(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년11월26일
(11) 등록번호 10-2037656
(24) 등록일자 2019년10월23일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *G06F 21/60* (2013.01)
(52) CPC특허분류
G06F 21/6218 (2013.01)
G06F 16/122 (2019.01)
(21) 출원번호 10-2017-7031893
(22) 출원일자(국제) 2016년05월19일
심사청구일자 2017년11월02일
(85) 번역문제출일자 2017년11월02일
(65) 공개번호 10-2017-0133485
(43) 공개일자 2017년12월05일
(86) 국제출원번호 PCT/US2016/033334
(87) 국제공개번호 WO 2016/196030
국제공개일자 2016년12월08일
(30) 우선권주장
201510295401.9 2015년06월02일 중국(CN)
15/158,423 2016년05월18일 미국(US)
(56) 선행기술조사문헌
US20110277013 A1*
US20130110967 A1*
US20140157363 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
알리바바 그룹 홀딩 리미티드
케이만군도, 그랜드 케이만, 피오박스 847, 원 캐피탈 플레이스 4층
(72) 발명자
린 창시옹
중국 311121 항저우 유 항 디스트릭트 969번 웨스트 웬 이로드 3 빌딩 5층 알리바바 그룹 리걸 디파트먼트
(74) 대리인
장훈

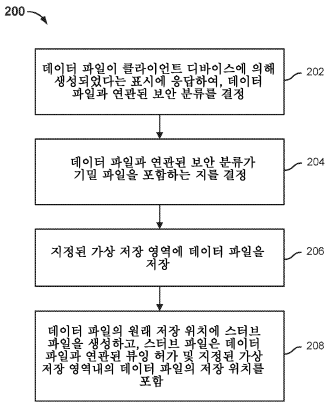
전체 청구항 수 : 총 18 항 심사관 : 정성훈

(54) 발명의 명칭 **데이터 파일들 보호**

(57) 요 약

데이터 파일들의 보호가 개시되고, 상기 데이터 파일들의 보호는: 데이터가 클라이언트 디바이스에 의해 생성되었다는 표시에 응답하여, 데이터 파일과 연관된 보안 분류를 결정하는 단계; 데이터 파일과 연관된 보안 분류가 기밀 파일을 포함하는 것을 결정하는 단계; 지정된 가상 저장 영역에 데이터 파일을 저장하는 단계; 및 데이터 파일의 원래 저장 위치에서 스터브 파일을 생성하는 단계를 포함하고, 스터브 파일은 데이터 파일과 연관된 뷰잉 허가 및 지정된 가상 저장 영역에 데이터 파일의 저장 위치를 포함한다.

대 표 도 - 도2



(52) CPC특허분류
G06F 21/604 (2013.01)
G06F 3/06 (2013.01)
H04L 29/00 (2019.05)
H04L 67/10 (2013.01)

명 세 서

청구범위

청구항 1

방법에 있어서:

하나 이상의 프로세서들을 사용하여, 데이터 파일이 제 1 클라이언트 디바이스에 의해 생성되었다는 표시에 응답하여, 상기 데이터 파일과 연관된 보안 분류를 결정하는 단계;

상기 하나 이상의 프로세서들을 사용하여, 상기 데이터 파일과 연관된 상기 보안 분류가 기밀 파일(classified file)을 포함하는지를 결정하는 단계;

상기 하나 이상의 프로세서들을 사용하여, 지정된 가상 저장 영역에 상기 데이터 파일을 저장하는 단계;

상기 데이터 파일의 원래 저장 위치에 제 1 스터브 파일(stub file)을 생성하는 단계로서, 상기 제 1 스터브 파일은 상기 데이터 파일과 연관된 뷰잉 허가 및 상기 지정된 가상 저장 영역 내의 상기 데이터 파일의 저장 위치를 포함하는, 상기 제 1 스터브 파일을 생성하는 단계;

제 2 사용자와 상기 데이터 파일을 공유하기 위해 제 1 사용자로부터 제 1 명령을 수신하는 단계;

상기 제 2 사용자와 연관된 사용자 정보를 결정하는 단계;

상기 제 2 사용자가 상기 제 2 사용자와 연관된 상기 사용자 정보에 적어도 부분적으로 기초하여 상기 데이터 파일에 액세스하기 위한 허가를 갖는지를 결정하는 단계; 및

상기 제 2 사용자와 연관된 제 2 클라이언트 디바이스에 제 2 명령을 전송하는 단계로서, 상기 제 2 명령은 상기 제 2 사용자와 연관된 상기 제 2 클라이언트 디바이스에서 상기 데이터 파일에 대응하는 제 2 스터브 파일을 생성하도록 구성되고, 상기 제 2 스터브 파일은 상기 지정된 가상 저장 영역 내의 상기 데이터 파일을 얻기 위해 사용되는, 상기 제 2 명령을 전송하는 단계를 포함하는, 방법.

청구항 2

제 1 항에 있어서,

상기 지정된 가상 저장 영역은 클라우드 서버와 연관되는, 방법.

청구항 3

제 1 항에 있어서,

상기 데이터 파일과 연관된 상기 보안 분류를 결정하는 단계는:

미리 설정된 조건에 대하여 상기 데이터 파일과 연관된 콘텐트 정보를 비교하는 단계; 및

상기 비교의 결과에 적어도 부분적으로 기초하여 상기 보안 분류를 결정하는 단계를 포함하는, 방법.

청구항 4

제 1 항에 있어서,

상기 데이터 파일과 연관된 상기 보안 분류는 제 3 사용자에 의해 설정되는, 방법.

청구항 5

제 1 항에 있어서,

상기 데이터 파일과 연관된 상기 원래 저장 위치에 상기 제 1 스터브 파일을 저장하는 단계를 더 포함하는, 방법.

청구항 6

제 1 항에 있어서,

상기 데이터 파일에 액세스하기 위해 상기 제 1 스터브 파일과 연관된 사용자 선택을 수신하는 단계;

상기 사용자 선택과 연관된 제 3 사용자가 상기 데이터 파일에 액세스하기 위한 허가를 갖는지의 여부를 결정하는 단계;

상기 제 3 사용자가 상기 데이터 파일에 액세스하기 위한 허가를 갖는 경우, 상기 데이터 파일에 대응하는 가상 애플리케이션을 실행하는 단계; 및

상기 가상 애플리케이션을 사용하여 상기 지정된 가상 저장 영역에 상기 데이터 파일에 대한 액세스를 제공하는 단계를 더 포함하는, 방법.

청구항 7

제 1 항에 있어서,

상기 데이터 파일에 액세스하기 위해 상기 제 1 스터브 파일과 연관된 사용자 선택을 수신하는 단계;

상기 사용자 선택과 연관된 제 3 사용자가 상기 데이터 파일에 액세스하기 위한 허가를 갖는지의 여부를 결정하는 단계;

상기 제 3 사용자가 상기 데이터 파일에 액세스하기 위한 허가를 갖는 경우, 상기 데이터 파일에 대응하는 가상 애플리케이션을 실행하는 단계; 및

상기 지정된 가상 저장 영역과 연관된 클라우드 서버에 상기 제 1 스터브 파일에 포함된 정보를 송신하고, 상기 클라우드 서버로부터 문서 편집기 프로그램과 연관된 사용자 인터페이스를 수신함으로써, 상기 가상 애플리케이션을 사용하여 상기 지정된 가상 저장 영역의 상기 데이터 파일에 대한 액세스를 제공하는 단계를 더 포함하는, 방법.

청구항 8

제 1 항에 있어서,

상기 데이터 파일에 액세스하기 위해 상기 제 1 스터브 파일과 연관된 사용자 선택을 수신하는 단계;

상기 사용자 선택과 연관된 제 3 사용자가 상기 데이터 파일에 액세스하기 위한 허가를 갖는지의 여부를 결정하는 단계;

상기 제 3 사용자가 상기 데이터 파일에 액세스하기 위한 허가를 갖는 경우, 상기 데이터 파일에 대응하는 가상 애플리케이션을 실행하는 단계; 및

상기 지정된 가상 저장 영역과 연관된 클라우드 서버에 상기 제 1 스터브 파일에 포함된 정보를 송신하고, 상기 클라우드 서버로부터 문서 편집기 프로그램과 연관된 사용자 인터페이스를 수신하고, 상기 사용자 인터페이스를 통해 상기 데이터 파일에 대해 수행될 동작을 수신하고, 상기 클라우드 서버에 상기 동작을 전송함으로써 포함하는 상기 가상 애플리케이션을 사용하여 상기 지정된 가상 저장 영역의 상기 데이터 파일에 대한 액세스를 제공하는 단계를 더 포함하는, 방법.

청구항 9

삭제

청구항 10

컴퓨터 명령들을 포함하는 컴퓨터 프로그램이 저장된 비-일시적 컴퓨터 판독 가능 저장 매체에 있어서,

상기 컴퓨터 명령들은:

데이터 파일이 제 1 클라이언트 디바이스에 의해 생성되었다는 표시에 응답하여, 상기 데이터 파일과 연관된 보안 분류를 결정하고;

상기 데이터 파일과 연관된 상기 보안 분류가 기밀 파일을 포함하는지를 결정하고;

지정된 가상 저장 영역에 상기 데이터 파일을 저장하고;

상기 데이터 파일의 원래의 저장 위치에 제 1 스터브 파일을 생성하는 것으로서, 상기 제 1 스터브 파일은 상기 지정된 가상 저장 영역에 상기 데이터 파일의 저장 위치 및 상기 데이터 파일과 연관된 뷰잉 허가를 포함하는, 상기 제 1 스터브 파일을 생성하고;

상기 데이터 파일을 제 2 사용자와 공유하기 위해 제 1 사용자로부터 제 1 명령을 수신하고;

상기 제 2 사용자와 연관된 사용자 정보를 결정하고;

상기 제 2 사용자가 상기 제 2 사용자와 연관된 상기 사용자 정보에 적어도 부분적으로 기초하여 상기 데이터 파일에 액세스하기 위한 허가를 갖는지를 결정하고;

상기 제 2 사용자와 연관된 제 2 클라이언트 디바이스에 제 2 명령을 전송하는 것으로서, 상기 제 2 명령은 상기 제 2 사용자와 연관된 상기 제 2 클라이언트 디바이스에서 상기 데이터 파일에 대응하는 제 2 스터브 파일을 생성하도록 구성되고, 상기 제 2 스터브 파일은 상기 지정된 가상 저장 영역 내의 상기 데이터 파일을 얻기 위해 사용되는, 상기 제 2 명령을 전송하는 것을 위한 것인, 비-일시적 컴퓨터 판독 가능 저장 매체.

청구항 11

제 10 항에 있어서,

상기 지정된 가상 저장 영역은 클라우드 서버와 연관되는, 비-일시적 컴퓨터 판독 가능 저장 매체.

청구항 12

제 10 항에 있어서,

상기 데이터 파일과 연관된 상기 보안 분류를 결정하는 것은:

미리 설정된 상태에 대해 상기 데이터 파일과 연관된 콘텐트 정보를 비교하는 것; 및

상기 비교의 결과에 적어도 부분적으로 기초하여 상기 보안 분류를 결정하는 것을 포함하는, 비-일시적 컴퓨터 판독 가능 저장 매체.

청구항 13

제 10 항에 있어서,

상기 데이터 파일과 연관된 상기 보안 분류는 제 3 사용자에 의해 설정되는, 비-일시적 컴퓨터 판독 가능 저장 매체.

청구항 14

제 10 항에 있어서,

상기 데이터 파일과 연관된 상기 원래의 저장 위치에 상기 제 1 스터브 파일을 저장하는 것을 더 위한 것인, 비-일시적 컴퓨터 판독 가능 저장 매체.

청구항 15

제 10 항에 있어서,

상기 데이터 파일에 액세스하기 위해 상기 제 1 스터브 파일과 연관된 사용자 선택을 수신하고;

상기 사용자 선택과 연관된 제 3 사용자가 상기 데이터 파일에 액세스하기 위한 허가를 갖는지의 여부를 결정하고;

상기 제 3 사용자가 상기 데이터 파일에 액세스하기 위한 허가를 갖는 경우, 상기 데이터 파일에 대응하는 가상 애플리케이션을 실행하고; 및

상기 가상 애플리케이션을 사용하여 상기 지정된 가상 저장 영역의 데이터 파일에 대한 액세스를 제공하는 것을 더 위한 것인, 비-일시적 컴퓨터 판독 가능 저장 매체.

청구항 16

제 10 항에 있어서,

상기 데이터 파일에 액세스하기 위해 상기 제 1 스터브 파일과 연관된 사용자 선택을 수신하고;

상기 사용자 선택과 연관된 제 3 사용자가 상기 데이터 파일에 액세스하기 위한 허가를 갖는지의 여부를 결정하고;

상기 제 3 사용자가 상기 데이터 파일에 액세스하기 위한 허가를 갖는 경우, 상기 데이터 파일에 대응하는 가상 애플리케이션을 실행하고; 및

상기 지정된 가상 저장 영역과 연관된 클라우드 서버에 상기 제 1 스터브 파일에 포함된 정보를 송신하고, 상기 클라우드 서버로부터 문서 편집기 프로그램과 연관된 사용자 인터페이스를 수신하는 것을 포함하는 상기 가상 애플리케이션을 사용하여 상기 지정된 가상 저장 영역의 상기 데이터 파일에 대한 액세스를 제공하는 것을 더 위한 것인, 비-일시적 컴퓨터 판독 가능 저장 매체.

청구항 17

제 10 항에 있어서,

상기 데이터 파일에 액세스하기 위해 상기 제 1 스터브 파일과 연관된 사용자 선택을 수신하고;

상기 사용자 선택과 연관된 제 3 사용자가 상기 데이터 파일에 액세스하기 위한 허가를 갖는지의 여부를 결정하고;

상기 제 3 사용자가 상기 데이터 파일에 액세스하기 위한 허가를 갖는 경우, 상기 데이터 파일에 대응하는 가상 애플리케이션을 실행하고; 및

상기 지정된 가상 저장 영역과 연관된 클라우드 서버로 상기 제 1 스터브 파일에 포함된 정보를 송신하고, 상기 클라우드 서버로부터 문서 편집기 프로그램과 연관된 사용자 인터페이스를 수신하고, 상기 사용자 인터페이스를 통해 상기 데이터 파일에 대해 수행될 동작을 수신하고, 상기 클라우드 서버에 상기 동작을 전송하는 것을 포함하는 상기 가상 애플리케이션을 사용하여 상기 지정된 가상 저장 영역의 상기 데이터 파일에 대한 액세스를 제공하는 것을 더 위한 것인, 비-일시적 컴퓨터 판독 가능 저장 매체.

청구항 18

삭제

청구항 19

시스템에 있어서,

하나 이상의 프로세서들을 포함하고,

상기 하나 이상의 프로세서들은:

데이터 파일이 제 1 클라이언트 디바이스에 의해 생성되었다는 표시에 응답하여, 상기 데이터 파일과 연관된 보안 분류를 결정하고;

상기 데이터 파일과 연관된 상기 보안 분류가 기밀 파일을 포함하는지를 결정하고;

지정된 가상 저장 영역에 상기 데이터 파일을 저장하고;

상기 데이터 파일의 원래의 저장 위치에 제 1 스터브 파일을 생성하는 것으로서, 상기 제 1 스터브 파일은 상기 지정된 가상 저장 영역에 상기 데이터 파일의 저장 위치 및 상기 데이터 파일과 연관된 뷰잉 허가를 포함하는, 상기 제 1 스터브 파일을 생성하고;

상기 데이터 파일을 제 2 사용자와 공유하기 위해 제 1 사용자로부터 제 1 명령을 수신하고;

상기 제 2 사용자와 연관된 사용자 정보를 결정하고;

상기 제 2 사용자가 상기 제 2 사용자와 연관된 상기 사용자 정보에 적어도 부분적으로 기초하여 상기

데이터 파일에 액세스하기 위한 허가를 갖는지를 결정하고;

상기 제 2 사용자와 연관된 제 2 클라이언트 디바이스에 제 2 명령을 전송하는 것으로서, 상기 제 2 명령은 상기 제 2 사용자와 연관된 상기 제 2 클라이언트 디바이스에서 상기 데이터 파일에 대응하는 제 2 스터브 파일을 생성하도록 구성되고, 상기 제 2 스터브 파일은 상기 지정된 가상 저장 영역 내의 상기 데이터 파일을 얻기 위해 사용되는, 상기 제 2 명령을 전송하도록 구성되는, 시스템.

청구항 20

제 19 항에 있어서,

상기 지정된 가상 저장 영역은 클라우드 서버와 연관되는, 시스템.

발명의 설명

기 술 분 야

[0001] 본 출원은 모든 목적을 위해 참조로서 여기에 통합된 2015년 6월 2일에 출원된 발명의 명칭이 "데이터 파일들을 보호하기 위한 방법, 장치 및 단말 장비"인 중화 인민 공화국 출원 번호 제 201510295401.9 호에 대한 우선권을 주장한다.

[0002] 본 출원은 인터넷 기술의 분야에 관한 것이다. 특히, 본 출원들은 데이터 파일들을 보호하기 위한 기술들에 관한 것이다.

배 경 기 술

[0003] 인터넷의 자유롭고 개방적인 환경에서, 데이터 사용, 저장, 및 송신 모두는 누설들의 위험을 제공한다. 종래에, 데이터는 투명한 파일 암호 및 복호 방법들에 의해 보호된다. 특히, 데이터 보호의 종래 기술의 일 예는 다음을 포함한다: 클라이언트 디바이스 운영 시스템이 기저 레벨 처리를 수행하는 동안, 데이터 파일은 암호화 처리가 된다. 사용자가 데이터 파일을 검색할 때, 운영 체계는 데이터 파일을 복호화하고 이후 사용자의 사용을 위해 그를 메모리에 배치한다. 사용자가 데이터 파일을 저장할 필요가 있을 때, 운영 시스템은 데이터 파일을 암호화하고 그를 자기 디스크로 기록하고, 그에 의해 사용자가 데이터 파일에 대해 수행된 암호 및 복호 동작들을 완전히 인식하지 못한다. 따라서, 종래에는, 데이터 누설들이 암호화된 데이터가 자기 디스크에 기록하고 메모리에서 데이터의 암호를 수행함으로써 방지된다.

발명의 내용

해결하려는 과제

[0004] 그러나, 이들 종래 기술들은 메모리 내의 파일이 누설되지 않는 것을 보장하지 않는다.

과제의 해결 수단

[0005] 본 발명은 장치; 시스템; 물질의 조성; 컴퓨터 판독 가능한 저장 매체상에 구현된 컴퓨터 프로그램 제품; 및/또는 프로세서에 연결된 메모리상에 저장되고 및/또는 그에 의해 제공된 명령들을 실행하도록 구성된 프로세서와 같은, 프로세서를 프로세스로서 포함하는 다수의 방식들로 구현될 수 있다. 본 명세서에서, 이들 구현들, 또는 본 발명이 취할 수 있는 임의의 다른 형태는 기술들이라고 칭해질 수 있다. 일반적으로, 개시된 프로세스들의 단계들의 순서는 본 발명의 범위 내에서 변경될 수 있다. 달리 언급되지 않으면, 태스크를 수행하도록 구성되는 것으로 설명되는 프로세서 또는 메모리와 같은 구성 요소는 태스크를 수행하도록 제작되는 특정한 구성 요소 또는 주어진 시간에 태스크를 수행하도록 시간적으로 구성되는 일반적인 구성 요소로서 구현될 수 있다. 여기에서 사용된 바와 같은, 용어 '프로세서'는 컴퓨터 프로그램 명령들과 같은 데이터를 처리하도록 구성된 하나 이상의 디바이스들, 회로들, 및/또는 처리 코어들을 지칭한다.

[0006] 본 발명의 하나 이상의 실시예들의 상세한 설명은 본 발명의 원리들을 예시하는 첨부하는 도면들과 함께 이하에 제공된다. 본 발명은 이러한 실시예와 함께 설명되지만, 본 발명은 임의의 실시예로 한정되지 않는다. 본 발명의 범위는 청구항들에 의해서만 한정되고, 본 발명은 다수의 대안들, 변경들, 및 동등물들을 포함한다. 다수의 상세한 설명들은 본 발명의 완전한 이해를 제공하기 위해 다음의 상세한 설명에서 설명된다. 이들 상세들은 예시의 목적들을 위해 제공되고 본 발명은 이들 특정한 상세들의 일부 또는 전부 없이 청구항들에 따라 실시될 수

있다. 명확성의 목적을 위해, 본 발명에 관련된 기술 분야들에서 알려진 기술적인 자료는 본 발명이 불필요하게 모호해지지 않도록 상세하게 설명되지 않는다.

[0007] 예시적인 실시예들이 여기에 상세히 설명될 것이다. 그의 예들은 도면들에 나타내진다. 다음의 설명들은 도면들에 관련하는 경우들에, 상이한 도면들의 동일한 번호들은 달리 표시되지 않으면 동일하거나 유사한 요소들을 나타낸다. 예시적인 실시예들에 설명된 구현들은 본 출원과 일치하는 구현들 모두를 나타내지는 않는다. 반대로, 그들은 단순히 청구항들에서 상세히 설명되는 본 출원의 일부 양태들과 일치하는 디바이스들 및 방법들의 예들이다.

[0008] 본 출원에서 사용된 용어들은 단순히 특정한 실시예들을 설명하는 역할을 하고, 본 출원을 제한하도록 의도되지 않는다. 본 출원 및 첨부된 청구항들에서 사용되는 단일 형태들은 또한 문맥에서 달리 명확하게 표시되지 않으면 복수 형태들을 포함하도록 의도된다. 또한, 본 문서에서 사용된 용어 "및/또는"이 하나 이상의 연관된 요소들 중 어느 하나 또는 모든 가능한 조합들을 지칭하고 그를 포함한다는 것을 이해해야 한다.

[0009] 본 출원은 다양한 정보를 설명하기 위해 용어들 "제 1", "제 2", "제 3" 등을 채용하지만, 이러한 정보는 이들 용어들에 의해 한정되지 않아야 한다는 것을 이해해야 한다. 이들 용어들은 단순히 동일한 카테고리의 정보의 부분들을 구별하는 역할을 한다. 예를 들면, 그들이 본 출원의 범위 내에 있는 한, 정보의 제 1 부분은 정보의 제 2 부분이라고 불릴 수 있다. 유사하게, 정보의 제 2 부분은 정보의 제 1 부분이라고 불릴 수 있다. 문맥에 따라, 예를 들면, 여기에 사용된 용어 "~인 경우"는 "~때" 또는 "~가 확인되면"이라고 해석될 수 있다.

[0010] 데이터 파일들을 보호하는 것의 실시예들이 여기에 설명된다. 클라이언트 디바이스에서 데이터 파일들의 생성의 표시에 응답하여, 데이터 파일과 연관된 보안 분류가 결정된다. 데이터 파일과 연관된 보안 분류는 기밀 파일(classified file)인지가 결정된다. 데이터 파일은 이후 지정된 가상 저장 영역에 저장된다. 예를 들면, 지정된 가상 저장 영역은 클라우드 서버의 일부분이다. 다양한 실시예들에서, "클라우드 서버"는 하나 이상의 서비스들을 제공하기 위해 협력하여 작동하는 하나 이상의 서버들을 지칭한다. 스터브 파일은 데이터 파일의 원래의 저장 위치에 생성된다. 또한, 데이터 파일의 사본은 클라이언트 디바이스로부터 제거/삭제된다. 스터브 파일은 데이터 파일과 연관된 뷰잉 허가(viewing permission) 및 지정된 가상 저장 영역 내의 데이터 파일의 저장 위치를 포함하지만, 데이터 파일의 실제 콘텐트가 아니다. 스터브 파일이 데이터 파일 자체로부터의 임의의 데이터를 포함하지 않기 때문에, 클라이언트 디바이스의 스터브 파일에 대해 사용자에 의해 수행된 임의의 동작들은 클라우드 서버에 저장되는 데이터 파일에 어떤 영향도 주지 않을 것이다.

도면의 간단한 설명

[0011] 도 1은 데이터 파일들을 보호하기 위한 시스템의 일 실시예를 도시하는 도면.

도 2는 데이터 파일들을 보호하기 위한 프로세스의 일 실시예를 도시하는 흐름도.

도 3은 보호된 데이터 파일을 공유하기 위한 프로세스의 일 실시예를 도시하는 흐름도.

도 4는 보호된 데이터 파일을 사용하기 위한 프로세스의 일 실시예를 도시하는 흐름도.

도 5는 보호된 데이터 파일에 액세스하기 위한 프로세스의 일 예를 도시하는 흐름도.

도 6은 데이터 파일들을 보호하기 위한 일 예시적인 클라이언트 디바이스를 도시하는 도면.

도 7은 데이터 파일들을 보호하기 위한 일 예시적인 클라이언트 디바이스를 도시하는 도면.

도 8은 데이터 파일들을 보호하기 위한 일 예시적인 클라이언트 디바이스를 도시하는 도면.

도 9는 일 예시적인 데이터 파일 검색 디바이스를 도시하는 도면.

도 10은 일 예시적인 데이터 파일 검색 디바이스를 도시하는 도면.

도 11은 데이터 파일들을 보호하기 위해 프로그래밍된 컴퓨터 시스템을 도시하는 기능도.

발명을 실시하기 위한 구체적인 내용

[0012] 본 발명의 다양한 실시예들이 다음의 상세한 설명 및 첨부하는 도면들에서 개시된다.

[0013] 도 1은 데이터 파일들을 보호하기 위한 시스템의 일 실시예를 도시하는 도면이다. 예에서, 시스템(100)은 클라이언트 디바이스(102), 네트워크(104), 및 클라우드 서버(106)를 포함한다. 일부 실시예들에서, 네트워크(104)

는 고속 네트워크들 및/또는 원격 통신 네트워크들을 포함한다.

[0014] 클라이언트 디바이스(102)는 데이터 파일을 생성한다. 클라이언트 디바이스(102)의 예들은 이동 장치, 스마트 폰들, 랩탑 컴퓨터, 데스크톱 컴퓨터, 태블릿 장치, 또는 임의의 컴퓨팅 장치를 포함한다. 일부 실시예들에서, 클라이언트 디바이스(102)는 다른 클라이언트 디바이스로부터 데이터 파일을 수신함으로써 데이터 파일을 생성한다. 일부 실시예들에서, 클라이언트 디바이스(102)는 데이터 파일을 클라이언트 디바이스(102)에서 수신된 메시지로부터의 첨부로서 다운로딩 및 웹사이트로부터 데이터 파일을 다운로딩함으로써 데이터 파일을 생성할 수 있다. 데이터 파일은 임의의 적절한 방식으로 클라이언트 디바이스(102)에 생성될 수 있다. 클라이언트 디바이스(102)는 수신된 데이터 파일과 연관된 보안 분류를 결정한다. 보안 분류는 데이터 파일이 기밀 파일인 것을 나타낸다. 데이터 파일이 기밀 파일이라는 것을 결정하는 것에 응답하여, 클라이언트 디바이스(102)는 지정된 가상 저장 영역에 데이터 파일을 저장하도록 구성된다. 다양한 실시예들에서, 지정된 저장 영역은 클라우드 서버(106)의 디스크(또는 고체 상태) 저장 장치이다. 클라이언트 디바이스(102)가 네트워크(104)를 통해 데이터 파일을 클라우드 서버(106)로 전송한 후, 클라이언트 디바이스(102)는 데이터 파일과 연관된 스터브 파일을 생성하고, 데이터 파일의 그의 사본을 제거하고, 클라이언트 디바이스(102)의 데이터 파일의 원래의 저장 위치에 스터브 파일을 저장한다. 이와 같이, 클라이언트 디바이스(102)가 클라우드 서버(106)에 데이터 파일을 업로딩하면, 클라이언트 디바이스(102)는 더 이상 데이터 파일의 사본을 보유하지 않고 데이터 파일과 연관되는 스터브 파일만을 보유한다. 클라우드 서버(106)가 데이터 파일을 성공적으로 저장하면, 클라우드 서버(106)는 네트워크(104)를 통해 지정된 가상 저장 영역에서의 데이터 파일의 저장 위치를 클라이언트 디바이스(102)로 전송하도록 구성된다. 다양한 실시예들에서, 스터브 파일은 데이터 파일과 연관된 뷰잉 허가 및 클라우드 서버(106)의 지정된 가상 저장 영역에서의 데이터 파일의 저장 위치를 포함한 데이터 파일과 연관된 다양한 정보를 기록한다. 데이터 파일과 연관된 뷰잉 허가는 어느 개별적인 사용자들 및/또는 사용자 역할들이 데이터 파일에 액세스(예를 들면, 판독, 기록, 판독 및 기록)할 수 있는지를 특정한다.

[0015] 데이터 파일에 액세스하기 위해, 클라이언트 디바이스(102)의 사용자는 클라이언트 디바이스(102)에서 실행하는 가상화된 제어 및 관리 애플리케이션을 사용하여 스터브 파일을 선택하도록 구성된다. 예를 들면, 클라이언트 디바이스(102)의 사용자는 클라이언트 디바이스(102)에서 가상화된 제어 및 관리 애플리케이션을 통해 클라우드 서버(106)에 저장되는 데이터 파일들의 스터브 파일들을 브라우징할 수 있다. 클라이언트 디바이스(102)의 사용자는 액세스할 데이터 파일에 대응하는 스터브 파일을 선택할 수 있다. 스터브 파일을 공유하기 위한 사용자의 선택에 응답하여, 가상화된 제어 및 관리 애플리케이션은 클라이언트 디바이스(102)의 사용자가 선택된 스터브 파일에 기록되는 뷰잉 허가와 사용자의 식별 정보를 비교함으로써 데이터 파일에 액세스하기 위한 허가를 갖는지의 여부를 결정하도록 구성된다. 예를 들면, 사용자의 식별 정보가 선택된 스터브 파일에 의해 스터브 파일을 판독할 것이 적어도 허가되도록 특정된 경우, 가상화된 제어 및 관리 애플리케이션은 액세스 동작을 허가하도록 구성된다. 사용자가 데이터 파일에 액세스할 수 있다고 결정되는 경우, 가상 애플리케이션은 클라이언트 디바이스(102)에서 론칭/실행하고 클라우드 서버(106)와 접속을 확립하도록 구성된다. 클라이언트 디바이스(102)의 사용자는 데이터 파일에 대해 단어 처리 동작들을 수행함으로써 포함하는 클라우드 서버(106)에 저장된 데이터 파일에 액세스하기 위해 클라이언트 디바이스(102)에서 실행하는 가상 애플리케이션을 사용할 수 있다. 가상 애플리케이션은 클라이언트 디바이스(102)의 운영 시스템으로부터 분리되고, 이는 가상 애플리케이션 내에 수행된 동작들이 클라이언트 디바이스(102)의 저장 장치 및/또는 클라이언트 디바이스(102)의 메모리로부터 분리된다는 것을 의미한다.

[0016] 일부 실시예들에서, 클라이언트 디바이스(102)의 사용자는 클라이언트 디바이스(102)에서 실행하는 가상화된 제어 및 관리 애플리케이션을 사용하여 다른 클라이언트 디바이스(도면에 도시되지 않음)와 데이터 파일을 공유할 수 있다. 클라이언트 디바이스(102)의 사용자는 다른 클라이언트 디바이스와 연관된 사용자와 공유할 데이터 파일에 대응하는 스터브 파일을 선택할 수 있다. 스터브 파일을 공유하기 위한 사용자의 선택에 응답하여, 가상화된 제어 및 관리 애플리케이션은 데이터 파일이 공유될 다른 사용자가 선택된 스터브 파일에 기록되는 뷰잉 허가와 다른 사용자의 식별 정보를 비교함으로써 데이터 파일에 액세스하기 위한 허가를 갖는지의 여부를 결정하도록 구성된다. 예를 들면, 사용자의 식별 정보가 선택된 스터브 파일에 의해 스터브 파일을 판독할 것이 적어도 허가되도록 특정되는 경우, 가상화된 제어 및 관리 애플리케이션은 공유 동작을 허가하도록 구성된다. 다른 사용자가 데이터 파일에 액세스할 수 있다는 것이 결정되는 경우, 가상화된 제어 및 관리 애플리케이션이 데이터 파일이 공유될 사용자의 클라이언트 디바이스에 명령을 전송하도록 구성된다. 전송된 명령은 다른 사용자가 스터브 파일을 사용하여 클라우드 서버(106)의 데이터 파일에 액세스할 수 있도록 데이터 파일이 공유될 사용자의 클라이언트 디바이스에 선택된 스터브 파일의 사본을 생성하도록 구성된다.

[0017] 이와 같이, 클라이언트 디바이스(102)로부터 액세스를 제공하면서 클라우드 서버(106)의 지정된 가상 저장 영역에 기밀 데이터 파일을 저장하는 것은 따라서 가상 환경에서 데이터 파일에 대해 수행된 동작들을 분리할 수 있다. 따라서, 가상 환경의 사용은 적절한 액세스 허가들 없이 또는 클라이언트 디바이스(102)를 조작함으로써 사용자 및/또는 프로그램에 의해 클라이언트 디바이스(102)의 데이터 파일에 임의의 악의적인 액세스들을 방지할 수 있다. 스터브 파일이 데이터 파일에 대한 뷰잉 허가 및 지정된 가상 저장 영역에서 데이터 파일의 저장 위치를 기록하지만 데이터 파일 자체로부터 어떠한 데이터도 포함하지 않기 때문에, 클라이언트 디바이스(102)에 저장되는 스터브 파일에 대해 사용자에 의해 수행된 임의의 동작들은 클라우드 서버(106)에 저장된 데이터 파일에 대해 어떠한 효과도 갖지 않을 것이다.

[0018] 도 2는 데이터 파일들을 보호하기 위한 프로세스의 일 실시예를 도시하는 흐름도이다. 일부 실시예들에서, 프로세스(200)는 도 1의 시스템(100)에서 구현된다.

[0019] 202에서, 데이터 파일이 클라이언트 디바이스에 의해 생성되었다는 표시에 응답하여, 데이터 파일과 연관된 보안 분류가 결정된다.

[0020] 예를 들면, 데이터 파일은 새로운 파일을 복사하거나, 새로운 파일을 다운로딩하거나, 새로운 파일을 생성하는 것을 통해 클라이언트 디바이스에서 생성될 수 있다.

[0021] 다양한 실시예들에서, 데이터 파일의 보안 분류는 예를 들면 파일을 생성한 사용자와 같은 사용자에 의해 설정된다. 일부 실시예들에서, 데이터 파일의 보안 분류는 데이터 파일의 비밀 등급을 포함한다. 예를 들면, 보안 분류는 레벨 0, 레벨 1, 또는 레벨 2로 설정될 수 있고, 각각의 레벨은 데이터 파일에 관하여 상이한 비밀 등급을 나타낸다. 예를 들면, 레벨 0은 사용자가 데이터 파일에 대한 보안 수단을 채용할 필요가 없다는 것을 나타내고, 레벨 1은 사용자가 데이터 파일에 대한 보안 수단을 취할 필요가 있다는 것을 나타낸다. 다른 예에서, 레벨 0은 사용자가 데이터 파일에 대해 보안 수단을 채용할 필요가 없다는 것을 나타내고, 레벨 1은 사용자가 클라이언트 디바이스상의 데이터 파일에 대한 보안 수단을 채용할 필요가 있다는 것을 나타내고, 레벨 2는 사용자가 클라이언트 디바이스 및 클라우드 서버상의 데이터 파일에 대한 보안 수단을 채용할 필요가 있다는 것을 나타낸다.

[0022] 일부 실시예들에서, 데이터 파일의 콘텐트 정보는 데이터 파일과 연관된 보안 분류를 결정할 것이 먼저 결정될 수 있다. 예를 들면, 데이터 파일의 콘텐트 정보는 제 1 미리 설정된 상태에 대해 매칭될 수 있고, 데이터 파일의 보안 분류는 제 1 매칭 결과에 따라 결정된다. 예를 들면, 제 1 미리 설정된 상태는 다수의 주요 어구들, 예컨대 "암호화된", "사적인", 또는 "비공개적인"을 포함할 수 있다. 시스템이 데이터 파일의 콘텐트 정보가 "암화화된" 또는 "사적인" 것과 같은 콘텐트를 포함한다는 것을 검출할 때, 제 1 매칭 결과에 따라 데이터 파일의 보안 분류는 레벨 1인 것으로 결정되고, 이는 사용자가 데이터 파일에 대한 보안 수단을 취할 필요가 있다는 것을 나타낸다. 콘텐트 정보가 전술한 주요 어구들을 포함하지 않는 경우, 제 1 매칭 결과에 따라 데이터의 분류 레벨이 레벨 0인 것을 결정하는 것이 가능하고, 레벨 0은 사용자가 데이터 파일에 대한 보안 수단을 취할 필요가 없다는 것을 나타낸다. 제 2 예에서, 데이터 파일의 파일명은 제 2 미리 설정된 상태에 대해 매칭될 수 있고, 데이터 파일의 보안 분류는 제 2 매칭 결과에 따라 결정된다. 예를 들면, 제 2 미리 설정된 상태는 "비밀" 또는 "암호화된" 것과 같은 다수의 주요 어구들을 포함할 수 있다. 시스템이 데이터 파일의 파일명이 "비밀" 또는 "암호화된" 것과 같은 콘텐트를 포함한다는 것을 검출한 경우, 제 1 매칭 결과에 따른 데이터 파일의 보안 분류는 레벨 1로 결정될 수 있고, 레벨 1은 사용자가 데이터 파일에 대해 보안 수단이 필요하다는 것을 나타낸다. 파일명이 전술한 주요 어구들을 포함하지 않는 경우, 제 2 매칭 결과에 따른 데이터의 분류 레벨이 레벨 0인 것을 결정할 수 있고, 레벨 0은 사용자가 데이터 파일에 대한 보안 수단을 취할 필요가 없다는 것을 나타낸다.

[0023] 204에서, 데이터 파일과 연관된 보안 분류가 기밀 파일을 포함한다는 것이 결정된다.

[0024] 데이터 파일과 연관된 보안 분류는 상기에 설명된 것과 같은 기술에 기초하여 결정되고, 데이터 파일이 보안 분류에 기초한 기밀 파일임이 결정된다.

[0025] 데이터 파일이 기밀이 아닌 파일(예를 들면, 보안 수단이 요구되지 않은 파일)인 것이 결정된 경우, 데이터 파일은 일반적으로 저장되고 및/또는 사용자에게 일반적으로 제공될 수 있다. 기밀이 아닌 파일들의 저장 및/또는 사용은 더 설명되지 않을 것이다.

[0026] 206에서, 데이터 파일은 지정된 가상 저장 영역에 저장된다.

[0027] 기밀 파일인 것이 결정되는 데이터 파일은 지정된 가상 저장 영역에 저장된다. 일부 실시예들에서, 가상 저장 영역은 클라이언트 디바이스의 자기 디스크상에 있고 보안 수단을 요구하는 데이터 파일들(예를 들면, 기밀 파일들)을 저장하기 위한 특정한 자기 디스크 어레이 섹션일 수 있다. 사용자가 가상 저장 영역에 저장된 데이터 파일에 액세스할 필요가 있을 때, 클라이언트 디바이스 운영 시스템으로부터 분리되는(및 저장 분리 및 메모리 분리, 등을 포함할 수 있는) 가상 애플리케이션은 클라이언트 디바이스에서 개시되고, 클라이언트 디바이스의 가상 저장 영역에 저장된 데이터 파일은 가상 애플리케이션을 통해 액세스될 수 있다.

[0028] 일부 실시예들에서, 가상 저장 영역은 (예를 들면, 원격) 클라우드 서버의 자기 디스크상에 있고 보안 수단을 요구하는 데이터 파일들(예를 들면, 기밀 파일들)을 저장하기 위한 특정한 자기 디스크 어레이 섹션일 수 있다. 사용자의 클라이언트 디바이스가 데이터 파일을 저장할 수 없거나 데이터 파일을 위한 보안 수단을 채택할 수 없을 때, 클라이언트 디바이스 운영 시스템으로부터 분리되는(및 저장 분리, 메모리 분리 등을 포함할 수 있는) 가상 애플리케이션이 클라이언트 디바이스에서 개시되고 클라우드 서버의 가상 저장 영역에 저장된 데이터 파일은 가상 애플리케이션을 통해 액세스될 수 있다. 따라서, 가상 환경 내의 클라우드 서버상의 가상 저장 영역에 저장된 데이터 파일에 대해 수행된 임의의 동작들을 분리하고 데이터 파일이 누설되는 것을 방지하는 것이 가능하다.

[0029] 208에서, 스터브 파일은 데이터 파일의 원래의 저장 위치에 생성되고, 스터브 파일은 데이터 파일과 연관된 뷰잉 허가 및 지정된 가상 저장 영역 내 데이터 파일의 저장 위치를 포함한다.

[0030] 데이터 파일은 지정된 가상 저장 영역에서 저장 위치에 저장되기 전에 원래의 저장 위치에(예를 들면, 클라이언트 디바이스와 연관된 저장 장치에) 저장된다. 다양한 실시예들에서, 데이터 파일이 지정된 가상 저장 영역에 저장되면, 데이터 파일의 사본은 원래의 저장 위치로부터 삭제되고 스터브 파일이 대신 원래의 저장 위치에 저장된다. 다양한 실시예들에서, 스터브 파일은 데이터 파일과 연관된 뷰잉 허가(들) 및 지정된 가상 저장 영역에서의 데이터 파일의 저장 위치를 기록한다. 다양한 실시예들에서, 데이터 파일과 연관된 뷰잉 허가(들)는 데이터 파일에 액세스(예를 들면, 판독, 기재, 판독 및 기재)하도록 허용된 지정된 하용자들 및/또는 사용자들의 역할들(예를 들면, 관리자 사용자들, 게스트 사용자들, 특정 그룹의 사용자들의 게스트들)을 특정한다.

[0031] 다양한 실시예들에서, 사용자가 클라이언트 디바이스에서 스터브 파일을 선택할 때, 데이터 파일의 원래의 저장 위치에 저장된 스터브 파일은 선택한 사용자가 뷰잉 허가를 갖는지의 여부를 결정하기 위해 클라이언트 디바이스(의 운영 시스템)에 의해 판독될 것이다. 데이터 파일은, 선택한 사용자가 데이터 파일에 액세스하기 위한 뷰잉 허가를 갖는다고 결정되는 경우에만 지정된 가상 저장 영역의 저장 위치로부터 검색될 수 있다. 그래서, 데이터 파일은 지정된 가상 저장 영역의 저장 위치로부터 뷰잉된다. 이하에 더 상세히 설명되는 바와 같이, 지정된 가상 저장 시스템으로부터의 데이터 파일에 액세스하는 것은 (예를 들면, 클라우드 서버의) 지정된 가상 저장 영역 내 데이터 파일에 대한 액세스를 제공하는 가상화된 환경을 구동하는 것을 포함한다. 그러나, 선택한 사용자가 뷰잉 허가를 갖지 않는 경우, 선택한 사용자는 지정된 가상 저장 영역 내 데이터 파일에 대한 액세스가 거부된다.

[0032] 도 3은 보호된 데이터 파일을 공유하기 위한 프로세스의 일 실시예를 도시하는 흐름도이다. 일부 실시예들에서, 프로세스(300)는 도 1의 시스템(100)에서 구현된다.

[0033] 302에서, 제 1 명령은 제 2 사용자와 데이터 파일을 공유하기 위해 제 1 사용자로부터 수신된다.

[0034] 일부 실시예들에서, 제 1 사용자는 지정된 다른 사용자와 스터브 파일을 공유하기를 개시하기 위해 클라이언트 디바이스 애플리케이션 또는 스터브 파일-공유 키를 사용함으로써 다른 사용자와 데이터 파일을 공유할 수 있다. 일부 실시예들에서, 공유될 데이터 파일은 이미 클라우드 서버에 업로드되고, 데이터 파일에 대응하는 스터브 파일만이 다른 사용자와 데이터 파일을 공유하기를 원하는 사용자의 클라이언트 디바이스에 저장된다.

[0035] 304에서, 제 2 사용자와 연관된 사용자 정보가 결정된다. 일부 실시예들에서, 사용자 정보는 클라이언트 애플리케이션에서 다른 사용자의 계정 번호를 포함할 수 있거나, 다른 사용자가 데이터 파일을 수신할 수 있는 이메일 어드레스를 포함할 수 있다. 다시 말해서, 본 출원은 데이터 파일들이 공유될 수 있는 사용자 정보에 포함된 어드레스에 관련하는 제한들을 부과하지 않는다. 필요한 것은 다른 사용자가 데이터 파일을 수신할 수 있게 되는 것이다.

[0036] 306에서, 제 2 사용자가 제 2 사용자와 연관된 사용자 정보에 적어도 부분적으로 기초하여 데이터 파일에 액세스하기 위한 허가를 갖는지의 여부가 결정된다. 제 2 사용자가 데이터 파일에 액세스하기 위한 허가를 갖는 것이 결정되는 경우, 제어는 308로 이동된다. 그와 달리, 제 2 사용자가 데이터 파일에 액세스하기 위한 허가를

갖지 않는 것이 결정되는 경우, 제 2 사용자는 데이터 파일에 대한 액세스가 거부되고(예를 들면, 데이터 파일이 그/그녀와 공유될 수 없다는 메시지가 제 2 사용자에게 전송된다), 프로세스(300)는 종료한다.

[0037] 제 2 사용자와 연관된 사용자 정보는 제 2 사용자가 데이터 파일에 액세스하기 위한 허가를 갖는지의 여부를 결정하기 위해 데이터 파일의 스터브 파일에 포함되는 데이터 파일과 연관된 뷰잉 허가와 비교된다. 예를 들면, 제 2 사용자와 연관된 사용자 정보는 제 2 사용자와 연관된 식별 정보 및 제 2 사용자와 연관된 역할들을 포함할 수 있다.

[0038] 308에서, 데이터 파일은 클라우드 서버의 지정된 가상 저장 영역에 업로드되고 그에 저장된다.

[0039] 일부 실시예들에서, 데이터 파일의 사본이 (예를 들면, 백업 저장을 위해) 클라우드 서버의 지정된 가상 저장 영역에 미리 업로딩되고 저장되지 않은 경우, 데이터 파일의 사본은 클라우드 서버의 지정된 가상 저장 영역에 업로딩된다. 예를 들면, 제 2 사용자와 데이터 파일을 공유하기를 원하는 제 1 사용자는 클라우드 서버에 데이터 파일을 업로딩하기 위해 클라이언트 디바이스 애플리케이션 또는 스터브 파일 업로드 키를 사용할 수 있다. 일부 실시예들에서, 클라이언트 애플리케이션은 클라이언트 디바이스상에 설치된 가상화된 제어 및 관리 소프트웨어일 수 있다.

[0040] 310에서, 제 2 명령은 제 2 사용자와 연관된 클라이언트 디바이스로 전송되고, 제 2 명령은 제 2 사용자와 연관된 클라이언트 디바이스에 데이터 파일에 대응하는 스터브 파일을 생성하도록 구성된다.

[0041] 일부 실시예들에서, 제 2 사용자와 연관된 식별 정보는 제 2 사용자와 연관된 사용자 정보로부터 결정된다. 제 2 사용자가 대응하는 클라이언트 디바이스를 통해 제 2 명령을 수신한 후, 제 2 사용자의 클라이언트 디바이스상의 데이터 파일에 대한 스터브 파일은 제 2 명령에 기초하여 생성된다. 예를 들면, 스터브 파일의 생성된 사본은 데이터 파일이 제 2 사용자의 클라이언트 디바이스에 저장된 원래의 위치에 저장된다. 제 2 사용자의 클라이언트 디바이스는 이후 클라우드 서버의 지정된 가상 저장 영역으로부터 데이터 파일을 획득하기 위한 것이 기초로서 스터브 파일을 사용할 수 있다. 상기에 기술되는, 다양한 실시예들에서, 스터브 파일은 데이터 파일과 연관된 뷰잉 허가(들) 및 지정된 가상 저장 영역에서의 데이터 파일의 저장 위치를 기록한다.

[0042] 프로세스(300)에서 설명된 바와 같이, 데이터 파일을 공유할 필요가 있을 때, 제 2 명령은 사용자 정보에 따라 제 2 사용자에게 전송된다. 제 2 사용자가 그들의 클라이언트 디바이스를 통해 데이터 파일의 수신을 확인한 후, 데이터 파일 스터브 파일은 제 2 사용자의 클라이언트 디바이스상에 생성된다. 따라서, 비밀이 유지될 필요가 있는 데이터 파일의 공유는 스터브 파일을 공유함으로써 가상으로 공유된다. 데이터 파일의 기본 데이터가 제 2 사용자에게 전송되지 않고 공유된 스터브 파일이 저장 위치 및 가상 저장 영역 내 데이터 파일의 뷰잉 허가를 단지 저장하고 데이터 파일 자체의 어떠한 데이터 정보도 포함하지 않기 때문에, 스터브 파일의 그 또는 그녀의 사본에 대해 제 2 사용자에 의해 수행된 임의의 동작들은 데이터 파일에 대해 어떠한 효과도 갖지 않을 것이다. 이는 비밀 정보가 공유 프로세스에서 데이터 파일로부터 누설되지 않을 것을 보장한다.

[0043] 도 4는 보호된 데이터 파일을 사용하기 위한 프로세스의 일 실시예를 도시하는 흐름도이다. 일부 실시예들에서, 프로세스(400)는 도 1의 시스템에서 구현된다.

[0044] 402에서, 스터브 파일과 연관된 사용자 선택이 클라이언트 디바이스에 수신된다.

[0045] 스터브 파일과 연관된 사용자 선택이 클라이언트 디바이스에 수신된다. 다양한 실시예들에서, 스터브 파일은 클라우드 서버의 지정된 가상 저장 영역에 저장되고 도 2의 프로세스(200) 또는 도 3의 프로세스(300)와 같은 프로세스에 기초하여 생성되는 데이터 파일에 대응한다. 예를 들면, 스터브 파일은 클라이언트 디바이스에서 실행하고 있는 파일 브라우저 애플리케이션에 디스플레이된다. 일부 실시예들에서, 스터브 파일은 클라우드 서버의 지정된 가상 저장 영역 대신에 클라이언트 디바이스에 로컬로 저장된 연관되는 데이터 파일이 디스플레이되는 것과 동일한 방식으로 파일 브라우저 애플리케이션에 디스플레이된다.

[0046] 일부 실시예들에서, 클라이언트 디바이스상에 설치된 클라이언트 애플리케이션은 스터브 파일-관련 클릭 이벤트들에 대해 모니터링하기 위해 사용될 수 있다. 일부 실시예들에서, 사용자는 이미 사용자의 자격들을 사용하여 클라이언트 애플리케이션에 로그온하였다. 일부 실시예들에서, 클릭 이벤트는 스터브 파일에 대한 더블-클릭 이벤트일 수 있거나 표시된 메뉴 또는 파일 브라우저 애플리케이션상에 디스플레이될 때 스터브 파일에 대한 클릭 이벤트일 수 있다. 일부 실시예들에서, 클라이언트 애플리케이션은 스터브 파일들을 기록할 수 있고 따라서 클릭된 파일이 스터브 파일인지 원래의 데이터 파일인지를 결정할 수 있다.

[0047] 404에서, 사용자 선택과 연관된 사용자가 스터브 파일에 포함되는 데이터 파일과 연관된 뷰잉 허가에 적어도 부

분적으로 기초하여 스터브 파일과 연관된 데이터 파일에 액세스하기 위한 허가를 갖는지의 여부가 결정된다. 사용자 선택과 연관된 사용자가 데이터 파일에 액세스하기 위한 허가를 갖는 경우, 제어는 406으로 이동한다. 그와 달리, 사용자 선택과 연관된 사용자가 데이터 파일에 액세스하기 위한 허가를 갖지 않는 경우, 사용자는 데이터 파일에 대한 액세스가 거부되고 프로세스(400)는 종료한다.

[0048] 상기에 기술된 바와 같이, 스터브 파일은 대응하는 데이터 파일의 뷰잉 허가 및 클라우드 서버의 지정된 가상 저장 영역에 데이터 파일의 저장 위치를 기록한다. 스터브 파일을 선택한 사용자와 연관된 사용자 정보는 선택과 연관된 사용자가 데이터 파일의 뷰잉 허가를 갖는 사용자인지의 여부를 결정하기 위해 스터브 파일에 포함된 뷰잉 허가들과 비교된다.

[0049] 406에서, 데이터 파일에 대응하는 가상 애플리케이션은 클라이언트 디바이스에서 개시된다.

[0050] 408에서, 지정된 가상 저장 영역의 데이터 파일에 대한 액세스가 가상 애플리케이션을 사용하여 제공된다.

[0051] 다양한 실시예들에서, 가상 애플리케이션은 클라이언트 디바이스상에 설치된 가상화된 제어 및 관리 소프트웨어 애플리케이션이다. 다양한 실시예들에서, 가상 애플리케이션은 클라이언트 디바이스의 운영 시스템으로부터 분리된다. 다양한 실시예들에서, 운영 시스템으로부터의 가상 애플리케이션의 분리는 운영 시스템으로부터 저장 장치 분리를 포함할 수 있고, 이는 또한 운영 시스템으로부터의 메모리 분리를 포함할 수 있다. 따라서, 가상 애플리케이션은 데이터 파일에 대해 사용자에 의해 수행된 임의의 동작이 가상 애플리케이션에 의해 제공되는 가상 환경 내에서 분리되고, 그에 의해 가상 애플리케이션에 대해 승인된 액세스가 아닌 악의적인 사용자들이 가상 애플리케이션 내로부터 임의의 데이터 자원들을 획득하는 것을 방지한다. 일부 실시예들에서, 가상 애플리케이션을 통한 데이터 파일에 대한 사용자의 액세스는 예를 들면, 일반적인 판독, 편집, 및 클립보드들의 사용을 포함할 수 있다. 일부 실시예들에서, 데이터 파일에 대한 사용자에 의해 수행된 동작들은 스터브 파일이 저장된 클라이언트 디바이스상에서가 아닌 데이터 파일이 저장된 클라우드 서버에서 실행될 것이다. 다양한 실시예들에서, 가상 애플리케이션은 스터브 파일에 포함되는 데이터 파일의 저장 위치를 사용하여 클라우드 서버의 지정된 가상 저장 영역에 저장된 데이터 파일의 위치를 찾도록 구성된다. 도 5는 이하에 클라우드 서버의 지정된 가상 저장 영역에 저장된 데이터 파일에 액세스하기 위해 가상 애플리케이션을 사용하는 일 예를 도시한다.

[0052] 도 5는 보호된 데이터 파일에 액세스하기 위한 프로세스의 일 예를 도시하는 흐름도이다. 일부 실시예들에서, 프로세스(500)는 도 1의 시스템(100)에서 구현된다.

[0053] 다양한 실시예들에서, (예를 들면, 기밀) 데이터 파일에 대응하는 스터브 파일은 클라이언트 디바이스상에 저장되고, 반면에 데이터 파일은 클라우드 서버상에 지정된 가상 저장 영역에 저장된다. 프로세스(500)는 스터브 파일이 클라이언트 디바이스에서 선택된 후(예를 들면, 상기에서 도 4의 프로세스(400)에 설명되는 바와 같이) 가상 애플리케이션을 사용하여 클라우드 서버상의 지정된 가상 저장 영역으로부터 데이터 파일을 획득하기 위한 프로세스의 일 예이다.

[0054] 502에서, 클라이언트 디바이스는 데이터 파일이 데이터 파일과 연관된 스터브 파일에 포함된 정보에 적어도 부분적으로 기초하여 저장되는 클라우드 서버에 연결된 원격 데스크톱 프로토콜(RDP) 구성 요소를 개시한다.

[0055] 사용자가 (예를 들면, 상기에서 도 4의 프로세스(400)와 같은 프로세스를 사용하여) 클라이언트 디바이스의 스터브 파일을 선택했다는 것을 검출한 후, 클라이언트 디바이스는 스터브 파일에 기록된 정보에 따라 원격 데스크톱 프로토콜(RDP) 구성 요소를 시작한다. RDP 구성 요소는 데이터 파일이 액세스되는 클라우드 서버에서의 데이터 파일에 액세스하기 위해 사용될 수 있는 예시적인 가상 애플리케이션이다. RDP 구성 요소는 데이터 파일이 저장되는 클라우드 서버에 연결하기 위해 사용된다.

[0056] 504에서, 클라이언트 디바이스는 RDP 구성 요소를 통해 스터브 파일에 포함된 정보를 클라우드 서버에 송신한다.

[0057] 일부 실시예들에서, 스터브 파일에 기록된 모든 데이터 정보는 클라이언트 애플리케이션에 의해 암호화된다. 암호화된 데이터 애플리케이션은 스터브 파일에 대응하는 데이터 파일과 연관된 정보를 기록하고, 상기 연관된 정보는 예를 들면: 클라우드 서버의 지정된 가상 저장 영역에서의 데이터 파일의 저장 위치, 데이터 파일에 대한 사용자 허가들, 데이터 파일-공유 절차, 및 데이터 파일의 사용에 대한 이력 기록들, 중 하나 이상을 포함한다. 일부 실시예들에서, 클라이언트 디바이스로부터 클라우드 서버로 송신되는 스터브 파일에 포함된 정보는, 예를 들면: 데이터 파일이 저장된 클라우드 서버의 지정된 가상 저장 영역의 저장 위치, 클라이언트 애플리케이션 사용자 허가들, 사용자가 확인할 필요가 있는 정보, 및 열리게 될 데이터 파일에 대한 서버에 대한 서버상의 가상

저장 경로, 중 하나 이상을 포함한다.

[0058] 506에서, 클라우드 서버가 송신된 정보를 확인한 후, 클라우드 서버는 클라이언트 디바이스상에 원격 가상화 프로그램을 시작하고 스터브 파일에 포함된 지정된 가상 저장 영역 저장 위치에 따라 클라우드 서버상에 데이터 파일을 연다.

[0059] 508에서, 클라우드 서버는 클라이언트 디바이스상에 문서 편집기 프로그램을 맵핑한다.

[0060] 일부 실시예들에서, 클라우드 서버는 문서 편집기 프로그램(예를 들면, 마이크로소프트 워드)를 사용하여 새로운 편집 가능한 파일을 확립할 수 있고 이후 클라이언트 디바이스상에 편집 가능한 파일에 대한 전체 가시적인 윈도우를 송신한다. 따라서, 원격 문서 편집기는 클라이언트 디바이스상에 맵핑될 수 있다. 일부 실시예들에서, 클라이언트 디바이스상에 문서 편집기를 맵핑하는 것은 클라이언트 디바이스에 표시될 문서 편집기의 사용자 인터페이스를 전송하는 것을 포함한다.

[0061] 510에서, 클라이언트 디바이스는 클라우드 서버상에 저장된 데이터 파일에 대해 동작들을 수행하기 위해 문서 편집기 프로그램을 사용한다.

[0062] 일부 실시예들에서, 클라이언트 디바이스상에 클라우드 서버에 의해 맵핑되는 문서 편집기 프로그램을 사용하여 데이터 파일에 수행할 사용자로부터 클라이언트 디바이스에 수신되는 동작들은 예를 들면, 데이터 파일 콘텐트들을 뷰잉하거나 편집하는 것 및 데이터 파일을 복사하는 것을 포함할 수 있다. 클라이언트 디바이스에서 문서 편집기 프로그램 사용자 인터페이스를 통해 수행된 사용자 동작들은 클라우드 서버에 전송되고 이후 클라우드 서버의 데이터 파일에 대해 실행된다. 본 출원은 데이터 파일에 관하여 특정한 동작들에 관한 제한들을 부과하지 않는다.

[0063] 제 1 예에서, 제 1 사용자가 제 2 사용자와 (예를 들면, 기밀 데이터 파일) 공유한 후(예를 들면, 도 3의 프로세스(300)와 같은 프로세스를 사용하여), 제 2 사용자는 데이터 파일 자체의 사본보다 오히려 사용자의 클라이언트 디바이스에서의 스터브 파일만을 수신한다. 제 2 사용자가 클라우드 서버로부터 데이터 파일을 획득하는 것에 기초하여 스터브 파일을 사용할 필요가 있을 때, 제 2 사용자는 제 2 사용자의 클라이언트 디바이스에 저장된 스터브 파일을 선택할 수 있고, 도 4의 프로세스(400) 및 도 5의 프로세스(500)와 같은 프로세스들은 클라우드 서버의 지정된 가상 저장 영역에 저장되는 데이터 파일에 대한 사용자 액세스를 제공하기 위해 사용될 수 있다.

[0064] 제 2 예에서, 데이터 파일이 클라이언트 디바이스 자기 디스크가 한정된 저장 공간을 갖거나 가상 저장 영역에 의해 설정되지 않기 때문에 클라우드 서버의 지정된 가상 저장 영역에 저장되는 경우, 도 4의 프로세스(400) 및 도 5의 프로세스(500)와 같은 프로세스들은, 사용자가 스터브 파일에 기초하여 클라우드 서버로부터 데이터 파일을 획득할 필요가 있을 때, 클라이언트 디바이스의 사용자에게 클라우드 서버의 가상 영역으로부터의 데이터 파일에 대한 액세스를 제공하기 위해 사용될 수 있다.

[0065] 제 3 예에서, 사용자가 상이한 클라이언트 디바이스를 통해 클라우드 서버로부터 데이터 파일에 대한 동작들을 수행할 필요가 있을 때, 도 4의 프로세스(400) 및 도 5의 프로세스(500)는 데이터 파일에 대한 액세스를 원격으로 제공하기 위해 사용될 수 있다. 예를 들면, 클라이언트 디바이스 A의 사용자는 데이터 파일에 대한 스터브 파일을 생성하고 클라이언트 디바이스 A의 가상 영역에 데이터 파일을 저장한다. 사용자가 클라이언트 디바이스 A로부터 클라이언트 디바이스 B로 스터브 파일을 전송할 때, 및 클라이언트 디바이스 A가 데이터 파일을 클라우드 서버에 업로드한 후, 사용자는, 사용자가 클라이언트 디바이스 B로부터 데이터 파일을 검색할 필요가 있는 경우, 클라우드 서버로부터의 데이터 파일에 대한 동작들을 수행하기 위해 도 4의 프로세스(400) 및 도 5의 프로세스(500)를 사용할 수 있다.

[0066] Citrix XenApp과 같은 애플리케이션들 및 다른 이러한 애플리케이션들의 가상화 비용은 꽤 클 수 있다. 따라서, 상기에 설명된 바와 같이, 본 출원은, 예를 들면, RDP 기반 애플리케이션 가상화 방식을 채용함으로써 윈도우 운영 시스템을 사용할 수 있다. RDP 제어 구성 요소, 메시지 후크(message hook), 및 윈도우 클립핑 기술을 사용함으로써, 원격 애플리케이션 가상화 기술이 달성될 수 있고, 따라서, 클라이언트 디바이스의 자체 운영 시스템에 대한 의존을 피하고 클라우드 서버가 임의의 윈도우 운영 시스템을 채용하게 하고, 이는 데이터 파일의 사용자에 대해 더 융통성이 있다.

[0067] 다음의 예는 상기 설명된 실시예들에 기초한다: 데이터 파일이 사용자에 의한 동작들을 경험하게 될 때, 클라이언트 디바이스상에 설치된 클라이언트 애플리케이션은 또한 데이터 파일에 대해 사용자에 의해 수행된 동작들을 모니터링하기 위해 사용될 수 있다. 일부 실시예들에서, 데이터 파일에 대해 사용자에 의해 수행된 동작들은 클

라이언트 디바이스에 대해 수행될 수 있거나, 그들은 클라우드 서버로부터 클라이언트 디바이스상에 맵핑된 문서 편집기를 통해 사용자에 의해 데이터 파일에 대해 수행될 수 있고, 따라서, 데이터 파일 열기, 조작, 플로잉, 및 사용자에 의해 수행되는 모든 다른 데이터 파일 관련 동작들의 효과적인 모니터링 및 관리를 허용한다.

[0068] 도 6은 데이터 파일들을 보호하기 위한 일 예시적인 클라이언트 디바이스를 도시하는 도면이다. 예에 도시된 바와 같이, 클라이언트 디바이스는 프로세서, 내부 버스, 네트워크 포트들, 내부 메모리, 및 비휘발성 메모리를 포함한다. 특히, 클라이언트 디바이스는 또한 비지니스 서비스들을 수행하기 위해 필요할 때 다른 하드웨어를 포함할 수 있다. 프로세서는 비휘발성 메모리로부터 내부 메모리로 대응하는 컴퓨터 프로그램을 획득할 수 있고, 이후 그를 실행한다. 데이터 파일 보호 디바이스는 로직 층에 형성된다. 본 출원은 소프트웨어 구현들 외에 다른 구현들, 예를 들면 로직 디바이스 또는 조합된 소프트웨어/하드웨어 형태를 배제하지 않는다. 다시 말해서, 상기에 설명되는 프로세스들을 실행하는 엔티티는 다양한 로직 유닛들로 한정될 필요는 없고, 하드웨어, 소프트웨어, 또는 그 둘의 조합일 수 있다.

[0069] 도 7은 데이터 파일들을 보호하기 위한 일 예시적인 클라이언트 디바이스를 도시하는 도면이다. 예에서, 디바이스(700)는 제 1 결정 모듈(71), 저장 모듈(72), 및 스터브 생성 모듈(73)을 포함한다.

[0070] 모듈들 및 유닛들은 프로그래밍 가능한 로직 디바이스들과 같은 하드웨어로서, 하나 이상의 프로세서들상에 실행하는 소프트웨어 구성 요소들로서 구현될 수 있고, 및/또는 소자들이 설계된 주문형 집적 회로들은 컴퓨터 디바이스(예컨대 개인용 컴퓨터들, 서버들, 네트워크 장비, 등)이 본 발명의 실시예들에서 설명된 방법들을 구현하게 하기 위한 다수의 명령들을 포함하는 비휘발성 저장 매체(예컨대 광 디스크, 플래시 저장 디바이스, 모바일 하드 디스크 등)에 저장될 수 있는 소프트웨어 제품들의 일 형태에 의해 구현될 수 있다. 모듈들 및 유닛들은 단일 디바이스상에 구현되거나 다수의 디바이스들에 걸쳐 분포될 수 있다.

[0071] 제 1 결정 모듈(71)은 클라이언트 디바이스상에 데이터 파일의 생성에 응답하여 데이터 파일의 원래의 저장 위치 및 데이터 파일의 보안 분류를 결정하도록 구성된다.

[0072] 저장 모듈(72)은 제 1 결정 모듈에 의해 결정된 보안 분류가 데이터 파일이 기밀 파일인 것을 나타내는 경우 지정된 가상 저장 영역에 데이터 파일을 저장하도록 구성된다.

[0073] 스터브 생성 모듈(73)은 제 1 결정 모듈(71)에 의해 결정된 원래의 저장 위치에 스터브 파일을 생성하도록 구성된다. 스터브 파일은 지정된 가상 저장 영역의 데이터 파일의 저장 위치 및 데이터 파일에 대한 뷰잉 허가를 기록하도록 구성된다.

[0074] 도 8은 데이터 파일들을 보호하기 위한 일 예시적인 클라이언트 디바이스를 도시하는 도면이다. 일부 실시예들에서, 디바이스(800)는 도 7의 디바이스(700)의 일 예시적인 구현이다. 디바이스(800)의 예에서, 디바이스(700)의 제 1 결정 모듈(71)은 제 1 결정 유닛(711), 제 1 매칭 유닛(712), 제 2 결정 유닛(173), 및 제 2 매칭 유닛(714)을 포함한다. 디바이스(800)는 모니터링 모듈(78), 저장 모듈(72), 제 2 결정 모듈(74), 전송 모듈(75), 제 3 결정 모듈(76), 업로딩 모듈(77), 및 스터브 생성 모듈(73)을 포함한다.

[0075] 제 1 결정 유닛(711)은 데이터 파일의 콘텐트 정보를 결정하도록 구성된다.

[0076] 일부 실시예들에서, 제 1 매칭 유닛(712)은 제 1 미리 설정된 상태에 대해 제 1 결정 유닛(711)에 의해 결정된 콘텐트 정보를 매칭하고 제 1 매칭 결과에 따라 데이터 파일의 보안 분류를 결정하도록 구성된다.

[0077] 일부 실시예들에서, 제 2 결정 유닛(173)은 데이터 파일의 파일명을 결정하도록 구성된다.

[0078] 제 2 매칭 유닛(714)은 제 2 미리 설정된 상태에 대해 제 2 결정 유닛(713)에 의해 결정된 파일명을 매칭하고 제 2 매칭 결과에 따라 데이터 파일의 보안 분류를 결정하도록 구성된다.

[0079] 제 2 결정 모듈(74)은 제 1 사용자가 저장 모듈(72)에 의해 저장된 데이터 파일을 제 1 사용자에 의해 지정되는 제 2 사용자의 클라이언트 디바이스와 공유할 것을 선택한 것을 나타내는 제 1 명령을 검출하면 제 2 사용자에 대한 사용자 정보를 결정하도록 구성된다.

[0080] 전송 모듈(75)은 제 2 사용자에게 데이터 파일을 수신할 것을 명령하기 위해 제 2 명령을 제 2 사용자에게 전송하는 것에 기초하여 제 2 결정 모듈(74)에 의해 결정된 사용자 정보를 사용하도록 구성된다. 제 2 사용자가 대응하는 클라이언트 디바이스를 통해 데이터 파일을 수신한 후, 전송 모듈(75)은 제 2 사용자의 클라이언트 디바이스 상에 데이터 파일에 대한 스터브 파일을 생성하도록 구성된다.

[0081] 제 3 결정 모듈(76)은 제 2 사용자가 데이터 파일에 대한 뷰잉 허가를 갖는지의 여부를 결정한 것에 기초하여 제 2 결정 모듈(74)에 의해 결정된 사용자 정보를 사용하도록 구성된다.

[0082] 업로딩 모듈(77)은 제 2 사용자가 데이터 파일에 대한 뷰잉 허가를 갖는다는 결정에 연관된 제 3 결정 모듈(76)로부터의 표시를 수신하도록 구성된다. 상기 표시에 응답하여, 업로딩 모듈(77)은 데이터 파일을 클라우드 서버로 업로딩하고 이를 저장하도록 구성되어 상기 결과는 제 2 사용자가 클라우드 서버로부터 데이터 파일을 획득하는 것에 기초하여 스터브 파일을 사용할 수 있는 것이다.

[0083] 모니터링 모듈(78)은 데이터 파일에 대해 사용자에 의해 수행되는 사용자 동작들을 모니터링하기 위해 클라이언트 디바이스상에 설치된 클라이언트 애플리케이션을 사용하도록 구성된다.

[0084] 도 9는 일 예시적인 데이터 파일 검색 디바이스를 도시하는 도면이다. 예에서, 디바이스(900)는 제 4 결정 모듈(91), 시작 모듈(92), 및 액세싱 모듈(93)을 포함한다.

[0085] 제 4 결정 모듈(91)은 스터브 파일을 선택하는 것과 연관된 사용자가 스터브 파일에 의해 기록된 뷰잉 허가에 따라 데이터 파일에 액세스하기 위한 허가를 갖는지의 여부를 결정하도록 구성된다.

[0086] 제 4 결정 모듈(91)이 사용자가 데이터 파일에 액세스하기 위한 허가를 갖는 것을 결정하는 경우, 시작 모듈(92)은 데이터 파일에 대응하는 가상 애플리케이션을 개시하도록 구성된다.

[0087] 액세싱 모듈(93)은 스터브 파일에 의해 기록된 지정된 가상 저장 영역 저장 위치에 저장된 데이터 파일에 액세스하기 위해 시작 모듈(92)에 의해 시작된 가상 애플리케이션을 사용하도록 구성된다.

[0088] 도 10은 일 예시적인 데이터 파일 검색 디바이스를 도시하는 도면이다. 일부 실시예들에서, 도 9의 디바이스(900)는 디바이스(1000)의 예를 사용하여 구현될 수 있다. 디바이스(1000)의 예에서, 액세싱 모듈(93)은 네트워크 접속 유닛(931), 송신 유닛(932), 및 운영 유닛(933)을 포함한다.

[0089] 네트워크 접속 유닛(931)은 액세스될 데이터 파일과 연관된 스터브 파일에 의해 기록된 정보에 기초하여 원격 데스크톱 프로토콜 구성 요소를 통해 클라우드 서버에 접속하도록 구성된다.

[0090] 송신 유닛(932)은, 클라우드 서버가 저장 파일에 의해 기록된 정보를 성공적으로 검증한 후, 클라우드 서버가 클라이언트 디바이스상에 원격 가상 프로그램을 개시하고 클라우드 서버상에 저장된 데이터 파일을 편집하기 위한 문서 편집기 프로그램을 클라이언트 디바이스에 맵핑하는 것에 기초하여 스터브 파일에 의해 기록된 지정된 가상 저장 위치를 사용한다.

[0091] 운영 유닛(933)은 문서 편집기를 통해 클라우드 서버상에 저장된 데이터 파일에 대한 동작들을 수행하도록 구성된다.

[0092] 도 11은 데이터 파일들을 보호하기 위해 프로그램된 컴퓨터 시스템의 일 예시적인 실시예를 도시하는 기능도이다. 명백한 바와 같이, 다른 컴퓨터 시스템 아키텍처들 및 구성들이 데이터 파일들을 보호하기 위해 사용될 수 있다. 이하에 설명되는 다양한 서브시스템들을 포함하는 컴퓨터 시스템(1100)은 적어도 하나의 마이크로프로세서 서브시스템(프로세서 또는 중앙 처리 장치(CPU)라고도 지칭됨)(1102)을 포함한다. 예를 들면, 프로세서(1102)는 단일칩 프로세서에 의해 또는 다수의 프로세서들에 의해 구현될 수 있다. 일부 실시예들에서, 프로세서(1102)는 컴퓨터 시스템(1100)의 동작을 제어하는 범용 디지털 프로세서이다. 메모리(1100)로부터 검색된 명령들을 사용하여, 프로세서(1102)는 입력 데이터의 수신 및 조작, 및 출력 디바이스들(예를 들면, 디스플레이(1118))상에 데이터의 출력 및 디스플레이를 제어한다.

[0093] 프로세서(1102)는 제 1 주기억 영역, 일반적으로 랜덤 액세스 메모리(RAM), 및 제 2 주기억 영역, 일반적으로 판독 전용 메모리(ROM)를 포함할 수 있는 메모리(1110)와 양방향 결합된다. 본 기술에 잘 알려진 바와 같이, 주기억 장치는 범용 기억 영역으로서 및 스크래치-패드 메모리로서 사용될 수 있고, 입력 데이터 및 처리된 데이터를 저장하기 위해 또한 사용될 수 있다. 주기억 장치는 또한 프로세서(1102)상에 동작하는 프로세스들을 위한 명령들 및 다른 데이터 외에 데이터 객체들 및 텍스트 객체들의 형태로 프로그래밍 명령들 및 데이터를 저장할 수 있다. 또한 본 기술에서 잘 알려진 바와 같이, 주기억 장치는 일반적으로 그의 기능들을 수행하기 위해 프로세서(1102)에 의해 사용된 기본 동작 명령들, 프로그램 코드, 데이터, 및 객체들(예를 들면, 프로그램된 명령들)을 포함한다. 예를 들면, 메모리(1110)는, 예를 들면, 데이터 액세스가 양방향일 필요가 있는지 단방향일 필요가 있는지에 따라, 이하에 설명된 임의의 적절한 컴퓨터 판독 가능한 저장 매체를 포함할 수 있다. 예를 들면, 프로세서(1102)는 또한 캐시 메모리(도시되지 않음)에 자주 필요한 데이터를 직접 및 매우 빠르게 검색하

고 그를 저장할 수 있다.

[0094] 제거 가능한 대용량 저장 디바이스(1112)는 컴퓨터 시스템(1100)에 대한 추가의 데이터 저장 용량을 제공하고, 프로세서(1102)에 양방향(판독/기록) 또는 단방향(판독 전용)으로 결합된다. 예를 들면, 저장 장치(1112)는 또한 자기 테이프, 플래시 메모리, PC-CARD들, 이동식 대용량 저장 디바이스들, 홀로그래픽 저장 디바이스들, 및 다른 저장 디바이스들과 같은 컴퓨터 판독 가능한 매체를 포함할 수 있다. 고정식 대용량 저장 장치(1120)는 또한, 예를 들면, 추가의 데이터 기억 용량을 제공할 수 있다. 고정식 대용량 저장 장치(1120)의 가장 일반적인 예는 하드 디스크 드라이브이다. 대용량 저장 장치들(1112, 1120)은 통상 프로세서(1102)에 의해 활성으로 사용되지 않는 추가의 프로그래밍 명령들, 데이터 등을 저장한다. 저장 장치들(1112, 1120) 내 보유된 정보는, 필요한 경우, 가상 메모리로서 메모리(1110)(예를 들면, RAM)의 일부로서 표준 방식으로 통합될 수 있다는 것이 이해될 것이다.

[0095] 프로세서(1102)에 저장 서브시스템들에 대한 액세스를 제공하는 것 외에, 버스(1114)는 또한 다른 서브시스템들 및 디바이스들에 대한 액세스를 제공하기 위해 사용될 수 있다. 도시된 바와 같이, 이들은 디스플레이(1118), 네트워크 인터페이스(1116), 키보드(1104), 및 포인팅 디바이스(1108), 뿐만 아니라 보조 입/출력 디바이스 인터페이스, 사운드 카드, 스피커들, 및 필요에 따른 다른 서브시스템들을 포함할 수 있다. 예를 들면, 포인팅 디바이스(1108)는 마우스, 스타일러스, 트랙볼, 또는 태블릿일 수 있고, 그래픽 사용자 인터페이스와 인터페이스하기에 유용하다.

[0096] 네트워크 인터페이스(1116)는 프로세서(1102)가 다른 컴퓨터, 컴퓨터 네트워크, 또는 도시된 네트워크 접속을 사용하는 원격 통신 네트워크에 결합되게 한다. 예를 들면, 네트워크 인터페이스(1116)를 통해, 프로세서(1102)는 방법/프로세스 단계들을 수행하는 과정으로 다른 네트워크로부터의 정보(예를 들면, 데이터 객체들 또는 프로그램 명령들)를 수신하거나 또는 다른 네트워크로 출력 정보를 출력할 수 있다. 프로세서상에 실행될 일련의 명령들로서 종종 나타내지는 정보는 다른 네트워크로부터 수신되고 그로 출력될 수 있다. 인터페이스 카드 또는 유사한 디바이스 및 프로세서(1102)(예를 들면, 그에 실행된/수행된)에 의해 구현된 적절한 소프트웨어는 컴퓨터 시스템(1100)을 외부 네트워크에 접속하고 표준 프로토콜들에 따라 데이터를 이동시키기 사용될 수 있다. 예를 들면, 여기에 개시된 다양한 프로세스 실시예들은 프로세서(1102)상에 실행될 수 있거나, 처리의 일부를 공유하는 원격 프로세서와 함께, 인터넷, 인트라넷 네트워크들, 또는 근거리 네트워크들과 같은 네트워크를 거쳐 수행될 수 있다. 추가의 대용량 저장 장치들(도시되지 않음)는 또한 네트워크 인터페이스(1116)를 통해 프로세서(1102)에 접속될 수 있다.

[0097] 보조 I/O 디바이스 인터페이스(도시되지 않음)는 컴퓨터 시스템(1100)과 함께 사용될 수 있다. 보조 I/O 디바이스 인터페이스는 프로세서(1102)가 마이크로폰들, 터치 감응식 디스플레이들, 트랜스듀서 카드 판독기들, 테이프 판독기들, 음성 또는 필기 인식기들, 생체 측정 판독기들, 카메라들, 이동식 대용량 저장 장치들, 및 다른 컴퓨터들과 같은 다른 디바이스들로부터 데이터를 전송 및 더 일반적으로 수신하게 하는 범용 및 맞춤화된 인터페이스들을 포함할 수 있다.

[0098] 상기 다양한 실시예들에 설명된 바와 같이, 데이터 파일이 기밀 파일임이 결정될 때, 데이터 파일은 지정된 가상 저장 영역에 저장된다. 따라서, 지정된 가상 저장 영역에 저장된 데이터 파일에 대한 사용자 동작들은 가상 환경 내에서 분리되고 데이터 파일이 액세스되는 클라이언트 디바이스에서 악의적인 사용자들 및/또는 프로그램들에 의해 조작되는 것을 방지할 수 있다. 스터브 파일은 클라이언트 디바이스에 데이터 파일의 원래의 저장 위치에서 생성된다. 스터브 파일은 데이터 파일에 대한 뷰잉 허가 및 가상 저장 영역에서 데이터 파일의 저장 위치만을 기록하고 데이터 파일 자체로부터의 임의의 파일을 포함하지 않기 때문에, 스터브 파일에 대해 사용자에 의해 수행된 임의의 동작들은 데이터 파일에 대해 어떠한 영향도 갖지 않을 것이다.

[0099] 여기에 개시된 발명을 고려하면, 설명 및 실시에서 당업자가 본 출원을 구현하기 위한 다른 방식들을 쉽게 생각할 것이다. 본 출원은 본 출원의 임의의 변형, 사용, 또는 적응을 포함하는 것을 의도하고, 이들 변형들, 사용들, 또는 적응들은 본 출원의 일반 원리들을 준수하고 본 출원에 의해 개시되지 않은 본 기술에서 공개적인 지식 또는 통상적인 기술적인 수단을 포함한다. 설명 및 실시예들은 단순히 예시적인 것으로 간주된다. 본 출원의 진실한 범위 및 정신은 이하의 청구항들에 의해 나타내진다.

[0100] 용어 "포함한다" 또는 "포함하는" 또는 임의의 그들의 변형들이 그들의 배제되지 않은 의미로 취해진다는 것을 또한 주의하라. 따라서, 프로세스들, 방법들, 물품, 또는 일련의 요소들을 포함하는 장비는 이들 요소들을 포함할 뿐만 아니라 명백하게 나열되지 않은 다른 요소들 또는 이러한 프로세스들, 방법들, 물품, 또는 장비에 고유한 요소들을 또한 포함한다. 다른 한정들이 없는 경우, 어구 "...를 포함한다"에 의해 한정된 요소들은 프로세

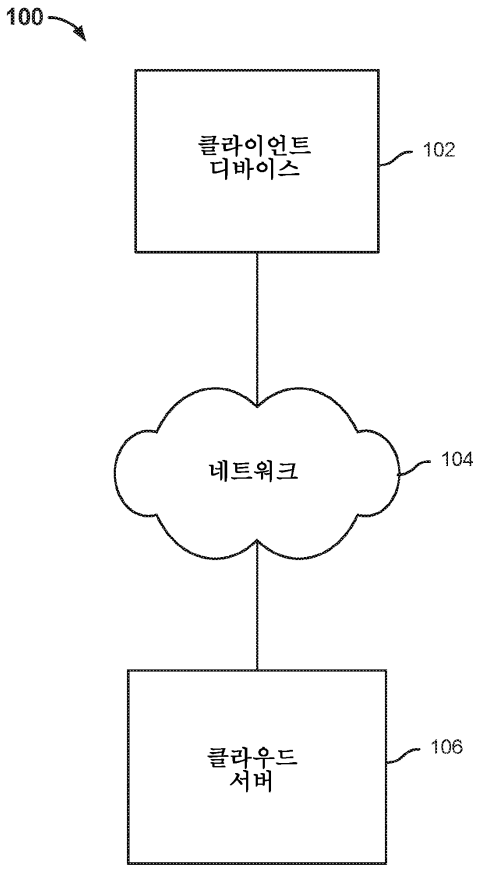
스들, 방법들, 물품, 또는 상기 요소들을 포함하는 장비에서 추가의 동일한 요소들의 존재를 배제하지 않는다.

[0101] 본 출원의 바람직한 실시예들이 단순히 상기에 설명되고 이는 본 출원을 한정하는 역할을 하지 않는다. 수행되는 임의의 변형들, 동등한 대체들, 또는 개선들은 본 출원의 보호 범위 내에 포함될 것이다.

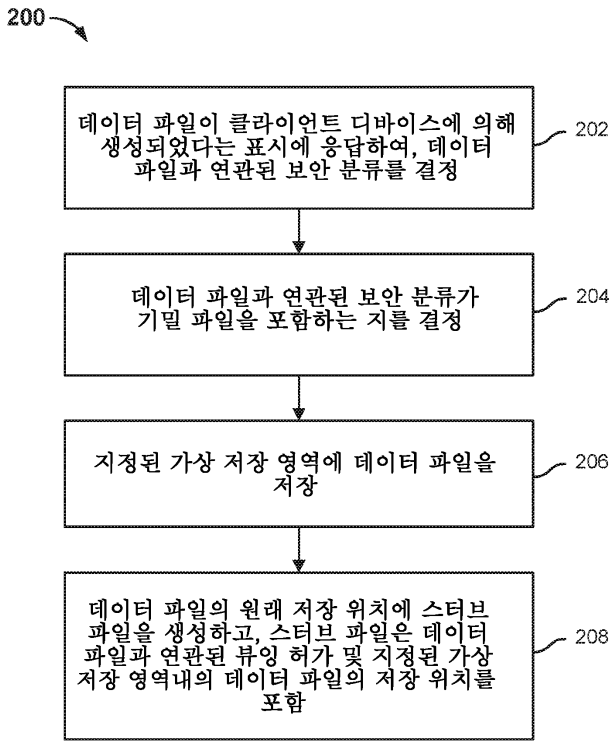
[0102] 다음의 실시예들은 이해의 명확성을 위해 일부 상세히 설명되었지만, 본 발명은 제공된 상세들로 한정되지 않는다. 본 발명을 구현하는 많은 대안적인 방식들이 존재한다. 개시된 실시예들은 예시적이고 제한적이 아니다.

도면

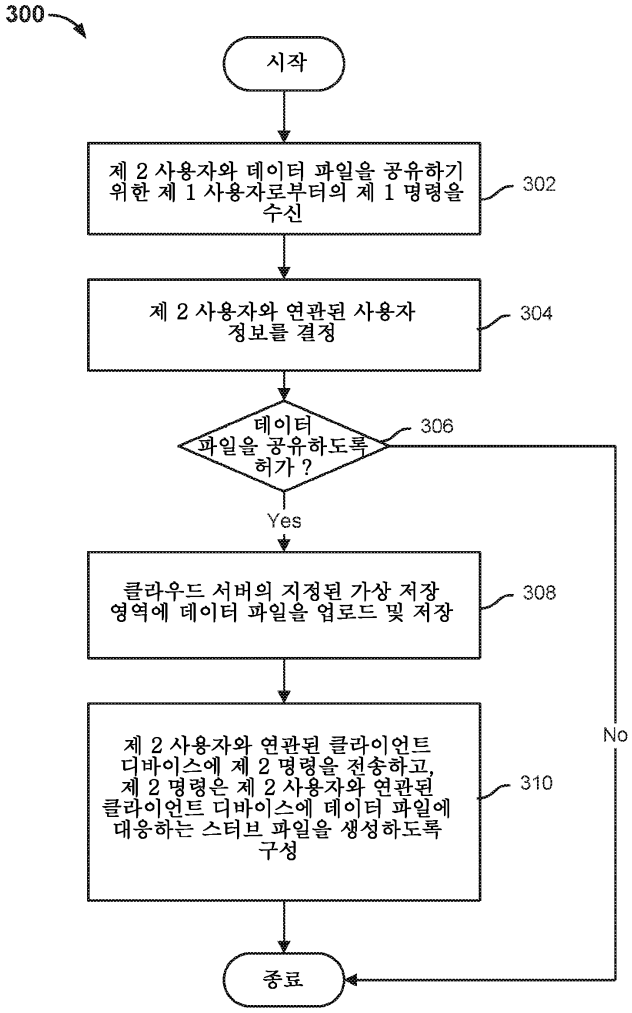
도면1



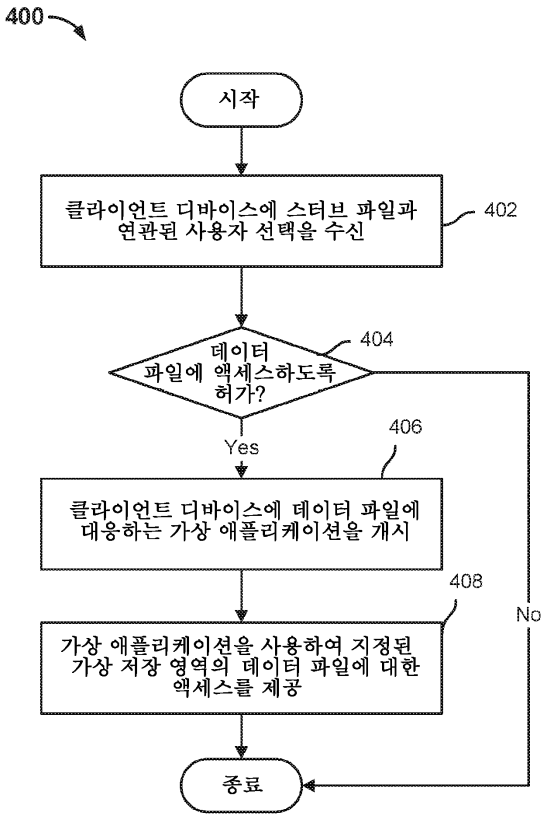
도면2


200
데이터 파일이 클라이언트 디바이스에 의해 생성되었다는 표시에 응답하여, 데이터 파일과 연관된 보안 분류를 결정
202
데이터 파일과 연관된 보안 분류가 기밀 파일을 포함하는 지를 결정
204
지정된 가상 저장 영역에 데이터 파일을 저장
206
데이터 파일의 원래 저장 위치에 스터브 파일을 생성하고, 스터브 파일은 데이터 파일과 연관된 뷰잉 허가 및 지정된 가상 저장 영역내의 데이터 파일의 저장 위치를 포함
208

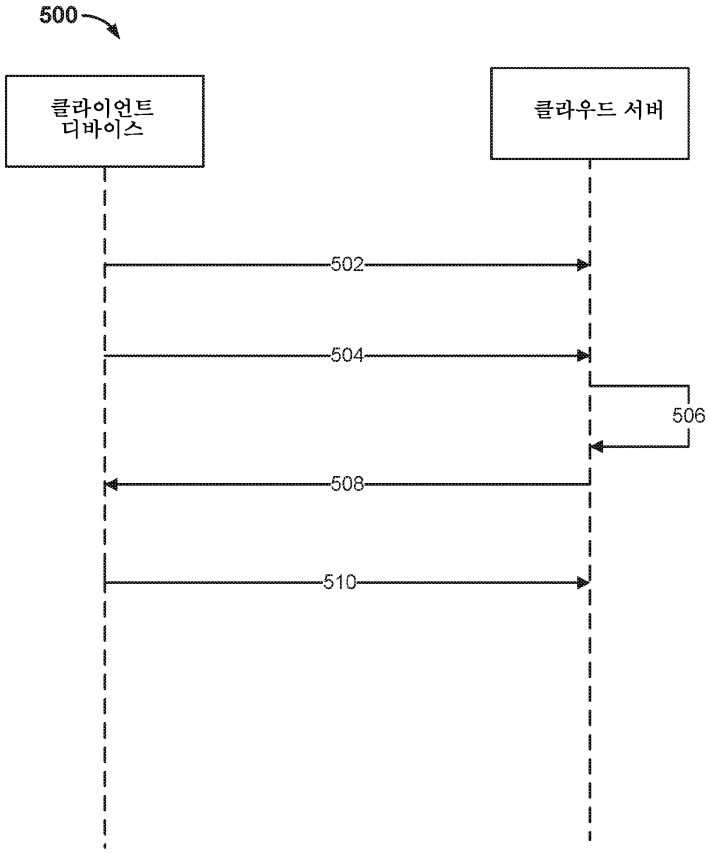
도면3


300
시작
제 2 사용자와 데이터 파일을 공유하기 위한 제 1 사용자로부터의 제 1 명령을 수신
302
제 2 사용자와 연관된 사용자 정보를 결정
304
데이터 파일을 공유하도록 허가 ?
306
Yes
No
클라우드 서버의 지정된 가상 저장 영역에 데이터 파일을 업로드 및 저장
308
제 2 사용자와 연관된 클라이언트 디바이스에 제 2 명령을 전송하고, 제 2 명령은 제 2 사용자와 연관된 클라이언트 디바이스에 데이터 파일에 대응하는 스터브 파일을 생성하도록 구성
310
종료

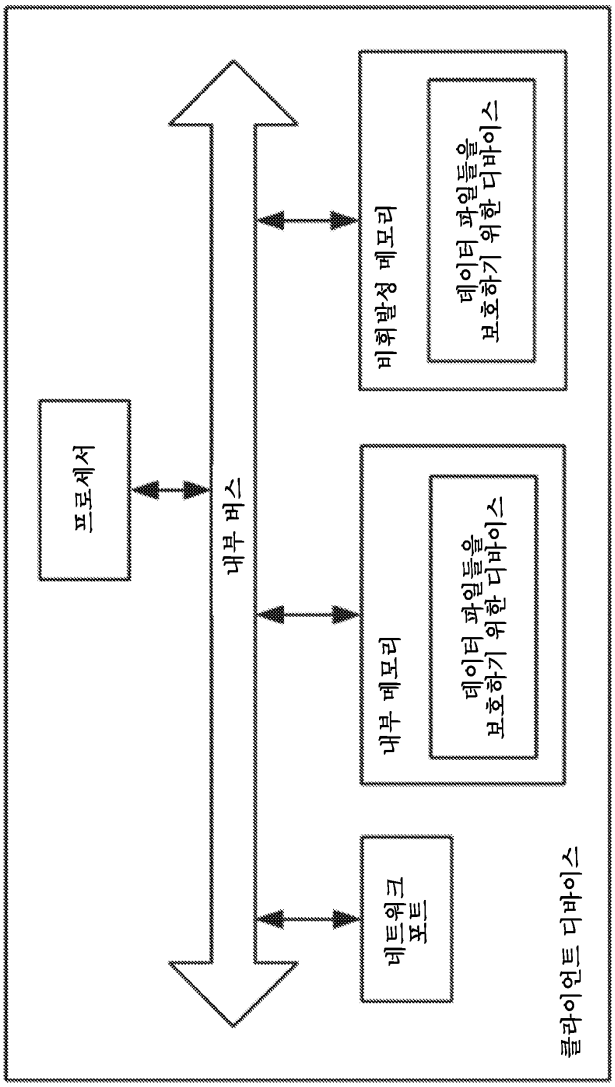
도면4


400
시작
클라이언트 디바이스에 스터브 파일과 연관된 사용자 선택을 수신
402
데이터 파일에 액세스하도록 허가?
404
Yes
406
클라이언트 디바이스에 데이터 파일에 대응하는 가상 애플리케이션을 개시
408
No
가상 애플리케이션을 사용하여 지정된 가상 저장 영역의 데이터 파일에 대한 액세스를 제공
종료

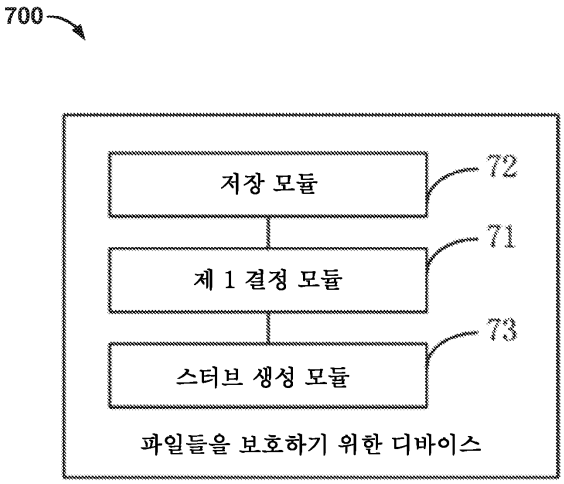
도면5


500
클라이언트 디바이스
클라우드 서버
502
504
506
508
510

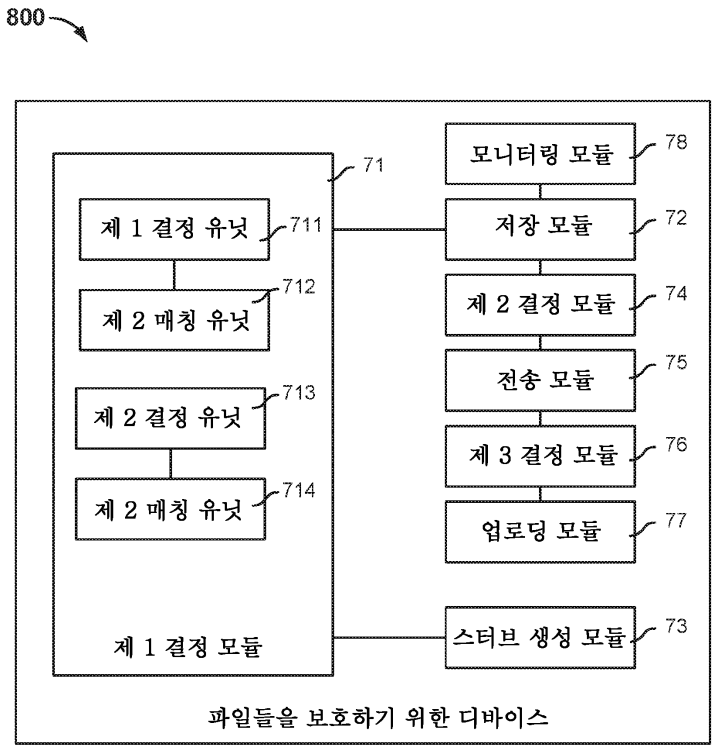
도면6


프로세서
내부 버스
비휘발성 메모리
데이터 파일들을
보호하기 위한 디바이스
내부 메모리
데이터 파일들을
보호하기 위한 디바이스
네트워크
포트
클라이언트 디바이스

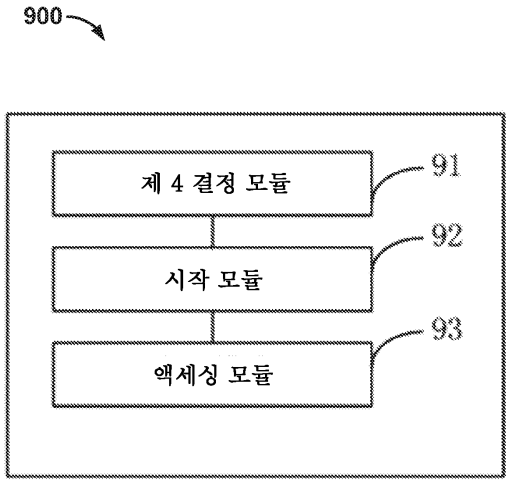
도면7


700
저장 모듈
72
제 1 결정 모듈
71
스터브 생성 모듈
73
파일들을 보호하기 위한 디바이스

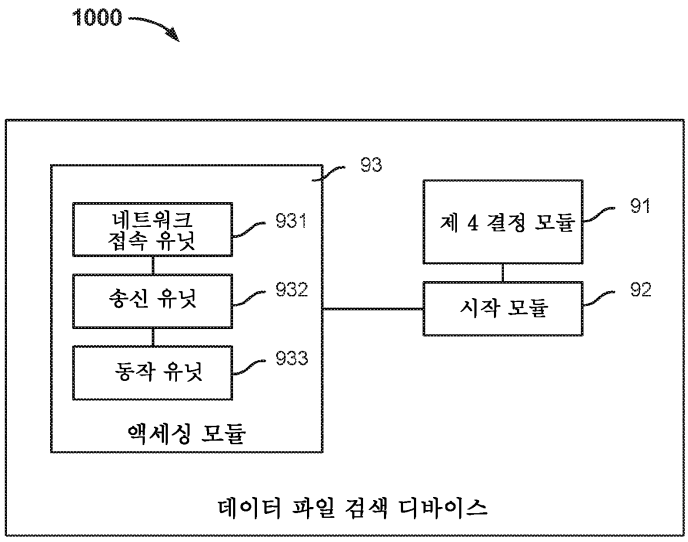
도면8


800
71
제 1 결정 유닛
711
제 2 매칭 유닛
712
제 2 결정 유닛
713
제 2 매칭 유닛
714
제 1 결정 모듈
모니터링 모듈
78
저장 모듈
72
제 2 결정 모듈
74
전송 모듈
75
제 3 결정 모듈
76
업로딩 모듈
77
스터브 생성 모듈
73
파일들을 보호하기 위한 디바이스

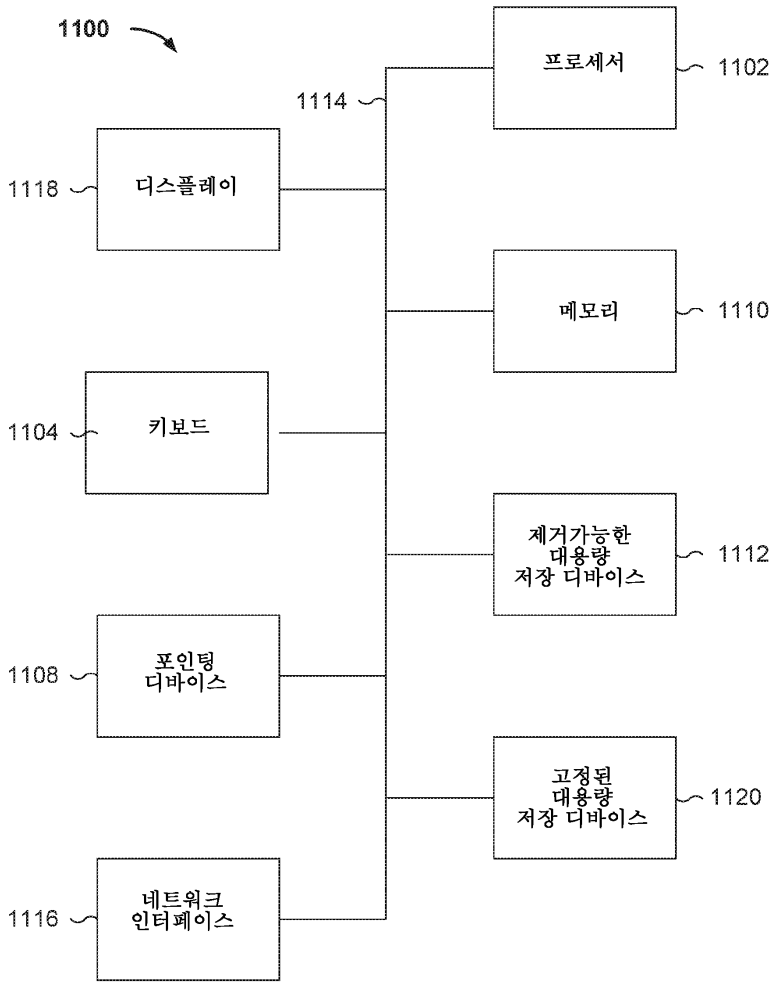
도면9


900
제 4 결정 모듈
91
시작 모듈
92
액세싱 모듈
93

도면10



도면11



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 19

【변경전】

전송도록

【변경후】

전송하도록

【직권보정 2】

【보정항목】 청구범위

【보정세부항목】 청구항 10

【변경전】

상기 기밀 파일

【변경후】

기밀 파일