(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년02월26일
(11) 등록번호 10-1928127
(24) 등록일자 2018년12월05일

(51) 국제특허분류(Int. Cl.)
G06F 21/12 (2013.01)
(21) 출원번호 10-2014-7006133
(22) 출원일자(국제) 2012년09월04일
심사청구일자 2017년08월03일
(85) 번역문제출일자 2014년03월06일
(65) 공개번호 10-2014-0066718
(43) 공개일자 2014년06월02일
(86) 국제출원번호 PCT/US2012/053623
(87) 국제공개번호 WO 2013/036472
국제공개일자 2013년03월14일
(30) 우선권주장
13/229,367 2011년09월09일 미국(US)
(56) 선행기술조사문헌
US20050091658 A1
US20100153671 A1
US6378071 B1
US20050256859 A1

(73) 특허권자
마이크로소프트 테크놀로지 라이센싱, 엘엘씨
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
그라함 스코트
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
라다크리쉬난 카비사
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
(뒷면에 계속)
(74) 대리인
제일특허법인(유)

전체 청구항 수 : 총 20 항 심사관 : 윤혜숙

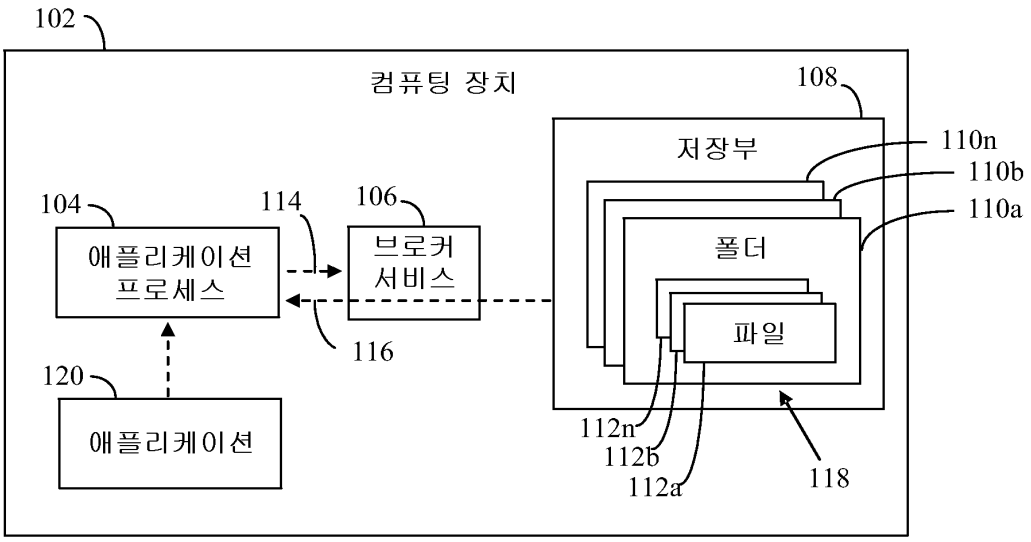
(54) 발명의 명칭 **애플리케이션용 선택적 파일 액세스 기법**

(57) 요 약

애플리케이션에 의한 선택적 파일 시스템 액세스를 가능하게 하는 방법, 시스템 및 컴퓨터 프로그램 제품이 제공된다. 애플리케이션은 컴퓨팅 장치 내에 설치된다. 애플리케이션과 연관된 애플리케이션 매니페스트가 수신된다. 애플리케이션 매니페스트는 애플리케이션이 액세스하도록 허용되는 하나 이상의 파일 타입을 표시한다. 표시된

(뒷면에 계속)

대 표 도 - 도1



파일 타입(들)은 브로커 서비스에 의해 액세스가능한 위치에 등록된다. 애플리케이션은 애플리케이션 프로세스로서 런칭된다. 애플리케이션 프로세스는 애플리케이션 컨테이너 내에 격리된다. 애플리케이션 컨테이너는 파일 시스템 데이터로의 애플리케이션 프로세스에 의한 직접 액세스를 차단한다. 파일 시스템 데이터의 제1 데이터와 관련된 액세스 요청은 애플리케이션 프로세스로부터 브로커 서비스에 수신된다. 브로커 서비스는 제1 데이터의 파일 타입이 등록된 파일 타입(들)에 포함되는지를 결정할 때, 제1 데이터로의 애플리케이션 프로세스에 의한 액세스가 가능하다.

(72) 발명자

이스킨 서메트

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

블랜치 카트리나 엠

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

볼 스티븐

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

하젠 존

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

빔 테일러 키엔

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

킴 알렌

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

퀸터로 구일러모 엔리퀘 루다

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

명 세 서

청구범위

청구항 1

컴퓨팅 장치에서 운영하는 브로커 서비스 내의 방법으로서,

상기 컴퓨팅 장치에서, 애플리케이션 프로세스로부터의 데이터를 포함하는 상기 컴퓨팅 장치의 파일 시스템의 제 1 데이터와 관련된 액세스 요청을 수신하는 단계－상기 애플리케이션 프로세스는 런칭된 버전의 애플리케이션이고, 상기 애플리케이션 프로세스는 상기 파일 시스템으로의 상기 애플리케이션 프로세스에 의한 직접 액세스를 차단하는 애플리케이션 컨테이너에 존재하며, 상기 액세스 요청은 상기 애플리케이션 컨테이너에 대한 식별자를 포함하는 상기 애플리케이션 프로세스에 대한 토큰 및 상기 액세스 요청에서 요청된 상기 제 1 데이터의 표시를 포함함－와,

상기 브로커 서비스가 상기 제 1 데이터의 파일 타입이 상기 애플리케이션과 현재 연관되고 상기 애플리케이션이 액세스하는 것이 허용된 파일 타입으로서 상기 애플리케이션에 대해 등록되는 하나 이상의 파일 타입에 포함된다고 판정할 경우, 상기 파일 시스템의 파일 저장소로부터 상기 제 1 데이터를 검색함으로써 상기 컴퓨팅 장치에서 운영하는 상기 브로커 서비스를 통해, 상기 제 1 데이터로의 상기 애플리케이션 프로세스에 의한 액세스를 가능하게 하는 단계를 포함하되, 상기 하나 이상의 파일 타입은 상기 애플리케이션 프로세스의 설치 동안 수신되는 애플리케이션 매니페스트로부터 판독되고, 상기 하나 이상의 파일 타입의 표시는 상기 브로커 서비스에 액세스 가능하고 상기 애플리케이션에 의해 액세스 불가능한 상기 컴퓨팅 장치의 안전한 위치에 저장되는

브로커 서비스 내의 방법.

청구항 2

제1항에 있어서,

상기 하나 이상의 파일 타입은 하나 이상의 파일 확장자, 파일 종류, 또는 다른 파일 속성 또는 메타데이터를 포함하고, 상기 가능하게 하는 단계는,

상기 브로커 서비스에 의해 액세스 가능하고 상기 애플리케이션 프로세스에 의해 액세스 불가능한 상기 안전한 위치에서 등록된 하나 이상의 파일 확장자, 파일 종류, 또는 다른 파일 속성 또는 메타데이터에 액세스하는 단계를 포함하는

브로커 서비스 내의 방법.

청구항 3

제2항에 있어서,

상기 애플리케이션 프로세스에 의한 액세스를 가능하게 하는 단계는,

상기 액세스 요청에서 요청된 상기 제 1 데이터의 표시에 기초하여 상기 제 1 데이터의 파일 타입을 결정하는 단계와,

상기 안전한 위치에서 상기 애플리케이션에 대한 상기 등록된 하나 이상의 파일 타입에 액세스하는 단계와,

상기 제 1 데이터의 파일 타입이 상기 등록된 하나 이상의 파일 타입에 포함되는지 여부를 판정하는 단계와,

상기 제 1 데이터의 파일 타입이 상기 등록된 하나 이상의 파일 타입에 포함되는 것으로 판정될 경우 상기 애플리케이션 프로세스가 상기 제 1 데이터에 액세스하는 것을 가능하게 하는

브로커 서비스 내의 방법.

청구항 4

제3항에 있어서,

상기 애플리케이션 프로세스에 의한 액세스를 가능하게 하는 단계는,

상기 제 1 데이터의 파일 타입이 상기 등록된 하나 이상의 파일 타입에 포함되지 않는 것으로 판정될 경우 상기 제 1 데이터로의 상기 애플리케이션 프로세스에 의한 액세스를 거부하는 단계를 더 포함하는

브로커 서비스 내의 방법.

청구항 5

제4항에 있어서,

상기 거부하는 단계는,

상기 제 1 데이터의 파일을 판독하거나, 상기 제1 데이터의 폴더의 컨텐츠를 판독하거나, 상기 제 1 데이터의 파일 또는 폴더 중 적어도 하나를 기록하거나, 상기 제 1 데이터의 파일 또는 폴더의 이름을 변경하거나, 상기 제 1 데이터의 파일 또는 폴더를 이동시키거나, 또는 상기 제 1 데이터의 파일 또는 폴더에 걸쳐 복사하기 위한 상기 애플리케이션 프로세스에 의한 액세스를 거부하는 단계를 포함하는

브로커 서비스 내의 방법.

청구항 6

제1항에 있어서,

상기 애플리케이션 컨테이너 내로 상기 애플리케이션 프로세스를 로딩하는 단계와,

상기 애플리케이션 컨테이너에 대한 식별자를 포함하는 상기 애플리케이션 프로세스를 위한 토큰을 생성하는 단계를 포함하되, 상기 토큰은 상기 애플리케이션 프로세스에 의해 변조되지 않는

브로커 서비스 내의 방법.

청구항 7

제1항에 있어서,

상기 애플리케이션 컨테이너는 파일 시스템 데이터로의 상기 애플리케이션 프로세스에 의한 직접 액세스를 거부하는

브로커 서비스 내의 방법.

청구항 8

기록된 프로그램 명령어를 갖는 컴퓨터 판독가능 저장 장치로서, 상기 명령어는 컴퓨팅 장치의 하나 이상의 프로세싱 장치에 의해 실행될 때, 상기 컴퓨팅 장치에서 운영하는 브로커 서비스를 내의 방법을 수행하고, 상기 방법은,

상기 컴퓨팅 장치에서, 애플리케이션 프로세스로부터의 데이터를 포함하는 상기 컴퓨팅 장치의 파일 시스템의 제 1 데이터와 관련된 액세스 요청을 수신하는 단계－상기 애플리케이션 프로세스는 런칭된 버전의 애플리케이션이고, 상기 애플리케이션 프로세스는 상기 파일 시스템으로의 상기 애플리케이션 프로세스에 의한 직접 액세

스를 차단하는 애플리케이션 컨테이너에 존재하며, 상기 액세스 요청은 상기 애플리케이션 컨테이너에 대한 식별자를 포함하는 상기 애플리케이션 프로세스에 대한 토큰 및 상기 액세스 요청에서 요청된 상기 제 1 데이터의 표시를 포함함－와,

상기 브로커 서비스가 상기 제 1 데이터의 파일 타입이 상기 애플리케이션과 현재 연관되고 상기 애플리케이션이 액세스하는 것이 허용된 파일 타입으로서 상기 애플리케이션에 대해 등록되는 하나 이상의 파일 타입에 포함된다고 판정할 경우, 상기 파일 시스템의 파일 저장소로부터 상기 제 1 데이터를 검색함으로써 상기 컴퓨팅 장치에서 운영하는 상기 브로커 서비스를 통해, 상기 제 1 데이터로의 상기 애플리케이션 프로세스에 의한 액세스를 가능하게 하는 단계를 포함하되, 상기 하나 이상의 파일 타입은 상기 애플리케이션 프로세스의 설치 동안 수신되는 애플리케이션 매니페스트로부터 판독되고, 상기 하나 이상의 파일 타입의 표시는 상기 브로커 서비스에 액세스 가능하고 상기 애플리케이션에 의해 액세스 불가능한 상기 컴퓨팅 장치의 안전한 위치에 저장되는

컴퓨터 판독가능 저장 장치.

청구항 9

제 8 항에 있어서,

상기 하나 이상의 파일 타입은 하나 이상의 파일 확장자, 파일 종류, 또는 다른 파일 속성 또는 메타데이터를 포함하고, 상기 가능하게 하는 단계는,

상기 브로커 서비스에 의해 액세스 가능하고 상기 애플리케이션 프로세스에 의해 액세스 불가능한 상기 안전한 위치에서 등록된 하나 이상의 파일 확장자, 파일 종류, 또는 다른 파일 속성 또는 메타데이터에 액세스하는 단계를 포함하는

컴퓨터 판독가능 저장 장치.

청구항 10

제 9 항에 있어서,

상기 애플리케이션 프로세스에 의한 액세스를 가능하게 하는 단계는,

상기 액세스 요청에서 요청된 상기 제 1 데이터의 표시에 기초하여 상기 제 1 데이터의 파일 타입을 결정하는 단계와,

상기 안전한 위치에서 상기 애플리케이션에 대한 상기 등록된 하나 이상의 파일 타입에 액세스하는 단계와,

상기 제 1 데이터의 파일 타입이 상기 등록된 하나 이상의 파일 타입에 포함되는지 여부를 판정하는 단계와,

상기 제 1 데이터의 파일 타입이 상기 등록된 하나 이상의 파일 타입에 포함되는 것으로 판정될 경우 상기 애플리케이션 프로세스가 상기 제 1 데이터에 액세스하는 것을 가능하게 하는 단계를 포함하는

컴퓨터 판독가능 저장 장치.

청구항 11

제 10 항에 있어서,

상기 애플리케이션 프로세스에 의한 액세스를 가능하게 하는 단계는,

상기 제 1 데이터의 파일 타입이 상기 등록된 하나 이상의 파일 타입에 포함되지 않는 것으로 판정될 경우 상기 제 1 데이터로의 상기 애플리케이션 프로세스에 의한 액세스를 거부하는 단계를 더 포함하는

컴퓨터 판독가능 저장 장치.

청구항 12

제 11 항에 있어서,

상기 거부하는 단계는,

상기 제 1 데이터의 파일을 판독하거나, 상기 제1 데이터의 폴더의 컨텐츠를 판독하거나, 상기 제 1 데이터의 파일 또는 폴더 중 적어도 하나를 기록하거나, 상기 제 1 데이터의 파일 또는 폴더의 이름을 변경하거나, 상기 제 1 데이터의 파일 또는 폴더를 이동시키거나, 또는 상기 제 1 데이터의 파일 또는 폴더에 걸쳐 복사하기 위한 상기 애플리케이션 프로세스에 의한 액세스를 거부하는 단계를 포함하는

컴퓨터 판독가능 저장 장치.

청구항 13

제 8 항에 있어서,

상기 애플리케이션 컨테이너 내로 상기 애플리케이션 프로세스를 로딩하는 단계와,

상기 애플리케이션 컨테이너에 대한 식별자를 포함하는 상기 애플리케이션 프로세스를 위한 토큰을 생성하는 단계를 포함하되, 상기 토큰은 상기 애플리케이션 프로세스에 의해 변조되지 않는

컴퓨터 판독가능 저장 장치.

청구항 14

제 8 항에 있어서,

상기 애플리케이션 컨테이너는 파일 시스템 데이터로의 상기 애플리케이션 프로세스에 의한 직접 액세스를 거부하는

컴퓨터 판독가능 저장 장치.

청구항 15

컴퓨팅 시스템으로서,

실행될 명령어를 저장하도록 구성된 적어도 하나의 메모리와,

상기 명령어를 실행하도록 구성된 적어도 하나의 프로세서 장치와,

상기 적어도 하나의 프로세서 장치 상에서 실행하는 브로커 서비스를 포함하되, 상기 브로커 서비스는,

애플리케이션 프로세스로부터의 데이터를 포함하는 상기 컴퓨팅 시스템의 파일 시스템의 제 1 데이터와 관련된 액세스 요청을 수신하고－상기 애플리케이션 프로세스는 런칭된 버전의 애플리케이션이고, 상기 애플리케이션 프로세스는 상기 파일 시스템으로의 상기 애플리케이션 프로세스에 의한 직접 액세스를 차단하는 애플리케이션 컨테이너에 존재하며, 상기 액세스 요청은 상기 애플리케이션 컨테이너에 대한 식별자를 포함하는 상기 애플리케이션 프로세스에 대한 토큰 및 상기 액세스 요청에서 요청된 상기 제 1 데이터의 표시를 포함함－,

상기 브로커 서비스가 상기 제 1 데이터의 파일 타입이 상기 애플리케이션과 현재 연관되고 상기 애플리케이션이 액세스하는 것이 허용된 파일 타입으로서 상기 애플리케이션에 대해 등록되는 하나 이상의 파일 타입에 포함된다고 판정할 경우, 상기 파일 시스템의 파일 저장소로부터 상기 제 1 데이터를 검색함으로써 상기 컴퓨팅 시스템에서 운영하는 상기 브로커 서비스를 통해, 상기 제 1 데이터로의 상기 애플리케이션 프로세스에 의한 액세스를 가능하게 하도록 구성되며, 상기 하나 이상의 파일 타입은 상기 애플리케이션 프로세스의 설치 동안 수신되는 애플리케이션 매니페스트로부터 판독되고, 상기 하나 이상의 파일 타입의 표시는 상기 브로커 서비스에 액세스 가능하고 상기 애플리케이션에 의해 액세스 불가능한 상기 컴퓨팅 장치의 안전한 위치에 저장되는

컴퓨팅 시스템.

청구항 16

제 15 항에 있어서,

상기 하나 이상의 파일 타입은 하나 이상의 파일 확장자, 파일 종류, 또는 다른 파일 속성 또는 메타데이터를 포함하고, 상기 브로커 서비스는,

상기 브로커 서비스에 의해 액세스 가능하고 상기 애플리케이션 프로세스에 의해 액세스 불가능한 상기 안전한 위치에서 등록된 하나 이상의 파일 확장자, 파일 종류, 또는 다른 파일 속성 또는 메타데이터에 액세스하도록 구성되는

컴퓨팅 시스템.

청구항 17

제 16 항에 있어서,

상기 브로커 서비스는,

상기 액세스 요청에서 요청된 상기 제 1 데이터의 표시에 기초하여 상기 제 1 데이터의 파일 타입을 결정하고,

상기 안전한 위치에서 상기 애플리케이션에 대한 상기 등록된 하나 이상의 파일 타입에 액세스하고,

상기 제 1 데이터의 파일 타입이 상기 등록된 하나 이상의 파일 타입에 포함되는지 여부를 판정하고,

상기 제 1 데이터의 파일 타입이 상기 등록된 하나 이상의 파일 타입에 포함되는 것으로 판정될 경우 상기 애플리케이션 프로세스가 상기 제 1 데이터에 액세스하는 것을 가능하게 하도록 구성되는

컴퓨팅 시스템.

청구항 18

제 17 항에 있어서,

상기 브로커 서비스는,

상기 제 1 데이터의 파일 타입이 상기 등록된 하나 이상의 파일 타입에 포함되지 않는 것으로 판정될 경우 상기 제 1 데이터로의 상기 애플리케이션 프로세스에 의한 액세스를 거부하도록 더 구성되는

컴퓨팅 시스템.

청구항 19

제 18 항에 있어서,

상기 브로커 서비스는,

상기 제 1 데이터의 파일을 판독하거나, 상기 제1 데이터의 폴더의 컨텐츠를 판독하거나, 상기 제 1 데이터의 파일 또는 폴더 중 적어도 하나를 기록하거나, 상기 제 1 데이터의 파일 또는 폴더의 이름을 변경하거나, 상기 제 1 데이터의 파일 또는 폴더를 이동시키거나, 또는 상기 제 1 데이터의 파일 또는 폴더에 걸쳐 복사하기 위한 상기 애플리케이션 프로세스에 의한 액세스를 거부하도록 구성되는

컴퓨팅 시스템.

청구항 20

제 15 항에 있어서,

상기 토큰은 상기 애플리케이션 프로세스에 의해 변조되지 않는

컴퓨팅 시스템.

발명의 설명

기 술 분 야

배 경 기 술

[0001] 애플리케이션은 하나 이상의 작업을 수행하기 위해 구현되고 컴퓨터 시스템 내에서 구동되는 실행가능 프로그램 코드를 포함한다. 애플리케이션에 대한 프로그램 코드를 형성하기 위해 사용될 수 있는 매우 다양한 타입의 프로그래밍 언어가 존재한다. 오피스 스위트 애플리케이션(office suite application), 데스크탑 애플리케이션, 모바일 애플리케이션, 웹 애플리케이션, 등을 포함하는 다양한 타입의 애플리케이션이 다양한 기능을 수행하기 위해 존재한다. 일부 애플리케이션은 이들의 기능을 수행할 때 사용될 이들의 호스트 컴퓨터 또는 다른 컴퓨터의 파일 시스템 내에 저장된 데이터를 액세스할 수 있다. 예를 들어, 워드 프로세싱 애플리케이션은 편집을 위해 텍스트 파일 또는 문서 파일을 액세스할 수 있다. 미디어 플레이어 애플리케이션은 재생을 위해 오디오 파일 및/또는 비디오 파일을 액세스할 수 있다. 데이터베이스 애플리케이션은 다양한 용도로 데이터베이스의 데이터베이스 파일 내의 데이터를 액세스할 수 있다.

[0002] 그러나, 애플리케이션은 일반적으로 그 애플리케이션과 관련되지 않은 파일 시스템 데이터를 포함하는 파일 시스템 데이터로의 액세스를 갖기 때문에, 매우 다양한 파일 시스템 데이터를 손상시키는 악성 프로그램 코드를 포함하는 애플리케이션에게 기회가 존재한다.

발명의 내용

[0003] 본 요약은 이하의 상세한 설명에서 추가로 기재되는 본 발명의 개념의 선택사항을 단순화된 형태로 소개하고자 제시된 것이다. 이 요약은 청구 대상의 주요 특징 또는 근본 특징을 식별하도록 의도된 것이 아니며, 청구 대상의 범주를 제한하기 위해 사용하도록 의도된 것도 아니다.

[0004] 애플리케이션에 의해 선택적 파일 시스템 액세스를 가능하게 하는 방법, 시스템 및 컴퓨터 프로그램 제품이 제공된다. 애플리케이션에 의한 파일 시스템 데이터의 액세스는 브로커 서비스에 의해 처리된다. 애플리케이션은 이와는 다르게 파일 시스템 데이터(그 자체 파일을 제외하고 그 자체 리소스의 다른 것)를 액세스하는 것이 차단된다. 브로커 서비스는 애플리케이션으로부터 파일 시스템 데이터를 액세스하기 위한 요청을 수신하고, 액세스될 요청된 데이터가 애플리케이션이 액세스되도록 허용되는 파일 타입으로 구성되는 경우, 브로커 서비스는 애플리케이션이 데이터를 액세스할 수 있도록 한다. 이와는 다르게, 애플리케이션은 데이터로의 액세스가 거부 또는 차단된다.

[0005] 일 방법 구현에 따라서, 애플리케이션은 컴퓨팅 장치 내에 설치된다. 애플리케이션과 연계된 애플리케이션 매니페스트가 수신된다. 애플리케이션 매니페스트는 애플리케이션이 액세스하도록 허용되는 하나 이상의 파일 타입을 표시한다. 표시된 파일 타입(들)은 브로커 서비스에 의해 액세스가능한 위치에 등록된다.

[0006] 게다가, 애플리케이션은 애플리케이션 프로세스로서 런칭될 수 있다. 애플리케이션 프로세스는 사용자 계정과 유사한 애플리케이션 컨테이너 내에 격리된다(사용자 계정을 갖는 사용자는 다른 사용자의 파일을 액세스할 수 없음). 애플리케이션 컨테이너는 파일 시스템 데이터로의 애플리케이션 프로세스에 의한 직접 액세스를 차단한다. 파일 시스템 데이터의 제1 데이터와 관련된 액세스 요청은 애플리케이션 프로세스로부터 브로커 서비스에 수신된다. 브로커 서비스는 제1 데이터의 파일 타입이 등록된 파일 타입(들)에 포함되는지를 결정할 때, 제1 데이터로의 애플리케이션 프로세스에 의한 액세스가 가능하다.

[0007] 시스템 구현에 따라서, 컴퓨팅 장치가 제공된다. 컴퓨팅 장치는 저장부 및 프로세싱 로직을 포함한다. 저장부는

컴퓨팅 장치 내에 설치된 애플리케이션 및 애플리케이션과 연계된 애플리케이션 매니페스트를 저장한다. 애플리케이션 매니페스트는 애플리케이션이 액세스하도록 허용되는 하나 이상의 파일 타입을 표시한다. 프로세싱 로직은 브로커 서비스를 포함하고, 브로커 서비스에 의해(애플리케이션에 의해서가 아님) 액세스가능한 위치에 파일 타입(들)을 등록한다. 브로커 서비스는 등록된 파일 타입(들)의 파일로의 애플리케이션에 의한 액세스를 제한하도록 구성된다.

[0008] 프로세싱 로직은 애플리케이션이 런칭될 때 애플리케이션 프로세스를 시작할 수 있고, 애플리케이션 컨테이너 내에 애플리케이션 프로세스를 포함할 수 있다. 애플리케이션 컨테이너는 파일 시스템 데이터로의 애플리케이션 프로세스에 의한 직접 액세스를 차단한다. 브로커 서비스는 애플리케이션 프로세스로부터 파일 시스템 데이터의 제1 데이터에 대한 액세스 요청을 수신한다. 프로세싱 로직은 브로커 서비스가 제1 데이터의 파일 타입이 등록된 파일 타입(들)에 포함되는지를 결정할 때 제1 데이터로의 애플리케이션 프로세스에 의한 액세스를 가능하게 한다.

[0009] 추가로, 애플리케이션에 의해 파일 시스템 데이터로의 선택적 액세스를 가능하게 하는 것을 포함하는 다양한 실시 형태, 및 추가 실시 형태를 가능하게 하기 위해 프로그램 코드/로직을 저장하는 컴퓨터-판독가능 저장 매체가 본 명세서에 기재된다.

[0010] 본 발명의 여러 실시 형태의 구조 및 동작뿐만 아니라 본 발명의 다른 특징 및 이점은 첨부된 도면을 참조하여 하기에서 상세하게 설명되어 있다. 본 발명은 본 명세서에 기재된 특정 실시 형태로 한정되지 않는다는 것을 주지하라. 이러한 실시 형태는 단지 예시를 목적으로 본 명세서에 제시되어 있다. 당업자라면 본 명세서에 포함된 교시에 기초한 추가적인 실시 형태가 명확할 것이다.

도면의 간단한 설명

[0011] 본 명세서에 포함되어 있고 본 명세서의 일부분을 형성하는 첨부된 도면은 본 발명을 설명하기 위한 것이고, 또한 그 상세한 설명과 함께 본 발명의 원리를 설명하고, 당업자들이 본 발명을 구성하고 사용할 수 있도록 하기 위해 제공되었다.

도 1은 예시적 실시 형태에 따라서 애플리케이션에 의해 파일 시스템 데이터로의 액세스를 조절하도록 구성된 컴퓨팅 장치의 블록 다이어그램을 도시한다.

도 2는 예시적 실시 형태에 따라서 브로커 서비스가 오퍼레이팅 시스템 내에 포함되는 컴퓨팅 장치의 블록 다이어그램을 도시한다.

도 3은 예시적 실시 형태에 따라서 애플리케이션에 의해 파일 시스템 데이터로의 액세스를 조절하기 위한 프로세스를 제공하는 흐름도를 도시한다.

도 4는 예시적 실시 형태에 따라서 파일 시스템 데이터로의 제어된 액세스를 위해 애플리케이션을 구성하고 설치하기 위한 프로세스를 제공하는 흐름도를 도시한다.

도 5는 예시적 실시 형태에 따라서 애플리케이션이 파일 시스템 데이터로의 제어된 액세스를 위해 구성되고 설치되는 컴퓨팅 장치의 블록 다이어그램을 도시한다.

도 6은 예시적 실시 형태에 따라서 애플리케이션 매니페스트의 블록 다이어그램을 도시한다.

도 7은 예시적 실시 형태에 따라서 애플리케이션 컨테이너 내에서 애플리케이션을 런칭하기 위한 프로세스를 제공하는 흐름도를 도시한다.

도 8은 예시적 실시 형태에 따라서 애플리케이션이 애플리케이션 컨테이너 내에서 런칭되는 컴퓨팅 장치의 블록 다이어그램을 도시한다.

도 9는 예시적 실시 형태에 따라서 애플리케이션 프로세스에 의해 파일 시스템 데이터로의 액세스를 제어하기 위하여 브로커 서비스를 사용하는 프로세스를 제공하는 흐름도를 도시한다.

도 10은 예시적 실시 형태에 따라서 브로커 서비스가 애플리케이션 프로세스에 의해 파일 시스템 데이터로의 액세스를 제어하는 컴퓨팅 장치의 블록 다이어그램을 도시한다.

도 11은 예시적 실시 형태에 따라서 애플리케이션 프로세스에 의해 파일 시스템 데이터로의 액세스를 제어하기

위하여 브로커 서비스를 사용하는 프로세스를 제공하는 흐름도를 도시한다.

도 12는 본 발명의 실시 형태를 구현하기 위하여 사용될 수 있는 예시적 컴퓨터의 블록 다이어그램을 도시한다.

본 발명의 특징 및 이점은 그 전체에 걸쳐 동일한 도면 부호가 대응하는 구성 요소를 식별하는 도면과 함께 이하에 제시된 상세한 설명을 숙지함으로써 더 명확해질 것이다. 도면에서, 동일한 도면 부호는 일반적으로 동일한, 기능적으로 유사한 및/또는 구조적으로 유사한 구성 요소를 나타낸다. 소정의 구성 요소가 첫 번째로 나타나는 도면은 대응하는 도면 부호 내에 가장 좌측 숫자로 표시되어 있다.

발명을 실시하기 위한 구체적인 내용

[0012] I. 도입

[0013] 본 명세서에는 본 발명의 특징들을 통합하는 하나 이상의 실시 형태가 개시된다. 개시된 실시 형태(들)는 단지 본 발명을 예시한다. 본 발명의 범위는 개시된 실시 형태(들)에 제한되지 않는다. 본 발명은 이에 첨부된 청구범위에 의해 정해진다.

[0014] 기재된 실시 형태가 특정 특징, 구조, 또는 특성을 포함할 수 있지만 모든 실시 형태가 특정 특징, 구조, 또는 특성을 필수적으로 포함하지 않을 수 있는 것을 나타내는 "일 실시 형태", "실시 형태", "예시적 실시 형태" 등이 본 명세서에서 참조된다. 게다가, 이러한 어구는 동일한 실시 형태를 필수적으로 지칭하지 않는다. 추가로, 특정 특징, 구조, 또는 특성이 실시 형태에 관하여 기재될 때, 이는 명시적으로 기재되든지 다른 실시 형태에 관하여 이러한 특징, 구조, 또는 특성을 구현하는 당업자의 지식 내에 있는 것으로 제안된다.

[0015] 본 발명의 다수의 예시적인 실시 형태가 다음과 같이 기재된다. 본 명세서에서 제공된 임의의 섹션/서브섹션도 제한을 의도하는 것이 아님을 알아야 한다. 실시 형태는 이 문헌 전체에 걸쳐서 기재되며, 임의의 유형의 실시 형태가 임의의 섹션/서브섹션 내에 포함될 수 있다.

[0016] II. 예시적 실시 형태

[0017] 실시 형태는 파일 시스템 데이터로의 애플리케이션에 의한 액세스를 조절/제한/제어하기 위한 기술에 관한 것이다. 애플리케이션은 이들의 기능을 수행하기 위하여 이들의 호스트 컴퓨터 시스템(및/또는 다른 컴퓨터 시스템)의 파일 시스템 내에 저장된 데이터를 액세스할 수 있다. 예를 들어, 워드 프로세싱 애플리케이션(word processing application)은 편집을 위해 텍스트 파일 또는 문서 파일을 액세스할 수 있다. 미디어 플레이어 애플리케이션은 재생을 위해 오디오 파일 및/또는 비디오 파일을 액세스할 수 있다. 데이터베이스 애플리케이션은 다양한 사용을 위해 데이터베이스 내에 저장된 데이터를 액세스할 수 있다. 그러나, 애플리케이션이 애플리케이션과 관련이 없는 파일 시스템 데이터를 포함할 수 있는 파일 시스템 데이터를 액세스할 수 있기 때문에, 악성 프로그램 코드를 포함하는 애플리케이션이 파일 시스템 데이터를 훔치거나, 매우 다양한 파일 시스템 데이터를 손상시키거나, 또는 다른 바람직하지 못한 행위를 할 기회가 존재한다.

[0018] 실시 형태는 애플리케이션이 상호작용하도록 구성되는 타입의 파일 시스템 데이터에 대해 애플리케이션에 의한 파일 시스템 데이터로의 액세스를 제한하는 이점을 제공한다. 예를 들어, 개발자 또는 다른 개인이 애플리케이션이 액세스가능하고/상호작용할 수 있는(예를 들어, 판독, 기록, 수정, 이름변경, 복사, 이동, 등) 하나 이상의 파일 타입의 표시(indication)을 제공할 수 있다. 파일 타입(들)(예를 들어, MP3 파일, 마이크로소프트(Microsoft)® 워드 파일(Word file), 등)은 애플리케이션이 컴퓨터 시스템에 설치될 때 등록될 수 있다. 애플리케이션이 실행되고 컴퓨터 시스템의 파일 시스템 데이터의 액세스를 시도할 때, 애플리케이션은 파일 시스템 데이터가 등록된 파일 타입(들)의 파일 타입을 갖는 경우 파일 시스템 데이터를 액세스할 수 있게 된다. 액세스되는 파일 시스템 데이터가 등록된 파일 타입(들)이 아닌 경우, 파일 시스템 데이터의 액세스는 거부 또는 차단될 수 있다. 애플리케이션은 예컨대, 그 자체의 파일 및 그 자체의 리소스의 다른 것들, 애플리케이션에 대한 임시 작업 디렉토리, 및 애플리케이션에 대한 셋팅 디렉토리와 같은 필수 애플리케이션 정보를 액세스할 수 있게 되지만, 이와는 달리 본 명세서에서 기재된 바와 같이 민감형 파일 시스템 데이터로의 액세스는 거부될 수 있다.

[0019] 실시 형태들이 다양한 환경에서 구현될 수 있다. 예를 들어, 도 1에는 예시적 실시 형태에 따른 컴퓨팅 장치(computing device, 102)의 블록 다이어그램이 도시된다. 도 1에 도시된 바와 같이, 컴퓨팅 장치(102)는 애플리케이션 프로세스(application process, 104), 브로커 서버(broker service, 106), 저장부(storage, 108), 및 애플리케이션(120)을 포함한다. 게다가, 저장부(108)는 복수의 폴더(110a- 110n)를 포함한다. 각각의 폴더(110a- 110n)는 하나 이상의 파일을 포함할 수 있다. 예를 들어, 폴더(110a)는 파일(112a-112n)을 포함하는 것

으로 도시된다. 폴더(110a-110n)와 파일(112a-112n)은 컴퓨팅 장치(102)의 파일 시스템의 파일 시스템 데이터(118) 내에 포함된다. 컴퓨팅 장치(102)는 하기와 같이 추가로 기재된다.

[0020] 컴퓨팅 장치(102)는 데스크탑 컴퓨터(예를 들어, 퍼스널 컴퓨터, 등), 모바일 컴퓨터 또는 컴퓨팅 장치(예를 들어, 팜(Palm)® 장치, 림 블랙베리(RIM Blackberry)® 장치, PDA(personal digital assistant), 랩탑 컴퓨터, 노트북 컴퓨터, 태블릿 컴퓨터(예를 들어, 애플 아이패드(Apple iPad)™), 넷북, 등), 모바일 폰(예를 들어, 휴대폰, 스마트폰(예컨대, 애플 아이폰(Apple iPhone), 구글 안드로이드(Google Android)™ 폰, 마이크로소프트 윈도우즈(Microsoft Windows)® 폰, 등), 또는 다른 타입의 모바일 장치를 포함하는 고정식 또는 이동식 컴퓨팅 장치의 임의의 타입일 수 있다.

[0021] 전술된 바와 같이, 컴퓨팅 장치(102)는 저장부(108)를 포함한다. 저장부(108)에는 자기 디스크(예를 들어, 하드 디스크 드라이브 내에), 광학 디스크(예를 들어, 광학 디스크 드라이브 내에), 자기 테이프(예를 들어, 테이프 드라이브 내에), 메모리 장치(예컨대, RAM 장치, ROM 장치, 등) 및/또는 임의의 다른 적합한 타입의 저장 매체를 포함하는, 폴더 및 파일을 저장하기 위한 하나 이상의 임의의 타입의 저장 기구가 포함될 수 있다. 저장부(108)는 도 1에 도시된 바와 같이 전적으로 로컬 저장부일 수 있거나, 또는 "클라우드(cloud)" 저장부 및 미디어 서버에서 이용가능한 저장부와 같이 네트워크에 걸쳐 액세스가능한 저장부를 포함하는, 컴퓨팅 장치(102)로부터 원격의 저장부를 선택적으로 포함할 수 있다. 게다가, 저장부(108)는 탈착가능 저장 장치를 포함할 수 있다. 도 1에 도시된 바와 같이, 파일 시스템 데이터(118)는 저장부(108) 내에 저장된다. 폴더(110a-110n)는 당업자에게 공지된 바와 같이 파일 시스템 데이터(118) 내에 포함된 가상 폴더이다. 폴더(110a-110n)는 계층으로(in a hierarchy) 및/또는 임의의 다른 배열로 조직화될 수 있다. 수십, 수백, 수천, 및 심지어 더 많은 개수의 폴더를 포함하는, 임의의 개수의 폴더(110)가 존재할 수 있고, 각각의 폴더(110)는 임의의 개수의 파일을 포함할 수 있다. 파일(112a-112n)은 당업자에게 공지된 바와 같이 데이터를 포함하는 컴퓨터 파일이다. 수십, 수백, 수천, 및 심지어 더 많은 개수의 파일의 포함하는, 임의의 개수의 파일(112)이 존재할 수 있다.

[0022] 브로커 서비스(106)는 컴퓨팅 장치(102) 내에서 실행될 수 있는(예를 들어, 하나 이상의 프로세서에 의해) 하나 이상의 프로세스(예를 들어, "브로커 프로세스")를 포함한다. 브로커 서비스(106)는 애플리케이션이 액세스하도록 허용되는 파일 시스템 데이터(118)의 데이터로의 애플리케이션에 의한 액세스를 제한하도록 구성된다. 브로커 서비스(106)의 프로그램 코드는 독립형 프로그램 코드일 수 있거나 또는 컴퓨터 장치(102)의 다른 프로그램 코드 내에 포함될 수 있다. 예를 들어, 도 2에는 예시적 실시 형태에 따른 컴퓨팅 장치(102)의 블록 다이어그램이 도시된다. 도 2에 도시된 바와 같이, 브로커 서비스(106)는 컴퓨팅 장치(102)의 오퍼레이팅 시스템(202) 내에 포함될 수 있다. 선택적으로, 브로커 서비스(106)는 하드웨어 및/또는 컴퓨팅 장치(102)의 다른 리소스로의 애플리케이션에 의한 액세스를 제한하는 것을 포함하는 컴퓨팅 장치(102)용 추가 서비스를 제공할 수 있다.

[0023] 애플리케이션(120)은 컴퓨팅 장치(102) 내에서 실행하고/동작하는 소프트웨어 애플리케이션이고, 컴퓨팅 장치(102)의 저장부(예를 들어, 저장부(108)) 내에 저장될 수 있다. 예를 들어, 애플리케이션(120)은 오피스 스위트 애플리케이션, 데스크탑 애플리케이션, 모바일 애플리케이션, 웹 애플리케이션, 등일 수 있다. 오피스 스위트 애플리케이션에는 예컨대, 워드 프로세싱 애플리케이션, 스프레드시트 애플리케이션, 프레젠테이션 애플리케이션, 등과 같은 다양한 타입의 생산성 향상 애플리케이션이 포함된다. 데스크탑 애플리케이션에는 일부 오피스 스위트 애플리케이션, 데스크탑 위젯 또는 가젯(예컨대, 뉴스 스트리밍, 현재의 날씨를 제공하고 현재의 주식 시세를 나타내며, 등과 같이 전형적으로 단일 목적의 서비스를 제공하는 상호작용 도구(interactive tool)), 웹 브라우저, 등을 포함하는, (예를 들어, 데스크탑 컴퓨터의) 컴퓨터 데스크탑 내에서 동작하도록 구성되는 다양한 타입의 애플리케이션이 포함된다. 모바일 애플리케이션에는 예컨대, 스마트 폰, 태블릿 컴퓨터, PMP(portable media player), PDA(personal digital assistant), 등과 같은 모바일 핸드헬드 장치 내에서 동작하는 다양한 타입의 애플리케이션(예를 들어, "앱(App)")이 포함된다. 웹 애플리케이션(또한, "웹 앱" 또는 "웹 앱"으로 알려짐)은 예컨대, 인터넷 또는 인트라넷과 같은 네트워크에 걸쳐서 액세스가능한 애플리케이션이며, 애플리케이션을 랜더링하는 웹 브라우저 내에서 호스팅될 수 있다. 예시 애플리케이션에는 소셜 네트워킹 애플리케이션, 탐색 지원 애플리케이션(예를 들어, 맵핑 애플리케이션, 레스토랑-위치찾기 애플리케이션, 교통 애플리케이션, 등), 게이밍 애플리케이션, 재무설계 애플리케이션, 등이 포함된다.

[0024] 애플리케이션(120)은 예컨대, 애플리케이션 프로세스(104)와 같이 하나 이상의 애플리케이션 인스턴스 또는 "프로세스"를 스포닝하도록(spawn) 실행될 수 있다. 애플리케이션 프로세스(104)에는 애플리케이션(120)의 프로그램 코드(명령) 및 이의 현재 활동(current activity)이 포함된다. 애플리케이션 프로세스(104)는 컴퓨팅 장치(102)의 하나 이상의 프로세서 내에서 실행된다. 애플리케이션 프로세스(104)는 하나 이상의 실행 스레드(execution thread)를 포함할 수 있다. 다수의 실행 스레드가 존재 시에, 스레드는 프로그램 코드를 동시에 실

행할 수 있다.

[0025] 애플리케이션 프로세스(104)가 실행 중에, 애플리케이션 프로세스(104)는 예컨대, 파일(112a)과 같이 파일 시스템 데이터(118)의 데이터를 액세스하는 시도를 할 수 있다. 통상적인 시스템에 따라서 애플리케이션 프로세스(104)는 일부 제한을 갖는 파일(112a)을 액세스할 수 있다. 그러나, 애플리케이션 프로세스(104)는 악성 프로그램 코드(예를 들어, 애플리케이션(120)의 원래의 설계에 의해, 애플리케이션(120)에 침투된 바이러스 코드에 의해, 등)를 포함할 수 있거나, 또는 애플리케이션(120)의 사용자가 예상하지 못한 방식으로 파일(112a)을 액세스할 수 있다. 어느 경우에나, 애플리케이션 프로세스(104)는 파일(112a)을 액세스가능함으로써 손상이 야기될 수 있다.

[0026] 실시 형태는 파일 시스템 데이터로의 액세스를 제한함으로써 악성 애플리케이션 코드에 의해 야기되는 손상의 감소를 돕는다. 실시 형태에 따라서, 애플리케이션 프로세스(104)는, 현재의 예시가 파일(112a)인, 액세스되도록 요구되는 파일 시스템 데이터(118)의 데이터를 표시하는 데이터 액세스(114)를 생성할 수 있다. 도 1에 도시된 바와 같이, 데이터 액세스(114)는 브로커 서비스(106)에 의해 수신된다. 브로커 서비스(106)는 파일(112a)이 애플리케이션(120)이 액세스하도록 허용되는 파일 타입으로 형성되는지를 결정하도록 구성된다. 브로커 서비스(106)는 파일(112a)이 애플리케이션(120)이 액세스하도록 허용되는 파일 타입으로 형성되는 경우, 애플리케이션 프로세스(104)가 파일(112a)을 액세스할 수 있도록 한다. 이와 같은 경우 도 1에 도시된 바와 같이, 데이터 액세스(114)에서 요청된 데이터는 응답 데이터(116)와 같이 브로커 서비스(106)를 통하여 저장부(108)로부터 애플리케이션 프로세스(104)로 제공될 수 있거나, 또는 응답 데이터(116)는 애플리케이션 프로세스(104)가 데이터를 액세스할 수 있는 방식으로 표시될 수 있다. 예를 들어, 파일 또는 폴더에 대한 핸들(handle)은 애플리케이션(104)이 파일 또는 폴더를 액세스하도록 허용되는 응답 데이터(116) 내에서 애플리케이션 프로세스(104)로 보내질 수 있다. 이와는 달리, 브로커 서비스(106)는, 파일(112a)이 애플리케이션(120)이 액세스하도록 허용되지 않는 파일 타입을 갖는 경우, 파일(112a)로의 액세스를 거부할 수 있다. 브로커 서비스(106)는 액세스가 허용되지 않을 때, 파일의 판독, 폴더의 컨텐츠의 판독, 파일 또는 폴더의 기록, 파일 또는 폴더의 이름변경, 파일 또는 폴더의 이동, 또는 제1 데이터의 파일 또는 폴더에 걸친 복사를 위해 애플리케이션 프로세스(104)에 의한 액세스의 거부를 포함하는, 애플리케이션 프로세스(104)에 의한 파일 및 폴더와의 다양한 상호작용을 거부할 수 있다.

[0027] 컴퓨팅 장치(102)는 이의 기능을 수행하도록 다양한 방식으로 동작할 수 있다. 예를 들어, 도 3에는 예시적 실시 형태에 따라 애플리케이션에 의해 파일 시스템 데이터로의 액세스를 조절하기 위한 프로세스를 제공하는 흐름도(300)가 도시된다. 흐름도(300)는 도 1에 관해 하기와 같이 기재된다. 추가 구조적 및 작동상 실시 형태가 흐름도(300)에 대한 하기 논의를 기초로 당업자(들)에게 자명할 것이다.

[0028] 흐름도(300)는 단계(302)로부터 시작된다. 단계(302)에서, 애플리케이션에 대한 액세스가능 파일 타입이 등록된다. 예를 들어, 실시 형태에서, 애플리케이션(120)의 애플리케이션 프로세스가 액세스하도록 허용되는 하나 이상의 파일 타입이 컴퓨팅 장치(102)의 데이터 구조물(예를 들어, 레지스트리) 내에 등록된다. 데이터 구조물은 저장부(108) 또는 컴퓨팅 장치(102)와 연계된 다른 저장부에 저장될 수 있다.

[0029] 단계(304)에서, 애플리케이션의 프로세스에 의한 액세스는 등록된 액세스가능 파일 타입으로 제한된다. 예를 들어, 실시 형태에서, 브로커 서비스(106)는 애플리케이션(120)에 대해 등록된 액세스가능 파일 타입을 포함하는 데이터 구조물을 액세스할 수 있다. 브로커 서비스(106)가 애플리케이션 프로세스(104)와 같이 애플리케이션(120)의 애플리케이션 프로세스로부터 데이터에 대한 요청을 수신할 때, 브로커 서비스(106)는 요청된 데이터가 애플리케이션 프로세스가 액세스하도록 허용되는 파일 타입을 갖는지 여부를 결정하기 위해 데이터 구조물을 액세스할 수 있다. 브로커 서비스(106)는 데이터가 허용가능 파일 타입인 경우 애플리케이션 프로세스가 데이터를 액세스하도록 허용할 수 있거나, 또는 데이터가 허용가능 파일 타입이 아닌 경우 요청에 대한 액세스를 거부할 수 있다. 애플리케이션(120)으로부터 형성되는 임의의 개수의 애플리케이션 프로세스는 심지어 동시에 이 방식으로 제한된 이들의 파일 시스템 데이터 액세스를 가질 수 있다.

[0030] 브로커 서비스(106)를 포함하는 컴퓨팅 장치(102)는 실시 형태에서 다양한 방식으로 그의 기능을 수행할 수 있다. 컴퓨팅 장치(102), 브로커 서비스(106), 및 흐름도(300)에 대한 다수의 예시적인 실시 형태가 하기 서브섹션에서 기재된다. 예를 들어, 다음의 서브섹션에는 파일 시스템 데이터로의 제어된 액세스를 위해 구성된 애플리케이션을 설치하는 예시적 실시 형태가 기재된다. 다음의 서브섹션에는 제어된 파일 시스템 데이터 액세스를 갖는 애플리케이션을 런칭하고, 뒤이어 런칭된 애플리케이션에 대해 파일 시스템 데이터로의 제한된 액세스를 제공하기 위한 예시적 실시 형태를 기재하는 섹션을 수반하는 예시적 실시 형태가 기재된다.

[0031] A. 제어된 파일 시스템 데이터 액세스에 대해 애플리케이션을 설치하기 위한 예시적 실시 형태

[0032] 예시적 실시 형태에 따라서, 애플리케이션은 파일 시스템 데이터로의 제어된 액세스를 갖도록 컴퓨팅 장치 내에 설치될 수 있다. 실시 형태에서, 설치의 일부로서, 개발자 또는 다른 사용자는 하나 이상의 안전 위치에서 그들의 애플리케이션에 대한 액세스가능 파일 타입을 등록가능하게 한다. 안전 위치(들)는 그 후에 애플리케이션에 의한 파일 시스템 데이터로의 액세스가 가능하도록 브로커 서비스에 의해 액세스될 수 있다. 그러나, 안전 위치(들)는 애플리케이션에 의해 액세스되지 않을 수 있다. 이 방식으로, 애플리케이션에 대한 액세스가능 파일 타입은 애플리케이션이 파일 시스템에 대한 손상을 야기할 수 있도록 템퍼링되지(tampered) 않을 수 있다.

[0033] 예를 들어, 도 4에는 예시적 실시 형태에 따라서 파일 시스템 데이터로의 제어된 액세스를 위해 애플리케이션을 설치 및 구성하기 위한 프로세스를 제공하는 흐름도(400)가 도시된다. 흐름도(400)는 도 3에서 흐름도(300)의 단계(302)의 예시 구현을 제공한다. 흐름도(400)는 실시 형태에서 도 1의 컴퓨팅 장치(102)에 의해 수행될 수 있다. 흐름도(400)는 도 5에 따라 다음과 같이 기재된다. 도 5에는 애플리케이션이 예시적 실시 형태에 따라 파일 시스템 데이터로의 제어된 액세스를 위해 설치 및 구성되는 컴퓨팅 장치(102)의 블록 다이어그램이 도시된다. 도 5에 도시된 바와 같이, 컴퓨팅 장치(102)를 프로세싱 로직(processing logic, 502) 및 저장부(108)를 포함한다. 프로세싱 로직(502)은 애플리케이션 인스톨러(506), 파일 시스템 등록 모듈(508), 및 식별자 생성기(identifier generator, 520)를 포함한다. 추가 구조적 및 작동상 실시 형태가 도 5의 컴퓨팅 장치(102) 및 흐름도(400)에 관한 하기 논의를 기초로 당업자(들)에게 자명할 것이다.

[0034] 흐름도(400)는 단계(402)로부터 시작된다. 단계(402)에서, 애플리케이션이 컴퓨팅 장치에 설치된다. 예를 들어, 도 1에 도시된 바와 같이 애플리케이션 정보(512)가 컴퓨팅 장치(102)에서 수신될 수 있다. 애플리케이션 정보(512)는 예컨대, 도 1의 애플리케이션(120)과 같이 애플리케이션을 형성하는 모든 파일 및/또는 데이터를 포함한다. 애플리케이션 정보(512)는 컴퓨팅 장치(102)와 연계된 (예를 들어, 디스크 드라이브 내에 삽입된, 커넥터 내에 플러깅된, 등) 컴퓨터-판독가능 저장 매체(예를 들어, CDROM(compact disc read only memory) 장치, 플로피 디스크, 메모리 스틱(예를 들어, USB(universal serial bus) 저장 장치), 등), 예컨대, LAN(근거리 네트워크), WAN(광대역 네트워크), 또는 인터넷과 같은 네트워크들의 조합(예를 들어, "클라우드"-기반 서비스)과 같은 네트워크에 걸친 원격 서비스, 및/또는 다른 소스를 포함하는 다양한 소스로부터 수신될 수 있다.

[0035] 도 5에 도시된 바와 같이, 애플리케이션 인스톨러(506)는 애플리케이션 정보(512)를 수신한다. 애플리케이션 인스톨러(506)는 애플리케이션을 설치하기 위해 컴퓨팅 장치(102)의 저장부(108) 내에 애플리케이션 정보(512)를 설치하도록 구성된다. 애플리케이션 인스톨러(506)는 본 명세서에 기재된 바와 같이 애플리케이션을 설치하도록 구성되고 당업자(들)에게 공지된 애플리케이션 설치 프로그램을 포함하는 독점적 또는 상용입수가능한 애플리케이션 설치 프로그램일 수 있다.

[0036] 도 5에 도시된 바와 같이, 애플리케이션 인스톨러(506)는 저장부(108) 내의 애플리케이션 패키지(510)로서 애플리케이션을 설치하기 위하여 애플리케이션 정보(512)를 처리한다. 애플리케이션 패키지(510)는 애플리케이션 프로그램 코드(514)를 포함한다. 애플리케이션 프로그램 코드(514)는 설치된 애플리케이션의 기능을 형성하는 실행가능 코드(하나 이상의 프로세서에 의해)이다. 애플리케이션 프로그램 코드(514)는 하나 이상의 파일의 형태 및/또는 다른 형태를 가질 수 있다. 애플리케이션 인스톨러(506)는 컴퓨팅 장치(102) 내에 애플리케이션 프로그램 코드(514)를 설치하도록 구성된다.

[0037] 재차 도 4를 참조하면, 단계(404)에서 애플리케이션과 연계된 애플리케이션 매니페스트가 수신되고, 애플리케이션 매니페스트는 애플리케이션이 액세스하도록 허용되는 하나 이상의 파일 타입을 표시한다. 예를 들어, 도 5에 도시된 바와 같이, 애플리케이션 패키지(510)는 애플리케이션 매니페스트(516)를 포함한다. 애플리케이션 매니페스트(516)는 객체(예를 들어, 하나 이상의 파일)이다. 애플리케이션 인스톨러(506)는 컴퓨팅 장치(102)의 저장부(108) 내에 애플리케이션 매니페스트(516)를 저장하도록 구성된다.

[0038] 애플리케이션 매니페스트(516)는 애플리케이션이 액세스하도록 허용되는 하나 이상의 파일 타입의 표시를 포함한다. 게다가, 애플리케이션 매니페스트(516)는 애플리케이션과 연계된 추가 정보를 선택적으로 포함할 수 있다. 예를 들어, 도 6에는 예시적 실시 형태에 따른 애플리케이션 매니페스트(516)의 블록 다이어그램이 도시된다. 도 6에 도시된 바와 같이, 애플리케이션 매니페스트(516)는 액세스가능 파일 타입 정보(602), 식별 정보(604), 및 능력 정보(606)를 포함한다. 다른 실시 형태에서, 애플리케이션 매니페스트(516)는 도 6에 도시된 것 이외에 추가 및/또는 대안의 정보를 포함할 수 있다.

[0039] 액세스가능 파일 타입 정보(602)는 연계된 애플리케이션이 액세스하도록 허용되는 하나 이상의 파일 타입의 표

시를 포함한다. "파일 타입"은 예컨대, 파일 확장자, 파일 종류 및/또는 다른 파일 속성 또는 메타데이터에 의해 파일의 클래스들을 형성하고 이들 간을 구별한다. 이와 같이, 파일 타입 정보(602)는 애플리케이션에 의해 액세스가능한 데이터(예를 들어, 파일, 폴더, 등)를 형성하기 위해 사용될 수 있는 하나 이상의 파일 타입(파일 확장자, 파일 종류, 및/또는 다른 파일 속성 또는 메타데이터에 의해)을 표시할 수 있다. 파일 타입은 다양한 방식으로 액세스가능 파일 타입 정보(602)로 표시될 수 있다. 예를 들어, 파일 타입은 파일 타입 패밀리 및/또는 파일 타입 클래스와 같이 파일 타입의 그룹으로 및/또는 개별 파일 타입으로서 액세스가능 파일 타입 정보(602)로 표시될 수 있다. 파일 타입은 전형적으로 파일 이름에서 마지막 점(last period) 이후의 몇몇 영숫자 문자인 파일 확장자에 의해 액세스가능 파일 타입 정보(602)로 표시될 수 있다. 예를 들어, 개별 파일 타입에 관하여, 텍스트 파일에 대한 파일 타입 확장자는 ".txt"일 수 있고, MPEG(moving pictures experts group) 비디오 파일에 대한 파일 타입 확장자는 ".mpg"일 수 있고, 파형 오디오 파일 포맷 오디오 파일에 대한 파일 타입 확장자는 ".wav", 등일 수 있다. 파일 타입 패밀리는 통상 제품에 대한 파일 타입(예를 들어, 제품의 상이한 버전과 연계된 상이한 파일 타입)의 그룹과 같이 패밀리로 관련되는 다수의 파일 타입(예를 들어, 해당 파일 확장자에 의해)을 포함한다. 예를 들어, 마이크로소프트® 워드(워드 프로세싱 애플리케이션) 파일 타입 패밀리는 파일 타입 확장자 ".doc" 및 ".docx"를 포함할 수 있고, 이는 이전의 마이크로소프트® 워드 2007 버전과 마이크로소프트® 워드 2007 및 후속 버전에 각각 관련된다. 파일 타입 클래스는 예컨대, 오디오 클래스, 비디오 클래스, 워드 프로세싱 클래스, 데이터베이스 클래스, 등과 같은 제품 클래스에 의해 관련되는 다수의 파일 타입을 포함한다. 예를 들어, 음악 또는 오디오 클래스 파일 타입은 예컨대, ".wav", ".mp3", ".aiff ', 등과 같은 음악 및/또는 음성과 연계된 다수의 파일 확장자를 포함할 수 있다.

[0040] 식별 정보(604)는 애플리케이션에 대한 식별 정보를 포함한다. 예를 들어, 식별 정보(604)는 애플리케이션 및/또는 애플리케이션 패키지의 하나 이상의 이름, 애플리케이션의 퍼블리셔, 애플리케이션의 아키텍처, 리소스 타입(예를 들어, en-us, 등과 같은 언어 타입), 애플리케이션의 버전 및/또는 다른 식별 정보를 포함할 수 있다.

[0041] 능력 정보(606)는 애플리케이션 프로그램 코드(514)의 실행을 통하여 형성된 애플리케이션 프로세스가 액세스하도록 허용되고 및/또는 허용되지 않는 컴퓨팅 장치(102)의 능력을 표시한다. 이와 같이 표시된 능력의 예시에는 컴퓨팅 장치(102)의 저장 장치가 액세스가능한지를 표시하는 것(예를 들어, 내부 및/또는 외부 저장 장치), 크레덴셜(credential)이 액세스가능한지를 표시하는 것, 소프트웨어 및/또는 하드웨어 인증이 액세스가능한지를 표시하는 것, 입력/출력 장치(예를 들어, 마이크로폰, 웹캠 등)가 액세스가능한지를 표시하는 것, 컴퓨팅 장치(102)로부터의 원격의 엔티티와의 통신이 수행될 수 있는지를 표시하는 것, 등이 포함된다. 능력 정보(606)는 선택적으로 존재하며, 애플리케이션이 데이터를 액세스할 수 있는 예시적 방법이다. 예를 들어, 표시된 능력은 브로커 서비스(106)가 액세스할 수 있는 특정 위치(예를 들어, 픽쳐 라이브러리)에 대한 모든 파일 타입을 나타낼 수 있다.

[0042] 재차 도 4를 참조하면, 단계(406)에서 애플리케이션 매니페스트에 의해 표시된 하나 이상의 파일 타입이 브로커 서비스에 의해 액세스가능한 위치에 등록된다. 예를 들어, 실시 형태에서, 도 5에 도시된 바와 같이, 파일 타입 등록 모듈(508)은 애플리케이션이 액세스하도록 허용되는(예를 들어, 액세스가능 파일 타입 정보(602)에 표시된 바와 같이) 하나 이상의 파일 타입을 결정하기 위하여 애플리케이션 매니페스트(516)를 판독할 수 있다. 파일 타입 등록 모듈(508)은 파일 타입(들)(518)과 같이 안전 저장 위치(504)에 하나 이상의 파일 타입의 표시를 저장함으로써 하나 이상의 파일 타입을 등록하도록 구성된다. 도 5에 도시된 바와 같이, 안전 저장 위치(504)는 저장부(108)의 저장 위치(예를 들어, 저장부의 영역)일 수 있거나, 또는 대안으로 개별 저장부 내에 있을 수 있다. 안전 저장 위치(504)는 안전한(예를 들어, 특권이 있는) 것으로 여겨지며, 이는 애플리케이션의 애플리케이션 프로세스가 이 내에 저장된 데이터를 액세스할 수 없기 때문이다. 이와 같이, 악성 애플리케이션은 파일 타입(들)(518)으로 형성된 것들 이외의 파일 타입을 액세스할 수 있도록 파일 타입(들)(518)을 변조하지 않을 수 있고, 이에 따라 악성 애플리케이션이 파일 시스템 데이터에 대한 손상을 야기하는 가능성이 줄어든다.

[0043] 게다가, 도 6에 도시된 바와 같이 식별자 생성기(520)는 애플리케이션 매니페스트(516)로부터 정보를 수신하고, 보안 식별자(security identifier, 522)를 생성할 수 있다. 보안 식별자(522)는 컴퓨팅 장치(102) 내에서, 애플리케이션에 대해 실행되는 애플리케이션 프로세스를 포함한, 애플리케이션 패키지(510)와 연계된 애플리케이션을 식별하기 위하여 사용될 수 있는 고유 식별자이다. 보안 식별자(522)는 제2 사용자의 액세스 파일로부터 제1 사용자 계정을 갖는 제1 사용자에 의해 액세스를 제한하는, 사용자 계정에 대한 사용자 식별자와 유사하다. 보안 식별자(522)는 애플리케이션 패키지와 일련의 파일 타입 및/또는 능력을 연계하고, 애플리케이션이 디폴트에 의해 파일 시스템의 데이터로의 액세스를 갖지 않도록 보장하기 위하여 사용될 수 있다. 예를 들어, 보안 식별자(522)는 ACL(access control list)를 포함하는 컴퓨팅 장치(102) 내에서 보안 동작에 관하여 애플리케이션

프로세스를 식별하기 위해 사용될 수 있다. 보안 식별자(522)를 포함하는 컴퓨팅 장치(102)의 ACL은 연계된 애플리케이션이 액세스할 수 있는 컴퓨팅 장치(102)의 리소스를 식별할 수 있다. 보안 식별자(522)가 ACL 내에 포함되지 않는 경우, 애플리케이션은 보안이 ACL에 의해 처리되는 임의의 리소스로의 액세스를 갖지 않는다.

[0044] 보안 식별자(SID)(522)는 상용입수가능한 기술 및/또는 독점 기술을 비롯한 임의의 방식으로 애플리케이션에 대해 생성될 수 있다. 예를 들어, 보안 식별자(522)는 애플리케이션 패키지(510)의 패키지 식별자(패키지 식별자 SID)를 기초로 생성될 수 있다. 패키지 식별자를 기초로 보안 식별자(522)의 생성은 애플리케이션 패키지(510)의 패키지 식별자의 모든 요소를 기초로 또는 단지 요소의 서브세트(예를 들어, 패키지의 패밀리 식별자 - 패키지 식별자로부터의 이름 및 퍼블리셔)를 기초로 보안 식별자를 생성하는 것을 포함할 수 있다. 또 다른 실시 형태에서, 보안 식별자(522)는 식별 정보(604)로부터 정보의 해시(hash)로서 생성될 수 있다. 예를 들어, 보안 식별자(522)는 애플리케이션 및/또는 애플리케이션 패키지(510)의 이름, 애플리케이션의 퍼블리셔, 애플리케이션의 아키텍처, 애플리케이션의 버전, 등 중 하나 이상의 해시로서 생성될 수 있다.

[0045] B. 제어된 파일 시스템 데이터 액세스를 갖는 애플리케이션을 런칭하기 위한 예시적 실시 형태

[0046] 예시적 실시 형태에 따라서, 애플리케이션 프로세스는 컴퓨팅 장치(102)에 등록되고 형성된 허용가능 파일 타입을 갖는 애플리케이션에 대해 런칭될 수 있다. 실시 형태에서, 애플리케이션 프로세스는 파일 시스템 데이터로의 애플리케이션 프로세스에 의한 액세스를 차단하는 애플리케이션 컨테이너 내에 포함될 수 있다.

[0047] 예를 들어, 도 7에는 예시적 실시 형태에 따라 파일 시스템 데이터로의 제어된 액세스를 갖는 애플리케이션을 런칭하기 위한 프로세스를 제공하는 흐름도(700)가 도시된다. 흐름도(700)는 실시 형태에서 도 1의 컴퓨팅 장치(102)에 의해 수행될 수 있다. 흐름도(700)는 도 8에 따라 다음과 같이 기재된다. 도 8에는 설치된 애플리케이션이 런칭되고 생성된 애플리케이션 프로세스가 예시적 실시 형태에 따라 파일 시스템 데이터로의 제어된 액세스를 갖는, 컴퓨팅 장치(102)의 블록 다이어그램이 도시된다. 도 8에 도시된 바와 같이, 컴퓨팅 장치(102)는 프로세싱 로직(502), 저장부(108), 및 메모리(810)를 포함한다. 프로세싱 로직(502)은 애플리케이션 런처(application launcher, 802)를 포함하고, 애플리케이션 런처(802)는 토큰 생성기(token generator, 804)를 포함한다. 추가 구조적 및 작동상 실시 형태가 도 8의 컴퓨팅 장치(102) 및 흐름도(700)에 관한 하기 논의를 기초로 당업자(들)에게 자명할 것이다.

[0048] 흐름도(700)는 단계(702)로부터 시작된다. 단계(702)에서, 애플리케이션은 애플리케이션 프로세스로서 런칭된다. 예를 들어, 도 8에 도시된 바와 같이 애플리케이션 런처(802)는 애플리케이션 프로세스(104)를 형성하기 위하여 도 1의 애플리케이션(120)과 같이 애플리케이션을 런칭하도록 구성될 수 있다. 애플리케이션 런처(802)는 당업자(들)에게 공지된 통상적인 기술에 따라 또는 독점 기술을 비롯한 다양한 방식으로 애플리케이션 프로세스(104)를 형성하기 위하여 애플리케이션(120)을 런칭하도록 구성될 수 있다. 도 8에 도시된 바와 같이, 애플리케이션 프로세스(104)는 메모리(810)에 로딩될 수 있다. 이 방식으로, 애플리케이션 프로세스(104)의 프로그램 코드는 애플리케이션 프로세스(104)를 실행하는 컴퓨팅 장치(102)의 하나 이상의 프로세스에 의해 용이하게 액세스될 수 있다.

[0049] 단계(704)에서, 애플리케이션 프로세스는 애플리케이션 컨테이너 내에 포함된다. 예를 들어, 도 8에 도시된 바와 같이, 애플리케이션 프로세스(104)는 애플리케이션 컨테이너(806)에 포함된다. 애플리케이션 컨테이너(806)는 파일 시스템 데이터로의 애플리케이션 프로세스(104)에 의한 직접 액세스를 차단하는 애플리케이션 프로세스(104)에 대한 가상 컨테이너이다. 애플리케이션에 대한 애플리케이션 컨테이너(806)는 사용자 계정이 다른 사용자의 정보로의 사용자에 의한 액세스를 제한하기 위해 사용되는 사용자에 대한 사용자 계정과 유사하다. 유사한 방식으로, 애플리케이션 컨테이너(806)는 다른 정보로의 애플리케이션에 의한 액세스를 제한한다. 애플리케이션 프로세스(104)는 예컨대, 디폴트를 통하여 파일 시스템의 민감형 부분으로의 애플리케이션 프로세스(104)에 의한 액세스를 제한하는 애플리케이션 프로세스(104)에 대한 토큰에 적용된 애플리케이션 컨테이너(806)와 연계된 보안 식별자를 가짐으로써 다양한 방식으로 애플리케이션 컨테이너(806) 내에 "포함"될 수 있다. 이러한 민감형 파일 시스템 부분은 예컨대, 애플리케이션 패키지(510)의 리소스, 작업 디렉토리, 및 설정 디렉토리와 같이 애플리케이션 프로세스(104) 자체에 대한 필수 파일/폴더를 포함하지 않는다. ACL은 애플리케이션 프로세스(104)가 이들 필수 아이템을 액세스할 수 있도록 적절히 설정될 수 있다.

[0050] 예를 들어, 실시 형태에서, 애플리케이션(120)에 대해 생성된 보안 식별자(522)(예를 들어, 전술된 바와 같이)는 애플리케이션 컨테이너(806)에 대한 액세스 제한을 형성하기 위하여 사용될 수 있고 애플리케이션 컨테이너(806)와 연계될 수 있다. 보안 식별자(522)에 대해 형성된 액세스가능 리소스(예를 들어, 하나 이상의 ACL 내에서)는 애플리케이션 컨테이너(806), 이에 따라 애플리케이션 컨테이너(806) 내의 애플리케이션 프로세스(104)에

적용될 수 있다. 예를 들어, 실시 형태에서, 보안 식별자(522)는 파일 시스템 데이터와 연계된 임의의 ACL 내에 포함되지 않을 수 있다. 이와 같이, 애플리케이션 컨테이너(806), 이에 따라 애플리케이션 프로세스(104)는 파일 시스템 데이터로의 직접 액세스를 갖는 것이 불가능할 수 있다. 이 방식으로, 애플리케이션 컨테이너(806)는 파일 시스템 데이터로부터 애플리케이션 프로세스(104)를 격리시킨다. 대신에, 애플리케이션 프로세스(104)는 본 명세서에 기재된 실시 형태에 따라서 브로커 서비스(106)를 통하여 파일 시스템 데이터의 액세스로 제한된다. 추가로 상세하게 본 명세서에서 어디든 다른 곳에 기재된 바와 같이, 브로커 서비스(106)는 애플리케이션 프로세스(104)가 액세스할 수 있는 파일 시스템 데이터의 타입을 제어한다.

[0051] 도 8에 도시된 바와 같이, 토큰 생성기(804)는 애플리케이션 컨테이너(806)와 연계된 보안 식별자(522)를 수신할 수 있고, 애플리케이션 프로세스(104)에 대한 프로세스 토큰(812)을 생성할 수 있다. 프로세스 토큰(812)은 컴퓨팅 장치(102) 내에서 애플리케이션 프로세스(104)를 고유하게 식별하기 위하여 사용될 수 있다. 예를 들어, 프로세스 토큰(812)은 애플리케이션 프로세스의 다른 타입뿐만 아니라 동일한 애플리케이션(120)에 대해 생성된 애플리케이션 프로세스(104)의 추가 인스턴스로부터 애플리케이션 프로세스(104)를 구별할 수 있다.

[0052] 토큰 생성기(804)는 애플리케이션 매니페스트(516)와 연계된 추가 정보를 포함할 수 있고, 프로세스 토큰(812)을 생성하여 애플리케이션 컨테이너(806)를 식별하는 보안 식별자(522)를 포함하도록 구성될 수 있다. 예를 들어, 프로세스 토큰(812)은 능력 정보(606), 등을 기초로 생성된 하나 이상의 보안 식별자를 포함하는, 애플리케이션(120)에 대한 애플리케이션 매니페스트(516)의 정보로부터 생성되는 추가 보안 식별자를 선택적으로 포함할 수 있다.

[0053] 실시 형태에서, 프로세스 토큰(812)이 애플리케이션 프로세스(104)에 의해 변조되지 않을 수 있는 것을 주지하라. 예를 들어, 프로세스 토큰(812)은 메모리(810) 내의 안전 위치, 안전 저장 위치(504), 또는 다른 안전 저장 위치에 저장될 수 있다. 이 방식으로, 애플리케이션 프로세스(104)는 이와는 달리 액세스불가 파일 시스템 데이터를 액세스하도록 허용되는 프로세스 토큰(812)의 보안 식별자를 변조할 수 없으며, 이에 따라 파일 시스템에 대해 손상이 야기되는 것이 차단된다. 메모리(810)는 임의의 개수의 메모리 장치, 예컨대 RAM(random access memory) 장치를 포함할 수 있고, 저장부(108) 내에 또는 이와 떨어져서 포함될 수 있다.

[0054] C. 런칭된 애플리케이션에 대해 파일 시스템 데이터로의 대한 액세스를 제공하기 위한 예시적 실시 형태

[0055] 예시적 실시 형태에 따라서, 애플리케이션 프로세스는 파일 시스템 데이터로의 액세스가 제공될 수 있다. 실시 형태에서, 애플리케이션 프로세스는 이의 연계된 보안 식별자로 인해 제한된 파일 시스템 액세스를 가지며, 애플리케이션 컨테이너 내에 포함되기 때문에 파일 시스템 데이터를 직접 액세스할 수 없다. 대신에, 애플리케이션 프로세스는 중간 - 브로커 서비스를 통하여 파일 시스템 데이터를 액세스함으로써 파일 시스템 데이터를 간접적으로 액세스하도록 허용될 수 있다.

[0056] 예를 들어, 도 9에는 예시적 실시 형태에 따라서 애플리케이션 프로세스에 대해 파일 시스템 데이터로의 제어된 액세스를 제공하기 위한 프로세스를 제공하는 흐름도(900)가 도시된다. 흐름도(900)는 실시 형태에서 도 1의 컴퓨팅 장치(102)에 의해 수행될 수 있다. 흐름도(900)는 도 10에 따라 다음과 같이 기재된다. 도 10에는 설치된 애플리케이션이 미리 런칭되고 생성된 애플리케이션 프로세스가 예시적 실시 형태에 따라서 파일 시스템 데이터로의 제어된 액세스가 제공되는 컴퓨팅 장치(102)의 블록 다이어그램이 도시된다. 도 10에 도시된 바와 같이, 컴퓨팅 장치(102)는 프로세싱 로직(502) 및 저장부(108)를 포함한다. 프로세싱 로직(502)은 브로커 서비스(106)를 포함하고, 브로커 서비스(106)는 상태 매칭 로직(1002)을 포함한다. 추가 구조적 및 작동상 실시 형태가 도 10의 컴퓨팅 장치(102) 및 흐름도(900)에 관한 하기 논의를 기초로 당업자(들)에게 자명할 것이다.

[0057] 흐름도(900)가 단계(902)로부터 시작된다. 단계(902)에서, 액세스 요청이 파일 시스템 데이터의 제1 데이터에 대해 애플리케이션 프로세스로부터 브로커 서비스에서 수신된다. 예를 들어, 도 10에 도시된 바와 같이, 애플리케이션 프로세스(104)는 액세스되는 것이 요구되는 파일 시스템 데이터(118)의 데이터를 표시하는 데이터 액세스(114)를 생성한다. 실시 형태에서, 데이터 액세스(114)는 판독되거나, 기록되거나, 또는 변조될 데이터를 표시할 수 있다. 예를 들어, 본 예시에서, 데이터 액세스(114)는 파일(112a)이 판독될 것을 표시할 수 있다. 데이터 액세스(114)는 또한 애플리케이션 프로세스(104)에 의해 생성되는 바와 같이 데이터 액세스(114)를 식별하도록 프로세스 토큰(812)을 포함할 수 있다. 도 10에 도시된 바와 같이, 데이터 액세스(114)는 브로커 서비스(106)에 의해 수신된다.

[0058] 단계(904)에서, 제1 데이터로의 애플리케이션 프로세스에 의한 액세스는 브로커 서비스가 제1 데이터의 파일 타입이 등록된 하나 이상의 파일 타입에 포함되는 것을 결정할 때 허용될 수 있다. 브로커 서비스(106)는 파일

(112a)이 애플리케이션 프로세스(104)기 액세스하도록 허용되는 파일 타입으로 형성되는지를 결정하도록 구성된다. 예를 들어, 브로커 서비스(106)는 파일(112a)이 애플리케이션 프로세스(104)가 액세스하도록 허용되는 파일 타입을 갖는 경우에 애플리케이션 프로세스(104)가 파일(112a)을 액세스하도록 허용할 수 있다. 게다가, 브로커 서비스(106)는 파일(112a)이 애플리케이션 프로세스(104)가 액세스하도록 허용되지 않는 파일 타입을 갖는 경우 파일(112a)로의 애플리케이션 프로세스(104)에 의한 액세스를 거부할 수 있다.

[0059] 실시 형태에서, 브로커 서비스(106)는 도 11에 따라 흐름도(900)를 수행할 수 있다. 도 11에는 애플리케이션 프로세스에 의해 파일 시스템 데이터로의 액세스를 제어하도록 브로커 서비스를 사용하기 위해 프로세스를 제공하는 흐름도(1100)가 도시된다. 추가 구조적 및 작동상 실시 형태가 흐름도(1100)에 관한 하기 논의를 기초로 당업자(들)에게 자명할 것이다.

[0060] 흐름도(1100)는 단계(1102)로부터 시작된다. 단계(1102)에서, 액세스 요청에서 요청된 제1 데이터의 표시 및 토큰이 수신된다. 예를 들어, 전술된 바와 같이, 브로커 서비스(106)는 애플리케이션 프로세스(104)를 식별하기 위한 프로세스 토큰(812)을 포함하고, 액세스되도록 요구되는 파일 시스템 데이터(118)의 데이터를 표시하는 데이터 액세스(114)를 수신할 수 있다. 동작은 단계(1102)로부터 단계(1104)로 진행된다.

[0061] 단계(1104)에서, 제1 데이터의 파일 타입이 결정된다. 예를 들어, 데이터 액세스(114)에서 표시된 데이터 요청을 기초로, 브로커 서비스(106)는 요청된 데이터의 파일 타입을 결정할 수 있다. 브로커 서비스(106)는 데이터 액세스(114)에 포함된 요청된 데이터의 파일 확장자(예를 들어, .txt, .wav, .mpeg, 등과 같은 확장자)에 의해, 요청된 데이터의 파일 확장자를 결정하기 위해 저장부(108)에서 요청된 데이터의 액세스에 의해, 및/또는 다른 기술에 의해 요청된 데이터의 파일 타입을 결정할 수 있다. 동작은 단계(1104)로부터 단계(1106)로 진행된다.

[0062] 단계(1106)에서, 애플리케이션에 대해 등록된 파일 타입(들)이 안전 위치에서 액세스된다. 예를 들어, 실시 형태에서, 브로커 서비스(106)는 데이터 액세스(114) 내에 포함된 애플리케이션 프로세스(104)의 보안 식별자(522)를 결정할 수 있다. 브로커 서비스(106)는 결정된 보안 식별자(522)와의 이들의 연계에 의해 안전 저장 위치(504)에 저장된 애플리케이션 프로세스(104)에 대한 파일 타입(들)(518)을 식별할 수 있다. 브로커 서비스(106)는 안전 저장 위치(504)로부터 식별된 파일 타입(들)(518)을 검색할 수 있다. 동작은 단계(1106)로부터 단계(1108)로 진행된다.

[0063] 단계(1108)에서, 제1 데이터의 파일 타입이 등록된 파일 타입(들)에 포함되는지가 결정된다. 예를 들어, 실시 형태에서, 브로커 서비스(106)의 상태 매칭 로직(1002)은 요청된 데이터의 결정된 파일 타입(단계(1104)에서 결정됨)이 파일 타입(들)(518)에 관한 상태(단계(1006)에서 액세스됨)를 매칭하는지를 결정하도록 구성된다. 예를 들어, 상태 매칭 로직(1002)은 요청된 데이터의 결정된 파일 타입이 파일 타입(들)(518)에 포함된 파일 타입과 동일한지를 결정할 수 있다. 요청된 데이터의 파일 타입이 등록된 파일 타입(들)에 포함되지 않는 경우, 동작은 단계(1108)로부터 단계(1110)로 진행된다. 요청된 데이터의 파일 타입이 등록된 파일 타입(들)에 포함되는 경우, 동작은 단계(1108)로부터 단계(1112)로 진행된다.

[0064] 단계(1110)에서, 제1 데이터로의 애플리케이션 프로세스에 의한 액세스가 거부되다. 요청된 데이터의 파일 타입이 파일 타입(들)(518)들 중 하나의 파일 타입과 동일하지 않는 것으로 결정될 때, 요청된 데이터로의 애플리케이션 프로세스(104)에 의한 액세스가 브로커 서비스(106)에 의해 거부될 수 있다. 예를 들어, 애플리케이션 프로세스(104)가 특정 데이터(예를 들어, 특정 파일, 등)를 요청하는 경우, 애플리케이션 프로세스(104)는 특정 데이터로의 액세스를 차단할 수 있고, 데이터 액세스(114)의 거부는 애플리케이션 프로세스(104)에 대해 브로커 서비스(106)에 의해 표시될 수 있다. 또 다른 예시에서, 애플리케이션 프로세스(104)가 특정 폴더의 컨텐츠의 표시를 요청하는 경우, 액세스불가 파일 타입을 갖는 폴더의 파일은 브로커 서비스(106)에 의해 애플리케이션 프로세스(104)에 대해 보이도록 구성되지 않을 수 있다. 흐름도(1100)의 동작은 단계(1110)가 수행된 후에 완료된다.

[0065] 단계(1112)에서, 애플리케이션은 제1 데이터를 액세스하도록 허용될 수 있다. 요청된 데이터의 파일 타입이 파일 타입(들)(518)들 중 하나의 파일 타입과 동일한 것으로 결정될 때, 요청된 데이터로의 애플리케이션 프로세스(104)에 의한 액세스는 브로커 서비스(106)에 의해 획득될 수 있고, 요청된 데이터는 응답 데이터(116) 내에서 브로커 서비스(106)에 의해 애플리케이션 프로세스(104)에 제공될 수 있다. 실시 형태에서, 애플리케이션 프로세스(104)는 저장부(108)로부터 직접 응답 데이터(116)를 수신하도록 허용되는 것보다 브로커 서비스(106)에 의해 응답 데이터(116)가 제공될 수 있는 것으로 주지된다. 이 방식으로, 애플리케이션 프로세스(104)의 보안/특권 레벨은 애플리케이션 프로세스(104)가 응답 데이터(116)를 수신하기 위하여 높아질 필요는 없다. 흐름도(1100)의 동작은 단계(1112)가 수행된 후에 완료된다.

[0066] 예를 들어, 도식적 목적으로 제공되는 일 예시에서, 애플리케이션 프로세스(104)는 c:/home/user/userfile.doc의 파일이름/경로를 갖는 파일을 요청하기 위해 데이터 액세스(114)를 전송할 수 있다. 브로커 서비스(106)는 애플리케이션 컨테이너(806)/애플리케이션 프로세스(104)에 대한 보안 식별자(522) 및 파일이름/경로를 포함하는 데이터 액세스(114)를 수신할 수 있다. 브로커 서비스(106)는 이 파일이름/경로의 파일 타입이 ".doc"이도록 결정할 수 있다. 브로커 서비스(106)는 애플리케이션 컨테이너(806)/애플리케이션 프로세스(104)에 대한 보안 식별자(522)와 연계된 파일 타입(들)(518)을 액세스할 수 있다. 이 예시에서, 파일 타입(들)(518)은 ".doc", ".docx", ".txt", 및 ".wpd"의 파일 확장자를 포함할 수 있다. 상태 매칭 로직(1002)은 요청된 데이터에 대한 ".doc"의 파일 타입이 파일 타입(들)(518)의 파일 확장자와 동일하도록 결정할 수 있다. 이와 같이, 브로커 서비스(106)는 응답 데이터(116) 내의 애플리케이션 프로세스(104)로 c:/home/user/userfile.doc의 파일이름/경로를 갖는 파일을 제공할 수 있다.

[0067] 따라서, 다양한 특징과 이점이 실시 형태에 의해 제공된다. 예를 들어, 브로커 서비스(106)는 애플리케이션 컨테이너 내에 포함되는 애플리케이션 프로세스에 대해 파일 시스템 앱스트랙션(file system abstraction)을 제공한다. 브로커 서비스(106)는 애플리케이션 프로세스에 의해 데이터 액세스를 제한하기 위하여 정적으로 공인된 파일 타입을 사용한다. 공인된 파일 타입이 설치 시에 이는 브로커 서비스(106)로 등록된다. 격리된 애플리케이션 프로세스(애플리케이션 컨테이너 내에서)는 애플리케이션 프로세스가 파일 시스템의 개별 부분(예를 들어, 문서, 라이브러리, 탈착가능 저장부, 등)에 대한 액세스를 갖는 브로커 서비스(106)와 통신하기 위하여 보안 식별자를 이용한다. 이 방식으로, 애플리케이션에 대해 파일 시스템 데이터로의 필터링된 액세스가 제공된다. 브로커 서비스(106)의 인스턴스는 컴퓨팅 장치(102)에서 각각의 사용자에 대해 제공될 수 있거나(다수의 브로커 서비스(106)가 존재할 수 있도록), 또는 단일 브로커 서비스(106)가 모든 사용자를 처리할 수 있는 것으로 주지된다. 브로커 서비스(106)는 다수의 애플리케이션을 동시에 처리하거나 또는 단일의 애플리케이션을 처리하도록 구성될 수 있다.

[0068] III 예시적 컴퓨팅 장치 실시 형태

[0069] 브로커 서비스(106), 프로세싱 로직(502), 애플리케이션 인스톨러(506), 파일 타입 등록 모듈(508), 식별자 생성기(520), 애플리케이션 런처(802), 토큰 생성기(804), 조건 매칭 로직(1002), 흐름도(300), 흐름도(400), 흐름도(700), 흐름도(900), 및 흐름도(1100)는 하드웨어, 소프트웨어, 펌웨어, 또는 이의 임의의 조합으로 구현될 수 있다. 예를 들어, 브로커 서비스(106), 프로세싱 로직(502), 애플리케이션 인스톨러(506), 파일 타입 등록 모듈(508), 식별자 생성기(520), 애플리케이션 런처(802), 토큰 생성기(804), 조건 매칭 로직(1002), 흐름도(300), 흐름도(400), 흐름도(700), 흐름도(900), 및/또는 흐름도(1100)는 하나 이상의 프로세서 내에서 실행되도록 구성되는 컴퓨터 프로그램 코드로서 구현될 수 있다. 대안으로, 브로커 서비스(106), 프로세싱 로직(502), 애플리케이션 인스톨러(506), 파일 타입 등록 모듈(508), 식별자 생성기(520), 애플리케이션 런처(802), 토큰 생성기(804), 조건 매칭 로직(1002), 흐름도(300), 흐름도(400), 흐름도(700), 흐름도(900), 및/또는 흐름도(1100)는 하드웨어 로직/전기 회로로서 구현될 수 있다. 예를 들어, 실시 형태에서, 하나 이상의 브로커 서비스(106), 프로세싱 로직(502), 애플리케이션 인스톨러(506), 파일 타입 등록 모듈(508), 식별자 생성기(520), 애플리케이션 런처(802), 토큰 생성기(804), 조건 매칭 로직(1002), 흐름도(300), 흐름도(400), 흐름도(700), 흐름도(900), 및/또는 흐름도(1100)는 SoC(system-on-chip)에서 구현될 수 있다. SoC는 하나 이상의 프로세서(예를 들어, 마이크로컨트롤러, 마이크로프로세서, DSP(digital signal processor), 등), 메모리, 하나 이상의 통신 인터페이스, 및/또는 추가 회로 및/또는 이의 기능을 수행하기 위한 임베디드 펌웨어를 포함하는 집적 회로 칩을 포함할 수 있다.

[0070] 도 12는 본 발명의 실시 형태가 구현될 수 있는 컴퓨터(1200)의 예시적인 구현을 도시한다. 예를 들어, 컴퓨팅 장치(102)는 컴퓨터(1200)의 하나 이상의 특징부 및/또는 대안의 특징부를 포함하는 컴퓨터(1200)와 유사한 컴퓨터 시스템 내에서 구현될 수 있다. 컴퓨터(1200)는 예를 들어, 통상적인 퍼스널 컴퓨터, 모바일 컴퓨터, 서버, 또는 워크스테이션(workstation)의 형태를 갖는 범용 컴퓨팅 장치일 수 있거나, 또는 컴퓨터(1200)는 전용 컴퓨팅 장치일 수 있다. 본 명세서에 제공된 컴퓨터(1200)에 관한 설명은 설명을 목적으로 제공된 것이고, 제한하려는 의도가 아니다. 본 발명의 실시 형태는 당업자(들)에게 공지된 바와 같이 추가 타입의 컴퓨터 시스템에서 구현될 수 있다.

[0071] 도 12에 도시된 바와 같이, 컴퓨터(1200)는 하나 이상의 프로세서(1202), 시스템 메모리(1204) 및 시스템 메모리(1204)를 포함하는 다양한 시스템 구성요소를 프로세서(1202)에 결합하는 버스(bus, 1206)를 포함한다. 버스(1206)는 메모리 버스 또는 메모리 컨트롤러, 주변 버스, 가속 그래픽 포트(accelerated graphics port) 및 프로세서 또는 다양한 버스 아키텍처 중 임의의 것을 사용하는 로컬 버스를 포함하는 몇몇 타입의 버스 구조 중

임의의 하나 이상의 것을 표시한다. 시스템 메모리(1204)는 ROM(read only memory)(1208) 및 RAM(random access memory)(1210)을 포함한다. 기본 입/출력 시스템(1212)(BIOS)은 ROM(1208) 내에 저장된다.

[0072] 컴퓨터(1200)는 또한 하드 디스크로부터 판독 및 이에 기록하는 하드 디스크 드라이브(1214), 탈착가능 자기 디스크(1218)로부터 판독 또는 이에 기록하는 자기 디스크 드라이브(1216) 및 예컨대, CD ROM, DVD ROM, 또는 다른 광학 매체와 같은 탈착가능 광학 디스크(1222)로부터 판독 또는 이에 기록하는 광학 디스크 드라이브(1220) 중 하나 이상의 드라이브를 갖는다. 하드 디스크 드라이브(1214), 자기 디스크 드라이브(1216), 및 광학 디스크 드라이브(1220)는 각각 하드 디스크 드라이브 인터페이스(1224), 자기 디스크 드라이브 인터페이스(1226), 및 광학 드라이브 인터페이스(1228)에 의해 버스(1206)에 접속된다. 드라이브 및 그의 연계된 컴퓨터-판독가능 매체는 컴퓨터-판독가능 명령, 데이터 구조, 프로그램 모듈, 및 컴퓨터를 위한 다른 데이터의 비휘발성 저장부를 제공한다. 하드 디스크, 탈착가능 자기 디스크 및 탈착가능 광학 디스크가 기재되어 있으나, 예컨대, 플래시 메모리 카드, 디지털 비디오 디스크, RAM(random access memory), ROM(read only memory), 등과 같은 다른 타입의 컴퓨터-판독가능 저장 매체가 데이터를 저장하기 위해 사용될 수 있다.

[0073] 다수의 프로그램 모듈은 하드 디스크, 자기 디스크, 광학 디스크, ROM, 또는 RAM에 저장될 수 있다. 이들 프로그램은 오퍼레이팅 시스템(1230), 하나 이상의 애플리케이션 프로그램(1232), 다른 프로그램 모듈(1234) 및 프로그램 데이터(1236)를 포함한다. 애플리케이션 프로그램(1232) 또는 프로그램 모듈(1234)은 예를 들어, 브로커 서비스(106)를 구현하기 위한 컴퓨터 프로그램 로직(예를 들어, 컴퓨터 프로그램 코드), 프로세싱 로직(502), 애플리케이션 인스톨러(506), 파일 타입 등록 모듈(508), 식별자 생성기(520), 애플리케이션 런처(802), 토큰 생성기(804), 조건 매칭 로직(1002), 흐름도(300), 흐름도(400), 흐름도(700), 흐름도(900), 및/또는 흐름도(1100)(흐름도(300, 400, 700, 900, 1100)의 임의의 단계를 포함함), 및/또는 본 명세서에 기재된 추가 실시 형태를 포함할 수 있다.

[0074] 사용자는 예컨대, 키보드(1238) 및 포인팅 장치(1240)과 같은 입력 장치를 통해 컴퓨터(1200)에 명령 및 정보를 입력할 수 있다. 다른 입력 장치(도시되지 않음)는 마이크로폰, 조이스틱, 게임 패드, 위성 접시, 스캐너, 등을 포함할 수 있다. 이들 및 다른 입력 장치는 대개 버스(1206)에 결합된 직렬 포트 인터페이스(1242)를 통해 프로세서(1202)에 접속되지만, 병렬 포트, 게임 포트, 또는 USB(universal serial bus)와 같은 다른 인터페이스에 의해 접속될 수도 있다.

[0075] 디스플레이 장치(1244)는 또한 비디오 어댑터(1246)와 같은 인터페이스를 통해 버스(1206)에 접속된다. 모니터에 추가하여, 컴퓨터(1200)는 스피커 및 프린터와 같은 다른 주변 출력 장치(도시하지 않음)를 포함할 수 있다.

[0076] 컴퓨터(1200)는 어댑터 또는 네트워크 어댑터(1250), 모뎀(1252), 또는 네트워크에 걸쳐 통신을 형성하는 다른 수단을 통해 네트워크(1248)(예를 들어, 인터넷)에 접속된다. 내장형이거나 또는 외장형일 수 있는 모뎀(1252)은 직렬 포트 인터페이스(1242)를 통해 버스(1206)에 접속된다.

[0077] 본 명세서에 사용된 바와 같이, "컴퓨터 프로그램 매체" 및 "컴퓨터-판독가능 매체" 및 "컴퓨터-판독가능 저장 매체"라는 용어는 일반적으로 예컨대, 하드 디스크 드라이브(1214)와 연계된 하드 디스크, 탈착가능 자기 디스크(1218), 탈착가능 광학 디스크(1222)와 같은 매체뿐만 아니라 플래시 메모리 카드, 디지털 비디오 디스크, RAM(random access memory), ROM(read only memory) 등과 같은 다른 매체를 지칭하는 데 사용된다. 이러한 컴퓨터-판독가능 저장 매체는 통신 매체와 구별되며 겹치지 않는다(통신 매체를 포함하지 않는다). 통신 매체는 전형적으로 컴퓨터-판독가능 명령, 데이터 구조물, 프로그램 모듈 또는 반송파와 같이 변조 데이터 신호 내의 다른 데이터를 포함한다. "변조 데이터 신호"라는 용어는 신호 내의 정보를 인코딩하는 방식으로 셋팅 또는 변경되는 하나 이상의 이의 특성을 갖는 신호를 의미한다. 제한되지 않은 예시로서, 통신 매체에는 예컨대, 음향, RF, 적외선 및 다른 무선 매체와 같은 무선 매체가 포함된다. 실시 형태는 또한 이러한 통신 매체에 관한 것이다.

[0078] 전술된 바와 같이, 컴퓨터 프로그램 및 모듈(애플리케이션 프로그램(1232) 및 다른 프로그램 모듈(1234)을 포함함)은 하드 디스크, 자기 디스크, 광학 디스크, ROM 또는 RAM에 저장될 수 있다. 이러한 컴퓨터 프로그램은 또한 네트워크 인터페이스(1250) 또는 직렬 포트 인터페이스(1242)를 통해 수신될 수 있다. 이러한 컴퓨터 프로그램은, 애플리케이션에 의해 실행 또는 로딩될 때, 컴퓨터(1200)가 본 명세서에 기재된 본 발명의 실시 형태의 특징을 구현할 수 있게 한다. 따라서 이러한 컴퓨터 프로그램은 컴퓨터(1200)의 컨트롤러를 나타낸다.

[0079] 본 발명은 또한 임의의 컴퓨터 사용가능 매체에 저장된 소프트웨어를 포함하는 컴퓨터 프로그램 제품에 관한 것이다. 이러한 소프트웨어는, 하나 이상의 데이터 프로세싱 장치에서 실행될 때, 데이터 프로세싱 장치(들)가 본

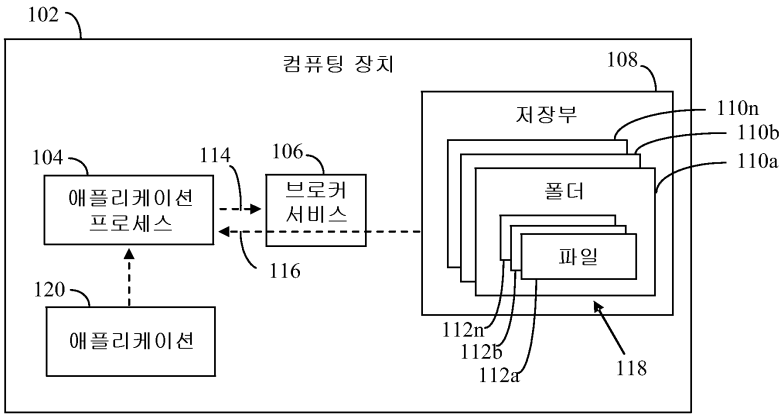
명세서에 기재된 바와 동작하도록 한다. 본 발명의 실시 형태는 현재 또는 미래에 공지되는 임의의 컴퓨터 사용 가능 또는 컴퓨터-판독가능 매체를 이용한다. 컴퓨터-판독가능 매체의 예에는 예컨대, RAM, 하드 드라이브, 플로피 디스크, CD ROM, DVD ROM, 집 디스크, 테이프, 자기 저장 장치, 광학 저장 장치, MEM, 나노기술-기반 저장 장치, 등과 같은 저장 장치가 포함하지만 이에 제한되지 않는다.

[0080] VI. 결론

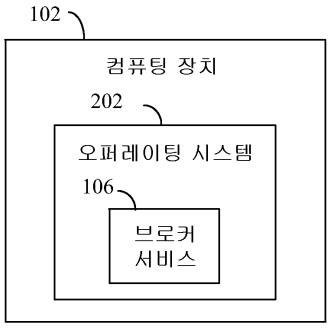
[0081] 본 발명의 다양한 실시 형태가 전술되어 있으나, 이것은 오로지 예시를 목적으로 제시된 것이고, 제한하기 위한 것이 아닌 것으로 이해되어야 것이다. 당업자라면 첨부된 청구항에서 정의된 본 발명의 정신 및 범주를 벗어나지 않으면서 그에 대한 형태 및 세부 사항에서의 다양한 변형이 이루어질 수 있다는 것을 이해할 것이다. 따라서 본 발명의 범위 및 범주는 전술된 예시적인 실시 형태 중 어느 것으로도 한정되지 않지만, 오로지 이하의 청구항 및 그 균등물에 따라서만 정의되어야 한다.

도면

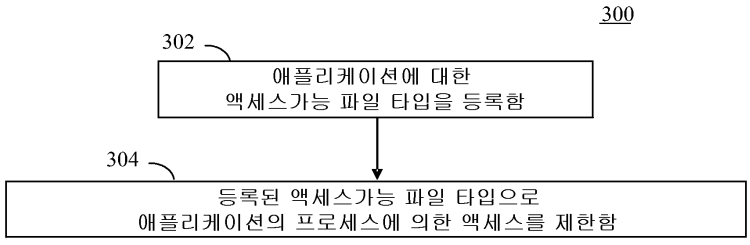
도면1



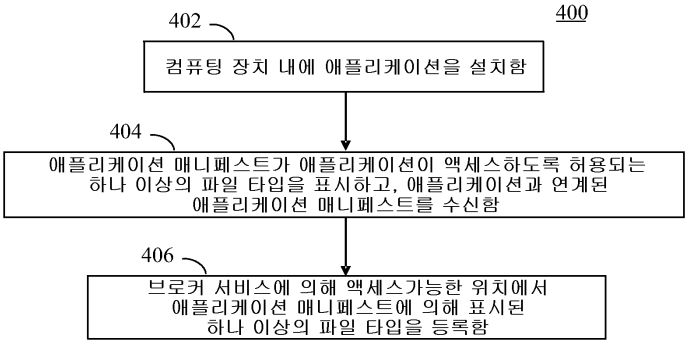
도면2



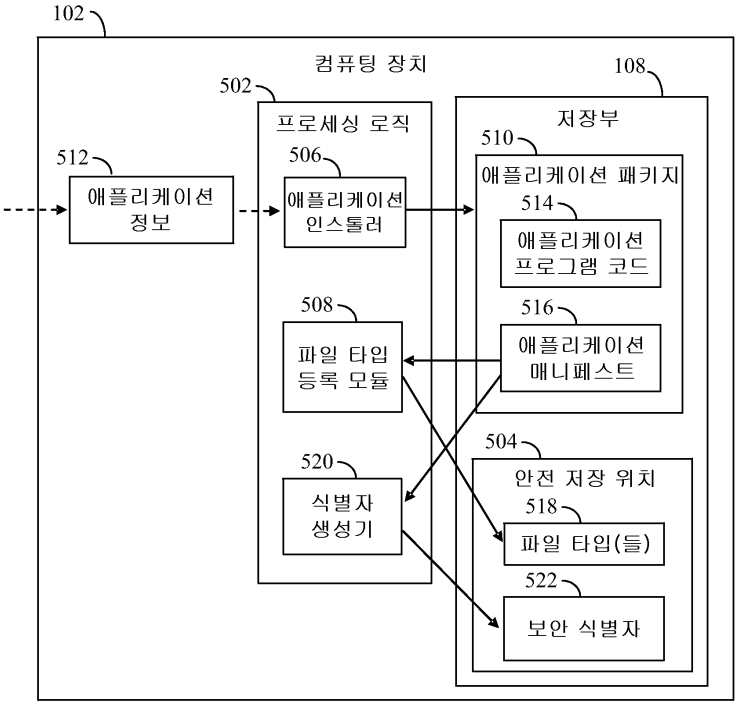
도면3



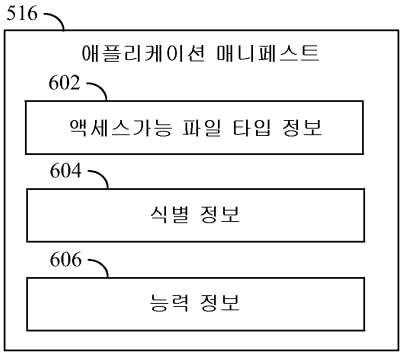
도면4


400
402
컴퓨팅 장치 내에 애플리케이션을 설치함
404
애플리케이션 매니페스트가 애플리케이션이 액세스하도록 허용되는 하나 이상의 파일 타입을 표시하고, 애플리케이션과 연계된 애플리케이션 매니페스트를 수신함
406
브로커 서비스에 의해 액세스가능한 위치에서 애플리케이션 매니페스트에 의해 표시된 하나 이상의 파일 타입을 등록함

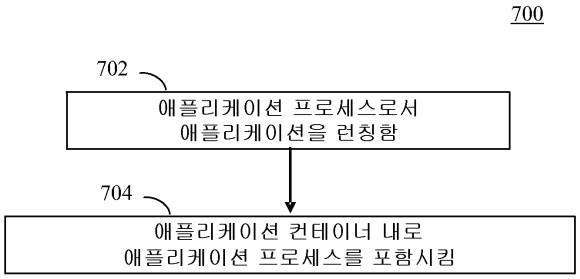
도면5


102
컴퓨팅 장치
108
502
프로세싱 로직
저장부
510
512
506
애플리케이션 정보
애플리케이션 인스톨러
애플리케이션 패키지
514
애플리케이션 프로그램 코드
508
516
파일 타입 등록 모듈
애플리케이션 매니페스트
504
520
안전 저장 위치
식별자 생성기
518
파일 타입(들)
522
보안 식별자

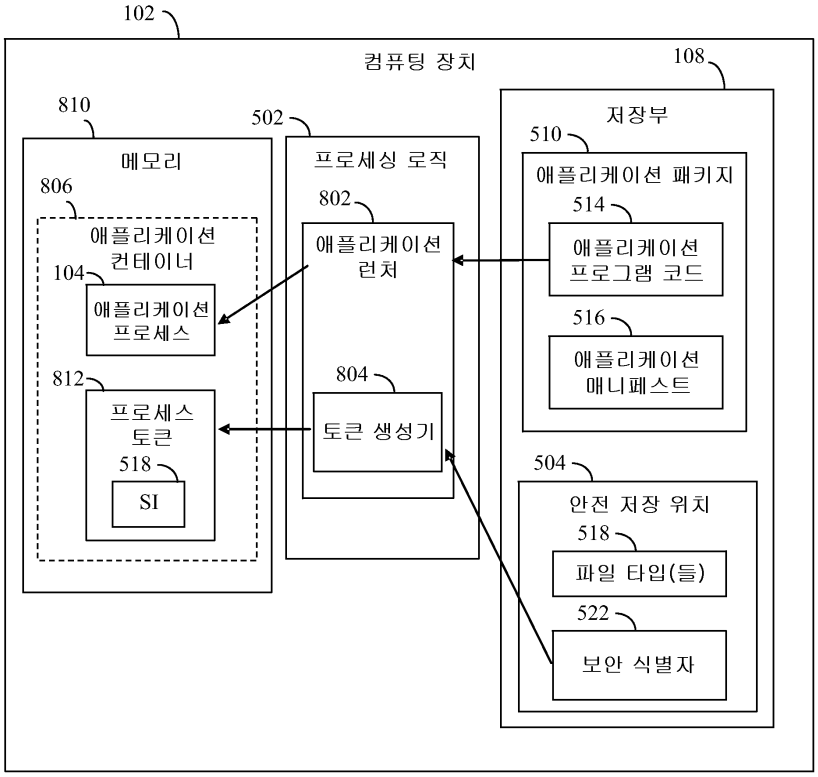
도면6


516
애플리케이션 매니페스트
602
액세스가능 파일 타입 정보
604
식별 정보
606
능력 정보

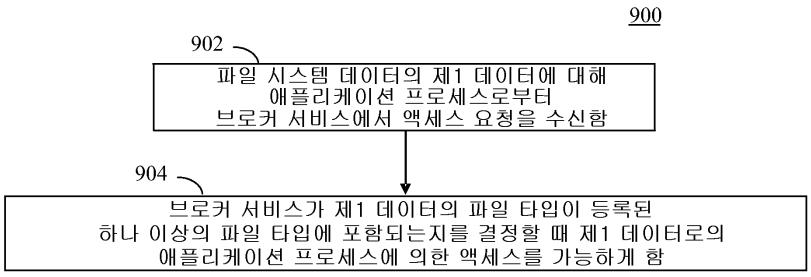
도면7


700
702
애플리케이션 프로세스로서
애플리케이션을 런칭함
704
애플리케이션 컨테이너 내로
애플리케이션 프로세스를 포함시킴

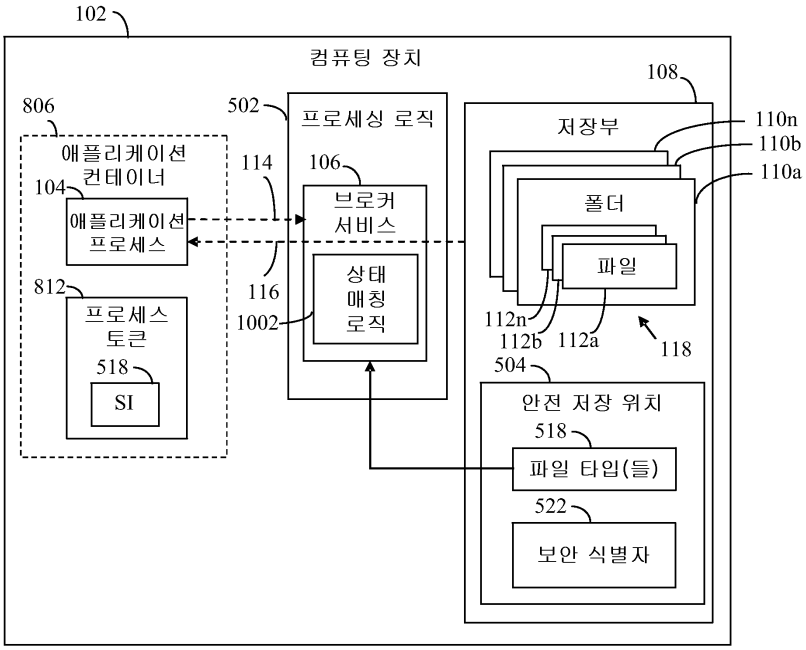
도면8


102
컴퓨팅 장치
108
저장부
510
애플리케이션 패키지
514
애플리케이션
프로그램 코드
516
애플리케이션
매니페스트
504
안전 저장 위치
518
파일 타입(들)
522
보안 식별자
810
메모리
806
애플리케이션
컨테이너
104
애플리케이션
프로세스
812
프로세스
토큰
518
SI
502
프로세싱 로직
802
애플리케이션
런처
804
토큰 생성기

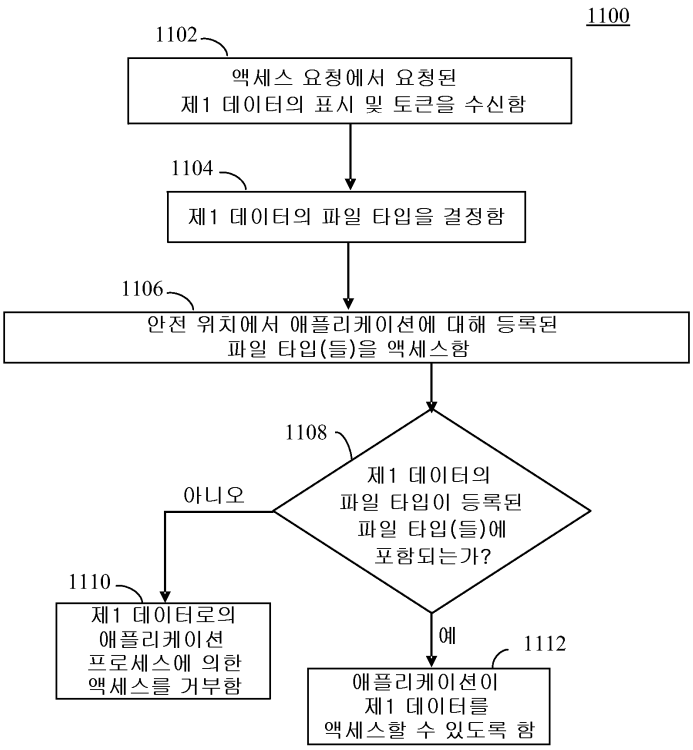
도면9


900
902
파일 시스템 데이터의 제1 데이터에 대해
애플리케이션 프로세스로부터
브로커 서비스에서 액세스 요청을 수신함
904
브로커 서비스가 제1 데이터의 파일 타입이 등록된
하나 이상의 파일 타입에 포함되는지를 결정할 때 제1 데이터로의
애플리케이션 프로세스에 의한 액세스를 가능하게 함

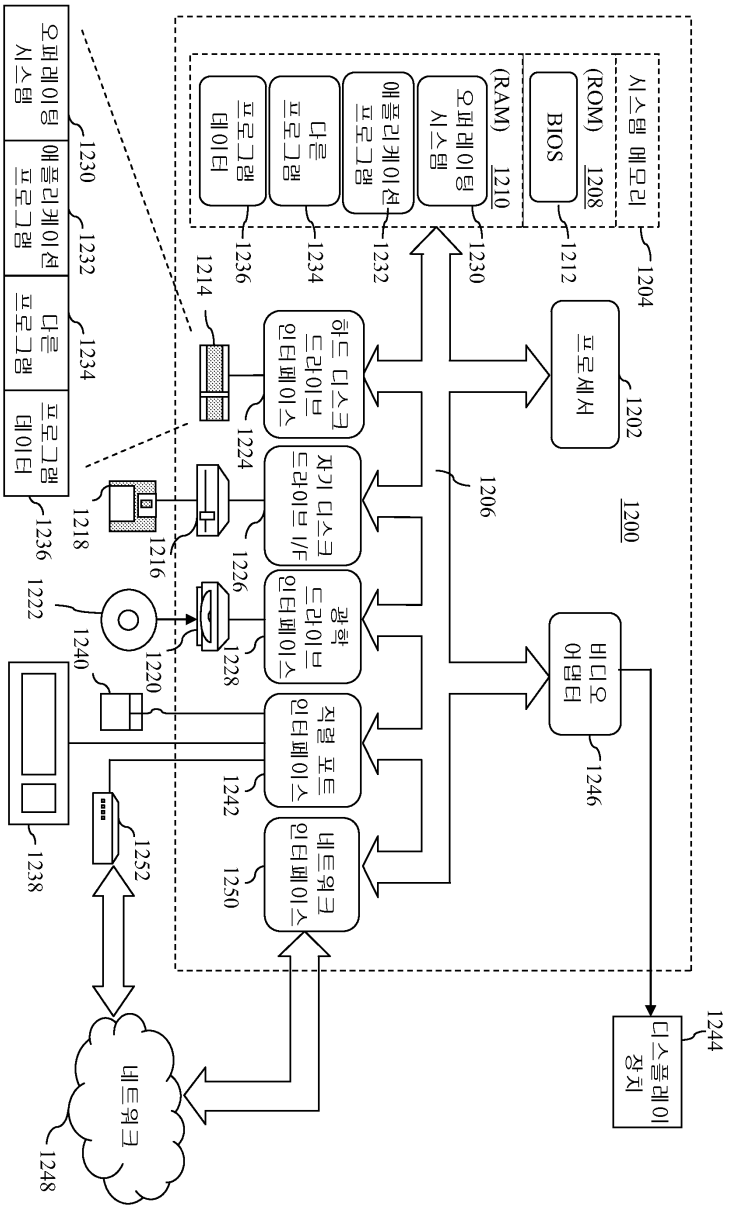
도면10


102
컴퓨팅 장치
108
806
502
프로세싱 로직
저장부
110n
110b
110a
애플리케이션
컨테이너
114
106
104
브로커
서비스
애플리케이션
프로세스
폴더
파일
812
상태
매칭
로직
116
1002
112n
112b
112a
118
프로세스
토큰
504
518
SI
안전 저장 위치
518
파일 타입(들)
522
보안 식별자

도면11


1100
1102
액세스 요청에서 요청된
제1 데이터의 표시 및 토큰을 수신함
1104
제1 데이터의 파일 타입을 결정함
1106
안전 위치에서 애플리케이션에 대해 등록된
파일 타입(들)을 액세스함
1108
제1 데이터의
파일 타입이 등록된
파일 타입(들)에
포함되는가?
아니오
예
1110
제1 데이터로의
애플리케이션
프로세스에 의한
액세스를 거부함
1112
애플리케이션이
제1 데이터를
액세스할 수 있도록 함

도면12



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 제15항

【변경전】

상기 컴퓨팅 장치의 파일 시스템

【변경후】

상기 컴퓨팅 시스템의 파일 시스템

【직권보정 2】

【보정항목】 청구범위

【보정세부항목】 제15항

【변경전】

상기 컴퓨팅 장치의 안전한 장치

【변경후】

상기 컴퓨팅 시스템의 안전한 장치

【직권보정 3】

【보정항목】 청구범위

【보정세부항목】 제15항

【변경전】

상기 컴퓨팅 장치에서 운영하는 상기 브로커 서비스

【변경후】

상기 컴퓨팅 시스템에서 운영하는 상기 브로커 서비스