중 키 조각을 저장할 호스트 서버(200)를 선택함에 있어, 키 조각의 기초가 된 마스터 키에 관한 이용자의 클라우드 서비스와 관련되지 않은 호스트 서버(200)를 선택할 수 있다. 즉, 키 액세스 서버(100)는 제1 이용자에 제공되는 클라우드 서비스와 관련되지 않은 호스트 서버(200)에 제1 이용자에 대한 마스터 키를 분산 저장할 수 있다.

[67] 따라서, 본 발명의 일 실시예에 따른 키 관리 시스템(10)은 제1 이용자에 제공되는 클라우드 서비스와 관련되지 않은 호스트 서버(200)에 제1 이용자에 대한 마스터 키를 분산 저장함으로써, 제1 이용자와 밀접한 관계를 가지는 자가 제1 이용자의 클라우드 서비스와 관련된 호스트 서버(200)로부터 키 조각을 수집할 수 없다.

[68] 다음으로, 키 액세스 서버(100)는 키 조각이 분산 저장된 n개의 호스트 서버(200)로부터 각각 해시 값을 수신한다(S140). 그리고, 키 액세스 서버(100)는 수신된 해시 값과 생성된 키 조각의 해시 값을 비교하여, 서로 동일한지 판단한다(S145). 판단 결과, n개의 호스트 서버(200)로부터 각각 수신된 해시 값과, 마스터 키를 기초로 생성된 각각의 키 조각의 해시 값 중 상이한 해시 값이 존재하는 경우, 키 액세스 서버(100)는 해당 호스트 서버(200)에 암호화된 키 조각을 다시 전송할 수 있다.

[69] 판단 결과, n개의 호스트 서버(200)로부터 각각 수신된 해시 값과, 마스터 키를 기초로 생성된 각각의 키 조각의 해시 값이 모두 동일한 경우, 키 액세스 서버(100)는 각각의 키 조각의 해시 값을 키 관리 데이터베이스(300)에 저장한다. 그리고, 키 액세스 서버(100)는 마스터 키가 메모리 또는 스토리지에 저장되어 있는 경우, 저장되어 있는 마스터 키를 삭제한다(S150).

[70] 따라서, 본 발명의 일 실시예에 따른 키 관리 시스템(10)은 클라우드 서비스에 사용되는 서비스 키를 별도의 마스터 키로 암호화한 후, 임계 수 이상이 존재하는 경우에만 마스터 키를 재생성할 수 있는 키 조각을 생성하여 분산 저장하고, 어떠한 서버 또는 장치에도 마스터 키를 저장하지 않음으로써, 마스터 키의 비밀성을 확보할 수 있다.

[71] 도 5는 본 발명의 일 실시예에 따른 마스터 키 재생성 방법을 설명하기 위한 순서도이다.

[72] 도 5를 참조하면, 키 액세스 서버(100)는 서비스 장치(400)의 인스턴스로부터 서비스 키의 제공 요청을 수신한다(S205). 키 액세스 서버(100)는 보안 소켓 계층/전송 계층 보안 프로토콜(SSL/TLS Protocol)을 이용하여, 서비스 장치(400)의 인스턴스로부터 서비스 키의 제공 요청을 수신할 수 있으나, 이에 한정되는 것은 아니다.

[73] 나아가, 키 액세스 서버(100)는 서비스 장치(400)의 인스턴스로부터 서비스 키의 제공 요청을 수신하기 이전에, 서비스 장치(400)의 인스턴스로부터 클라우드 서비스 이용자의 식별자 및 서비스 키의 식별자를 수신하고, 수신된 서비스 이용자의 식별자 및 서비스 키의 식별자를 이용하여 인스턴스를 인증할 수 있으나, 이에 한정되는 것은 아니다.

[74] 다음으로, 키 액세스 서버(100)는 키 액세스 서버(100)의 메모리 또는 메모리 기반 데이터베이스(700)에 서비스 키의 제공을 요청한 인스턴스에 관한 마스터 키가 존재하는지 판단한다(S210).

[75] 판단 결과, 키 액세스 서버(100)의 메모리 및 메모리 기반 데이터베이스(700)에 해당 마스터 키가 존재하지 않는 경우, 키 조각을 분산 저장하고 있는 n개의 호스트 서버(200) 중 마스터 키 재생성에 필요한 키 조각의 임계 수 k보다 크거나 같은 수의 호스트 서버(200)를 식별한다. 그리고, 키 액세스 서버(100)는 식별된 각각의 호스트 서버(200)에 대한 암호화 키를 이용하여, 키 조각 요청 메시지를 각각 암호화한다(S215).

[76] 다음으로, 키 액세스 서버(100)는 식별된 각각의 호스트 서버(200)에 암호화된 키 조각 요청 메시지를 전송한다(S220). 여기서, 키 액세스 서버(100)는 키 조각을 분산 저장하고 있는 n개의 호스트 서버(200) 모두에 암호화된 키 조각 요청 메시지를 전송하지 아니하고, 키 조각을 분산 저장하고 있는 n개의 호스트 서버(200) 중 마스터 키 재생성에 필요한 키 조각의 임계 수 k보다 크거나 같은 수의 호스트 서버(200)에 대해서만 암호화된 키 조각 요청 메시지를 전송할 수 있다.

[77] 또한, 키 액세스 서버(100)는 키 분산 프로토콜을 이용하여, 암호화된 키 조각 요청 메시지를 전송할 수 있다. 여기서, 키 분산 프로토콜은 호스트 그룹(20)에 포함된 호스트 서버(200) 사이의 데이터 송수신이 허용되지 않도록 정의된 고유의 프로토콜이다. 또한, 키 분산 프로토콜은 데이터 송수신의 일 측이 키 액세스 서버(100)인 경우에 한하여, 데이터 송수신이 허용되도록 정의된

프로토콜이다.

[78] 다음으로, 키 액세스 서버(100)는 키 조각 요청 메시지를 전송한 각각의 호스트 서버(200)로부터 암호화된 키 조각을 수신한다(S225). 키 액세스 서버(100)는 키 분산 프로토콜을 이용하여, 암호화된 키 조각을 수신할 수 있다. 그리고, 키 액세스 서버(100)는 키 조각 요청 메시지를 전송한 호스트 서버(200)에 대한 암호화 키를 이용하여, 암호화된 각각의 키 조각을 복호화한다(S230).

[79] 다음으로, 키 액세스 서버(100)는 복호화된 각각의 키 조각의 해시 값과, 키 관리 데이터베이스(300)에 각각 저장된 해시 값을 비교하여, 서로 동일한지 판단한다(S235). 판단 결과, 복호화된 각각의 키 조각의 해시 값과, 키 관리 데이터베이스(300)에 각각 저장된 해시 값 중 상이한 해시 값이 존재하는 경우, 키 액세스 서버(100)는 해당 호스트 서버(200)에 암호화된 키 전송 요청 메시지를 다시 전송할 수 있다.

[80] 판단 결과, 복호화된 각각의 키 조각의 해시 값과, 키 관리 데이터베이스(300)에 각각 저장된 해시 값이 모두 동일한 경우, 키 액세스 서버(100)는 키 조각을 기초로 마스터 키를 재생성한다(S240). 구체적으로, 키 액세스 서버(100)는 라그레인지 보간법(Lagrange interpolation)을 이용하여, 마스터 키를 재생성할 수 있다. 이하, 키 액세스 서버(100)의 마스터 키 재생성 방법에 대하여 구체적으로 설명한다.

[81] 마스터 키를 재생성하기 위해 필요한 키 조각의 임계 수를 k, 호스트 서버(200) i에 대한 키 조각을 y_i라 하자. 키 액세스 서버(100)는 마스터 키 f(0)를 아래의 수학식 2를 이용하여 계산할 수 있다.

[82] [수학식 2]

[83]
$$f(0) = \sum_{j=1}^{k} y_{i_j} \prod_{1 \le l \le k, l \ne j} \frac{x_{i_l}}{x_{i_l} - x_{i_j}}$$

[84] 따라서, 본 발명의 일 실시예에 따른 키 관리 시스템(10)은 n개의 호스트 서버(200)에 분산 저장된 n개의 키 조각 중 임계 수 k보다 적은 수의 키 조각이 존재하는 경우에는 마스터 키를 재생성할 수 없으며, 임계 수 k보다 크거나 같은 수의 키 조각이 존재하는 경우에만 마스터 키를 재생성할 수 있다.

[85] 다음으로, 키 액세스 서버(100)는 재생성된 마스터 키를 메모리 기반 데이터베이스(700)에 저장할 수 있다(S245). 본 발명의 일 실시예에 따른 키 관리 시스템(10)에 메모리 기반 데이터베이스(700)가 포함되지 않은 경우, 본 단계가 생략되고 수행될 수 있음은 통상의 기술자에게 자명하다.

[86] 다음으로, 키 액세스 서버(100)는 인스턴스의 요청과 관련된 암호화된 서비스 키를 키 관리 데이터베이스(300)로부터 추출한다(S250). 키 액세스 서버(100)는 마스터 키를 이용하여, 암호화된 서비스 키를 복호화한다(S255). 그리고, 키 액세스 서버(100)는 복호화된 서비스 키를 서비스 장치(400)의 인스턴스에 전송한다(S260).

[87] 따라서, 본 발명의 일 실시예에 따른 키 관리 시스템(10)은 분산 저장된 키 조각의 일부가 분실되더라도 마스터 키를 재생성할 수 있어, 마스터 키의 가용성을 확보할 수 있다. 또한, 마스터 키를 생성하기 위해 필요한 임계 수 이상의 키 조각이 유출되더라도, 키 조각들이 각기 다른 암호화 키로 암호화되어 있어 유출된 키 조각만으로는 마스터 키를 재생성할 수 없다.

[88] 이하, 본 발명의 다른 실시예에 따른 마스터 키 분산 저장 방법 및 마스터 키 재생성 방법에 대하여 구체적으로 설명한다.

[89] 도 6은 본 발명의 다른 실시예에 따른 마스터 키 분산 저장 방법을 설명하기 위한 신호 흐름도이다.

[90] 도 6을 참조하면, 서비스 장치(400)의 인스턴스는 클라우드 서비스의 데이터를 서비스 키로 암호화한 후, 서비스 키를 키 액세스 서버(100)에 전송한다(S305). 구체적으로, 서비스 장치(400)의 인스턴스는 키 관리 상호운용 프로토콜(KMIP)을 이용하여, 서비스 키를 키 액세스 서버(100)에 전송할 수 있으나, 이에 한정되는 것은 아니다.

[91] 키 액세스 서버(100)는 수신된 서비스 키를 암호화하기 위한 마스터 키를 생성한다(S310). 키 액세스 서버(100)는 생성된 마스터 키를 이용하여, 수신된 서비스 키를 암호화한다(S315). 그리고, 키 액세스 서버(100)는 암호화된 서비스 키를 키 관리 데이터베이스(300)에 전송한다(S320).

[92] 키 관리 데이터베이스(300)는 암호화된 서비스 키의 수신에 응답하여, 암호화된 서비스 키를 저장한다(S325).

[93] 키 액세스 서버(100)는 마스터 키를 재생성하기 위한 둘 이상의 키 조각을 생성한다(S330). 구체적으로, 키 액세스 서버(100)는 임계 수 이상이 존재하는 경우에만, 마스터 키를 재생성할 수 있는 키 조각을 생성할 수 있다. 키 액세스 서버(100)의 키 조각 생성 방법에 대한 보다 구체적인 설명은, 도 4를 참조하여 상술한 바와 동일하므로 중복하여 설명하지 않는다.

[94] 키 액세스 서버(100)는 호스트 서버(200)별로 상이한 암호화 키를 이용하여, 키 조각을 각각 암호화한다(S335). 여기서, 암호화 키는 호스트 서버(200)에 키 관리를 위한 에이전트가 설치될 당시 키 액세스 서버(100)에 설정될 수 있으나, 이에 한정되지 않고, 실시간으로 지정된 임시 키를 호스트 서버(200)로부터 수신할 수도 있다.

[95] 키 액세스 서버(100)는 암호화된 각각의 키 조각을 호스트 서버(200)들에 전송한다(S340). 키 액세스 서버(100)는 키 분산 프로토콜을 이용하여, 키 조각을 호스트 서버(200)들에 전송할 수 있다.

[96] 호스트 서버(200)들은 각각의 암호화 키를 이용하여, 수신된 키 조각을 복호화한다(S345). 호스트 서버(200)들은 복호화된 키 조각의 해시 값을 생성한다(S350). 호스트 서버(200)들은 복호화된 키 조각을 저장한다(S355). 그리고, 호스트 서버(200)들은 생성된 해시 값을 키 액세스 서버(100)에 전송한다(S360).

[97] 키 액세스 서버(100)는 호스트 서버(200)들로부터 수신된 해시 값과, 마스터 키를 기초로 생성된 키 조각의 해시 값을 비교하여, 서로 동일한지 판단한다(S365). 판단 결과, 호스트 서버(200)들로부터 수신된 해시 값과, 마스터 키를 기초로 생성된 키 조각의 해시 값 중 상이한 해시 값이 존재하는 경우, 키 액세스 서버(100)는 해당 호스트 서버(200)에 암호화된 키 조각을 다시 재전송할 수 있다.

[98] 판단 결과, 호스트 서버(200)들로부터 수신된 해시 값과, 마스터 키를 기초로 생성된 키 조각의 해시 값이 모두 동일한 경우, 키 액세스 서버(100)는 메모리 또는 스토리지에 저장되어 있는 마스터 키를 삭제한다(S370).

[99] 도 7은 본 발명의 다른 실시예에 따른 마스터 키 재생성 방법을 설명하기 위한 신호 흐름도이다. 이하, 키 액세스 서버(100)의 메모리 및 메모리 기반 데이터베이스(700)에 마스터 키가 존재하지 않는 것으로 가정한다.

[100] 도 7을 참조하면, 서비스 장치(400)의 인스턴스는 클라우드 서비스의 데이터를 복호화하기 위하여, 서비스 키의 제공 요청을 키 액세스 서버(100)에 전송한다(S405). 구체적으로, 서비스 장치(400)의 인스턴스는 보안 소켓 계층/전송 계층 보안 프로토콜(SSL/TLS Protocol)을 이용하여, 서비스 키의 제공 요청을 키 액세스 서버(100)에 전송할 수 있으나, 이에 한정되는 것은 아니다.

[101] 키 액세스 서버(100)는 서비스 키의 제공 요청 수신에 응답하여, 서비스 키를 복호화하기 위한 마스터 키의 키 조각을 분산 저장하고 있는 호스트 서버(200)들을 식별한다. 키 액세스 서버(100)는 식별된 각각의 호스트 서버(200)에 대한 암호화 키를 이용하여, 키 조각 요청 메시지를 각각 암호화한다(S410). 그리고, 키 액세스 서버(100)는 식별된 각각의 호스트 서버(200)에 암호화된 키 조각 요청 메시지를 전송한다(S415).

[102] 호스트 서버(200)들은 암호화된 키 조각 요청 메시지를 각각의 암호화 키로 복호화한다. 그리고, 호스트 서버(200)들은 키 액세스 서버(100)가 악의적인(malicious) 서버인지 검증한다(S420). 이하, 호스트 서버(200)들의 펠드맨(Feldman)이 제안한 이상 대수를 이용한 검증 방법에 대하여 보다 구체적으로 설명한다.

[103] 키 액세스 서버(100)가 호스트 서버(200)들에 대하여, 키 조각을 생성한 함수의 계수 t의 암호화된 값 E(a), $E(a_1)$, ..., $E(a_{t-1})$를 공개하였다고 하자. 호스트 서버(200) i는 아래의 수학식 3이 성립하지 않는 경우, 키 액세스 서버(100)가 악의적인 서버인 것으로 판단할 수 있다.

[104] [수학식 3]

[105] $$E(f(i)) \equiv E(a^0) + (E(a^1) \times E(i^1)) + \cdots + (E(a^{t-1}) \times E(i^{t-1}))$$

[106] 그러나, 호스트 서버(200)들은 펠드맨이 제안한 검증 방법에 한정되지 않고, 페더슨(Pederson)이 제안한 검증 방법을 이용하여 키 액세스 서버(100)를 검증할 수도 있다.

[107] 호스트 서버(200)들은 키 액세스 서버(100)가 악의적인 서버가 아닌 경우,

각각에 저장된 키 조각을 추출하고, 추출된 키 조각을 각각의 암호화 키로 암호화한다(S425). 그리고, 호스트 서버(200)들은 암호화된 키 조각을 키 액세스 서버(100)에 전송한다(S430).

[108] 키 액세스 서버(100)는 키 조각을 전송한 각각의 호스트 서버(200)에 대한 암호화 키를 이용하여, 암호화된 키 조각을 복호화한다(S435). 그리고, 키 액세스 서버(100)는 키 관리 데이터베이스(300)에 키 조각의 해시 값 제공 요청을 전송한다(S440).

[109] 키 관리 데이터베이스(300)는 키 조각의 해시 값 제공 요청에 응답하여, 키 조각의 해시 값을 추출한다(S445). 그리고, 키 관리 데이터베이스(300)는 추출된 해시 값을 키 액세스 서버(100)에 전송한다(S450).

[110] 키 액세스 서버(100)는 복호화된 키 조각의 해시 값과, 키 관리 데이터베이스(300)로부터 수신된 해시 값을 비교하여, 서로 동일한지 판단한다(S455). 판단 결과, 복호화된 키 조각의 해시 값과, 키 관리 데이터베이스(300)로부터 수신된 해시 값 중 상이한 해시 값이 존재하는 경우, 키 액세스 서버(100)는 해당 호스트 서버(200)에 암호화된 키 조각 요청 메시지를 다시 전송할 수 있다.

[111] 판단 결과, 복호화된 키 조각의 해시 값과, 키 관리 데이터베이스(300)로부터 수신된 해시 값이 모두 동일한 경우, 키 액세스 서버(100)는 키 조각을 기초로 마스터 키를 재생성한다(S460). 구체적으로, 키 액세스 서버(100)는 라그레인지 보간법을 이용하여, 마스터 키를 재생성할 수 있다. 키 액세스 서버(100)의 마스터 키 재생성 방법에 대한 보다 구체적인 설명은, 도 5를 참조하여 상술한 바와 동일하므로 중복하여 설명하지 않는다.

[112] 키 액세스 서버(100)는 키 관리 데이터베이스(300)에 암호화된 서비스 키 제공 요청을 전송한다(S465).

[113] 키 관리 데이터베이스(300)는 암호화된 서비스 키 제공 요청에 응답하여, 암호화된 서비스 키를 추출한다(S470). 그리고, 키 관리 데이터베이스(300)는 추출된 암호화된 서비스 키를 키 액세스 서버(100)에 전송한다(S475).

[114] 키 액세스 서버(100)는 재생성된 마스터 키를 이용하여, 암호화된 서비스 키를 복호화한다(S480). 그리고, 키 액세스 서버(100)는 복호화된 서비스 키를 서비스 장치(400)의 인스턴스에 전송한다(S485).

[115] 지금까지, 도4 내지 도 7을 참조하여 설명한 본 발명의 실시예에 따른 방법들은 컴퓨터가 읽을 수 있는 코드로 구현된 컴퓨터 프로그램의 실행에 의하여 수행될 수 있다. 컴퓨터 프로그램은 인터넷 등의 네트워크를 통하여, 제1 컴퓨팅 장치로부터 제2 컴퓨팅 장치에 전송되어 제2 컴퓨팅 장치에 설치될 수 있고, 이로써 제2 컴퓨팅 장치에서 사용될 수 있다. 여기서, 제1 컴퓨팅 장치 및 제2 컴퓨팅 장치는, 데스크탑(Desktop), 서버(Server) 또는 워크스테이션(Workstation) 등과 같은 고정식 컴퓨팅 장치, 스마트폰(Smart phone), 태블릿(Tablet), 패블릿(Phablet) 또는 랩탑(Laptop) 등과 같은 모바일 컴퓨팅 장치 및 스마트

와치(Smart watch), 스마트 안경(Smart glasses) 또는 스마트 밴드(Smart band) 등과 같은 웨어러블(Wearable) 컴퓨팅 장치를 모두 포함할 수 있다.

[116] 이하, 도 8 및 도 9를 참조하여, 본 발명의 일 실시예에 따른 키 액세스 서버(100)의 논리적 구성에 대하여 구체적으로 설명하기로 한다.

[117] 도 8은 본 발명의 일 실시예에 따른 키 액세스 서버(100)의 블록도이다. 도 8을 참조하면, 키 액세스 서버(100)는 통신부(105), 저장부(110), 마스터 키 생성부(115), 서비스 키 암복호화부(120), 마스터 키 분산 저장부(125) 및 마스터 키 재생성부(130)를 포함할 수 있다.

[118] 각각의 구성에 대하여 설명하면, 통신부(205)는 키 분산 프로토콜을 이용하여, 호스트 서버(200)와 데이터를 송수신할 수 있다. 통신부(205)는 데이터 제공을 요청하기 위한 쿼리(query)를 작성하여, 키 관리 데이터베이스(300)와 데이터를 송수신할 수 있다. 또한, 통신부(205)는 키 관리 상호운용 프로토콜(KMIP) 또는 보안 소켓 계층/전송 계층 보안 프로토콜(SSL/TLS Protocol)을 이용하여, 서비스 장치(400)와 데이터를 송수신할 수도 있다.

[119] 저장부(110)는 키 액세스 서버(100)의 동작에 필요한 데이터를 저장할 수 있다. 특히, 서비스 장치(400)의 인스턴스로부터 서비스 키가 반복적으로 요청되어, 키 액세스 서버(100)가 특정 서비스를 위한 마스터 키를 반복적으로 이용하는 경우, 저장부(110)는 마스터 키에 대한 접근 속도를 향상시키기 위하여, 메모리 기반 저장소에 마스터 키(135)를 더 포함하여 저장할 수 있다.

[120] 마스터 키 생성부(115)는 서비스 키를 암호화하기 위한 마스터 키를 생성할 수 있다. 구체적으로, 마스터 키 생성부(115)는 통신부(105)를 통해 호스트 서버(200)에 랜덤 시드(seed)의 요청을 전송한다. 마스터 키 생성부(115)는 통신부(105)를 통해 호스트 서버(200)로부터 랜덤 시드를 수신한다. 마스터 키 생성부(115)는 랜덤 시드를 기초로, 기 지정된 랜덤 생성 매커니즘에 따라 마스터 키를 생성한다. 따라서, 마스터 키 생성부(115)가 생성한 마스터 키는 클라우드 서비스의 이용자(tenant), 클라우드 서비스를 통해 제공되는 서비스 또는 클라우드 서비스와 관련된 비즈니스 등에 따라 무작위적이며 유일한 값을 가질 수 있다. 또한, 마스터 키 생성부(115)는 새로운 마스터 키가 필요한 시점에 안정적으로 연결된 호스트 서버(200)들로부터 랜덤 시드를 수신하고, 수신된 랜덤 시드를 기초로 마스터 키를 생성함으로써, 생성된 마스터 키 값의 예측 가능성을 낮출 수 있다.

[121] 서비스 키 암복호화부(120)는 통신부(105)를 통해 서비스 키가 수신되면, 마스터 키 생성부(115)를 통해 생성된 마스터 키를 기초로 서비스 키를 암호화할 수 있다. 또한, 서비스 키 암복호화부(120)는 마스터 키 재생성부(130)를 통해 마스터 키가 재생성되면, 암호화된 서비스 키를 복호화할 수 있다.

[122] 마스터 키 분산 저장부(125)는 마스터 키를 재생성하기 위한 둘 이상의 키 조각을 생성하고, 생성된 키 조각을 통신부(105)를 통해 전송할 수 있다. 구체적으로, 마스터 키 분산 저장부(125)는 임계 수 이상이 존재하는 경우에만,

마스터 키를 재생성할 수 있는 키 조각을 생성할 수 있다. 마스터 키 분산 저장부(125)의 키 조각 생성 방법에 대한 보다 구체적인 설명은, 도 4를 참조하여 상술한 바와 동일하므로 중복하여 설명하지 않는다.

[123] 그리고, 마스터 키 분산 저장부(125)는 호스트 서버(200)별로 상이한 암호화 키를 이용하여, 키 조각을 각각 암호화할 수 있다. 마스터 키 분산 저장부(125)는 통신부(105)를 통해, 암호화된 각각의 키 조각을 호스트 서버(200)들에 전송할 수 있다. 마스터 키 분산 저장부(125)는 통신부(105)를 통해, 해시 값을 수신할 수 있다. 그리고, 마스터 키 분산 저장부(125)는 수신된 해시 값과 키 조각의 해시 값을 비교하여, 서로 동일한지 판단할 수 있다.

[124] 마스터 키 재생성부(130)는 둘 이상의 키 조각을 이용하여 마스터 키를 재생성할 수 있다. 구체적으로, 마스터 키 재생성부(130)는 통신부(105)를 통해 암호화된 키 조각을 수신할 수 있다. 마스터 키 재생성부(130)는 키 조각을 전송한 각각의 호스트 서버(200)에 대한 암호화 키를 이용하여, 암호화된 키 조각을 복호화할 수 있다. 마스터 키 재생성부(130)는 통신부(105)를 통해 키 관리 데이터베이스(300)로부터 해시 값을 수신할 수 있다. 마스터 키 재생성부(130)는 복호화된 키 조각의 해시 값과, 키 관리 데이터베이스(300)로부터 수신된 해시 값을 비교하여, 서로 동일한지 판단할 수 있다.

[125] 그리고, 마스터 키 재생성부(130)는 복호화된 키 조각을 기초로 마스터 키를 재생성할 수 있다. 구체적으로, 마스터 키 재생성부(130)는 라그레인지 보간법을 이용하여, 마스터 키를 재생성할 수 있다. 마스터 키 재생성부(130)의 마스터 키 재생성 방법에 대한 보다 구체적인 설명은, 도 5를 참조하여 상술한 바와 동일하므로 중복하여 설명하지 않는다.

[126] 지금까지, 도 8의 각 구성요소는 소프트웨어(Software) 또는, 현장 프로그래머블 게이트 어레이(Field-Programmable Gate Array, FPGA)나 에이직(Application-Specific Integrated Circuit, ASIC)과 같은 하드웨어(hardware)를 의미할 수 있다. 그렇지만, 상기 구성 요소들은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니며, 어드레싱(Addressing)할 수 있는 저장 매체에 있도록 구성될 수도 있고, 하나 또는 그 이상의 프로세서들을 실행시키도록 구성될 수도 있다. 상기 구성 요소들 안에서 제공되는 기능은 더 세분화된 구성요소에 의하여 구현될 수 있으며, 복수의 구성요소들을 합하여 특정한 기능을 수행하는 하나의 구성요소로 구현될 수도 있다.

[127] 도 9는 본 발명의 일 실시예에 따른 키 액세스 서버(100)의 하드웨어 구성도이다. 도 9를 참조하면, 키 액세스 서버(100)는 프로세서(155), 메모리(160), 네트워크 인터페이스(165), 데이터 버스(170) 및 스토리지(175)를 포함하여 구성될 수 있다.

[128] 메모리(160)는 키 관리 방법이 구현된 컴퓨터 프로그램 데이터(180a)가 상주될 수 있다. 또한, 키 액세스 서버(100)가 반복적으로 마스터 키를 이용하는 경우,

메모리(160)는 마스터 키(135)를 더 포함하여 저장할 수 있다.

[129] 네트워크 인터페이스(165)는 호스트 서버(200), 키 관리 데이터베이스(300)와 데이터를 송수신할 수 있다. 또한, 네트워크 인터페이스(165)는 서비스 장치(400)와 데이터를 송수신할 수도 있다.

[130] 데이터 버스(170)는 프로세서(155), 메모리(160), 네트워크 인터페이스(165) 및 스토리지(175)와 연결되어, 각 구성 요소간의 데이터를 전달하는 이동 통로이다.

[131] 그리고, 스토리지(175)는 컴퓨터 프로그램 실행을 위해 필요한 에이피아이(API), 라이브러리(Library) 또는 리소스(Resource) 파일 등을 저장할 수 있다. 또한, 스토리지(175)는 키 관리 방법이 구현된 컴퓨터 프로그램 데이터(180b)를 저장할 수 있다.

[132] 보다 구체적으로는, 스토리지(175)에는 클라우드 서비스의 제1 이용자의 인스턴스에 의하여 사용되는 서비스 키를 마스터 키를 이용하여 암호화하는 인스트럭션(instruction), 마스터 키를 재생성하기 위한 둘 이상의 키 조각을 생성하는 인스트럭션, 네트워크 인터페이스를 통해, 클라우드 서비스의 제공을 위한 호스트 그룹에 포함된 둘 이상의 호스트 서버에, 키 조각을 분산하여 저장하는 인스트럭션, 네트워크 인터페이스를 통해, 제1 이용자의 인스턴스로부터 서비스 키의 제공 요청을 수신하는 인스트럭션, 네트워크 인터페이스를 통해, 둘 이상의 호스트 서버로부터 키 조각들을 수신하고, 수신된 키 조각을 기초로 마스터 키를 재생성하는 인스트럭션, 및 암호화된 서비스 키를 마스터 키를 이용하여 복호화하는 인스트럭션을 포함하는 컴퓨터 프로그램이 저장될 수 있다.

[133] 이상 첨부된 도면을 참조하여 본 발명의 실시예들을 설명하였지만, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해되어야만 한다.

청구범위

[청구항 1] 클라우드 서비스의 제1 이용자의 인스턴스에 의하여 사용되는 서비스 키를 마스터 키를 이용하여 암호화하는 단계;
상기 마스터 키를 재생성하기 위한 둘 이상의 키 조각을 생성하는 단계;
상기 클라우드 서비스의 제공을 위한 호스트 그룹에 포함된 둘 이상의 호스트 서버에, 상기 키 조각을 분산하여 저장하는 단계;
상기 제1 이용자의 인스턴스로부터, 상기 서비스 키의 제공 요청을 수신하는 단계;
상기 둘 이상의 호스트 서버로부터 상기 키 조각들을 수신하고, 상기 수신된 키 조각을 기초로 상기 마스터 키를 재생성하는 단계; 및
상기 암호화된 서비스 키를 상기 재생성된 마스터 키를 이용하여 복호화하는 단계를 포함하는, 키 관리 방법.

[청구항 2] 제1 항에 있어서,
상기 키 조각을 생성하는 단계는,
상기 마스터 키를 재생성하기 위해 필요한 키 조각의 임계 수보다 많거나 같은 수의 키 조각을 생성하는 단계를 포함하는, 키 관리 방법.

[청구항 3] 제1 항에 있어서,
상기 조각 키를 생성하는 단계는,
상기 마스터 키를 재생성하기 위해 필요한 키 조각의 임계 수와 같은 차수의 다항식을 생성하되, 상기 다항식의 0차 항의 계수가 마스터 키인 다항식을 생성하는 단계; 및
상기 다항식의 함수 값을 기초로 상기 키 조각을 생성하는 단계를 포함하는, 키 관리 방법.

[청구항 4] 제3 항에 있어서,
상기 키 조각을 생성하는 단계는,
상기 함수 값을 상기 마스터 키가 가질 수 있는 최대 크기로 나눈 나머지를 기초로 상기 키 조각을 생성하는 단계를 포함하는, 키 관리 방법.

[청구항 5] 제1 항에 있어서,
상기 키 조각을 분산하여 저장하는 단계는,
상기 키 조각이 저장된 상기 호스트 서버로부터 해시 값을 수신하는 단계; 및
상기 수신된 해시 값과 상기 호스트 서버에 전송한 키 조각의 해시 값을 비교하는 단계를 포함하는, 키 관리 방법.

[청구항 6] 제1 항에 있어서,
상기 키 조각을 분산하여 저장하는 단계는,
상기 호스트 서버별로 서로 상이한 상기 호스트 서버의 암호화 키를

이용하여, 상기 키 조각을 각각 암호화하는 단계; 및
상기 암호화된 키 조각을 상기 호스트에 전송하는 단계를 포함하는, 키 관리 방법.

[청구항 7] 제1 항에 있어서,
상기 키 조각을 분산하여 저장하는 단계는,
상기 호스트 그룹에 포함된 호스트 서버 사이에서 이용될 수 없도록 정의된 프로토콜을 이용하여, 상기 키 조각을 상기 호스트 서버에 전송하는 단계를 포함하는, 키 관리 방법.

[청구항 8] 제1 항에 있어서,
상기 키 조각을 분산하여 저장하는 단계는,
상기 호스트 그룹에 포함된 호스트 서버 중 상기 제1 이용자에 제공되는 클라우드 서비스와 관련되지 않은 호스트 서버에, 상기 키 조각을 분산하여 저장하는 단계를 포함하는, 키 관리 방법.

[청구항 9] 제1 항에 있어서,
상기 마스터 키를 재생성하는 단계는,
상기 키 조각이 분산 저장된 호스트 서버 중 상기 마스터 키를 재생성하기 위해 필요한 키 조각의 임계 수보다 크거나 같은 수의 호스트 서버에 키 조각 요청 메시지를 전송하는 단계를 포함하는, 키 관리 방법.

[청구항 10] 제1 항에 있어서,
상기 마스터 키를 재생성하는 단계는,
상기 호스트 서버별로 서로 상이한 상기 호스트 서버의 암호화 키를 이용하여, 키 조각 요청 메시지를 각각 암호화하는 단계; 및
상기 암호화된 키 조각 요청 메시지를 상기 호스트 서버에 전송하는 단계를 포함하는, 키 관리 방법.

[청구항 11] 제1 항에 있어서,
상기 마스터 키를 재생성하는 단계는,
상기 재생성된 마스터 키를 메모리 기반 데이터베이스에 저장하는 단계를 포함하는, 키 관리 방법.

[청구항 12] 제1 항에 있어서,
상기 마스터 키를 재생성하는 단계는,
메모리 기반 데이터베이스에 상기 마스터 키가 존재하는지 판단한 후,
상기 메모리 기반 데이터베이스에 상기 마스터 키가 존재하지 않는 경우,
상기 마스터 키를 재생성하는 단계를 포함하는, 키 관리 방법.

[청구항 13] 제1 항에 있어서,
상기 마스터 키는,
클라우드 서비스의 이용자별로 서로 상이한 값을 가지도록 생성된, 키 관리 방법.

[청구항 14] 클라우드 서비스의 제1 이용자의 인스턴스에 의하여 사용되는 서비스

키를 마스터 키를 이용하여 암호화한 후, 상기 마스터 키를 재생성하기 위한 둘 이상의 키 조각을 생성하여 분산 저장하고, 상기 제1 이용자의 인스턴스로부터 서비스 키 제공 요청이 수신되면, 상기 분산 저장된 키 조각을 기초로 마스터 키를 재생성하여 상기 암호화된 서비스 키를 복호화하는 키 액세스 서버; 및

상기 키 액세스 서버로부터 상기 키 조각을 수신하여 저장하고, 상기 키 액세스 서버로부터 키 조각 제공 요청이 수신되면 상기 키 조각을 전송하는 호스트 서버를 포함하는, 키 관리 시스템.

[청구항 15] 제14 항에 있어서,

상기 키 액세스 서버로부터 상기 재생성된 마스터 키를 수신하여 저장하고, 상기 키 액세스 서버로부터 마스터 키 제공 요청이 수신되면 상기 마스터 키를 전송하는 메모리 기반 데이터베이스를 더 포함하는, 키 관리 시스템.

[청구항 16] 컴퓨팅 장치와 결합하여,

클라우드 서비스의 제1 이용자의 인스턴스에 의하여 사용되는 서비스 키를 마스터 키를 이용하여 암호화하는 단계;

상기 마스터 키를 재생성하기 위한 둘 이상의 키 조각을 생성하는 단계;

상기 클라우드 서비스의 제공을 위한 호스트 그룹에 포함된 둘 이상의 호스트 서버에, 상기 키 조각을 분산하여 저장하는 단계;

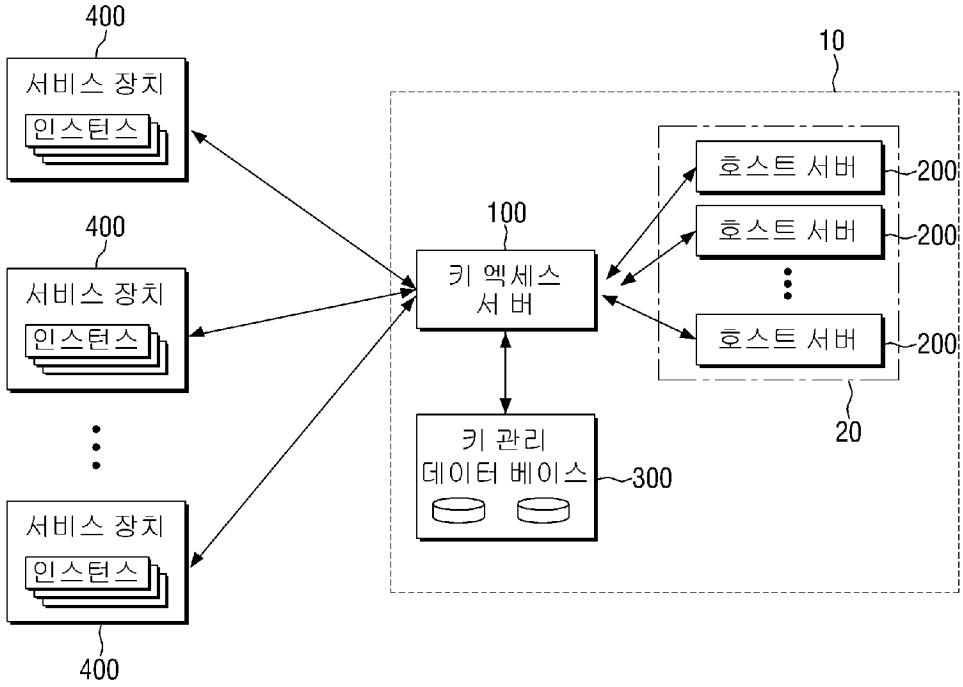
상기 제1 이용자의 인스턴스로부터, 서비스 키 제공 요청을 수신하는 단계;

상기 둘 이상의 호스트 서버로부터 상기 키 조각들을 수신하고, 상기 수신된 키 조각을 기초로 상기 마스터 키를 재생성하는 단계; 및

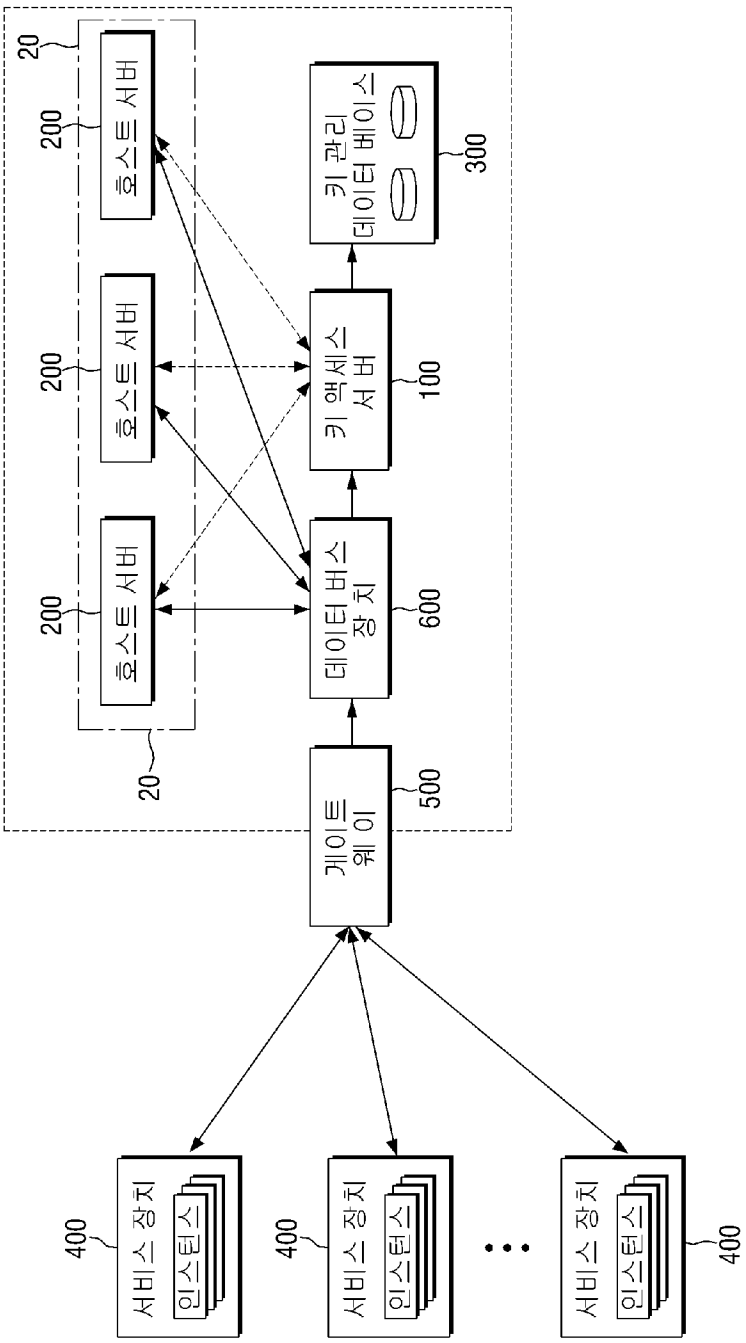
상기 암호화된 서비스 키를 상기 재생성된 마스터 키를 이용하여 복호화하는 단계를 실행시키기 위하여, 기록매체에 기록된 컴퓨터 프로그램.

WO 2016/190476 PCT/KR2015/006238

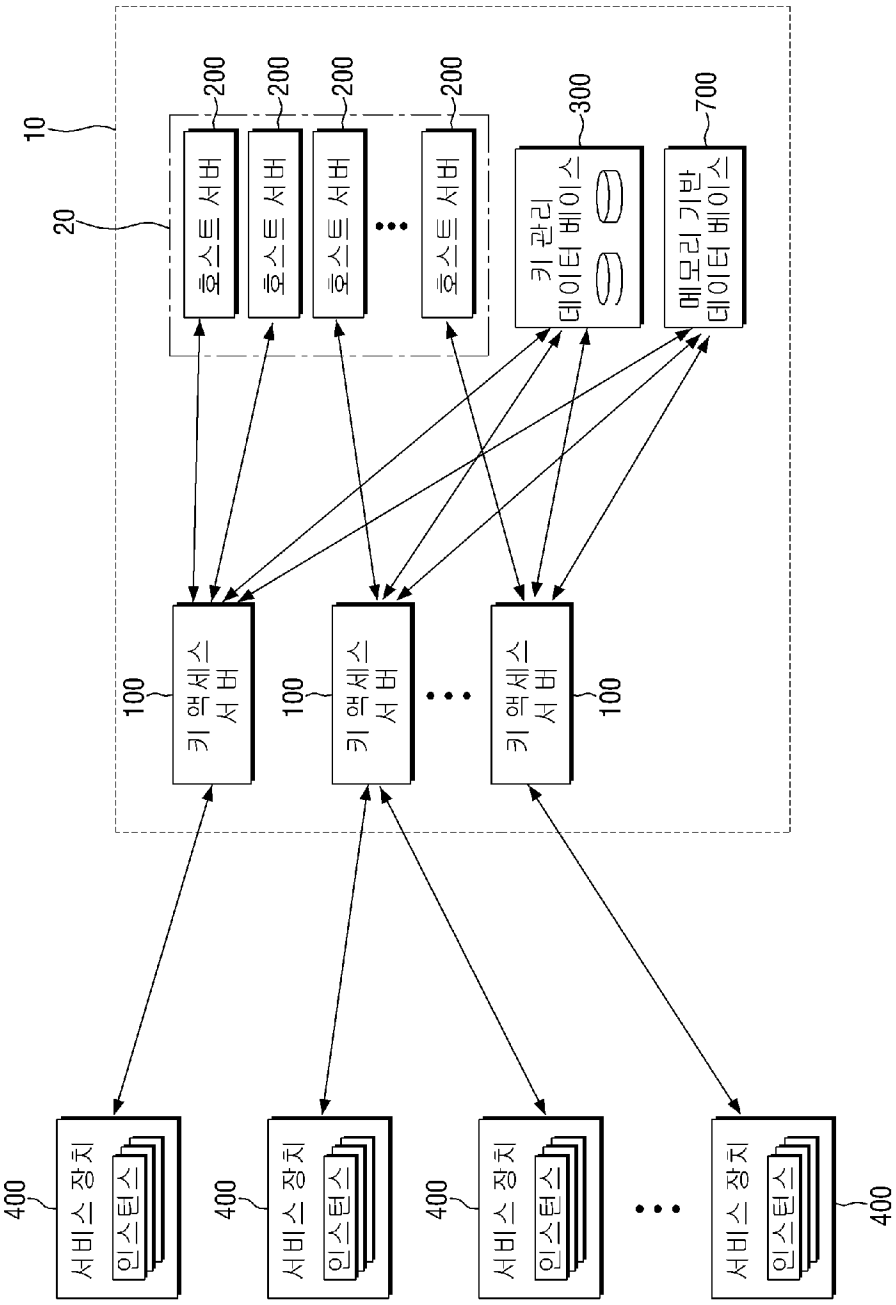
[도1]



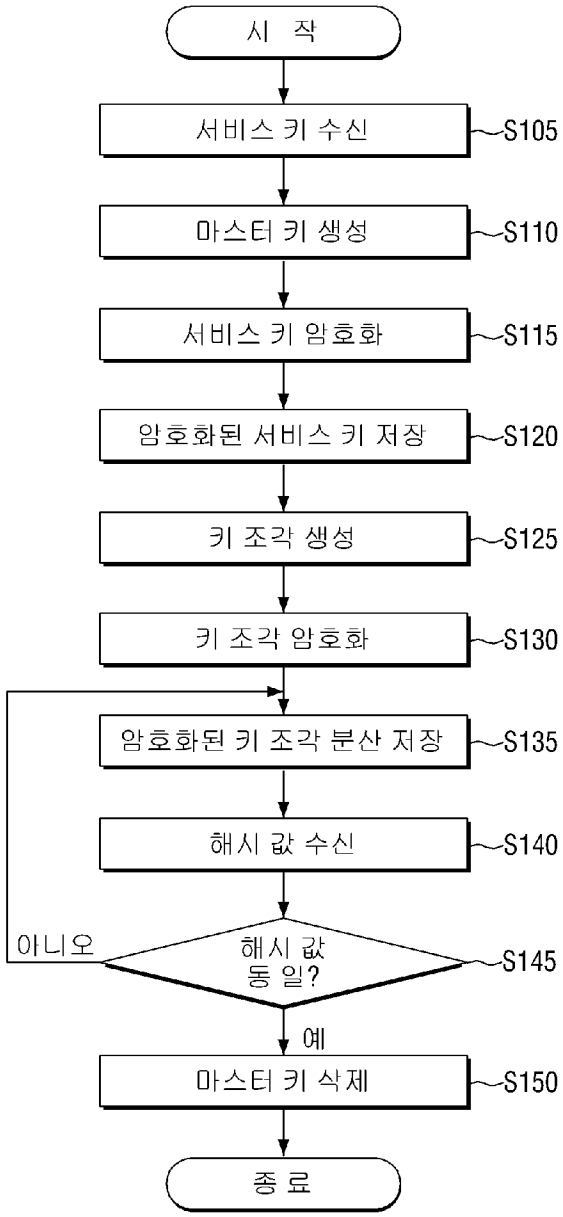
[도2]


20
200
호스트 서버
200
호스트 서버
200
호스트 서버
20
키 관리
데이터 베이스
300
키 액세스
서 버
100
데이터 버스
장 치
600
게이트
웨 이
500
400
서비스 장치
인스턴스
400
서비스 장치
인스턴스
400
서비스 장치
인스턴스

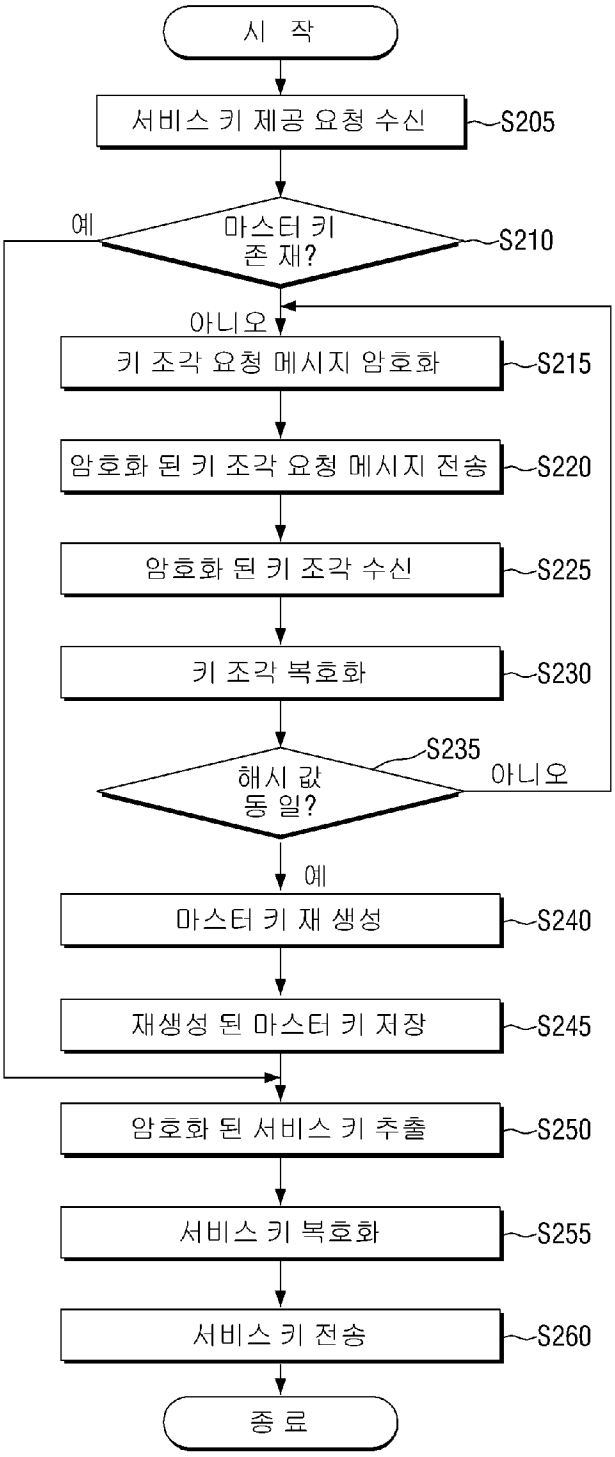
[도3]


10
20
200
호스트 서버
호스트 서버
호스트 서버
호스트 서버
300
키 관리 데이터 베이스
700
메모리 기반 데이터 베이스
100
키 액세스 서 버
키 액세스 서 버
키 액세스 서 버
400
서비스 장치
인스턴스
서비스 장치
인스턴스
서비스 장치
인스턴스
서비스 장치
인스턴스

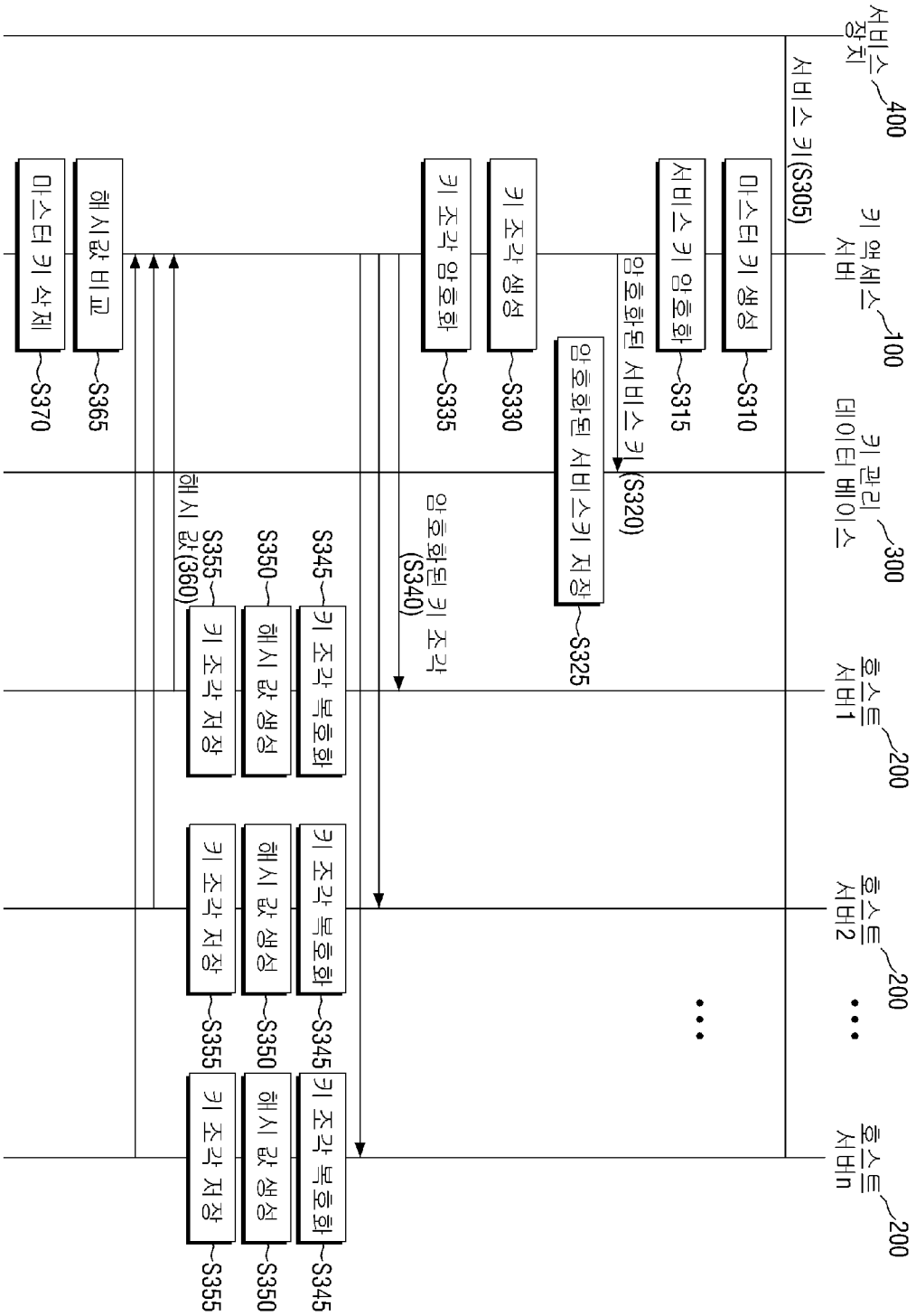
[도4]


시 작
서비스 키 수신
S105
마스터 키 생성
S110
서비스 키 암호화
S115
암호화된 서비스 키 저장
S120
키 조각 생성
S125
키 조각 암호화
S130
암호화된 키 조각 분산 저장
S135
해시 값 수신
S140
아니오
해시 값 동 일?
S145
예
마스터 키 삭제
S150
종 료

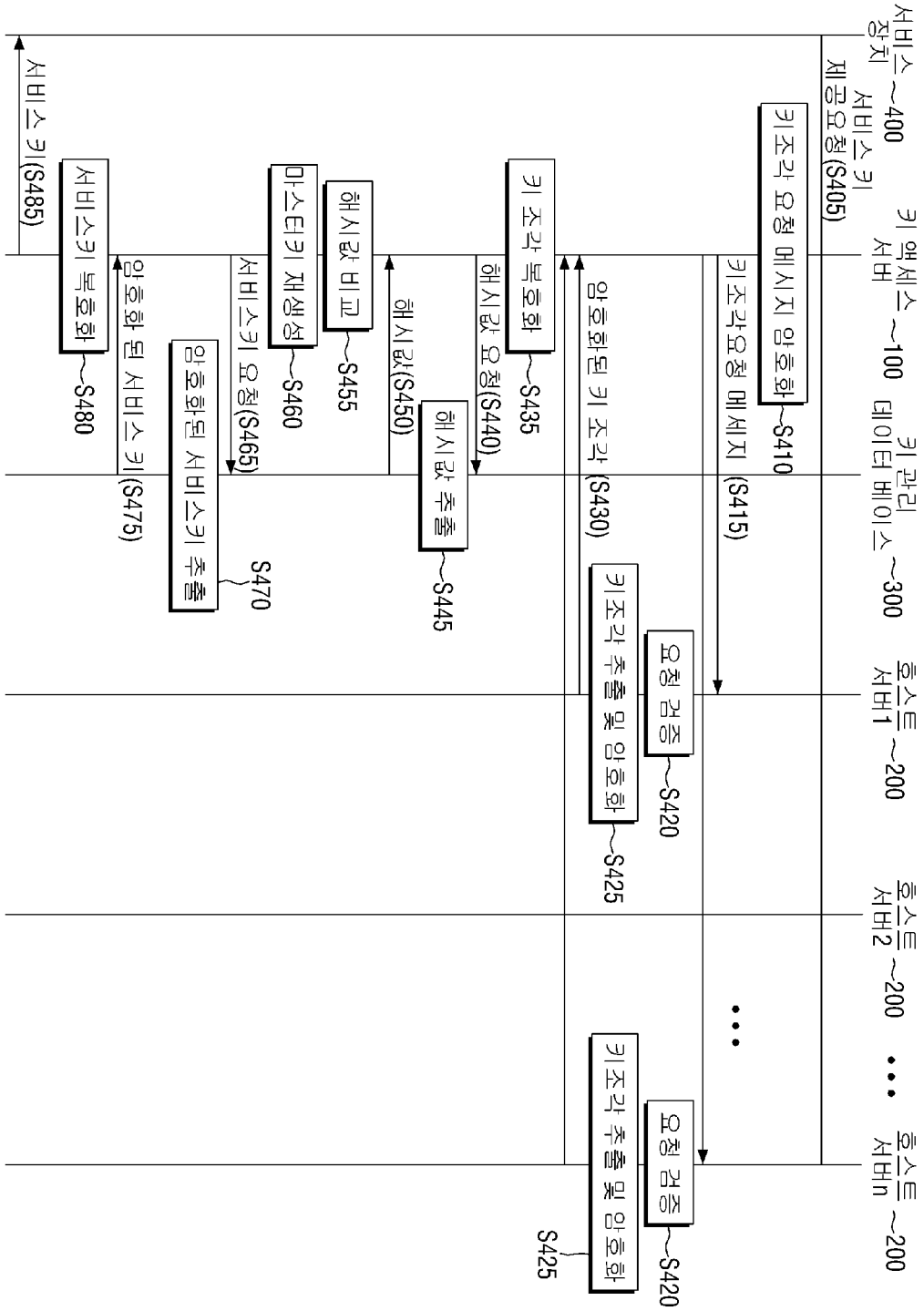
[도5]


시 작
서비스 키 제공 요청 수신
S205
마스터 키 존 재?
S210
예
아니오
키 조각 요청 메시지 암호화
S215
암호화 된 키 조각 요청 메시지 전송
S220
암호화 된 키 조각 수신
S225
키 조각 복호화
S230
해시 값 동 일?
S235
아니오
예
마스터 키 재 생성
S240
재생성 된 마스터 키 저장
S245
암호화 된 서비스 키 추출
S250
서비스 키 복호화
S255
서비스 키 전송
S260
종 료

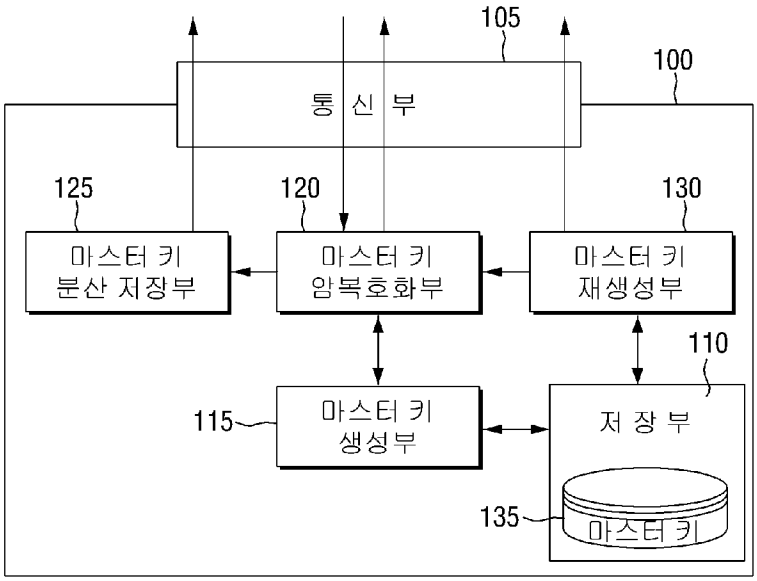
[도6]


서비스 장치
400
키 액세스 서버
100
키 관리 데이터 베이스
300
호스트 서버1
200
호스트 서버2
200
호스트 서버n
200
서비스 키(S305)
마스터 키 생성
S310
서비스 키 암호화
S315
암호화된 서비스 키(S320)
키 조각 생성
S330
키 조각 암호화
S335
암호화된 서비스키 저장
S325
암호화된 키 조각(S340)
해시값 비교
S365
마스터 키 삭제
S370
키 조각 복호화
S345
해시 값 생성
S350
키 조각 저장
S355
해시 값(360)

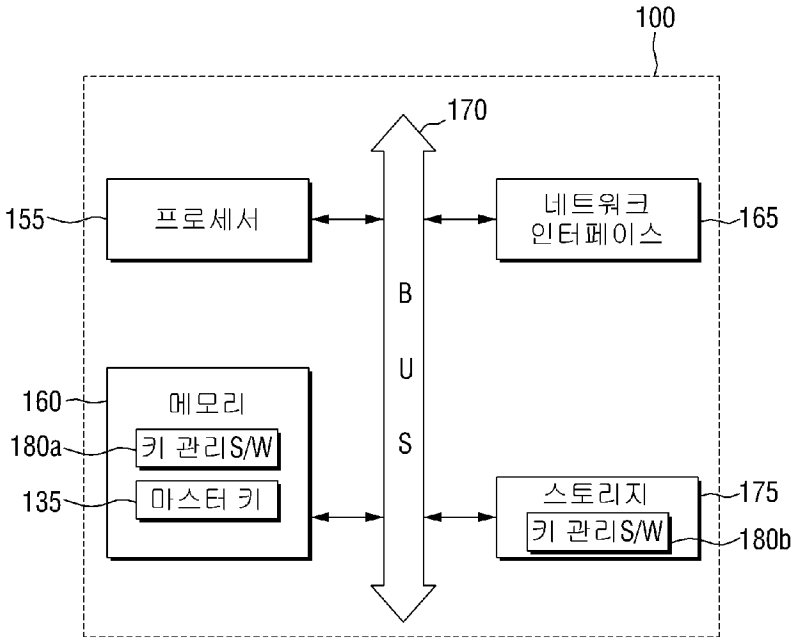
[도7]


서비스 장치 ~400
키 액세스 서버 ~100
키 관리 데이터 베이스 ~300
호스트 서버1 ~200
호스트 서버2 ~200
호스트 서버n ~200
서비스 키 제공요청(S405)
키조각 요청 메시지 암호화 ~S410
키조각요청 메세지 (S415)
요청 검증 ~S420
키조각 추출 및 암호화 ~S425
암호화된 키 조각 (S430)
키 조각 복호화 ~S435
해시값 요청(S440)
해시값 추출 ~S445
해시값(S450)
해시값 비교 ~S455
마스터키 재생성 ~S460
서비스키 요청(S465)
암호화된 서비스키 추출 S470
암호화된 서비스 키(S475)
서비스키 복호화 ~S480
서비스 키(S485)
요청 검증 ~S420
키조각 추출 및 암호화 S425

[도8]


105
100
통 신 부
125
120
130
마스터 키
분산 저장부
마스터 키
암복호화부
마스터 키
재생성부
110
115
마스터 키
생성부
저 장 부
135
마스터 키

[도9]


100
170
155
프로세서
네트워크
인터페이스
165
B
U
S
160
메모리
180a
키 관리S/W
135
마스터 키
스토리지
175
키 관리S/W
180b

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2015/006238

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/08; H04L 9/14; H04K 1/00; H04L 9/32; H04L 9/00; H04L 12/22

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: master key, key fragment, distributed storage, master key regeneration

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015-0019870 A1 (CISCO TECHNOLOGY, INC.) 15 January 2015 See paragraphs [0023]-[0044] and figures 1, 6A-6C.	1-4,6,9-16
Y		5,7,8
Y	US 2012-0243687 A1 (LI, Jun et al.) 27 September 2012 See paragraphs [0023], [0053] and figures 1, 8, 9.	5,7,8
A	US 2012-0179911 A1 (ZHENG, Yuliang et al.) 12 July 2012 See paragraphs [0041]-[0058] and figures 3-6.	1-16
A	US 2002-0067832 A1 (JABLON, David P.) 06 June 2002 See paragraphs [0109]-[0114] and figure 2.	1-16
A	US 2012-0121088 A1 (HATA, Yoichi et al.) 17 May 2012 See paragraphs [0074]-[0095] and figures 7-9.	1-16

☐ 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
20 APRIL 2016 (20.04.2016)	**22 APRIL 2016 (22.04.2016)**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2015/006238

Patent document cited in search report	Publication date	Patent family member	Publication date
US 2015-0019870 A1	15/01/2015	US 8855318 B1	07/10/2014
US 2012-0243687 A1	27/09/2012	US 8538029 B2	17/09/2013
US 2012-0179911 A1	12/07/2012	US 2005-0138374 A1	23/06/2005
		US 8139770 B2	20/03/2012
		US 8630421 B2	14/01/2014
US 2002-0067832 A1	06/06/2002	AU 6816101 A	17/12/2001
		CN 1249972 C	05/04/2006
		CN 1446331 A	01/10/2003
		JP 04833489 B2	07/12/2011
		JP 2003-536320 A	02/12/2003
		KR 10-0769482 B1	24/10/2007
		KR 10-2003-0010667 A	05/02/2003
		TW I233739 B	01/06/2005
		US 7139917 B2	21/11/2006
		WO 01-95545 A2	13/12/2001
		WO 01-95545 A3	04/07/2002
US 2012-0121088 A1	17/05/2012	CN 102415049 A	11/04/2012
		CN 102415049 B	06/08/2014
		JP 05269984 B2	21/08/2013
		JP 2009-135871 A	18/06/2009
		US 2010-0020966 A1	28/01/2010
		US 8634553 B2	21/01/2014
		WO 2009-060826 A2	14/05/2009
		WO 2010-125654 A1	04/11/2010

국 제 조 사 보 고 서

국제출원번호
PCT/KR2015/006238

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 9/08(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
H04L 9/08; H04L 9/14; H04K 1/00; H04L 9/32; H04L 9/00; H04L 12/22

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: 마스터 키, 키 조각, 분산 저장, 마스터 키 재생성

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	US 2015-0019870 A1 (CISCO TECHNOLOGY, INC.) 2015.01.15 단락 [0023]-[0044] 및 도면 1, 6A-6C 참조.	1-4,6,9-16
Y		5,7,8
Y	US 2012-0243687 A1 (JUN LI 등) 2012.09.27 단락 [0023], [0053] 및 도면 1, 8, 9 참조.	5,7,8
A	US 2012-0179911 A1 (YULIANG ZHENG 등) 2012.07.12 단락 [0041]-[0058] 및 도면 3-6 참조.	1-16
A	US 2002-0067832 A1 (DAVID P. JABLON) 2002.06.06 단락 [0109]-[0114] 및 도면 2 참조.	1-16
A	US 2012-0121088 A1 (YOICHI HATA 등) 2012.05.17 단락 [0074]-[0095] 및 도면 7-9 참조.	1-16

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

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

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

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

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

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

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

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

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

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2016년 04월 20일 (20.04.2016)	2016년 04월 22일 (22.04.2016)

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

심사관
김기호
전화번호 +82-42-481-8691

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2015/006238

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2015-0019870 A1	2015/01/15	US 8855318 B1	2014/10/07
US 2012-0243687 A1	2012/09/27	US 8538029 B2	2013/09/17
US 2012-0179911 A1	2012/07/12	US 2005-0138374 A1	2005/06/23
		US 8139770 B2	2012/03/20
		US 8630421 B2	2014/01/14
US 2002-0067832 A1	2002/06/06	AU 6816101 A	2001/12/17
		CN 1249972 C	2006/04/05
		CN 1446331 A	2003/10/01
		JP 04833489 B2	2011/12/07
		JP 2003-536320 A	2003/12/02
		KR 10-0769482 B1	2007/10/24
		KR 10-2003-0010667 A	2003/02/05
		TW I233739 B	2005/06/01
		US 7139917 B2	2006/11/21
		WO 01-95545 A2	2001/12/13
		WO 01-95545 A3	2002/07/04
US 2012-0121088 A1	2012/05/17	CN 102415049 A	2012/04/11
		CN 102415049 B	2014/08/06
		JP 05269984 B2	2013/08/21
		JP 2009-135871 A	2009/06/18
		US 2010-0020966 A1	2010/01/28
		US 8634553 B2	2014/01/21
		WO 2009-060826 A2	2009/05/14
		WO 2010-125654 A1	2010/11/04