



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2020년06월01일

(11) 등록번호 10-2117727

(24) 등록일자 2020년05월26일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01)
(52) CPC특허분류
G06F 21/6227 (2013.01)
(21) 출원번호 10-2015-7002722
(22) 출원일자(국제) 2013년07월30일
심사청구일자 2018년07월06일
(85) 번역문제출일자 2015년01월30일
(65) 공개번호 10-2015-0036323
(43) 공개일자 2015년04월07일
(86) 국제출원번호 PCT/US2013/052601
(87) 국제공개번호 WO 2014/022323
국제공개일자 2014년02월06일
(30) 우선권주장
13/561,113 2012년07월30일 미국(US)
(56) 선행기술조사문헌
US20070143546 A1*
US20100138830 A1*
US6587854 B1
JP2007531941 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
마이크로소프트 테크놀로지 라이선싱, 엘엘씨
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원
마이크로소프트 웨이
(72) 발명자
조리 비제타
미국 워싱턴주 98052-6399 레드몬드 원 마이크로
소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마
이크로소프트 코포레이션
날라 아마르
미국 워싱턴주 98052-6399 레드몬드 원 마이크로
소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마
이크로소프트 코포레이션
나투 마단 지
미국 워싱턴주 98052-6399 레드몬드 원 마이크로
소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마
이크로소프트 코포레이션
(74) 대리인
제일특허법인(유)

전체 청구항 수 : 총 20 항

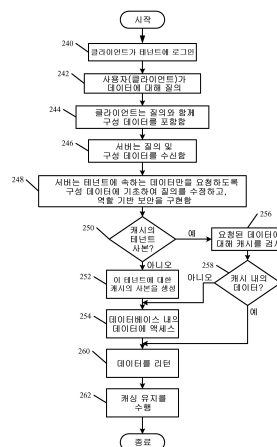
심사관 : 구대성

(54) 발명의 명칭 비즈니스 데이터 시스템에서 테넌트들에 대한 보안 및 데이터 격리 기법

(57) 요약

멀티 테넌트 호스팅 시스템은 테넌트로부터 비즈니스 데이터 및 테넌트 식별 데이터를 수신한다. 다수의 상이한 테넌트로부터의 데이터는 단일 데이터베이스에 저장되지만, 각 테넌트에 대응하는 데이터는 데이터베이스 내에서 파티션 식별자로 그 데이터를 마킹함으로써 파티셔닝된다. 따라서, 호스팅 시스템은 개개의 테넌트들이 그들 자신의 데이터에 대해서만 액세스하게 한다.

대표도 - 도5



명세서

청구범위

청구항 1

멀티 테넌트 데이터 저장소(multi-tenant data store)에서 데이터 조작 요청을 서비스하는 컴퓨터 구현 방법으로서,

각 테넌트는 다수의 사용자를 갖는 조직이고, 상기 방법은,

주어진 테넌트 외에 적어도 하나의 다른 테넌트를 갖는 비즈니스 데이터 애플리케이션에서 상기 주어진 테넌트를 생성하기 위해 사용자 입력을 수신하는 사용자 입력 메카니즘을 갖는 테넌트 생성 관리자 디스플레이를 디스플레이하는 단계와,

상기 주어진 테넌트에서 소정의 클라이언트를 상기 주어진 테넌트와 연관된 사용자에게 대한 보안 규칙을 식별하는 보안 관리자로서 식별하는 사용자 입력을 수신하는 사용자 입력 메카니즘을 갖는 보안 관리자 지정 디스플레이를 디스플레이하는 단계와,

상기 비즈니스 데이터 애플리케이션에서, 요청 클라이언트를 상기 주어진 테넌트로부터의 것으로 식별하는 테넌트 식별 데이터를 포함하는 상기 요청 클라이언트로부터의 데이터 조작 요청을 수신하는 단계와,

상기 주어진 테넌트와 연관된 제 1 데이터 및 상기 적어도 하나의 다른 테넌트와 연관된 제 2 데이터를 저장하는 상기 멀티 테넌트 데이터 저장소로부터, 컴퓨터 프로세서를 사용하여 상기 데이터 조작 요청을 서비스하는 단계- 상기 주어진 테넌트에 대한 상기 제 1 데이터는, 상기 적어도 하나의 다른 테넌트에 의한 상기 제 1 데이터에 대한 액세스를 제한하기 위해 연관성에 기초하여 상기 멀티 테넌트 데이터 저장소에서 상기 다른 테넌트들에 대한 제 2 데이터로부터 파티셔닝되고, 상기 데이터 조작 요청은 상기 테넌트 식별 데이터에 기초하여, 상기 데이터 조작 요청을 상기 주어진 테넌트와 연관되어 저장된 데이터로 한정함으로써 서비스됨 -

를 포함하는 컴퓨터 구현 방법.

청구항 2

제1항에 있어서,

상기 데이터 조작 요청을 수신하는 단계는 상기 멀티 테넌트 데이터 저장소 상에 데이터를 저장하기 위한 요청을 수신하는 단계를 포함하는

컴퓨터 구현 방법.

청구항 3

제2항에 있어서,

상기 데이터 조작 요청을 서비스하는 단계는,

상기 요청의 상기 데이터를 상기 멀티 테넌트 데이터 저장소에 저장하는 단계와,

상기 데이터가 상기 주어진 테넌트에 속한다는 것을 나타내는 파티션 식별자로 상기 멀티 테넌트 데이터 저장소에 저장된 상기 데이터를 마킹하는 단계

를 포함하는 컴퓨터 구현 방법.

청구항 4

제3항에 있어서,

상기 데이터를 마킹하는 단계는 상기 파티션 식별자로 상기 멀티 테넌트 데이터 저장소의 상기 데이터를 포함하는 하나 이상의 테이블 각각을 마킹하는 단계를 포함하는

컴퓨터 구현 방법.

청구항 5

제4항에 있어서,

상기 테이블 각각은 적어도 하나의 행(row)을 가지고,

상기 하나 이상의 테이블 각각을 마킹하는 단계는 상기 파티션 식별자로 상기 테이블 각각의 각 행을 마킹하는 단계를 포함하는

컴퓨터 구현 방법.

청구항 6

제1항에 있어서,

상기 데이터 조작 요청은 상기 멀티 테넌트 데이터 저장소에서 액세스될 데이터를 식별하고, 상기 식별된 데이터는 상기 다른 테넌트들 중 하나 이상으로부터의 데이터를 포함하도록 정의되는

컴퓨터 구현 방법.

청구항 7

제6항에 있어서,

상기 데이터 조작 요청을 서비스하는 단계는

상기 주어진 테넌트에 속하는 데이터만을 정의하는 수정된 데이터 조작 요청을 얻기 위해 상기 데이터 조작 요청을 수정하는 단계와,

상기 수정된 데이터 조작 요청을 서비스하는 단계

를 포함하는 컴퓨터 구현 방법.

청구항 8

제7항에 있어서,

상기 데이터 조작 요청을 수신하는 단계는 상기 다른 테넌트들 중 하나 이상으로부터의 데이터를 포함하는 데이터에 대한 질의를 수신하는 단계를 포함하는

컴퓨터 구현 방법.

청구항 9

제8항에 있어서,

상기 데이터 조작 요청을 수정하는 단계는 파티션 식별자에 의해 상기 주어진 테넌트에 속하는 것으로 식별된 데이터만을 리턴하도록 상기 질의를 수정하는 단계를 포함하는

컴퓨터 구현 방법.

청구항 10

제1항에 있어서,
상기 주어진 테넌트에 대해 구현될 보안 규칙을 상기 보안 관리자로부터 수신하는 단계와,
상기 보안 규칙을 저장하는 단계
를 더 포함하는 컴퓨터 구현 방법.

청구항 11

제10항에 있어서,
상기 보안 규칙을 수신하는 단계는
사용자 입력 메카니즘을 갖는 보안 규칙 디스플레이를 디스플레이하는 단계와,
상기 보안 규칙 디스플레이 상에서 상기 사용자 입력 메카니즘을 통해 상기 보안 규칙을 수신하는 단계
를 포함하는 컴퓨터 구현 방법.

청구항 12

제10항에 있어서,
상기 데이터 조작 요청을 서비스하는 단계는
상기 데이터 조작 요청의 상기 테넌트 식별 데이터에 기초하여, 상기 주어진 테넌트에 대한 상기 보안 규칙에 액세스하는 단계와,
상기 데이터 조작 요청을 서비스하는 동안 상기 주어진 테넌트에 대한 상기 보안 규칙을 구현하는 단계
를 포함하는 컴퓨터 구현 방법.

청구항 13

제12항에 있어서,
상기 보안 규칙을 수신하는 단계는 역할 기반 보안 규칙을 수신하는 단계를 포함하는
컴퓨터 구현 방법.

청구항 14

제1항에 있어서,
상기 데이터 조작 요청을 서비스하는 단계는 캐시 메모리에서 각 테넌트에 대한 캐싱된 데이터의 별도의 사본을 유지하는 단계를 포함하는
컴퓨터 구현 방법.

청구항 15

제14항에 있어서,

상기 데이터 조작 요청은 질의 요청 데이터를 포함하고,

상기 캐싱된 데이터의 별도의 사본을 유지하는 단계는 상기 주어진 테넌트에 대한 캐싱된 데이터만을 저장하는 캐시 메모리에 요청된 데이터를 저장하는 단계를 포함하는

컴퓨터 구현 방법.

청구항 16

비즈니스 데이터 시스템으로서,

제1 테넌트 및 제2 테넌트에 대해 동일한 비즈니스 데이터 애플리케이션을 호스팅하는 서버 계층- 각 테넌트는 복수의 상이한 클라이언트를 갖는 조직이고,

상기 서버 계층은

상기 제1 테넌트로부터 제1 데이터를 수신하고 상기 제2 테넌트로부터 제2 데이터를 수신하며,

멀티 테넌트 데이터 저장소에 상기 제1 데이터 및 상기 제2 데이터를 저장하고,

상기 제1 데이터가 상기 제2 테넌트에 액세스가능하지 않고 상기 제2 데이터가 상기 제1 테넌트에 액세스가능하지 않도록 상기 제1 데이터를 상기 제2 데이터로부터 파티셔닝하도록 구성됨 -과,

상기 시스템의 기능 부분을 형성하고 상기 서버 계층에 의해 활성화되며 상기 서버 계층의 기능을 수행하게 하는 컴퓨터 프로세서

를 포함하는 비즈니스 데이터 시스템.

청구항 17

제16항에 있어서,

상기 서버 계층은 클라우드 아키텍처의 클라우드에 배치되는

비즈니스 데이터 시스템.

청구항 18

제16항에 있어서,

상기 서버 계층은 상기 제1 테넌트 및 상기 제2 테넌트로부터 구성 데이터를 수신하고 상기 구성 데이터에 기초하여 상기 제1 데이터를, 상기 제1 데이터를 상기 제1 테넌트에게만 액세스가능한 것으로 식별하는 파티션 식별자로 마킹하여 저장하는

비즈니스 데이터 시스템.

청구항 19

제18항에 있어서,

캐시 메모리를 더 포함하되,

상기 서버 계층은 상기 캐시 메모리가 상기 제1 테넌트에 대응하는 캐싱된 데이터의 제1 사본 및 상기 제2 테넌트에 대응하는 캐싱된 데이터의 제2 사본을 갖도록 상기 캐시 메모리를 유지하고, 상기 캐싱된 데이터의 제1 사본은 상기 제2 테넌트에 액세스가능하지 않고 상기 캐싱된 데이터의 제2 사본은 상기 제1 테넌트에 액세스가능

하지 않도록 상기 캐싱된 데이터의 상기 제1 사본 및 상기 제2 사본이 상기 캐시 메모리에서 서로 파티셔닝되는 비즈니스 데이터 시스템.

청구항 20

컴퓨터 판독가능 명령어가 저장된 컴퓨터 판독가능 저장 매체로서,

상기 컴퓨터 판독가능 명령어는 컴퓨터에 의해 실행되는 경우에 상기 컴퓨터로 하여금 방법을 수행하게 하고, 상기 방법은,

주어진 테넌트 외에 적어도 하나의 다른 테넌트를 갖는 비즈니스 데이터 애플리케이션에서 상기 주어진 테넌트를 생성하기 위해 사용자 입력을 수신하는 사용자 입력 메카니즘을 갖는 테넌트 생성 관리자 디스플레이를 디스플레이하는 단계와,

상기 주어진 테넌트에서 소정의 클라이언트를 보안 관리자로서 식별하는 사용자 입력을 수신하는 사용자 입력 메카니즘을 갖는 보안 관리자 지정 디스플레이를 디스플레이하는 단계와,

상기 비즈니스 데이터 애플리케이션에서, 요청 클라이언트를 상기 주어진 테넌트로부터의 것으로 식별하고 조작될 데이터를 식별하는 테넌트 식별 데이터를 포함하는 상기 요청 클라이언트로부터의 데이터 조작 요청을 수신하는 단계와,

상기 주어진 테넌트 및 상기 적어도 하나의 다른 테넌트에 대한 데이터를 저장하는 멀티 테넌트 데이터 저장소로부터, 상기 비즈니스 데이터 애플리케이션을 사용하여 상기 데이터 조작 요청을 서비스하는 단계- 상기 주어진 테넌트에 대한 데이터는, 상기 멀티 테넌트 데이터 저장소에서 상기 다른 테넌트에 대한 데이터로부터 파티셔닝되고, 상기 데이터 조작 요청은 상기 테넌트 식별 데이터에 기초하여 상기 데이터 조작 요청을 상기 주어진 테넌트에 대한 데이터로 한정함으로써 서비스됨 - 를 포함하고,

상기 데이터 조작 요청을 서비스하는 단계는

상기 데이터 조작 요청의 상기 테넌트 식별 데이터에 기초하여, 상기 주어진 테넌트에 대한 보안 규칙에 액세스하는 단계와,

상기 데이터 조작 요청을 서비스하는 동안 상기 주어진 테넌트에 대한 상기 보안 규칙을 구현하는 단계와,

각 테넌트에 대해, 상기 데이터 조작 요청에서 식별된 데이터에 기초하여, 캐시 메모리에 캐싱된 데이터의 별도의 사본을 유지하는 단계를 더 포함하는

컴퓨터 판독가능 저장 매체.

발명의 설명

기술 분야

배경 기술

[0001] 비즈니스 조직들은 흔히 다수의 다양한 유형의 비즈니스 컴퓨터 프로그램 또는 애플리케이션을 사용한다. 몇몇 이러한 프로그램들은 기업 자원 계획(ERP) 시스템, 고객 자원 관리(CRM) 시스템, LOB(line of business) 애플리케이션, 및 다수의 다른 비즈니스 관련 프로그램을 포함한다.

[0002] 많은 조직들은 또한 비즈니스 프로그램에 역할 기반 보안을 구현한다. 즉, 사용자는 회사에서 특정 역할을 수행할 수 있으며, 그 역할을 갖는 사용자는 특정 데이터에 대한 액세스를 가질 수 있지만, 다른 데이터에 대한 액세스는 가지지 않을 수 있다. 예를 들어, 인적 자원 역할을 맡은 사용자는 다양한 직원의 급여 및 개인 파일에 액세스할 수 있지만, 판매 데이터 또는 다른 유형의 일반적인 비즈니스 정보에는 액세스할 수 없다. 대조적

으로, 판매 관리자의 역할을 맡은 사용자는 다양한 제품 라인에 걸쳐 회사의 여러 레벨의 영업 데이터에 대한 액세스를 가질 수 있지만, 다른 직원의 개인 파일 및 급여 정보에 액세스하지 못할 수 있다.

[0003] 또한, 많은 기업들은 그들의 비즈니스 관련 데이터의 대부분을 기밀 또는 독점적인 것으로 간주한다. 예를 들어, 많은 기업들은 판매 기록, 판매 리드(sales leads), 개인 파일 정보, 및 수많은 기타 비즈니스 정보를 회사 자체에 대한 기밀 및 독점적인 것으로 간주한다. 회사는 경쟁자 또는 심지어 관련 회사와 같은 다른 회사가 그 데이터에 액세스하는 것을 원하지 않는다.

[0004] 이러한 맥락에서, 회사들이 특정 방식으로 서로와 관련될 수 있지만, 이들 회사는 여전히 서로 정보를 공유하기를 원하지 않는 상황이 발생할 수 있다. 예를 들어, 회사는 독립적인 회사 (또는 자회사)를 인수함으로써 성장하는 지주 회사인 상황이 있을 수 있다. 자회사들은 자신들에 대한 상당한 관리 및 운영 통제를 유지하고, 각 자회사에 대한 데이터와 프로세스는 다른 자회사와 공유되지 않는다.

[0005] 몇몇 현재의 솔루션은 각 자회사가 자신의 비즈니스 데이터를 저장하기 위한 그 자회사 소유의 데이터베이스를 가질 것을 요구한다. 다른 현재의 솔루션에서, 각각의 별도의 자회사에는 그 자회사 소유의 별도의 데이터베이스 제품이 제공된다. 각 자회사에 대해 주어진 비즈니스 데이터 프로그램이 완전히 별개로 설치된다. 예를 들어, 각 자회사는 ERP 시스템에 대해 그 자회사 소유의 별개의 설치를 가질 수 있다.

[0006] 그러나, 자회사들이 그들의 정보 기술(IT) 자원을 모으고 단일 비즈니스 소프트웨어 애플리케이션을 활용하고자 하는 경우가 발생할 수 있다. 즉, 자회사들 (또는 자회사들의 부분집합)이 하나의 비즈니스 애플리케이션 설치 비용을 공유하기를 희망할 수 있지만, 그들은 여전히 동일한 비즈니스 애플리케이션을 공유하는 다른 자회사들과는 완전히 별개로 또한 분리되어 그들의 비즈니스 데이터를 유지하고자 할 수 있다. 마찬가지로, 각 자회사는 자신의 역할 기반 보안 규칙 또는 기타 보안 규칙을 구현하기를 희망할 수 있다.

[0007] 위의 설명은 단지 일반적인 배경 정보를 위해 제공되는 것이며, 본 발명의 범위를 결정하는 보조로서 사용되는 것은 아니다.

발명의 내용

[0008] 멀티 테넌트(multi-tenant) 호스팅 시스템은 테넌트로부터, 비즈니스 데이터 및 테넌트 식별 데이터를 수신한다. 여러 다른 테넌트로부터의 데이터는 단일 데이터베이스에 저장되어 있지만, 각각의 테넌트에 대응하는 데이터는 데이터베이스 내에서, 파티션 식별자로 데이터를 표시함으로써 파티셔닝된다. 따라서, 호스팅 시스템은 개별 테넌트가 그들 자신의 데이터에 액세스하는 것을 허용하기만 하면 된다.

[0009] 본 요약부는 이하의 상세한 설명에서 더 설명되는 개념들 중 선택된 것들을 간단하게 소개하고자 하는 것이다. 본 요약부는 청구대상의 핵심적인 특징이나 필수적인 특징들을 밝히고자 함이 아니며, 청구대상의 범위를 결정하는 데 도움이 되고자 함도 아니다. 청구대상은 배경기술에서 언급한 임의의 또는 모든 단점을 해결하는 구현 예에 한정되지 않는다.

도면의 간단한 설명

[0010] 도 1은 비즈니스 데이터 시스템의 일 실시예의 블록도이다.

도 2는 테넌트를 설정함에 있어서의 도 1에 도시된 시스템의 전체 동작의 일 실시 예를 나타내는 흐름도이다.

도 2a 내지 도 2e는 예시적인 사용자 인터페이스를 나타낸다.

도 3은 파티셔닝된 데이터에 대한 데이터 구조의 일 실시예를 도시한다.

도 3a 내지 도 3c는 파티셔닝된 데이터를 테이블에 나타내는 예시적인 사용자 인터페이스 디스플레이를 도시한다.

도 4는 비즈니스 데이터에 대한 멀티 테넌트 액세스를 호스팅함에 있어서의 도 1에 도시되어 있는 시스템의 전체 동작의 일 실시예를 나타내는 흐름도이다.

도 5는 데이터 액세스 및 캐싱 동작을 제공함에 있어서의 도 1에 도시되어 있는 시스템의 동작의 일 실시예를

나타내는 흐름도이다.

도 5a는 테넌트들의 부분집합이 데이터를 공유하도록 데이터 저장소가 파티셔닝되는 아키텍처를 나타낸다.

도 6은 다양한 아키텍처에서 도 1의 시스템의 일 실시예를 나타내는 블록도이다.

도 7 내지 도 10은 모바일 장치의 다양한 실시예를 도시한다.

도 11은 하나의 예시적인 컴퓨팅 환경의 블록도를 나타낸다.

발명을 실시하기 위한 구체적인 내용

- [0011] 도 1은 비즈니스 데이터 시스템(100)의 일 실시예의 블록도를 나타낸다. 비즈니스 데이터 시스템(100)은 테넌트들(102, 104)을 도시하고, 각 테넌트는 제각각 복수의 클라이언트(또는 사용자)(106, 108 및 110, 112)를 갖는다. 테넌트(102, 104)는 그 자체가 복수의 서버(116, 118, 120)를 갖는 서버 계층(114)에 대한 액세스를 갖는다. 도 1에 도시되어 있는 바와 같이, 테넌트(102, 104)는 화살표(124, 126)로 각각 표시되어 있는 바와 같이, 네트워크(122)를 통해 또는 직접적으로 서버 계층(114)에 대한 액세스를 갖는다. 서버 계층(114)은 데이터 저장소(128)에 저장된 데이터를 액세스하기 위한 (테넌트(102, 104)로부터의) 요청을 서비스한다. 서버 계층(114)은 또한 캐시(120)를 사용하여 캐싱을 구현한다.
- [0012] 일 실시예에서, 시스템(100)은 또한 비즈니스 시스템(100)에서 새로운 테넌트를 설정하기 위해 관리자에 의해 사용될 수 있는 관리자 컴포넌트(132)를 포함한다. 각각의 새로운 테넌트는 동일한 시스템(예를 들어, 동일한 ERP 또는 CRM 설치 또는 다른 비즈니스 애플리케이션 설치)을 사용한다. 또한, 일 실시예에서, 서버 계층(114)은 테넌트(102, 104) 각각에 대한 보안 규칙에 대한 액세스를 갖는다. 보안 규칙은 블록(134)으로 표시된다. 따라서, 서버 계층(114)은 각 테넌트(102, 104)에 대한 보안을 구현할 수 있다. 일 실시예에서, 보안 규칙은 클라이언트가 테넌트(102 또는 104)에 로그인할 때의 인증 절차를 정의하고, 또한 테넌트마다 역할 기반 보안을 정의한다. 물론, 다른 유형의 보안 규칙 또는 보안 절차가 또한 구현될 수 있다.
- [0013] 도 1은 적어도 각 테넌트(102, 104)가 프로세서(136, 138)를 구비하고 있는 것을 나타낸다. 물론, 각 클라이언트는 자신의 프로세서도 구비할 수 있고, 간략함을 위해 각 테넌트에 대해 하나의 프로세서가 도시되어 있다. 도 1은 또한 각 서버(116, 118, 120)가 자신의 프로세서(140, 142, 144)를 구비할 수 있음을 보여준다. 서버 계층(114)은 각 서버에 의해 액세스되는 단일 프로세서를 구비할 수 있지만, 예시를 위해 각 서버의 개별 프로세서가 도시되어 있다. 일 실시예에서, 각 프로세서는 메모리 및 타이밍 회로(미도시)와 연관된 컴퓨터 프로세서를 포함한다. 프로세서는 시스템(100)의 기능 부분을 형성하고 시스템(100) 내의 다른 컴포넌트에 의해 활성화되고 그 컴포넌트의 기능을 용이하게 한다.
- [0014] 데이터 저장소(128)는 단일 데이터 저장소로 도시되어 있지만, 다수의 별개의 데이터 저장소로도 구현될 수 있고, 또한 서버 계층(114)에 대해 로컬로 또는 원격으로 위치할 수 있다. 데이터 저장소(128)는 예를 들어 시스템(100) 내의 모든 테넌트에 의해 사용되는 단일 데이터베이스 설치를 위한 저장소이다. 마찬가지로, 캐시(130)는 단일의 메모리 내(in-memory) 캐시로서 도시되어 있지만, 예를 들어 다수의 다른 메모리 내에서 다른 방식으로 구현될 수 있다.
- [0015] 또한, 도 1은 일 실시예에서, 각 클라이언트(106, 112)가 제각기의 구성 데이터(146, 148, 150, 152)를 가지고 있음을 나타낸다. 구성 데이터는 예시적으로 각 클라이언트의 역할 및 각 클라이언트가 속하는 특정 테넌트를 식별한다. 테넌트는 그의 다수의 클라이언트를 위한 공통의 구성 데이터 세트를 구비할 수 있지만, 각 클라이언트에 대한 별도의 구성 데이터(또는 구성 파일)는 단지 예로서 도시되어 있다.
- [0016] 시스템(100)의 동작에 대한 자세한 설명이 나머지 도면과 관련하여 이하에서 제공되지만, 나머지 설명의 이해를 돕기 위해 개요가 이제 제공된다. 시스템(100)은 예시적으로 테넌트(102, 104)가 단일 ERP 애플리케이션(또는 다른 비즈니스 관련 애플리케이션)을 사용함으로써 그리고 그들의 데이터 모두를 공통 데이터베이스(128)에 저장함으로써 정보 기술 리소스를 모으지만, 다른 테넌트들이 보거나 액세스할 수 없도록 그들 자신의 개별 데이터의 파티셔닝을 유지하기를 희망하는 시나리오를 나타낸다. 예를 들어, 일 예에서, 테넌트(102, 104)는 모두 공동으로 소유되는 비즈니스(예를 들어, 모회사의 자회사)이다. 이 경우, 각 테넌트(102, 104)는 예시적으로 자신 소유의 관리 및 동작 제어를 유지하고, 자신의 데이터가 다른 테넌트로부터 안전하게 파티셔닝되기를 희망한다. 이 경우, 클라이언트(106-108)는 테넌트(102)에 의해 사용되는 비즈니스 관련 애플리케이션(예를 들어, ERP 애플리케이션)의 사용자에게 대응하고, 클라이언트(110, 112)는 테넌트(104)에 의해 사용되는 동일한 애플리케이션의 사용자에게 대응한다. 테넌트(102, 104)는 모두 비즈니스 관련 애플리케이션의 동일한 설치를 사용한다.

- [0017] 새로운 조직이 모회사에 추가되는 경우(즉, 새로운 테넌트가 시스템(100)에 추가되는 경우), 관리자(133)는 예시적으로 관리자 컴포넌트(132)를 통해 서버 계층(114)에 액세스한다. 컴포넌트(132)는 예시적으로 관리자(133)에 제공되는 사용자 인터페이스 디스플레이(135)를 생성하는 사용자 인터페이스 컴포넌트를 구비한다. 사용자 인터페이스 디스플레이(135)는 예시적으로 관리자(133)가 서버 계층(114)에 의해 구현되고 시스템의 다양한 테넌트의 다양한 클라이언트에 의해 사용되는 비즈니스 관련 애플리케이션을 조작하기 위한 사용자 입력을 제공할 수 있게 해주는 사용자 입력 메카니즘을 포함한다. 이 사용자 입력 메카니즘은 포인트 및 클릭 장치(예를 들어, 마우스 또는 트랙볼)로부터, (가상 또는 하드웨어) 키보드, 디스플레이 스크린이 터치 감지 스크린인 터치 제스처, 음성 입력 등으로부터 사용자 입력을 수신할 수 있다. 도 2a는 관리자가 새로운 테넌트를 설정할 수 있게 해주는 사용자 인터페이스 디스플레이(179)의 일 실시예를 나타낸다. 관리자는 사용자 입력 메카니즘(181,183)을 사용하여 새로운 테넌트를 식별 및 설정(또는 생성)한다.
- [0018] 새로운 테넌트를 설정하기 위해, 관리자(133)는 예시적으로 새로운 테넌트의 클라이언트들 중 하나를 보안 관리자로서 식별한다. 예를 들어, 테넌트(102)가 추가되는 새로운 테넌트인 것으로 가정한다. 관리자(133)는 클라이언트(106)를 테넌트(102)에 대한 보안 관리자인 것으로 식별할 수 있다.
- [0019] 도 2b는 사용자 인터페이스 디스플레이(125)의 또 다른 실시예를 나타낸다. 디스플레이(125)는 새로운 테넌트를 생성하기 위해 관리자에게 제시될 수 있다. 디스플레이(125)는 파티션 키 컬럼(127) 및 이름 컬럼(129)을 포함하는 컬럼들의 집합을 포함한다. 사용자는 파티션 키 컬럼(127) 내의 하나의 셀을 선택할 수 있고 파티션 키를 입력할 수 있으며 대응하는 파티션 이름을 컬럼(129)의 인접 셀에 입력할 수 있다. 이런 식으로, 관리자는 다양한 클라이언트에 대한 데이터를 파티셔닝하기 위해 데이터 저장소(128) 및 캐시(130)에서 사용될 수 있는 테넌트(즉, 파티션)를 설정할 수 있다. 도 2b에서 알 수 있는 바와 같이, 파티션 키 컬럼(127)은 3개의 파티션 키, 즉 "초기", "P1" 및 "P2"를 포함한다. 대응하는 이름은 각각 "초기 파티션", "P1" 및 "P2"이다.
- [0020] 도 2c는 관리자(133)가 새로운 테넌트의 클라이언트를 보안 관리자로서 지정할 수 있게 하는 사용자 인터페이스 디스플레이(185)의 일 실시예이다. 관리자는 이를 위해 사용자 입력 메카니즘(187)을 사용할 수 있다.
- [0021] 이것은 클라이언트(106)가 로그인할 수 있고 데이터 저장소(128) 내의 정보를 액세스하기 위해 테넌트(102)를 사용할 다른 사용자(예를 들어, 클라이언트(108))를 설정할 수 있도록 보안 컴포넌트를 클라이언트(106)에 배포한다. 보안 관리자(이제는 클라이언트(106))는 또한 보안 규칙 및 테넌트(102)의 각 사용자의 역할을 식별할 수 있다. 도 2d는 보안 관리자(예를 들어, 이제는 클라이언트(106))가 이를 행할 수 있게 해주는 사용자 인터페이스 디스플레이(189)의 일 실시예를 나타낸다. 테넌트에 대한 사용자 또는 클라이언트는 사용자 입력 메카니즘(191)을 사용하여 설정될 수 있고, 보안 규칙은 입력 메카니즘(193)을 사용하여 설정될 수 있다. 보안 규칙 역할 및 사용자는 도 1에 참조번호(134)로 표시된 각 테넌트에 대한 보안 규칙으로서 저장된다. 클라이언트(108)에 대응하는 역할 정보, 및 클라이언트(108)가 테넌트(102)에 속한다는 사실은 그 클라이언트(108)에 대응하는 구성 파일(또는 구성 데이터)(148)에 저장된다. 구성 파일은 보안 관리자가 도 2d의 메카니즘(195)과 같은 사용자 입력 메카니즘을 구동시킨 경우 클라이언트에 자동으로 배포 또는 전송될 수 있다.
- [0022] 도 2e는 관리자가 주어진 테넌트에 대해 사용자를 설정하기 위해 사용할 수 있는 사용자 인터페이스 디스플레이(131)의 또 다른 실시예를 나타낸다. 관리자는 관리자가 텍스트 박스(text boxes)의 집합 내에 사용자에게 다양한 정보를 입력할 수 있고, 박스들을 체크할 수 있게 해주는 사용자 탭(133)을 선택하였음을 알 수 있다. 예를 들어, 관리자는 텍스트 박스(135)에 사용자 ID를, 박스(137)에 사용자 이름을, 박스(139)에 네트워크 도메인을, 박스(141)에 별명을 입력할 수 있다. 사용자는 또한 예시적으로 드롭다운 메뉴(143)를 이용하여 계정 유형을 정의할 수 있고 또 다른 드롭다운 메뉴(145)를 사용하여 기본 회사를 선택할 수 있다. 이후, 관리자는 체크 박스(147)를 체크함으로써 이 사용자를 인에이블링할 수 있고, 사용자는 박스(149)를 체크함으로써 기본 파티션에 이 사용자를 할당할 수 있다.
- [0023] 관리자는 예시적으로 박스(151)에 정보를 입력함으로써 이 사용자에게 대한 프로파일을 설정할 수 있다. 관리자는 또한 버튼(153)을 작동시킴으로써 하나 이상의 역할을 이 사용자에게 할당할 수 있다. 이것은 예시적으로 관리자에 의해 선택되거나 이 사용자에게 할당될 수 있는 역할들(155)의 집합을 불러온다. 유사하게, 드롭다운 박스(157)를 작동시킴으로써, 관리자는 선택된 역할에 대한 특권을 검토할 수 있고, 드롭다운 박스(159)를 작동시킴으로써, 관리자는 선택된 역할에 할당된 다른 사용자를 검토할 수 있다. 물론, 도 2e에 도시되어 있는 사용자 인터페이스 디스플레이(131)는 예시적이며, 사용자를 식별하고 역할을 할당하는 다른 방식도 사용될 수 있다.
- [0024] 클라이언트(108)가 데이터 저장소(128) 상의 정보를 액세스하거나 데이터 저장소(128)에 정보를 저장하려 하는

경우, 클라이언트(108)는 먼저 테넌트(102)에 로그인한다. 구성 데이터(148)는 클라이언트(108)의 역할 및 클라이언트(108)가 어떤 테넌트에 속하는지를 서버 계층(114)에 알려준다. 따라서, 예를 들어, 클라이언트(108)가 데이터 저장소(128)에 저장될 정보를 제공하는 경우, 서버 계층(114)은 그 데이터를 테넌트 데이터(154)로서 데이터 저장소(128)에 저장한다. 서버 계층(114)은 또한 예시적으로 테넌트 데이터(154)를 테넌트(102)로부터의 것으로 식별한다. 따라서, 서버 계층(114)은 테넌트 데이터(154, 156, 158) 모두를 주어진 테넌트에 특정하는 것으로 식별한다. 이어서 클라이언트가 로그인하고 데이터 저장소(128) 상의 데이터에 대한 액세스를 요청하는 경우, 서버 계층(114)은 그 특정 클라이언트의 액세스를, 클라이언트가 로그인할 때 이용한 테넌트(102 또는 104)에 대응하는 데이터(154, 156, 158)로 한정한다. 예를 들어, 클라이언트(110)가 이어서 클라이언트(104)를 통해 로그인하는 경우, 서버 계층(114)은 클라이언트(110)가 주어진 역할을 가지고 있으며 테넌트(104)에 로그인하였음을 구성 데이터(150)를 통해 식별한다. 따라서, 서버 계층(114)은 테넌트(104)에서의 클라이언트(110)의 역할이 주어진 경우 클라이언트(100)의 액세스를 테넌트(104)에 대응하는 데이터에 국한시킨다.

[0025] 물론, 시스템(100)은 자신 소유의 별개의 테넌트 데이터(154-156)를 갖는 각 개별 테넌트(102-104)를 나타낸다. 그러나, 테넌트(102-104)의 부분집합은 그들의 데이터가 테넌트(102-104)의 또 다른 부분집합으로부터 파티셔닝되기를 원할 수 있다. 이 경우, 각 부분집합은 자신의 데이터가 그 부분집합 내의 임의의 테넌트에 의해 액세스될 수 있도록 서버 계층(114)에 의해 파티셔닝되도록 한다. 그러나, 그 부분집합 밖의 임의의 테넌트에 의해서는 액세스가능하지 않을 것이다. 데이터는 단지 예시를 위해 도 1에서는 (부분집합 단위 대신에) 테넌트 단위로(on a tenant-by-tenant basis) 파티셔닝된 것으로 도시되어 있다.

[0026] 서버 계층(114)이 데이터 저장소(128)로의 다수의 왕복 이동을 행하는 것은 바람직하지 않을 수 있기 때문에, 서버 계층(114)은 캐시(130)를 구현한다. 메모리 내 캐시(130) 내에서도 데이터 격리를 유지하기 위해, 서버 계층(114)은 시스템(100) 내의 각 테넌트에 대해 캐싱된 데이터의 별도의 사본을 설정한다. 따라서, 예를 들어, 캐싱된 테넌트 데이터(160)는 테넌트(102)에 대한 캐싱된 메모리의 사본이다. 캐싱된 테넌트 데이터(162)는 테넌트(104)에 대한 캐싱된 데이터의 사본이고, 캐싱된 테넌트 데이터(164)는 시스템(100) 내의 또 다른 테넌트에 대한 캐싱된 데이터의 사본이다. 서버 계층(114)은 시스템(100) 내의 각 개별 테넌트(102-104)에 대응하는 캐싱된 데이터(162-164)의 별개의 사본을 유지한다.

[0027] 소정의 공유 데이터(166)는 테넌트(102-104) 모두에 공통일 수 있다. 예를 들어, 공유 데이터(166)는 테넌트들 각각의 모회사에 대한 일반적인 정보를 포함할 수 있다. 이 경우, 서버 계층(114)은 공유 데이터(166)가 임의의 테넌트(또는 테넌트들의 임의의 부분집합)에 의해 액세스될 수 있도록 그 공유 데이터(166)를 저장한다. 공유 데이터(166)는 선택사항이므로 점선으로 도시되어 있으며, 또 다른 실시예에서, 테넌트들 간에는 데이터가 공유되지 않는다.

[0028] 이제 시스템(100)의 동작에 대한 보다 자세한 설명이 주어질 것이다. 도 2 내지 도 11을 참조할 것이다.

[0029] 도 2는 관리자(133)가 새로운 테넌트를 설정하는 경우 시스템(100)의 동작에 대한 실시예를 나타내는 흐름도이다. 도 2는 관리자가 먼저 시스템에 로그인하고 관리자 컴포넌트(132)가 사용자 인터페이스 디스플레이(예를 들어, 도 2a의 디스플레이(179) 또는 도 2b의 디스플레이(125))를 생성하는 것을 보여주는데, 이 사용자 인터페이스 디스플레이는 관리자(133)가 새로운 테넌트 또는 파티션을 생성할 수 있게 해주는 사용자 입력 메카니즘(181, 183, 127, 129)을 갖는다. 이는 도 2의 블록(170)으로 표시되어 있다. 관리자 컴포넌트(132)는 관리자(133)로부터 새로운 테넌트를 생성하는 입력을 수신한다.

[0030] 새로운 테넌트가 생성되면, 관리자 컴포넌트(132)는 새로운 테넌트(예를 들어, 테넌트(102))에 대한 보안 관리자로서 또 다른 사용자(예를 들어, 클라이언트(106))를 할당하는 입력을 관리자(133)로부터 수신하는 사용자 입력 메카니즘(187)을 갖는 사용자 인터페이스 디스플레이(예를 들어, 도 2c의 디스플레이(185))를 디스플레이한다. 테넌트(102)에 대해 클라이언트(106)를 보안 관리자로서 할당하는 것은 도 2의 블록(174)으로 표시되어 있다. 이것은 서버 계층(114)으로 하여금 클라이언트(106)가 비즈니스 데이터 시스템(예를 들어, ERP 애플리케이션)에 로그인할 수 있고 새로운 테넌트(102)에 대해 (예를 들어, 도 2d에 도시되어 있는 디스플레이(189) 또는 도 2e의 디스플레이(131)를 사용하여) 사용자를 설정할 수 있게 한다. 이것은 도 2에서 블록(176)으로 표시된다. 예를 들어, 이것은 보안 관리자(예를 들어, 클라이언트(106))가 테넌트(102)의 사용자들 각각에 대한 구성 파일(146-148)을 로딩할 수 있게 해준다. 구성 파일의 로딩은 도 2에서 블록(178)으로 표시되어 있다. 보안 관리자는 또한 테넌트(102) 내의 클라이언트들 각각에 역할을 할당할 수 있다. 이것은 블록(180)으로 표시되어 있다. 따라서, 보안 관리자는 다양한 역할 기반 보안 규칙, 인증 규칙, 또는 다른 유형의 보안 규칙을 비즈니스 데이터 시스템에 입력할 수 있고 이들 규칙들은 서버 계층(114)에 의해 134에서 액세스가능하다. 물론, 보

안 관리자는 다른 작업도 수행할 수 있고, 이것은 도 2의 블록(182)으로 표시되어 있다.

- [0031] 비즈니스 데이터 시스템 상에서 새로운 테넌트(102)가 설정되면, 테넌트(102)는 비즈니스 데이터를 데이터 저장소(128)에 저장하기를 희망한다. 그럴 경우, 데이터 전달을 개시하는 특정 클라이언트(106-108)에 대한 구성 데이터(146-148)가 또한 데이터 저장소(128)에 데이터를 저장하기 위한 요청과 함께 포함된다.
- [0032] 서버 계층(114)은 새로운 테넌트(102)의 데이터를 테넌트(102)에 속하는 테넌트 데이터(154)로서 식별함으로써 데이터 저장소(128)에서 구현되는 데이터베이스 내에서 그 새로운 테넌트(102)의 데이터를 파티셔닝한다. 이러한 식의 데이터 파티셔닝은 도 2에서 블록(184)으로 도시되어 있다. 서버 계층(114)은 이를 다양한 방식으로 수행할 수 있다. 예를 들어, 서버 계층(114)은 테넌트 데이터(154)를 특정 테넌트에 속하는 것으로 식별하는 파티션 식별자를 테넌트 데이터(154) 내의 각 테이블에 제공할 수 있다. 테이블 단위로 데이터를 파티셔닝하는 것은 도 2에서 블록(186)으로 표시되어 있다. 또한, 서버 계층(114)은 각 테이블의 각 개별 행 상의 데이터를 파티셔닝할 수 있다. 즉, 서버 계층은 테넌트(102)에 속하는 모든 테이블에서 테넌트(102)에 속하는 모든 데이터 행을, 해당 행 내의 데이터가 테넌트(102)에 속함을 나타내는 파티션 식별자로 스트라이핑(stripe)할 수 있다. 행 단위로의 파티셔닝은 블록(188)으로 표시되어 있다. 서버 계층(114)은 또한 다른 방식으로 파티셔닝할 수 있다. 예를 들어, 서버 계층(114)은 테넌트(102)에 의해서만 액세스가능한 스키마(schema)에 따라 테넌트 데이터(154)의 테이블 내에 데이터를 정렬할 수 있다. 스키마 기반 방식으로 데이터를 파티셔닝하는 것은 블록(190)으로 표시되어 있다. 서버 계층(114)은 다른 방식으로도 데이터를 파티셔닝할 수 있고, 이는 블록(192)으로 표시되어 있다.
- [0033] 도 3은 테넌트(102,104)에 대한 테넌트 데이터(154,156)가 데이터베이스(128) 내에서 어떻게 저장되는지에 대한 예시인 테이블(194,196)의 집합의 일 실시예를 나타낸다. 도 3의 이 실시예에서, 테이블(194)은 테이블 레벨, 행 레벨일 수 있거나, 또는 스키마 기반일 수 있는 파티션 식별자를 갖는다. 파티션 식별자(198)는 데이터(200)를 테넌트(102)에 속하는 것으로 식별한다. 마찬가지로, 테이블(196)은 데이터(204)를 테넌트(104)에 속하는 것으로 식별하는 파티션 식별자(202)를 갖는다. 데이터를 파티셔닝하는 다른 방식도 본 명세서에서 고려된다.
- [0034] 도 3a 내지 도 3c는 예를 들어 테이블 내의 파티셔닝된 데이터를 나타내는 사용자 인터페이스 디스플레이를 보여준다. 도 3a는 속성 탭(213)이 선택된 경우 고객 테이블에 대한 속성들을 디스플레이하는 사용자 인터페이스 디스플레이(211)를 보여준다. 다양한 속성들이 예시되어 있고 박스(215)로 표시된 부분은 데이터가 파티션 식별자에 기초하여 파티셔닝될 뿐만 아니라, 회사 단위로도 파티셔닝됨을 보여준다. 따라서, 그 데이터에 액세스하는 테넌트는 관련 파티션에 속할뿐만 아니라, 관련 회사에도 속해야 한다.
- [0035] 도 3b는 다른 테이블에 대한 속성을 나타내는 사용자 인터페이스 디스플레이(217)를 보여준다. 박스(215)는 이제 데이터가 파티션 식별자에만 기초하여 파티셔닝됨을 보여준다. 즉, 관련 파티션에 할당된 임의의 테넌트는 예시되어 있는 테이블에 액세스할 수 있다. 따라서, (예를 들어) 회사들의 부분집합은 동일한 데이터를 액세스할 수 있다.
- [0036] 도 3c는 또 다른 테이블에 대한 속성을 보여주는 사용자 인터페이스 디스플레이(219)를 보여준다. 사용자 인터페이스 디스플레이(219)에서 박스(221) 내에 도시된 테이블에 대한 속성은 테이블이 시스템 데이터를 포함하고 있음을 나타낸다. 테이블이 회사 단위로 파티셔닝되어 있지 않을 뿐만 아니라 파티션 단위로도 파티셔닝되어 있지 않음을 나타냄으로써, 또한 그 테이블이 프레임워크 테이블 그룹에 속한다는 것을 나타냄으로써, 박스(223) 내의 속성은 테이블이 시스템에서 공유되는 공유 데이터를 포함하고 있음을 보여준다.
- [0037] 도 4는 테넌트(102)가 데이터 저장소(128)에 대한 데이터 조작 요청을 수행할 수 있게 함에 있어서 시스템(100)의 동작에 대한 일 실시예를 나타낸다. 일 실시예에서, 클라이언트(108)는 테넌트(102)에 로그인한다. 이는 도 4에서 블록(210)으로 표시되어 있다. 클라이언트(108)는 테넌트(102)의 보안 관리자가 클라이언트(108)를 설정하는 경우에 수립되는 인증 절차를 거침으로써 이를 수행한다. 인증은 도 4에서 블록(212)으로 표시되어 있다. 서버 계층(114)은 클라이언트(108)가 속한 특정 테넌트를 결정한다. 이것은 다양한 방식으로 행해질 수 있다. 예를 들어, 서버 계층(114)은 클라이언트(108)가 속한 테넌트를 검증할 것을 클라이언트(108)에게 요구하는 사용자 인터페이스 디스플레이를 제공할 수 있다. 마찬가지로, 서버 계층(114)은 클라이언트(108)가 속한 특정 테넌트를 식별하기 위해, 클라이언트(108)가 기록하는 애플리케이션 프로그램 인터페이스를 노출시킬 수 있다. 이것은 도 4에서 블록(214)으로 표시되어 있다. 물론, 클라이언트(108)는 구성 데이터(148)를 또한 서버 계층(114)에 자동으로 제공할 수 있고, 구성 데이터는 예시적으로 테넌트(102)에 대한 클라이언트(108)의 역할뿐만 아니라 클라이언트(108)가 시스템에 로그인했을 때 이용한 테넌트(102)의 신원을 포함한다. 이것은 도

4에서 블록(216)으로 표시되어 있다. 서버 계층(114)은 클라이언트(108)가 속한 특정 테넌트(102)를 식별하는 다른 방식도 사용할 수 있고, 이는 도 4에서 블록(218)으로 표시되어 있다.

[0038] 테넌트에 로그인한 경우, 클라이언트(108)는 데이터 조작 요청을 제출하고, 구성 데이터(148)는 그 요청과 함께 전송된다. 이것은 도 4에서 블록(220)으로 표시되어 있다. 데이터 조작 요청은 데이터베이스(128) 내의 데이터를 조작하거나 추가하기 위한 임의의 부류의 요청일 수 있다. 예를 들어, 데이터 조작 요청은 도 4의 블록(222)으로 표시되어 있는 바와 같이 데이터베이스(128)에 저장될 새로운 데이터를 생성할 수 있다. 이 요청은 블록(224)으로 표시되어 있는 바와 같이, 데이터 저장소(128)로부터 데이터를 삭제하기 위한 요청일 수 있다. 그것은 데이터 저장소(128) 내의 데이터를 업데이트하기 위한 데이터 수정 요청일 수 있다. 이것은 블록(226)으로 표시되어 있다. 그것은 또한 블록(228)으로 표시되어 있는 바와 같이, 간단히 데이터 저장소(128) 내의 데이터에 대한 검색 및 판독 요청일 수 있다. 물론, 데이터 조작 요청은 또한 임의의 다른 부류의 요청일 수 있고, 이는 블록(230)으로 표시되어 있다.

[0039] 서버 계층(114)은 요청과 함께 제출된 구성 데이터를 판독하여, 클라이언트(108)가 속한 특정 테넌트(102)를 판정하고, 또한 (예를 들어) 클라이언트(108)가 테넌트(102)에서 맡고 있는 역할을 판정할 수 있다. 서버 계층(114)은 클라이언트(108)가 저장소(128) 내의 데이터에 대해 가지고 있는 액세스를 구성 데이터(148)에서 식별된 특정 테넌트(102)에 대한 데이터로 한정함으로써 데이터 조작 요청을 서비스한다. 서버 계층(114)은 또한 명시적으로 테넌트(102)에 대한 보안 규칙(134)에 액세스하여 클라이언트(108)의 역할을 식별하고, 이 규칙에 따라 보안을 구현한다. 대응 테넌트 데이터만을 사용하여 요청을 서비스하는 것과, 그 테넌트에 대한 보안을 구현하는 것은 도 4에서 블록(232)으로 표시되어 있다.

[0040] 시스템(100)의 동작을 보다 자세히 설명하기 위해, 도 5는 데이터 저장소(128)로부터 데이터를 획득하기 위해 클라이언트(108)에 의해 제출되는 특정 데이터 액세스 요청을 나타내는 흐름도이다. 또 다시, 클라이언트(108)는 명시적으로 인증 또는 다른 특정 로그인 절차를 사용하여 테넌트(102)에 로그인한다. 이것은 도 5에서 블록(240)으로 표시되어 있다. 클라이언트(108)는 데이터 저장소(128) 내의 테넌트 데이터에 대한 질의를 제출한다. 이것은 도 5에서 블록(242)으로 표시되어 있다. 질의는 제한을 받지 않는다면 저장소(128) 내의 다른 테넌트에 대한 테넌트 데이터를 포함할 수 있다. 예를 들어, 질의가 11월달에 생성된 모든 판매 리드(sales leads)를 찾는 경우, 그 질의는 데이터베이스(128) 내의 모든 테넌트에 대한 테넌트 데이터를 포함할 수 있다. 클라이언트(108)는 질의와 함께 구성 데이터(148)를 서버 계층(114)에 전송한다. 이것은 도 5의 블록(244)으로 표시되어 있다. 서버 계층(114)은 블록(246)으로 표시되어 있는 바와 같이 질의 및 대응하는 구성 데이터를 수신한다. 서버 계층(114)은 구성 데이터(148)를 검사하여, 어느 테넌트로부터 질의가 유래되었는지와 클라이언트(108)가 테넌트에서 맡고 있는 역할을 결정한다. 서버 계층(114)은 테넌트(102)에 속하는 데이터만을 요청하도록 구성 데이터에 기초하여 질의를 수정하고, 테넌트(102)에 대한 역할 기반 보안(또는 보안 규칙(134)에 의해 정의된 다른 보안)을 구현한다. 이것은 도 5에서 블록(248)으로 표시되어 있다. 서버 계층(114)은 사실상 클라이언트(108)가 속하는 테넌트에 속하는 데이터만을 포함하도록 데이터 요청을 한정한다(이 경우, 클라이언트(102)).

[0041] 일 실시예에서, 서버 계층(114)은 데이터 요청을 캐시(130)로부터 서비스할 수 있는지를 결정한다. 그를 수행할 때, 서버 계층(114)은 먼저 이 특정 테넌트(102)에 대한 캐싱된 테넌트 데이터(160)의 사본이 실제로 존재하는지 여부를 결정한다. 이것은 도 5에서 블록(250)으로 표시되어 있다. 그렇지 않은 경우, 서버 계층(114)은 블록(252)으로 표시되어 있는 바와 같이, 테넌트(102)에 대한 캐시의 사본을 생성하고, 데이터 저장소(128)에 액세스하여 요청된 데이터를 획득한다. 이것은 블록(254)으로 표시되어 있다.

[0042] 그러나, 서버 계층(114)이 블록(250)에서 테넌트(102)에 대한 캐시의 사본이 존재하는 것으로 판정하면, 서버 계층(114)은 요청된 데이터에 대한 그 캐싱된 테넌트 데이터를 체크한다. 이것은 도 5에서 블록(256)으로 표시되어 있다. 서버 계층(114)이 캐시(130)로부터 요청을 서비스할 수 있는 경우, 그렇게 한다. 그러나, 그럴 수 없는 경우, 서버 계층(114)은 데이터베이스(128) 내의 데이터를 액세스해야 한다. 캐시(130)로부터 요청이 서비스될 수 있는지 여부를 판정하는 것은 도 5에서 블록(258)으로 표시되어 있다.

[0043] 서버 계층(114)이 캐시(130)로부터 데이터를 획득했든 또는 데이터 저장소(128)로부터 데이터를 획득하였든, 질의에 응답하는 데이터는 테넌트(102) 내의 클라이언트(108)로 리턴된다. 이것은 도 5에서 블록(260)으로 표시되어 있다. 서버 계층(114)은 임의의 다른 원하는 캐싱 동작을 수행한다. 예를 들어, (캐시의 테넌트의 사본에 있지 않은) 새로운 데이터가 데이터 저장소(128)로부터 검색된 경우, 서버 계층(114)은 그 데이터를 테넌트(102)에 대한 캐싱된 테넌트 데이터에 추가한다. 물론, 서버 계층(114)은 캐시의 테넌트의 사본을 다른 방식의

로도 업데이트할 수 있고, 캐시(130)를 유지하기 위한 캐싱 동작의 수행은 도 5에서 블록(262)으로 표시되어 있다. 따라서, 서버 계층(114)은 복수의 테넌트에 대한 데이터를 (안전하고 파티셔닝된 방식으로) 저장할 수 있도록 데이터베이스(128)를 파티셔닝할 뿐만 아니라, 서버 계층(114)은 복수의 테넌트에 대한 데이터를 저장할 수 있도록 캐시(130)를 제어한다. 캐싱된 데이터의 각 사본은 주어진 테넌트에 속하는 것으로 마킹되고 어떠한 다른 테넌트도 캐싱된 데이터의 그 사본을 액세스할 수 없다. 그것은 다른 테넌트의 캐싱된 데이터와는 별개로 유지되고 파티셔닝된다.

[0044] 도 5a는 테넌트들의 부분집합이 함께 파티셔닝되기는 하지만 다른 테넌트들과는 별개인 또 다른 실시예를 보여준다. 도 5a는 도 1에 도시되어 있는 것과 유사한 시스템(100)을 보여주며, 유사한 항목들에는 유사하게 번호가 주어진다. 그러나, 도 5a의 시스템(100)은 테넌트(102,104)가 예시적으로 부분집합(161)으로 함께 그룹화되는 두 개의 비즈니스인 것임을 보여준다. 따라서, 부분집합(161)의 테넌트들은 서로의 데이터에 대해 액세스를 가지기를 원하지만, 그 데이터가 테넌트(105)와 같은 추가의 테넌트에 대한 데이터와는 별개이고 격리될 것을 희망한다. 따라서, 관리자는 테넌트(102,104)를 동일한 파티션에 할당한다. 이러한 식으로, 서버 계층(114)은 테넌트(102,104)가 그 데이터 모두를 액세스할 수 있도록 테넌트(102,104)에 대해 파티셔닝된 데이터(163)를 저장할 것이다. 그러나, 데이터(163)는 테넌트(105)에 대한 파티션에 할당된 데이터(165)와는 분리되어 파티셔닝된다. 따라서, 테넌트(105)는 데이터(163)에 대한 액세스를 가지지 않고, 테넌트(102,104)의 부분집합(161)은 데이터(165)에 대한 액세스를 가지지 않는다.

[0045] 일 실시예에서, 캐시(130)는 또한 데이터 저장소(128)와 동일한 방식으로 별개로 파티셔닝됨을 주목한다. 따라서, 캐시(130)는 테넌트(102,104)의 부분집합(161)에 대한 캐싱된 데이터의 별개의 사본, 및 테넌트(105)에 대한 캐싱된 데이터의 별도로 파티셔닝된 사본을 포함한다. 따라서, 캐시(130)는 캐시(130)로부터 요청된 임의의 데이터가 동일한 방식으로 또한 파티셔닝되도록 데이터 저장소(128)와 동일한 방식으로 파티셔닝된다.

[0046] 본 명세서에서 설명되는 비즈니스 데이터는 고객 기록, 판매 주문, 공급 업체, 리드, 제안서, 견적, 판매 데이터, 제품 데이터, 위치 데이터, 회사 금융 및 마케팅 데이터 및 전략, 개인 데이터, 임금 또는 다른 사람 자원 정보 등과 같은 다양한 비즈니스 데이터를 포함한다. 다른 비즈니스 데이터 또는 비즈니스 기록도 또한 사용될 수 있다.

[0047] 도 6은 클라우드 컴퓨팅 아키텍처(500)에 노출된다는 점을 제외하면, 도 1에 도시되어 있는 시스템(100)의 블록도이다. 클라우드 컴퓨팅은 서비스를 전달하는 시스템의 물리적 위치 또는 구성에 대한 최종 사용자의 지식을 요구하지 않는 계산, 소프트웨어, 데이터 액세스 및 저장 서비스를 제공한다. 다양한 실시예에서, 클라우드 컴퓨팅은 적절한 프로토콜을 사용하여 인터넷과 같은 광역 네트워크를 통해 서비스를 전달한다. 예를 들어, 클라우드 컴퓨팅 제공자는 광역 네트워크를 통해 애플리케이션을 전달하고, 이 제공자는 웹 브라우저 또는 임의의 다른 컴퓨팅 컴포넌트를 통해 액세스될 수 있다. 시스템(100)의 소프트웨어 또는 컴포넌트, 및 대응하는 데이터는 원격 위치의 서버에 저장될 수 있다. 클라우드 컴퓨팅 환경에서의 컴퓨팅 리소스는 원격 데이터 센터 위치에서 통합될 수 있거나 분산될 수 있다. 클라우드 컴퓨팅 인프라스트럭처는 공유 데이터 센터가 사용자에 대한 단일 액세스 지점으로서 나타날지라도 그 공유 데이터 센터를 통해 서비스를 전달할 수 있다. 따라서, 본 명세서에서 기술된 컴포넌트 및 기능은 클라우드 컴퓨팅 아키텍처를 사용하여 원격 위치에서의 서비스 제공자로부터 제공될 수 있다. 이와 달리, 그들은 종래의 서버로부터 제공될 수 있고, 또는 클라이언트 장치에 직접적으로 또는 다른 방식으로 설치될 수 있다.

[0048] 본 명세서는 공용 클라우드 컴퓨팅 및 사설 클라우드 컴퓨팅 모두를 포함하려 한다. 클라우드 컴퓨팅(공용 및 사설 모두)은 사실상 끊임없는 리소스 풀링(seamless pooling of resources)과, 기본 하드웨어 인프라스트럭처를 관리하고 구성할 감소된 필요성을 제공한다.

[0049] 공용 클라우드는 공급업체에 의해 관리되고 전형적으로 동일한 인프라스트럭처를 사용하여 다수의 고객을 지원한다. 또한, 사설 클라우드에 반대인 공용 클라우드는 최종 사용자가 하드웨어를 관리하지 않아도 되게 할 수 있다. 사설 클라우드는 조직 자체에 의해 관리될 수 있고 인프라스트럭처는 전형적으로 다른 조직과 공유되지 않는다. 조직은 설치 및 수리 등과 같이 어느 정도 하드웨어를 유지한다.

[0050] 도 6에 도시되어 있는 실시예에서, 소정의 항목들은 도 1에 도시되어 있는 것과 유사하고, 유사하게 번호가 주어진다. 도 6은 서버 계층(114), 데이터 저장소(128), 캐시(130) 및 보안 규칙(134)이 (공용, 사설, 또는 일부는 공용이고 일부는 사설인 조합일 수 있는) 클라우드(502)에 위치해 있는 것을 구체적으로 보여준다. 따라서, 테넌트(102) 내의 클라이언트(108)(또는 사용자(103))는 사용자 장치(504)를 사용하여 클라우드(502)를 통해 시스템에 액세스한다.

- [0051] 도 6은 또한 클라우드 아키텍처의 또 다른 실시예를 나타낸다. 도 6은 시스템(100)의 소정의 요소들이 클라우드(502)에 배치되어 있으나 그 밖의 것들은 배치되지 않은 경우를 나타낸다. 예를 들어, 데이터 저장소(128)는 클라우드(502) 밖에 배치될 수 있고 클라우드(502)를 통해 액세스될 수 있다. 또 다른 실시예에서, 보안 규칙(134)도 클라우드(502) 밖에 위치한다. 그들의 위치와는 무관하게, 그들은 네트워크(광역 네트워크 또는 근거리 네트워크)를 통해 장치(504)에 의해 직접 액세스될 수 있거나, 그들은 원격 사이트에서 서비스에 의해 호스팅될 수 있거나, 그들은 클라우드를 통해 서비스로서 제공되거나 클라우드 내에 상주하는 연결 서비스에 의해 액세스될 수 있다. 본 명세서에서는 이들 아키텍처 모두가 고려된다.
- [0052] 시스템(100), 또는 이의 일부는 다양한 장치에 배치될 수 있다. 이들 장치 중 일부는 서버, 데스크탑 컴퓨터, 랩탑 컴퓨터, 태블릿 컴퓨터, 또는 팜 탑 컴퓨터, 셀룰러 폰, 스마트 폰, 멀티미디어 플레이어, 개인 보조 단말기와 같은 다른 이동 장치 등을 포함한다.
- [0053] 도 7은 본 시스템(또는 이의 일부)이 배치될 수 있는 사용자 또는 클라이언트의 핸드헬드 장치(16)로부터 사용될 수 있는 핸드헬드 또는 이동 컴퓨팅 장치의 하나의 예시적인 실시예에 대한 간단한 블록도이다. 도 8 내지 도 10은 핸드헬드 또는 이동 장치의 예이다.
- [0054] 도 7은 시스템(100)의 컴포넌트들(예를 들어, 태넌트 또는 클라이언트 또는 다른 컴포넌트들)을 실행시킬 수 있고 또는 시스템(100)과 상호작용할 수 있고 또는 이 둘 다를 할 수 있는 클라이언트 장치(16)의 컴포넌트들의 일반적인 블록도를 제공한다. 장치(16)에서, 핸드헬드 장치가 다른 컴퓨팅 장치와 통신할 수 있도록 해주는 통신 링크(13)가 제공되고 이 통신 링크(13)는 소정의 실시예에서 예를 들어 스캐닝을 통해 정보를 자동으로 수신하는 채널을 제공한다. 통신 링크(13)의 예는 적외선 포트, 직렬/USB 포트, 이더넷 포트와 같은 케이블 네트워크 포트, 및 네트워크에의 셀룰러 액세스를 제공하는데 사용된 무선 서비스인 일반적인 패킷 무선 서비스(GPRS), LTE, HSPA, HSPA+ 및 다른 3G 및 4G 무선 프로토콜, 1Xrtt, 및 단문 메시지 서비스, 및 네트워크에의 로컬 무선 연결을 제공하는 802.11 및 802.11b (Wi-Fi) 프로토콜, 및 블루투스 프로토콜을 포함하는 하나 이상의 통신 프로토콜을 통해 통신을 가능하게 하는 무선 네트워크 포트를 포함한다.
- [0055] 다른 실시예에서, (시스템(100)의 ERP 애플리케이션과 같은) 애플리케이션 또는 시스템은 SD 카드 인터페이스(15)에 연결된 이동식 보안 디지털(SD) 카드 상에서 수신된다. SD 카드 인터페이스(15) 및 통신 링크(13)는 메모리(21) 및 입/출력(I/O) 컴포넌트(23), 클록(25) 및 위치 시스템(27)에 연결된 버스를 따라 (도 1의 프로세서(136 또는 138)를 또한 포함할 수 있는) 프로세서(17)와 통신한다.
- [0056] 일 실시예에서, I/O 컴포넌트(23)는 입력 및 출력 동작을 용이하게 하도록 제공된다. 장치(16)의 다양한 실시예를 위한 I/O 컴포넌트(23)는 버튼, 터치 센서, 멀티 터치 센서, 광학 또는 비디오 센서, 음성 센서, 터치 스크린, 근접 센서, 마이크로폰, 경사 센서, 및 중력 스위치와 같은 입력 컴포넌트와 디스플레이 장치, 스피커, 및/또는 프린터 포트와 같은 출력 컴포넌트를 포함한다. 다른 I/O 컴포넌트(23)도 사용될 수 있다.
- [0057] 클록(25)은 예시적으로 시간과 날짜를 출력하는 실시간 클록 컴포넌트를 포함한다. 클록(25)은 또는 예시적으로 프로세서(17)에 타이밍 기능을 제공한다.
- [0058] 위치 센서(27)는 예시적으로 위치(16)의 현재 지리적 위치를 출력하는 컴포넌트를 포함한다. 이것은 예를 들어 GPS 수신기, LORAN 시스템, 데드 레코닝 시스템(dead reckoning system), 셀룰러 삼각측량 시스템 또는 다른 포지셔닝 시스템을 포함할 수 있다. 그것은 또한 원하는 지도, 네비게이션 루트 및 그 밖의 다른 지리적 기능을 생성하는 맵핑 소프트웨어 또는 네비게이션 소프트웨어를 포함할 수 있다.
- [0059] 메모리(21)는 운영 체제(29), 네트워크 설정(31), 애플리케이션(33), 애플리케이션 구성 설정(35), 데이터 저장소(37), 통신 드라이버(39) 및 통신 구성 설정(41)을 저장한다. 메모리(21)는 모든 유형의 물리적인 휘발성 및 비휘발성 컴퓨터 판독가능 메모리 장치를 포함할 수 있다. 메모리(21)는 또한 (이하에서 설명되는) 컴퓨터 저장 매체를 포함할 수 있다. 메모리(21)는 프로세서(17)에 의해 실행되는 경우 프로세서로 하여금 명령어에 따라 컴퓨터 구현 단계 또는 기능을 수행하게 하는 컴퓨터 판독가능 명령어를 저장한다. 시스템(100) 또는 데이터 저장소(128) 또는 캐시(130) 내의 항목은 메모리(21)에 상주할 수 있다. 유사하게, 장치(16)는 다양한 비즈니스 애플리케이션을 실행할 수 있거나 비즈니스 시스템(100)의 일부 또는 전부를 구현할 수 있는 클라이언트 비즈니스 시스템(24)을 구비할 수 있다. 프로세서(17)는 다른 컴포넌트들에 의해 활성화되어 이들의 기능도 용이하게 할 수 있다.
- [0060] 네트워크 설정(31)의 예는 프록시 정보, 인터넷 연결 정보 및 맵핑과 같은 것을 포함한다. 애플리케이션 구성 설정(35)은 특정 기업 또는 사용자에 대한 애플리케이션을 맞춤화하는 설정을 포함한다. 통신 구성 설정(41)은

다른 컴퓨터와 통신하기 위한 파라미터를 제공하고 GPRS 파라미터, SMS 파라미터, 연결 사용자 이름 및 패스워드와 같은 항목을 포함한다.

[0061] 애플리케이션(33)은 장치(16) 상에 이전에 저장된 애플리케이션일 수 있거나, 사용 동안 설치된 애플리케이션일 수 있지만, 이들은 운영 체제(28)의 일부일 수 있거나, 장치(16) 외부에서도 호스팅될 수 있다.

[0062] 도 8은 장치(16)가 태블릿 컴퓨터(600)인 일 실시예를 나타낸다. 도 8에서, 컴퓨터(600)는 디스플레이 스크린(602) 상에 디스플레이된 (새로운 테넌트를 생성하기 위해 사용된) 사용자 인터페이스 디스플레이(179)와 함께 도시되어 있다. 스크린(602)은 터치스크린일 수 있거나(따라서, 사용자의 손가락(604)으로부터의 터치 제스처가 애플리케이션과 상호작용하는데 사용됨) 또는 펜 또는 스타일러스로부터 입력을 수신하는 펜 인에이블링된 인터페이스일 수 있다. 스크린(602)은 또한 온-스크린 가상 키보드를 사용할 수 있다. 물론, 그것은 예를 들어 무선 링크 또는 USB 포트와 같은 적절한 첨부 메카니즘을 통해 키보드 또는 다른 사용자 입력 장치에 부착될 수 있다. 컴퓨터(600)는 또한 예시적으로 음성 입력도 수신할 수 있다.

[0063] 도 9 및 도 10은 사용될 수 있는 장치(16)의 추가 예를 제공하지만, 다른 예들도 사용될 수 있다. 도 9에서, 스마트폰 또는 이동 전화기(45)가 장치(16)로서 제공된다. 전화기(45)는 전화를 걸기 위한 키패드들의 집합(47), 애플리케이션 이미지, 아이콘, 웹 페이지, 사진을 포함한 이미지 및 비디오를 디스플레이할 수 있는 디스플레이(49), 및 디스플레이에 도시되어 있는 항목들을 선택하기 위한 제어 버튼(51)을 포함한다. 전화기는 일반적인 패킷 무선 서비스(GPRS) 및 1Xrtt, 및 단문 메시지 서비스(SMS) 신호와 같은 셀룰러 전화기 신호를 수신하는 안테나(53)를 포함한다. 몇몇 실시예에서, 전화기(45)는 SD 카드(57)를 수용하는 보안 디지털(SD) 카드 슬롯(55)을 또한 포함한다.

[0064] 도 10의 이동 전화기는 개인 보조 단말기(PDA)(59) 또는 멀티미디어 플레이어 또는 태블릿 컴퓨팅 장치 등(이하에서는 PDA(59)로 지칭됨)이다. PDA(59)는 스타일러스가 스크린 위에 배치되는 경우 스타일러스(63)(또는 사용자의 손가락과 같은 다른 포인터)의 위치를 감지하는 유도성 스크린(61)을 포함한다. 이것은 사용자가 스크린 상에서 항목을 선택, 강조 및 이동시킬 뿐만 아니라 그리고 쓸 수 있게 해준다. PDA(59)는 또한 사용자가 디스플레이(61)에 디스플레이되는 메뉴 옵션들 또는 다른 디스플레이 옵션들을 스크롤할 수 있게 해주고, 또한 사용자가 디스플레이(61)와 접촉하지 않고서 애플리케이션을 변경하거나 사용자 입력 기능을 선택할 수 있게 해주는 다수의 사용자 입력 키 또는 버튼(예를 들어 버튼(65))을 포함한다. 도시되어 있지는 않지만, PDA(59)는 다른 컴퓨터와의 무선 통신을 가능하게 하는 내부 안테나 및 적외선 송신기/수신기와 다른 컴퓨팅 장치와의 하드웨어 접속을 가능하게 하는 접속 포트를 포함할 수 있다. 이러한 하드웨어 접속은 전형적으로 직렬 또는 USB 포트를 통해 다른 컴퓨터에 접속되는 크래들을 통해 이루어진다. 그에 따라, 이들 접속은 비-네트워크 접속이다. 일 실시예에서, 이동 장치(59)는 또한 SD 카드(69)를 수용하는 SD 카드 슬롯(67)을 포함한다.

[0065] 다른 형태의 장치(16)도 가능함을 알아야 한다.

[0066] 도 11은 (예를 들어) 시스템(100)이 배치될 수 있는 컴퓨팅 환경의 일 실시예이다. 도 11을 참조하면, 소정의 실시예를 구현하는 예시적인 시스템은 컴퓨터(810) 형태의 범용 컴퓨팅 장치를 포함한다. 컴퓨터(810)의 컴포넌트들은 (서버 또는 테넌트용 프로세서를 포함할 수 있는) 처리 장치(820), 시스템 메모리(830), 및 시스템 메모리를 포함하는 다양한 시스템 컴포넌트를 처리 장치(820)에 연결하는 시스템 버스(821)를 포함할 수 있으나, 이에 국한되지 않는다. 시스템 버스(821)는 메모리 버스 또는 메모리 제어기, 주변 버스, 및 임의의 다양한 버스 아키텍처를 이용하는 로컬 버스를 포함하는 임의의 몇몇 유형의 버스 구조일 수 있다. 제한이 아닌 예로서, 이러한 아키텍처는 산업 표준 아키텍처(ISA) 버스, 마이크로 채널 아키텍처(MCA) 버스, 개선된 ISA(EISA) 버스, 비디오 전자 표준 협회(VESA) 로컬 버스, 및 메자닌 버스로도 알려져 있는 주변 컴포넌트 상호연결(PCI) 버스를 포함한다. 도 1과 관련하여 기술된 메모리 및 프로그램은 도 11의 대응하는 부분에 배치될 수 있다.

[0067] 컴퓨터(810)는 전형적으로 다양한 컴퓨터 판독가능 매체를 포함한다. 컴퓨터 판독가능 매체는 컴퓨터(810)에 의해 액세스될 수 있고 휘발성 및 비휘발성 매체, 이동식 및 고정식 매체를 포함하는 임의의 이용가능 매체일 수 있다. 제한이 아닌 예로서, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 포함할 수 있다. 컴퓨터 저장 매체는 변조된 데이터 신호 또는 반송파와는 다르며, 또한 그를 포함하지 않는다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 다른 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술에서 구현된 휘발성 및 비휘발성, 이동식 및 고정식 매체를 포함하는 하드웨어 저장 매체를 포함한다. 컴퓨터 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 다른 메모리 기술, CD-ROM, 디지털 다기능 디스크 (DVD) 또는 다른 광학 디스크 저장소, 자기 카세트, 자기 테이프, 자기 디스크 저장소 또는 다른 자기 저장 장치, 또는 원하는 정보를 저장하는데 사용될 수 있고 컴퓨터(810)에 의해 액세스될 수 있는 임의의 다른

매체를 포함하나, 이에 국한되지 않는다. 통신 매체는 통상적으로 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터를 전송 메카니즘으로 구현하고 임의의 정보 전달 매체를 포함한다. "변조된 데이터 신호"라는 용어는 정보를 신호 내에 인코딩하는 방식으로 자신의 특성들 중 하나 이상이 설정되거나 변경된 신호를 의미한다. 제한이 아닌 예로서, 통신 매체는 유선 네트워크 또는 직접 유선 접속과 같은 유선 매체와, 음향, RF, 적외선 및 다른 무선 매체와 같은 무선 매체를 포함한다. 상기의 임의의 조합도 컴퓨터 판독 가능 매체의 범위 내에 포함되어야한다.

[0068] 시스템 메모리(830)는 판독 전용 메모리(ROM)(831) 및 랜덤 액세스 메모리(RAM)(832)와 같은 휘발성 및/또는 비휘발성 메모리의 형태의 컴퓨터 저장 매체를 포함한다. 예를 들어 시동 중에 컴퓨터(810) 내의 소자들 간의 정보 전달을 돕는 기본 루틴을 포함하는 기본적인 입/출력 시스템(833)(BIOS)이 일반적으로 ROM(831)에 저장된다. RAM(832)은 전형적으로 처리 장치(820)에 의해 즉시 액세스가능하고 및/또는 현재 동작중인 데이터 및/또는 프로그램 모듈을 포함한다. 제한이 아닌 예로서, 도 11은 운영 체제(834), 애플리케이션 프로그램(835), 기타 프로그램 모듈(836), 및 프로그램 데이터(837)를 도시한다.

[0069] 컴퓨터(810)는 또한 다른 이동식/고정식의 휘발성/비휘발성 컴퓨터 저장 매체를 포함할 수 있다. 오직 예로서, 도 11은 고정식의 비휘발성 자기 매체에 대해 판독 또는 기록하는 하드 디스크 드라이브(841), 이동식의 비휘발성 자기 디스크(852)에 대해 판독 또는 기록하는 자기 디스크 드라이브(851), 및 CD ROM 또는 다른 광학 매체와 같은 이동식의 비휘발성 광학 디스크(856)를 나타낸다. 예시적인 동작 환경에서 사용될 수 있는 다른 이동식/고정식, 휘발성/비휘발성 컴퓨터 저장 매체는 자기 테이프 카세트, 플래시 메모리 카드, DVD, 디지털 비디오 테이프, 고체 상태 RAM, 고체 상태 ROM 등을 포함하나 이에 국한되지 않는다. 하드 디스크 드라이브(841)는 통상적으로 인터페이스(840)와 같은 고정식 메모리 인터페이스를 통해 시스템 버스(821)에 연결되고, 자기 디스크 드라이브(851) 및 광학 디스크 드라이브(855)는 일반적으로 인터페이스(850)와 같은 이동식 메모리 인터페이스에 의해 시스템 버스(821)에 연결된다.

[0070] 전술한 및 도 11에 도시되어 있는 드라이브 및 그 관련 컴퓨터 저장 매체는 컴퓨터(810)를 위해 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 및 기타 데이터의 저장을 제공한다. 도 11에서, 예를 들어, 하드 디스크 드라이브(841)는 운영 체제(844), 애플리케이션 프로그램(845), 기타 프로그램 모듈(846), 및 프로그램 데이터(847)를 저장하는 것으로 도시되어 있다. 이들 컴포넌트는 운영 체제(834), 애플리케이션 프로그램(835), 기타 프로그램 모듈(836) 및 프로그램 데이터(837)와 동일 또는 상이할 수 있다. 운영 체제(844), 애플리케이션 프로그램(845), 기타 프로그램 모듈(846), 및 프로그램 데이터(847)는 최소한 이들이 서로 다른 사본임을 나타내기 위해 본 명세서에서 다른 번호가 주어져 있다.

[0071] 사용자는 예컨대 키보드(862), 마이크로폰(863), 및 마우스, 트랙볼 또는 터치 패드와 같은 포인팅 장치(861)와 같은 입력 장치를 통해 컴퓨터(810)에 명령과 정보를 입력할 수 있다. 다른 입력 장치(미도시)는 조이스틱, 게임 패드, 위성 안테나, 스캐너 등을 포함할 수 있다. 이들 및 다른 입력 장치는 종종 시스템 버스에 연결된 사용자 입력 인터페이스(860)를 통해 처리 장치(820)에 접속되지만, 병렬 포트, 게임 포트 또는 범용 직렬 버스(USB)와 같은 다른 인터페이스 및 버스 구조에 의해 연결될 수 있다. 시각적 디스플레이(891) 또는 다른 유형의 디스플레이 장치는 또한 비디오 인터페이스(890)와 같은 인터페이스를 통해 시스템 버스(821)에 연결된다. 모니터 외에, 컴퓨터는 또한 출력 주변 인터페이스(895)를 통해 접속될 수 있는 스피커(897) 및 프린터(896)와 같은 다른 주변 장치 출력 장치를 포함할 수 있다.

[0072] 컴퓨터(810)는 원격 컴퓨터(880)와 같은 하나 이상의 원격 컴퓨터로의 논리적 접속을 이용하여 네트워크 환경에서 동작한다. 원격 컴퓨터(880)는 퍼스널 컴퓨터, 핸드헬드 장치, 서버, 라우터, 네트워크 PC, 피어 장치 또는 다른 공통 네트워크 노드일 수 있고, 통상적으로 컴퓨터(810)에 대하여 위에서 설명한 요소들 중 다수 또는 전부를 포함할 수 있다. 도 8에 도시된 논리적 접속은 근거리 네트워크(LAN)(871) 및 광역 네트워크(WAN)(873)를 포함하지만, 다른 네트워크도 포함 할 수 있다. 이러한 네트워크 환경은 사무실, 기업 컴퓨터 네트워크, 인터넷 및 인터넷에서 일반적이다.

[0073] LAN 네트워크 환경에서 사용될 때, 컴퓨터(810)는 네트워크 인터페이스 또는 어댑터(870)를 통해 LAN(871)에 연결된다. WAN 네트워크 환경에서 사용되는 경우, 컴퓨터(810)는 일반적으로 인터넷과 같은 WAN(873)을 통해 통신을 수립하기 위한 모뎀(872) 또는 다른 수단을 포함한다. 내장형 또는 외장형일 수 있는 모뎀(872)은 사용자 입력 인터페이스(860) 또는 다른 적절한 메카니즘을 통해 시스템 버스(821)에 연결될 수 있다. 네트워크 환경에서, 컴퓨터(810)에 대해 설명한 프로그램 모듈들, 또는 이들의 일부는 원격 메모리 저장 장치에 저장될 수 있다. 제한이 아닌 예로서, 도 11은 원격 애플리케이션 프로그램(885)을 원격 컴퓨터(880)에 상주하는 것으로 도

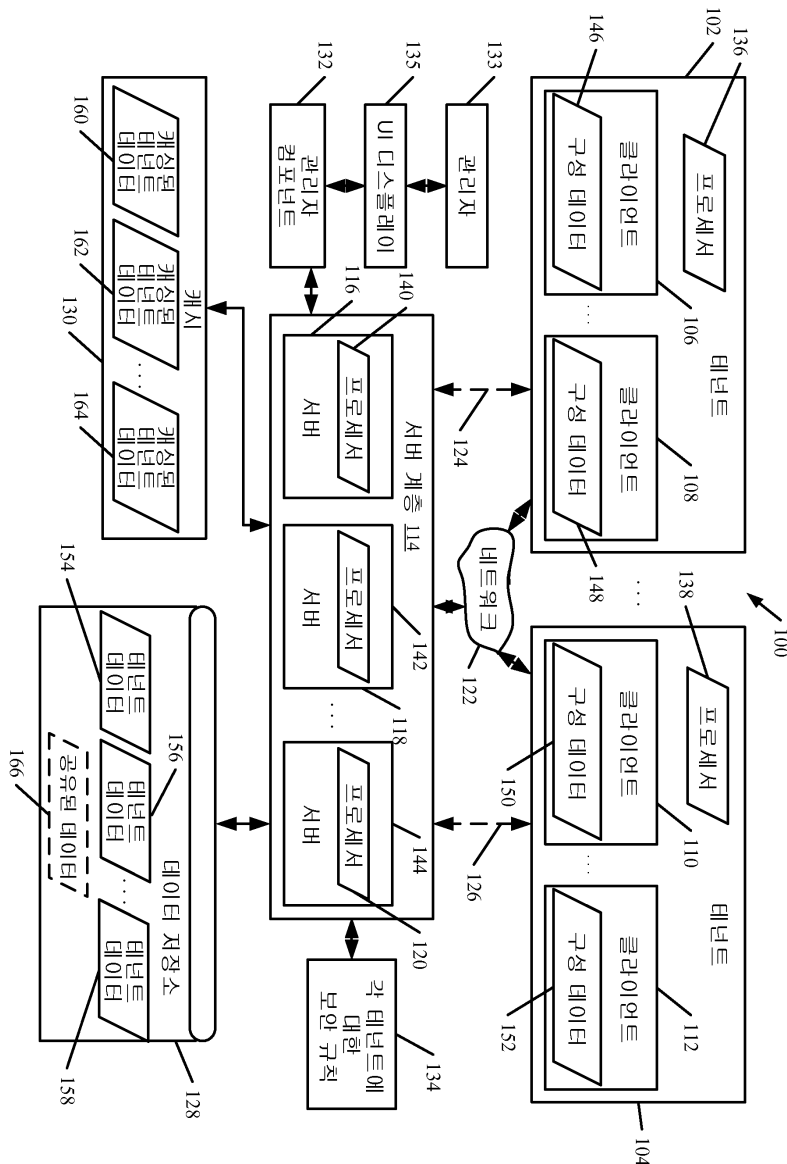
시한다. 도시되어 있는 네트워크 연결들은 예시적이며 컴퓨터들 간의 통신 링크를 수립하는 다른 수단이 사용될 수 있다.

[0074]

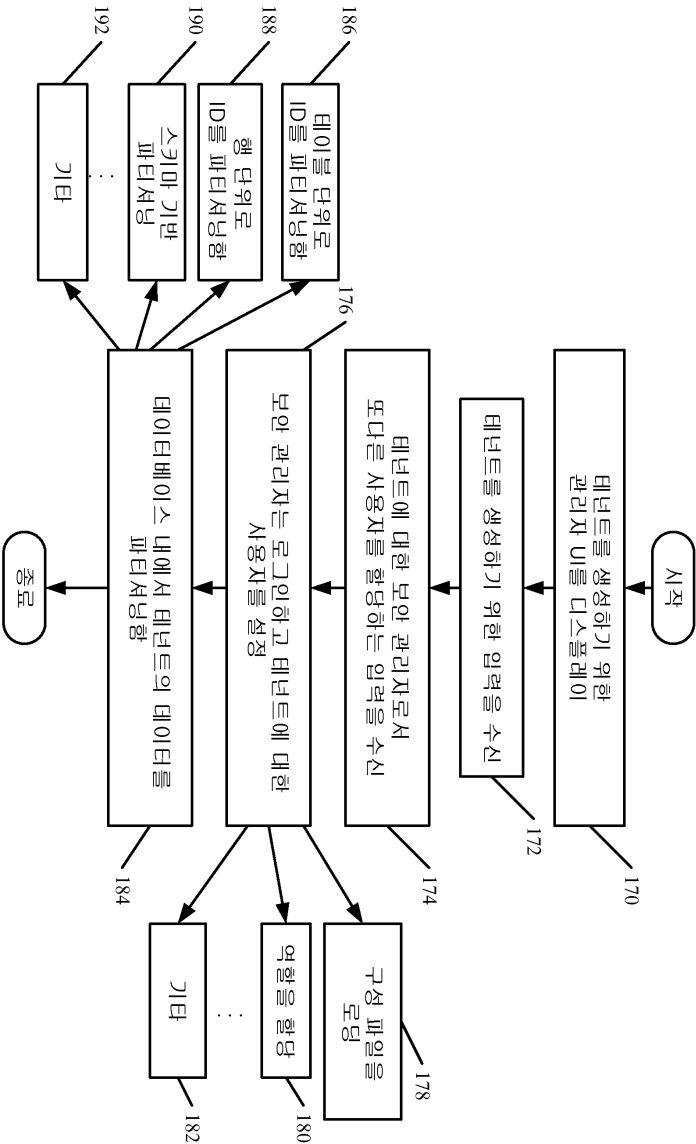
본 발명은 구조적 특징 및/또는 방법론적 동작에 특정한 언어로 기술되었지만, 첨부한 청구항에 정의된 본 발명은 전술한 바와 같은 특정 특징 또는 동작들에 반드시 국한될 필요는 없다. 그 보다, 전술한 특정 특징 및 동작들은 청구대상을 구현하기 위한 예시적인 형식으로 개시되어 있다.

도면

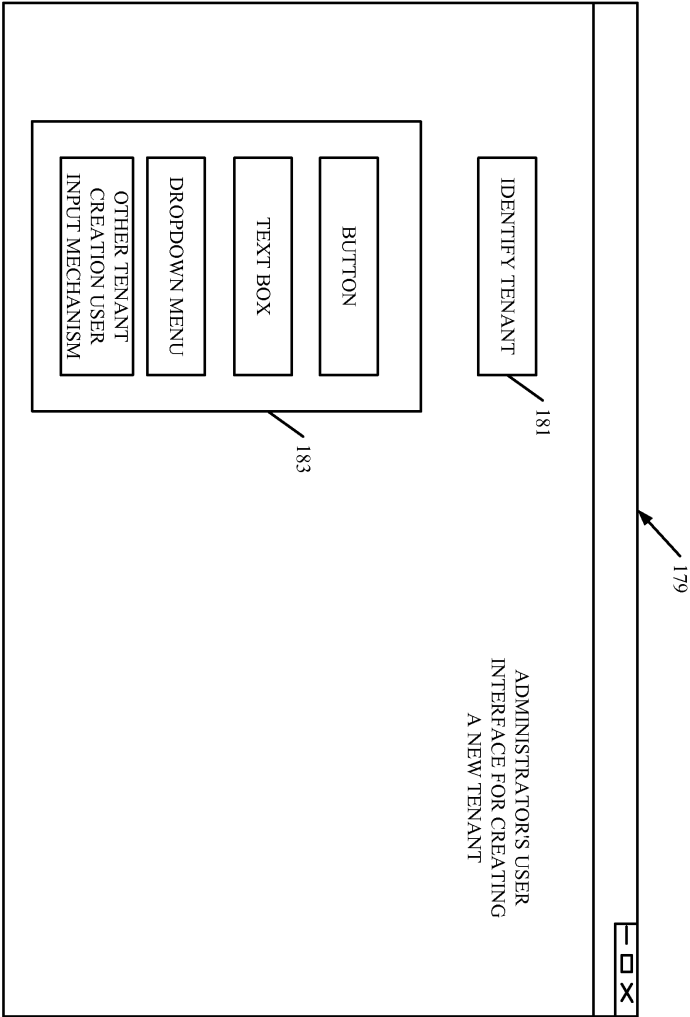
도면1



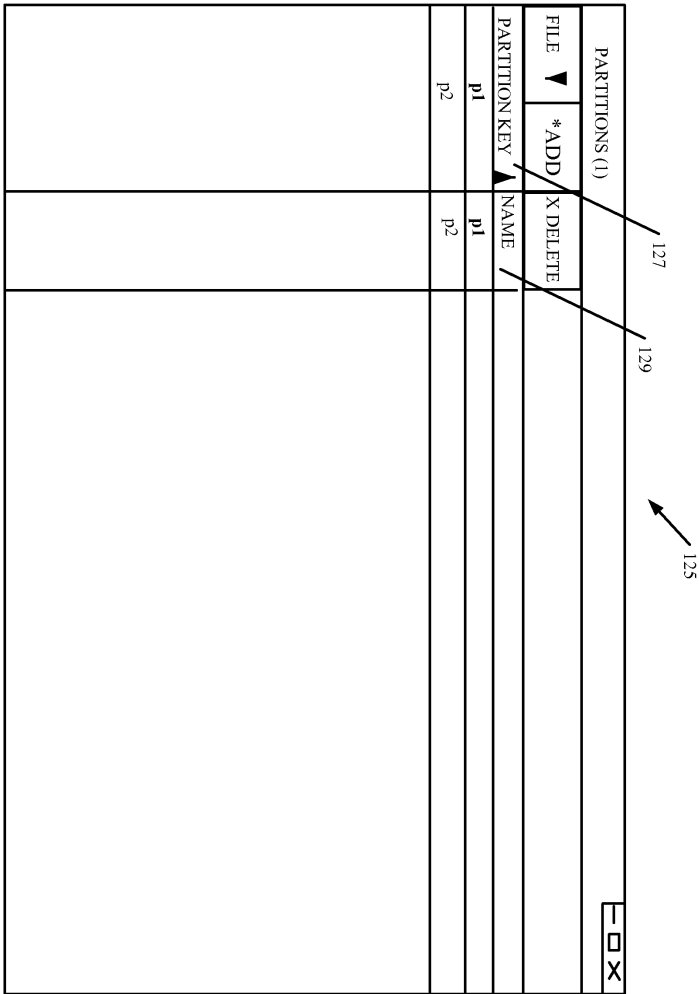
도면2



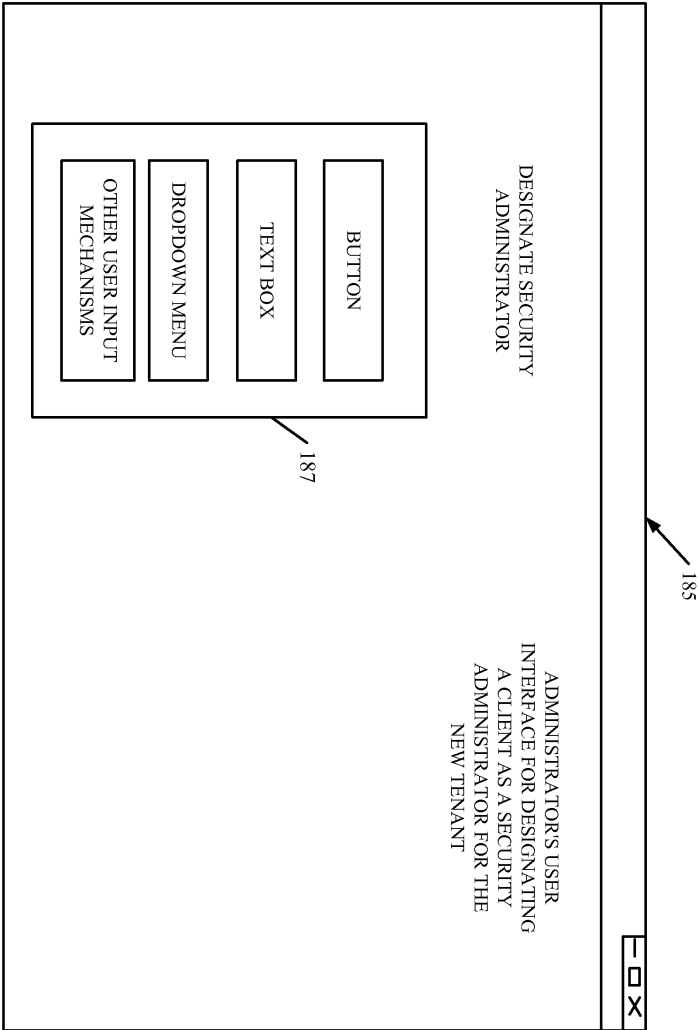
도면2a



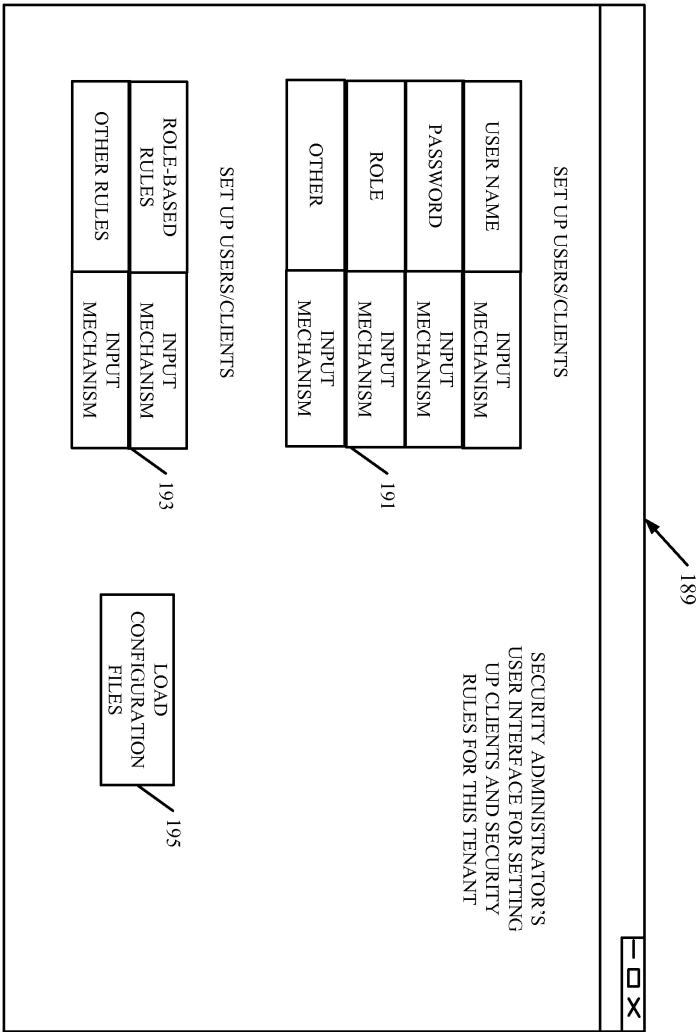
도면2b



도면2c



도면2d



도면2e

User(1) - New Record

File ▼ User

133

131

✎

Edit

✕

Delete

👤

Users

📁

Import

⚙️

Options

👤

Relations

🖨️

Set up

📄

log

🕒

Online time

📎

Attachments

🔧

Maintain

👤

New

📄

Related information

📄

Profiles for selected user

User ID: 135

Account type: 137

User name: 143

Default company: 145

Network domain: 139

Alias: 141

Enabled: 147

Current partition is default partition: 157

External: 159

Active Directory user: 143

DAT: 145

Privileges in selected role: 151

This grid is empty

☐ Assign roles

☒ Remove

☐ Assign Organizations

☐ Edit role

☐ Roles

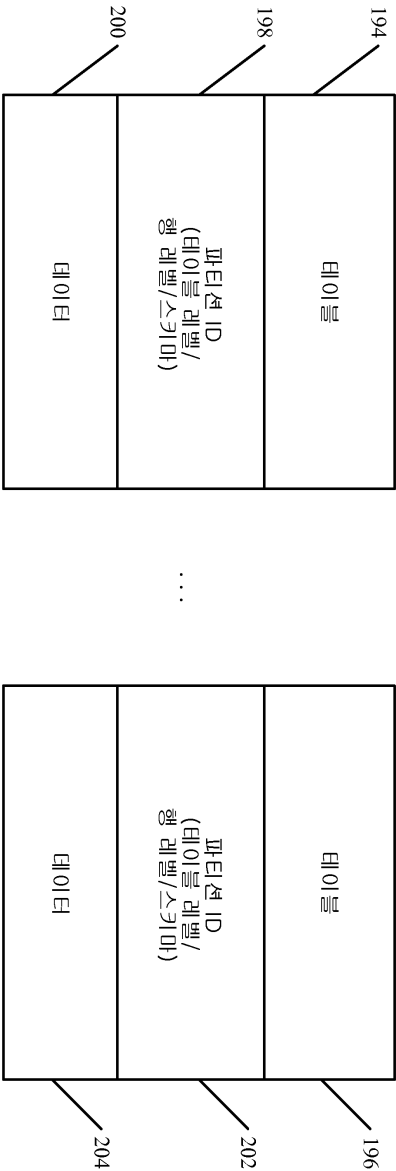
155

153

312

- 23 -

도면3



도면3a

213 Table CustTable

211 Properties | Categories

ID	77
Name	CustTable
Label	Customers
FormRel	
ListPageRel	
ReportRel	
PreviewPartRel	
SearchLinkRelType	Util
SearchLinkRelName	EPCustTableInfo
TitleField1	AccountNum
TitleField2	Party
TableType	Regular
TableContents	Not specified
Systemtable	No
ConfigurationKey	LedgerBasic
SecurityKey	CustTables
Visible	Yes
AQSAuthorization	None
CacheLookup	Found
CreateHectIndex	Yes
SaveDataPerCompany	Yes
SaveDataPerPartition	Yes
TableGroup	Main
PrimaryIndex	AccountIdx
ClusterIndex	AccountIdx

215

회사 단위의 테이블

도면3b

217 Table DirPartyEcoResCategory

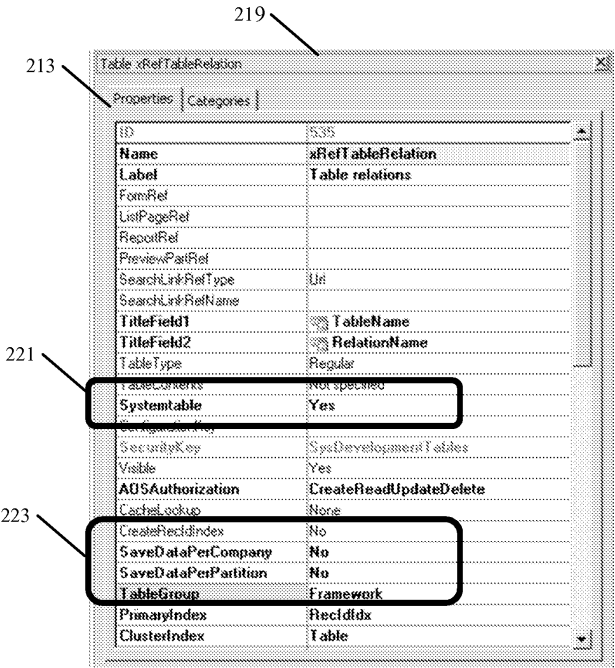
213 Properties | Categories

ID	4071
Name	DirPartyEcoResCategory
Label	Set up categories
FormRel	
ListPageRel	Yes
ReportRel	
PreviewPartRel	
SearchLinkRelType	Util
SearchLinkRelName	
TitleField1	Party
TitleField2	relationType
TableType	Regular
TableContents	Not specified
Systemtable	No
ConfigurationKey	LogisticsBasic
SecurityKey	DirAddressService
Visible	Yes
AQSAuthorization	None
CacheLookup	Found
CreateHectIndex	Yes
SaveDataPerCompany	No
SaveDataPerPartition	Yes
TableGroup	Main
PrimaryIndex	SurrogateKey
ClusterIndex	ValidCategory_AK

215

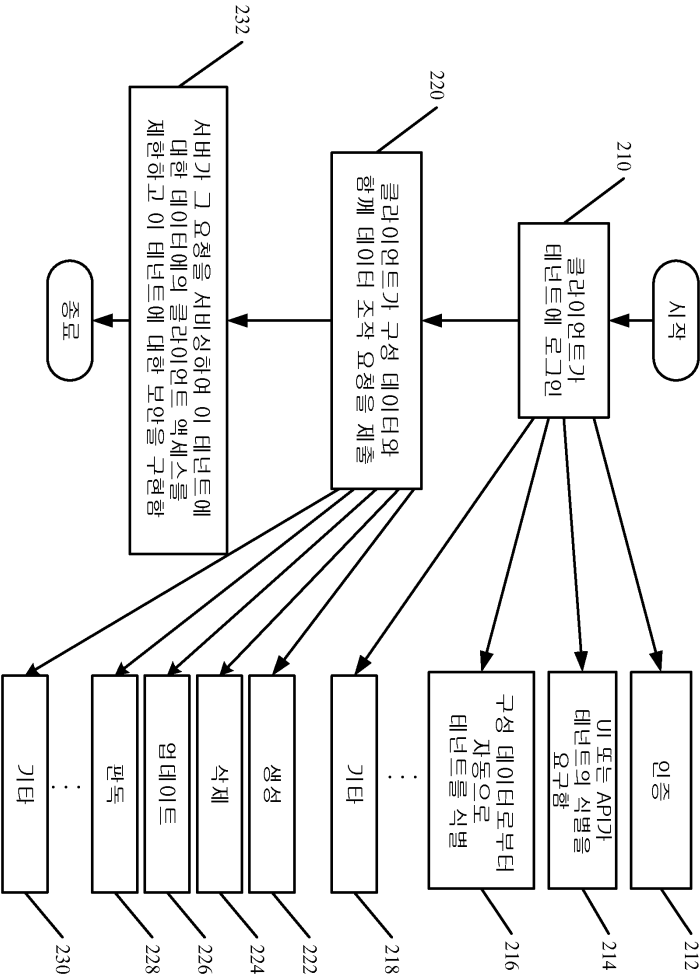
파티션 단위의 테이블

도면3c

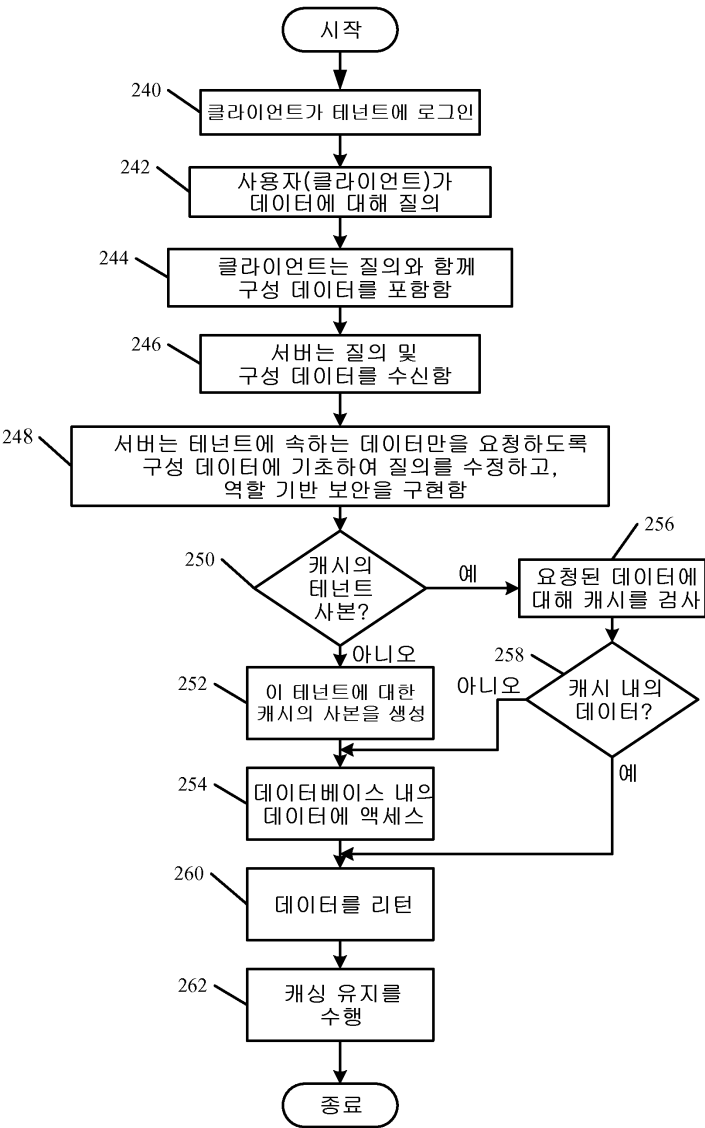


공유 테이블(시스템 전용)

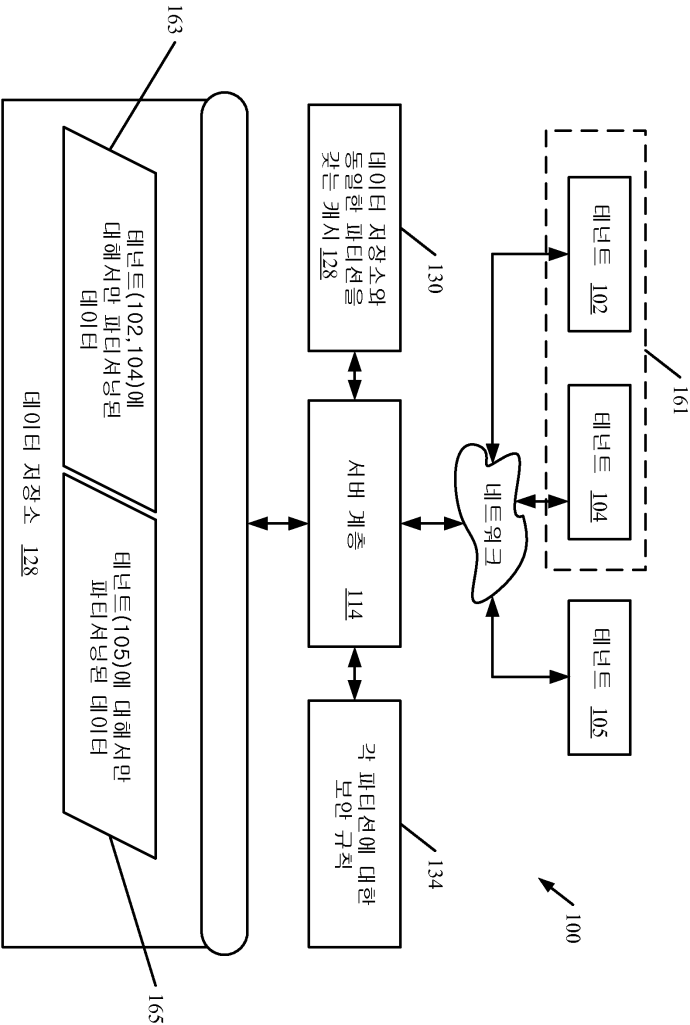
도면4



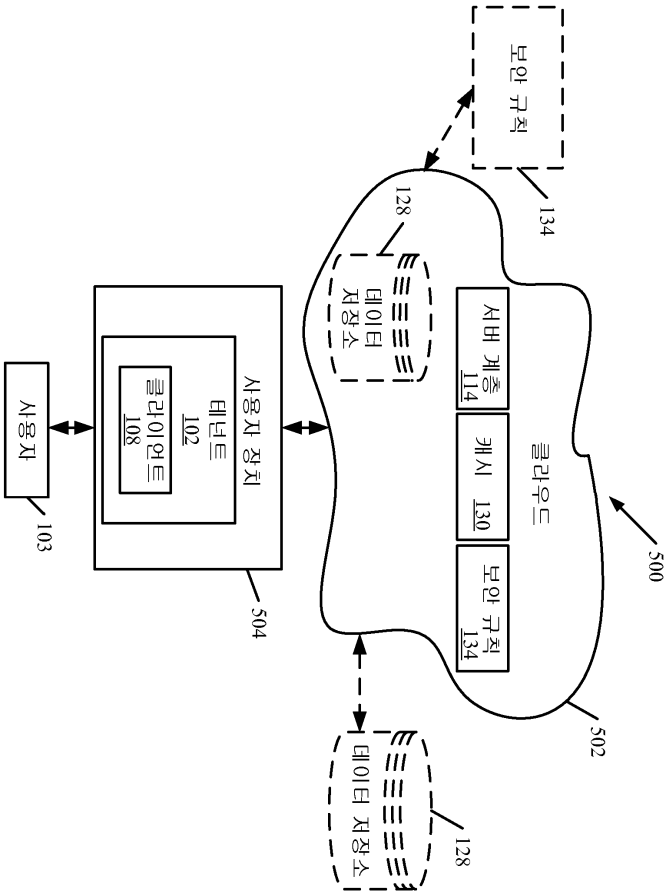
도면5



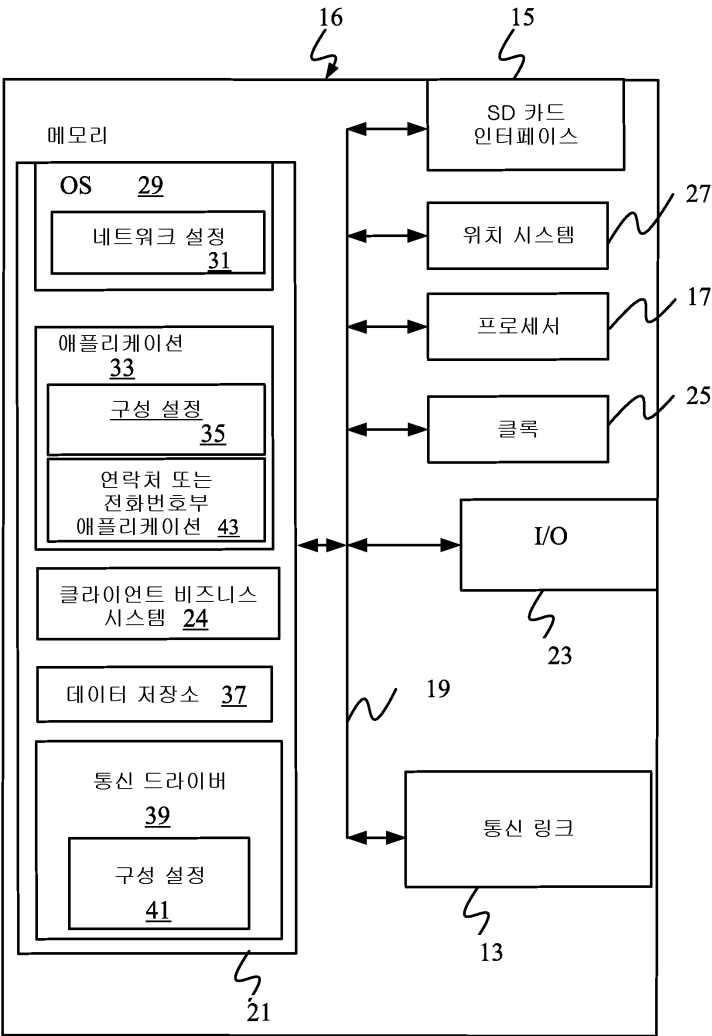
도면5a



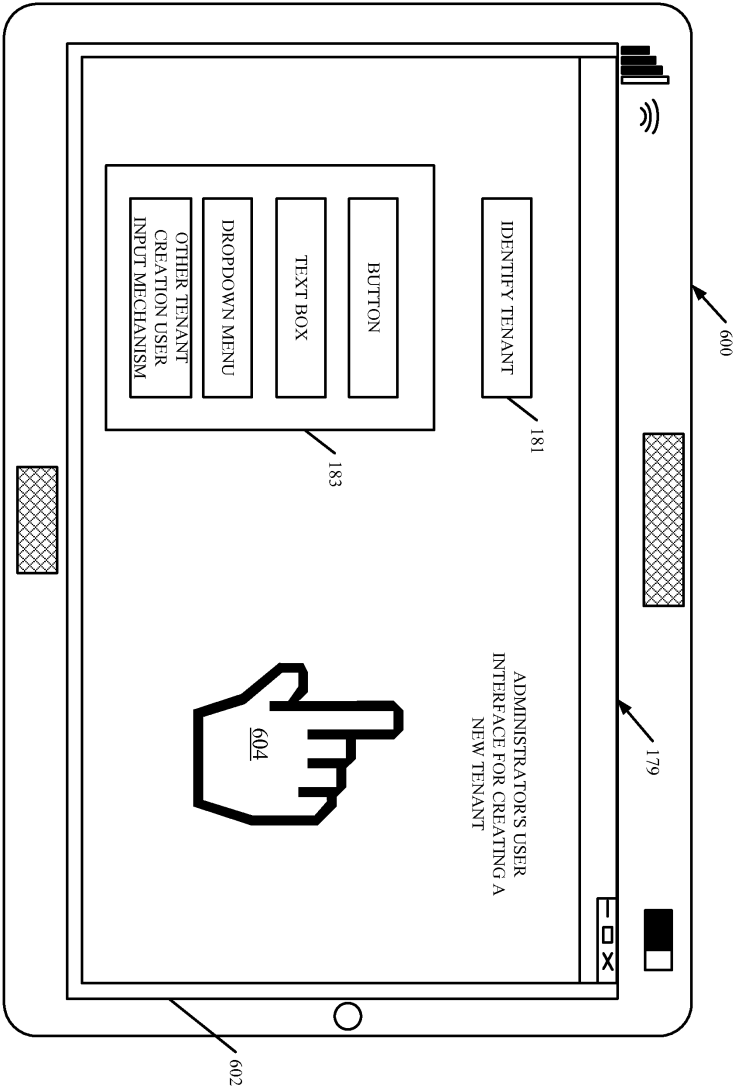
도면6



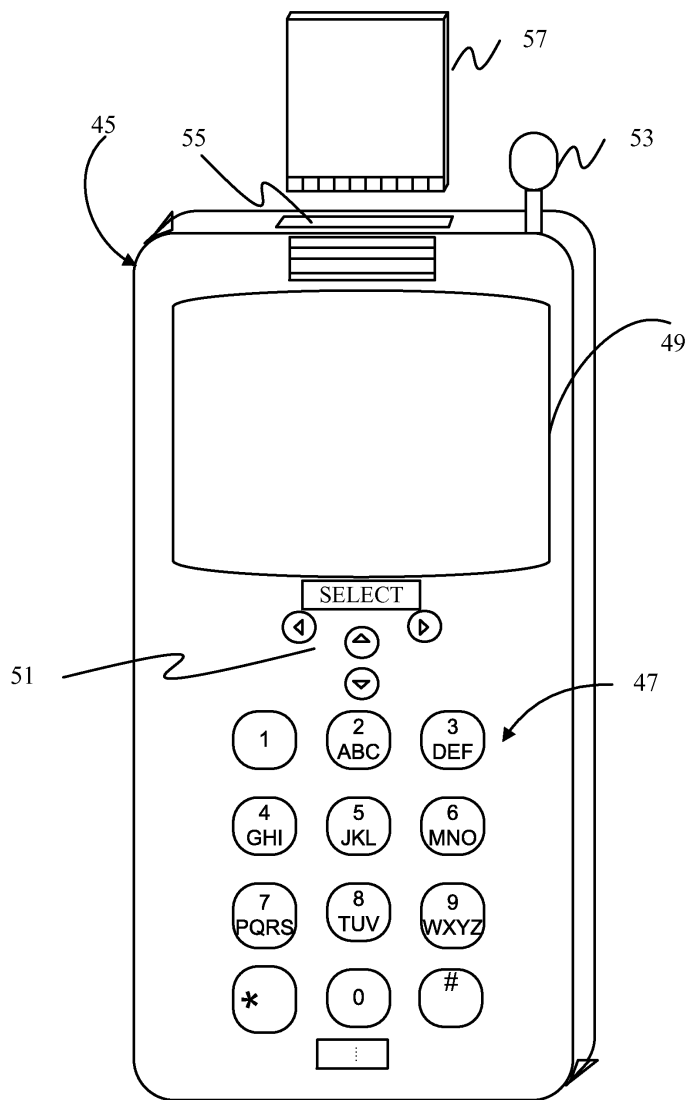
도면7



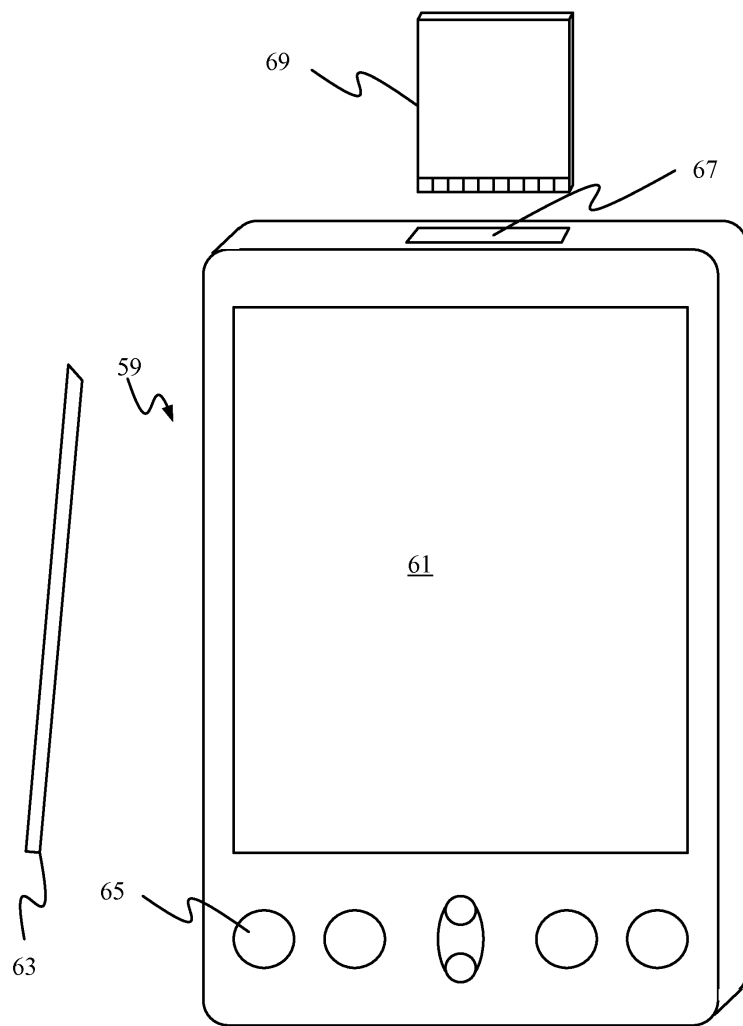
도면8



도면9



도면10



도면11

