(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년06월25일
(11) 등록번호 10-2270096
(24) 등록일자 2021년06월22일

(51) 국제특허분류(Int. Cl.)
G06F 21/84 (2013.01) *G06F 21/32* (2013.01)
G06K 9/00 (2006.01)
(52) CPC특허분류
G06F 21/84 (2013.01)
G06F 21/32 (2013.01)
(21) 출원번호 10-2017-7000157
(22) 출원일자(국제) 2014년06월27일
심사청구일자 2019년05월27일
(85) 번역문제출일자 2017년01월03일
(65) 공개번호 10-2017-0023063
(43) 공개일자 2017년03월02일
(86) 국제출원번호 PCT/CN2014/080944
(87) 국제공개번호 WO 2015/196448
국제공개일자 2015년12월30일
(56) 선행기술조사문헌
JP2013214219 A*
KR1020090108591 A*
US20100266162 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
마이크로소프트 테크놀로지 라이센싱, 엘엘씨
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
후앙 제리
중국 베이징 100080 하이디안 디스트릭트 단 링 스트리트 넘버 5 빌딩 2 마이크로소프트 아시아 퍼시픽 알앤디 헤드쿼터즈 14층 내
리우 젠
중국 베이징 100080 하이디안 디스트릭트 단 링 스트리트 넘버 5 빌딩 2 마이크로소프트 아시아 퍼시픽 알앤디 헤드쿼터즈 14층 내
(뒷면에 계속)
(74) 대리인
김태홍, 김진희

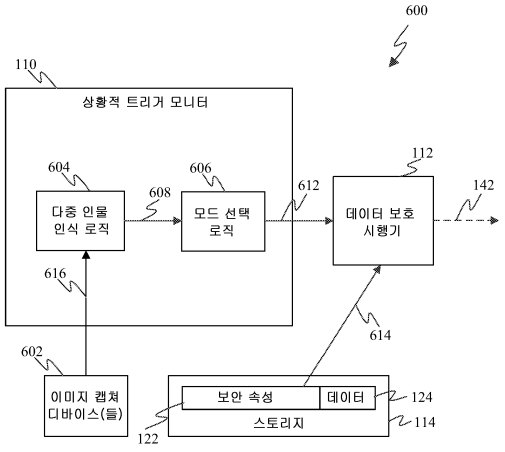
전체 청구항 수 : 총 17 항 심사관 : 구대성

(54) 발명의 명칭 **유저 및 제스처 인식에 기초한 데이터 보호**

(57) 요 약

소정 수의 사람이 컴퓨팅 디바이스에 근접하여 위치한다는 것, 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스에 근접하여 위치하지 않는다는 것, 또는 소정의 유저 제스처가 인식되었거나 또는 인식되지 않았다는 것을 결정하는 것에 응답하여, 데이터 보호 모드에 자동적으로 진입하는 컴퓨팅 디바이스가 본원에서 설명된다. 디바이스가 데이터 보호 모드에 진입하면, 자동적으로, 디바이스 상에 저장되어 있는 민감 데이터는 자신의 유저가 볼 수 없게 및/또는 액세스할 수 없게 된다. 민감 데이터는, 컴퓨팅 디바이스의 유저에게 명백하지 않을 방식으로 보이지 않게 및/또는 액세스불가능하게 될 수도 있다.

대 표 도 - 도6



(52) CPC특허분류
G06K 9/00335 (2013.01)
G06K 9/00362 (2013.01)
G06F 2221/2143 (2013.01)
(72) 발명자
리 칭후
중국 베이징 100080 하이디안 디스트릭트 단 링 스트리트 넘버 5 빌딩 2 마이크로소프트 아시아 퍼시픽 알앤디 헤드쿼터즈 14층 내
리우 첸
중국 베이징 100080 하이디안 디스트릭트 단 링 스트리트 넘버 5 빌딩 2 마이크로소프트 아시아 퍼시픽 알앤디 헤드쿼터즈 14층 내

명 세 서

청구범위

청구항 1

컴퓨팅 디바이스에 있어서,

상기 컴퓨팅 디바이스에 연결되거나 상기 컴퓨팅 디바이스와 통합되는 하나 이상의 이미지 캡쳐 디바이스로부터 이미지 데이터를 수신하도록 그리고 상기 컴퓨팅 디바이스에 근접하여 위치한 사람의 수를 결정하기 위해 상기 이미지 데이터를 분석하도록 구성되는 적어도 하나의 프로세서 회로를 포함하고,

상기 적어도 하나의 프로세서 회로는 또한, 상기 컴퓨팅 디바이스에 근접하여 위치한 사람의 수가 임계 값(thresold value)을 초과하는지를 결정하도록, 상기 컴퓨팅 디바이스에 근접하여 위치한 사람의 수가 상기 임계 값을 초과하지 않는다는 결정에 응답하여 상기 컴퓨팅 디바이스의 제1 동작 모드를 활성화하도록, 그리고 상기 컴퓨팅 디바이스에 근접하여 위치한 사람의 수가 상기 임계 값을 초과한다는 결정에 응답하여 상기 컴퓨팅 디바이스의 제2 동작 모드를 활성화하도록 구성되며,

상기 컴퓨팅 디바이스의 상기 제1 동작 모드는, 상기 컴퓨팅 디바이스 상에 저장되어 있는 민감 데이터(sensitive data) 및 상기 컴퓨팅 디바이스 상에 저장되어 있는 비민감 데이터(non-sensitive data)를 유저가 보는 것과 액세스하는 것 둘 다가 가능한 모드이고, 상기 컴퓨팅 디바이스의 상기 제2 동작 모드는, 상기 컴퓨팅 디바이스 상에 저장되어 있는 상기 비민감 데이터는 상기 유저가 볼 수 있고 액세스할 수 있고, 상기 컴퓨팅 디바이스 상에 저장되어 있는 상기 민감 데이터는 상기 유저가 볼 수 없게 되는 것 및 액세스할 수 없게 되는 것 중 하나 이상으로 되는 모드이며,

상기 컴퓨팅 디바이스의 상기 제2 동작 모드는, 민감 데이터의 적어도 하나의 항목을,

민감 데이터의 상기 항목을 하드 삭제하는(hard deleting) 것;

민감 데이터의 상기 항목을 소프트 삭제하는(soft deleting) 것; 또는

민감 데이터의 상기 항목에 대한 파일 시스템 요청이 무시되게 하는 것

중 하나 이상을 수행하는 것에 의해, 상기 유저가 볼 수 없게 또는 상기 유저가 액세스할 수 없게 되는 모드인, 컴퓨팅 디바이스.

청구항 2

제1항에 있어서,

상기 하나 이상의 이미지 캡쳐 디바이스는 하나 이상의 카메라를 포함하는, 컴퓨팅 디바이스.

청구항 3

제1항에 있어서,

상기 적어도 하나의 프로세서 회로는, 상기 이미지 데이터를 분석하여 별개의 얼굴의 수를 식별하는 것에 의해, 상기 컴퓨팅 디바이스에 근접하여 위치한 사람의 수를 결정하도록 구성되는, 컴퓨팅 디바이스.

청구항 4

제1항에 있어서,

상기 적어도 하나의 프로세서 회로는, 상기 이미지 데이터를 분석하여 별개의 몸(body)의 수를 식별하는 것에 의해, 상기 컴퓨팅 디바이스에 근접하여 위치한 사람의 수를 결정하도록 구성되는, 컴퓨팅 디바이스.

청구항 5

제1항에 있어서,

상기 적어도 하나의 프로세서 회로는 또한,

유저가 상기 임계 값을 지정할 수 있게 하는 유저 인터페이스를 제공하도록 구성되는, 컴퓨팅 디바이스.

청구항 6

제1항에 있어서,

상기 적어도 하나의 프로세서 회로는, 상기 컴퓨팅 디바이스의 일정 거리 내에 있는 사람의 수를 결정하기 위해 상기 이미지 데이터를 분석하는 것에 의해,

상기 컴퓨팅 디바이스에 근접하여 위치한 사람의 수를 결정하도록 구성되는, 컴퓨팅 디바이스.

청구항 7

제6항에 있어서,

상기 적어도 하나의 프로세서 회로는 또한,

유저가 상기 일정 거리를 지정할 수 있게 하는 유저 인터페이스를 제공하도록 구성되는, 컴퓨팅 디바이스.

청구항 8

컴퓨팅 디바이스 상에 저장되어 있는 민감 데이터를 보호하기 위한 방법에 있어서,

상기 컴퓨팅 디바이스에 연결되거나 상기 컴퓨팅 디바이스와 통합되는 하나 이상의 이미지 캡쳐 디바이스로부터 이미지 데이터를 수신하는 단계;

소유자 또는 권한 소지자(authorized person)가 상기 컴퓨팅 디바이스에 근접하여 위치하는지를 결정하기 위해 상기 이미지 데이터를 분석하는 단계;

상기 소유자 또는 권한 소지자가 상기 컴퓨팅 디바이스에 근접하여 위치한다는 결정에 응답하여, 상기 컴퓨팅 디바이스 상에 저장되어 있는 민감 데이터 및 상기 컴퓨팅 디바이스 상에 저장되어 있는 비민감 데이터를 유저가 보는 것과 액세스하는 것 둘 다가 가능한 상기 컴퓨팅 디바이스의 제1 동작 모드를 활성화하는 단계; 및

상기 소유자 또는 권한 소지자가 상기 컴퓨팅 디바이스에 근접하여 위치하지 않는다는 결정에 응답하여, 상기 컴퓨팅 디바이스 상에 저장되어 있는 상기 비민감 데이터는 상기 유저가 볼 수 있고 액세스할 수 있고, 상기 컴퓨팅 디바이스 상에 저장되어 있는 상기 민감 데이터는 상기 유저가 볼 수 없게 되는 것 및 액세스할 수 없게 되는 것 중 하나 이상으로 되는 상기 컴퓨팅 디바이스의 제2 동작 모드를 활성화하는 단계

를 포함하고,

상기 컴퓨팅 디바이스의 상기 제2 동작 모드는, 민감 데이터의 적어도 하나의 항목을,

민감 데이터의 상기 항목을 하드 삭제하는 것;

민감 데이터의 상기 항목을 소프트 삭제하는 것; 또는

민감 데이터의 상기 항목에 대한 파일 시스템 요청이 무시되게 하는 것

중 하나 이상을 수행하는 것에 의해, 상기 유저가 볼 수 없게 또는 상기 유저가 액세스할 수 없게 되는 모드인, 민감 데이터 보호 방법.

청구항 9

제8항에 있어서,

상기 하나 이상의 이미지 캡쳐 디바이스는 하나 이상의 카메라를 포함하는, 민감 데이터 보호 방법.

청구항 10

제8항에 있어서,

상기 소유자 또는 권한 소지자가 상기 컴퓨팅 디바이스에 근접하여 위치하는지를 결정하기 위해 상기 이미지 데이터를 분석하는 단계는,

상기 소유자 또는 권한 소지자의 얼굴을 식별하기 위해 상기 이미지 데이터를 분석하는 단계를 포함하는, 민감 데이터 보호 방법.

청구항 11

제8항에 있어서,

상기 소유자 또는 권한 소지자가 상기 컴퓨팅 디바이스에 근접하여 위치하는지를 결정하기 위해 상기 이미지 데이터를 분석하는 단계는,

상기 소유자 또는 권한 소지자의 몸을 식별하기 위해 상기 이미지 데이터를 분석하는 단계를 포함하는, 민감 데이터 보호 방법.

청구항 12

제8항에 있어서,

상기 소유자 또는 권한 소지자가 컴퓨팅 디바이스에 근접하여 위치하는지를 결정하기 위해 이미지 데이터를 분석하는 단계는,

상기 소유자 또는 권한 소지자가 상기 컴퓨팅 디바이스의 일정 거리 내에 있는지를 결정하기 위해 상기 이미지 데이터를 분석하는 단계를 포함하는, 민감 데이터 보호 방법.

청구항 13

제12항에 있어서,

유저가 상기 일정 거리를 지정할 수 있게 하는 유저 인터페이스를 제공하는 단계를 더 포함하는, 민감 데이터 보호 방법.

청구항 14

적어도 하나의 프로세서에 의한 실행시, 상기 적어도 하나의 프로세서로 하여금 컴퓨팅 디바이스 상에 저장되어 있는 민감 데이터를 보호하기 위한 방법을 수행하게 하는 컴퓨터 프로그램 로직이 기록된 컴퓨터 판독가능 메모리에 있어서,

상기 방법은,

상기 컴퓨팅 디바이스에 연결되거나 상기 컴퓨팅 디바이스와 통합되는 하나 이상의 이미지 캡쳐 디바이스로부터 이미지 데이터를 수신하는 단계;

특정한 유저 제스쳐가 인식되는지의 여부를 결정하기 위해 상기 이미지 데이터를 분석하는 단계; 및

상기 결정에 기초하여, 상기 컴퓨팅 디바이스 상에 저장되어 있는 민감 데이터 및 상기 컴퓨팅 디바이스 상에 저장되어 있는 비민감 데이터를 유저가 보는 것과 액세스하는 것 둘 다가 가능한 상기 컴퓨팅 디바이스의 제1 동작 모드, 및 상기 컴퓨팅 디바이스 상에 저장되어 있는 상기 비민감 데이터는 상기 유저가 볼 수 있고 액세스할 수 있고, 상기 컴퓨팅 디바이스 상에 저장되어 있는 상기 민감 데이터는 상기 유저가 볼 수 없게 되는 것 및 액세스할 수 없게 되는 것 중 하나 이상으로 되는 상기 컴퓨팅 디바이스의 제2 동작 모드 중 하나를 선택적으로 활성화하는 단계

를 포함하고,

상기 컴퓨팅 디바이스의 상기 제2 동작 모드는, 민감 데이터의 적어도 하나의 항목을,

민감 데이터의 상기 항목을 하드 삭제하는 것;

민감 데이터의 상기 항목을 소프트 삭제하는 것; 또는

민감 데이터의 상기 항목에 대한 파일 시스템 요청이 무시되게 하는 것

중 하나 이상을 수행하는 것에 의해, 상기 유저가 볼 수 없게 또는 상기 유저가 액세스할 수 없게 되는 모드인, 컴퓨터 판독가능 메모리.

청구항 15

제14항에 있어서,

상기 하나 이상의 이미지 캡쳐 디바이스는 하나 이상의 카메라를 포함하는, 컴퓨터 판독가능 메모리.

청구항 16

제14항에 있어서,

상기 특정한 유저 제스쳐는, 얼굴 제스쳐, 손 제스쳐, 팔 제스쳐, 몸 제스쳐, 다리 제스쳐, 및 발 제스쳐 중 하나 이상을 포함하는, 컴퓨터 판독가능 메모리.

청구항 17

제14항에 있어서,

상기 방법은, 유저가 상기 특정한 유저 제스쳐를 지정할 수 있게 하는 유저 인터페이스를 제공하는 단계를 더 포함하는, 컴퓨터 판독가능 메모리.

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

발명의 설명

기 술 분 야

배 경 기 술

[0001] 점점 더 많은 데이터가 디바이스, 특히 모바일 디바이스 상에 저장되고 있다. 예를 들면, 사람들은 개인 데이터를 저장할 수도 있고, 직원은 회사 데이터, 정부 데이터(governmental data), 클라이언트 관련 데이터, 지적 재산, 및/또는 다른 민감한 형태의 데이터를 그들의 디바이스 상에 저장할 수도 있다. 이 민감 데이터(sensitive data)는, 디바이스가 분실되거나, 도난되거나, 또는 어떤 다른 방식으로 침해되는(compromised) 경우, 위험에 처해진다.

[0002] 이 문제를 해결하기 위해, 디바이스 상의 민감 데이터를 보호하기 위한 기술이 개발되었다. 종래의 디바이스 데이터 보호 기술은, 통상적으로, 유저 인증, 암호화, 또는 이들의 조합의 어떤 형태에 의존한다. 예를 들면, 유저는, 디바이스 상에서 데이터가 액세스될 수도 있기 이전에 특정한 패스워드 또는 PIN이 입력되는 것을 필요로 하도록, 자신의 디바이스를 셋업할 수도 있다. 추가적으로, 몇몇 디바이스는 저장되는 파일 또는 폴더를 유저가 암호화하는 것을 허용하는데, 이것은, 파일을 볼 수 있거나 복사할 수 있기 이전에 코드가 입력되어야 한다는 것을 의미한다. 이러한 메커니즘이 민감 데이터를 인가되지 않은 액세스로부터 보호하는 것을 도울 수 있지만, 이들은 절대 안전한 것은 아니다. 예를 들면, 유저가 자신의 의지에 반하여 자신의 패스워드를 제공하도록 강제되는 경우, 또는 디바이스가 액티브 동작 상태에서(즉, 유저가 이미 자신의 패스워드를 입력한 이후) 빼앗기는 경우, 패스워드 메커니즘은 동작하지 않을 것이다. 유저 인증 및 암호화 스킴을 극복하기 위해 또 다른 수단이 사용될 수도 있다. 이들 데이터 보호 조치가 극복되면, 통상적으로는, 민감 데이터를 인가되지 않은 액세스로부터 보호할 방법이 없다.

[0003] 유저가 자신의 디바이스가 도난 당할 가능성이 있는 장소에 있다는 것을 유저가 결정하면, 유저는 민감 데이터를 보호하기 위해 능동적 조치를 취할 수도 있다. 예를 들면, 유저는 모든 민감 데이터를 삭제하기 위한 입력을

디바이스에 입력할 수도 있다. 시나리오에 따라서, 이것은 유저의 개인 안전(personal safety)뿐만 아니라 민감 데이터를 보호하는 데 필요할 수도 있다. 그러나, 많은 상황에서, 유저는 자신의 디바이스가 도난 당할 것을 예상하지 못할 것이고 따라서 이러한 조치를 취하지 않을 것이다. 유저가 디바이스 도난을 예상할 수 있는 상황에서도, 유저는 자신의 뜻대로 자신의 디바이스와 상호작용하여 민감 데이터를 디바이스로부터 삭제할 충분한 시간이 없을 수도 있다.

발명의 내용

[0004] 소정 수의 사람이 컴퓨팅 디바이스에 근접하여 위치한다는 것, 소유자 또는 권한 소지 유저(authorized user)가 컴퓨팅 디바이스에 근접하여 위치하지 않는다는 것, 또는 소정의 유저 제스처가 인식되었거나 또는 인식되지 않았다는 것을 결정하는 것에 응답하여, 데이터 보호 모드에 자동적으로 진입하는 컴퓨팅 디바이스가 본원에서 설명된다. 디바이스가 데이터 보호 모드에 진입하면, 자동적으로, 디바이스 상에 저장되어 있는 민감 데이터는 자신의 유저가 볼 수 없게 및/또는 액세스할 수 없게 된다. 민감 데이터는, 컴퓨팅 디바이스의 유저에게 명백하지 않을 방식으로 보이지 않게 및/또는 액세스불가능하게 될 수도 있다.

[0005] 이 개요는 하기의 상세한 설명에서 더 설명되는 개념의 선택을 간소화된 형태로 소개하기 위해 제공된다. 이 개요는 청구된 주제의 주요 특징이나 또는 본질적인 특징을 식별하도록 의도된 것이 아니며, 청구된 주제의 범위를 제한하는 데 사용되도록 의도된 것도 아니다. 또한, 청구되는 주제는 상세한 설명 및/또는 본 문서의 다른 섹션에서 설명되는 특정 실시형태로 제한되지 않는다는 것을 유의한다. 이러한 실시형태는 본원에서 단지 예시적 목적을 위해 제시된다. 본원에 포함되는 교시에 기초한 추가적인 실시형태가 관련 기술분야(들)의 숙련된 자에게는 명백할 것이다.

도면의 간단한 설명

[0006] 본원에 통합되며 본 명세서의 일부를 형성하는 첨부의 도면은 본 출원의 실시형태를 예시하며, 설명과 함께, 실시형태의 원리를 설명하도록 그리고 관련 기술분야의 숙련된 자가 실시형태를 만들고 사용하는 것을 가능하게 하도록 더 기능한다.

도 1은, 예시적인 실시형태에 따른, 컴퓨팅 디바이스 상에 저장되어 있는 데이터를 보호하도록 구성되는 데이터 보호 시스템을 포함하는 데이터 보호 환경의 블록도이다.

도 2는, 예시적인 실시형태에 따른, 저장된 데이터에 대한 보호를 구성하기 위한 프로세스의 플로우차트를 묘사한다.

도 3은, 예시적인 실시형태에 따른, 데이터에 대한 데이터 보호 응답을 선택하기 위한 프로세스의 플로우차트를 묘사한다.

도 4는, 예시적인 실시형태에 따른, 하나 이상의 상이한 데이터 보호 응답을 선택하기 위한 프로세스의 플로우차트를 묘사한다.

도 5는, 예시적인 실시형태에 따른, 데이터 보호 응답의 시행(enactment)을 트리거하는 데이터와 관련되는 상황적 트리거를 모니터링하기 위한 프로세스의 플로우차트를 묘사한다.

도 6은, 예시적인 실시형태에 따른, 컴퓨팅 디바이스에 근접하여 위치한 사람의 결정된 수를, 데이터 보호를 위한 상황적 트리거로서 사용하도록 구성되는 데이터 보호 시스템의 블록도이다.

도 7은, 예시적인 실시형태에 따른, 컴퓨팅 디바이스에 근접하여 위치한 사람의 결정된 수에 기초하여, 데이터에 대한 데이터 보호 응답을 시행하기 위한 프로세스의 플로우차트를 묘사한다.

도 8은, 예시적인 실시형태에 따른, 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스에 근접하여 위치하는지의 여부에 관한 결정을, 데이터 보호를 위한 상황적 트리거로서 사용하도록 구성되는 데이터 보호 시스템의 블록도이다.

도 9는, 예시적인 실시형태에 따른, 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스에 근접하여 위치하지 않는다는 결정에 기초하여 데이터에 대한 데이터 보호 응답을 시행하기 위한 프로세스의 플로우차트를 묘사한다.

도 10은, 예시적인 실시형태에 따른, 유저 제스처의 인식 또는 유저 제스처의 인식의 부재를, 데이터 보호를 위한 상황적 트리거로서 사용하도록 구성되는 데이터 보호 시스템의 블록도이다.

도 11은, 예시적인 실시형태에 따른, 유저 제스처의 인식 또는 유저 제스처의 인식의 부재에 기초하여 데이터에 대한 데이터 보호 응답을 시행하기 위한 프로세스의 플로우차트를 묘사한다.

도 12는, 본원에서 설명되는 다양한 실시형태를 구현하기 위해 사용될 수도 있는 예시적인 모바일 디바이스의 블록도이다.

도 13은, 본원에서 설명되는 다양한 실시형태를 구현하기 위해 사용될 수도 있는 예시적인 프로세서 기반 컴퓨터 시스템의 블록도이다.

본 발명의 특징 및 이점은, 도면과 연계하여 취해질 때 하기에서 개시되는 상세한 설명으로부터 더욱 명확해질 것인데, 도면에서 동일한 도면 부호는 전체에 걸쳐 대응하는 엘리먼트를 식별한다. 도면에서, 동일한 도면 부호는, 일반적으로, 동일한, 기능적으로 유사한, 및/또는 구조적으로 유사한 엘리먼트를 나타낸다. 한 엘리먼트가 처음 나타나는 도면은, 대응하는 도면 부호에서 가장 왼쪽의 숫자(들)에 의해 나타내어진다.

발명을 실시하기 위한 구체적인 내용

[0007] I. 서론

[0008] 본 명세서 및 첨부의 도면은, 본 발명의 특징을 통합하는 하나 이상의 실시형태를 개시한다. 본 발명의 범위는 개시된 실시형태로 제한되지 않는다. 개시된 실시형태는 본 발명을 예시화하는 것에 불과하며, 개시된 실시형태의 수정된 버전도 또한 본 발명에 의해 포함된다. 본 발명의 실시형태는 본원에 첨부되는 청구범위에 의해 정의된다.

[0009] 명세서에서의 "하나의 실시형태", "한 실시형태", "예시적인 실시형태" 등등에 대한 참조는, 설명되는 실시형태가 특정한 특징, 구조, 또는 특성을 포함할 수도 있지만, 모든 실시형태가 그 특정한 특징, 구조, 또는 특성을 반드시 포함하지는 않을 수도 있다는 것을 나타낸다. 또한, 이러한 어구(phrase)는 반드시 동일한 실시형태를 가리키는 것은 아니다. 또한, 특정한 특징, 구조, 또는 특성이 한 실시형태와 연계하여 설명되는 경우, 다른 실시형태와 연계하여 이러한 특징, 구조, 또는 특성을 달성하는 것은, 명시적으로 설명되든 또는 그렇지 않든 간에, 기술분야의 숙련된 자의 지식 내에 있다는 것이 제시된다.

[0010] 다양한 예시적인 실시형태가 다음과 같이 설명된다. 본원에서 제공되는 임의의 섹션/하위섹션 표제(heading)는 제한하는 것으로 의도되지 않는다는 것을 유의한다. 실시형태가 이 문서 전체에 걸쳐 설명되며, 임의의 타입의 실시형태가 임의의 섹션/하위섹션 하에 포함될 수도 있다. 또한, 임의의 섹션/하위섹션에서 개시되는 실시형태는, 동일한 섹션/하위섹션 및/또는 상이한 섹션/하위섹션에서 설명되는 임의의 다른 실시형태와 임의의 방식으로 결합될 수도 있다.

[0011] 소정 수의 사람이 컴퓨팅 디바이스에 근접하여 위치한다는 것, 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스에 근접하여 위치하지 않는다는 것, 또는 소정의 유저 제스처가 인식되었거나 또는 인식되지 않았다는 것을 결정하는 것에 응답하여, 데이터 보호 모드에 자동적으로 진입하는 컴퓨팅 디바이스가 본원에서 설명된다. 디바이스가 데이터 보호 모드에 진입하면, 자동적으로, 디바이스 상에 저장되어 있는 민감 데이터는 자신의 유저가 볼 수 없게 및/또는 액세스할 수 없게 된다. 민감 데이터는, 컴퓨팅 디바이스의 유저에게 명백하지 않을 방식으로 보이지 않게 및/또는 액세스불가능하게 될 수도 있다.

[0012] 상기한 특징은, 컴퓨팅 디바이스가 위험한 환경에 있을 때, 컴퓨팅 디바이스에 의해 저장되어 있는 민감 데이터를, 컴퓨팅 디바이스가 자동적으로, 재빨리 그리고 이산적으로 숨기거나 또는 삭제하는 것을 가능하게 한다. 예를 들면, 상기한 특징은, 컴퓨팅 디바이스의 소유자 또는 권한 소지 유저가 타인에 의해 둘러싸일 때, 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스로부터 멀어질 때, 컴퓨팅 디바이스가 자신의 소유자 또는 권한 소지 유저 이외의 어떤 타인에 의해 소유되고 있을 때, 또는 컴퓨팅 디바이스의 소유자 또는 권한 소지 유저가 데이터 보호 동작 모드를 트리거하기 위한 또는 트리거하지 않기 위한 소정의 유저 제스처를 행했을 때 또는 행하는 것을 실패했을 때, 컴퓨팅 디바이스에 의해 저장되어 있는 민감 데이터를, 컴퓨팅 디바이스가 자동적으로, 재빨리 그리고 이산적으로 숨기거나 또는 삭제하는 것을 가능하게 할 수도 있다. 또한, 실시형태가 데이터 보호 모드에서 동작하는 동안 비민감 데이터(non-sensitive data)를 여전히 제시할 것이고 그리고 다르게는 정상적으로 기능할 것이기 때문에, 그 임의의 인가되지 않은 또는 악의적 유저는 데이터 보호가 활성화되었다는 것을 인식하지 못할 수도 있다. 이 방식으로 민감 데이터를 자동적으로, 재빨리 그리고 이산적으로 숨기거나 또는 삭제하는 것에 의해, 본원에서 설명되는 실시형태는 컴퓨팅 디바이스 상에 저장되어 있는 민감 데이터뿐만 아니라 디바이스의 소유자 또는 권한 소지 유저의 개인 안전을 효과적으로 보호할 수 있다.

[0013] 섹션 II는, 하기에서, 상황에 맞게 트리거되는 데이터 보호를 구현하는 컴퓨팅 디바이스를 포함하는 예시적인 데이터 보호 환경을 설명한다. 섹션 III은, 소정 수의 사람이 컴퓨팅 디바이스에 근접하여 배치된다는 결정이 데이터 보호를 위한 상황적 트리거로서 사용되는 예시적인 실시형태를 설명한다. 섹션 IV는, 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스에 근접하여 위치하지 않는다는 결정이 데이터 보호를 위한 상황적 트리거로서 사용되는 예시적인 실시형태를 설명한다. 섹션 V는, 소정의 유저 제스쳐가 컴퓨팅 디바이스에 의해 인식되었다는 또는 인식되지 않았다는 사실이 데이터 보호를 위한 상황적 트리거로서 사용되는 예시적인 실시형태를 설명한다. 섹션 VI는, 컴퓨팅 디바이스의 예시적인 모바일 디바이스 구현예 및 데스크탑 디바이스 구현예를 설명한다. 섹션 VII은 어떤 추가적인 예시적 실시형태를 제공한다. 섹션 VIII은 어떤 결론을 제공한다.

[0014] II. 상황적으로 트리거되는 데이터 보호를 위한 예시적인 실시형태

[0015] 본원에서 설명되는 실시형태는, 상황에 기초하여 구성 가능하고 자동적인 방식으로 디바이스 상에 저장되어 있는 데이터의 보호를 가능하게 한다. 상황 기반의 데이터 보호는, 예컨대 디바이스가 분실된 상황에서, 디바이스가 유저의 의지에 반하여 사용되고 있는 상황(예를 들면, 유저가 디바이스 패스워드를 제공하도록 강제된 상황, 디바이스가 액티브 동작 상태에서 빼앗긴 상황, 등등)에서, 그리고 다른 상황에서, 디바이스 상의 데이터를 보호하기 위한 정책을 유저가 설정하는 것을 가능하게 한다. 위험한 외부적 상황이 검출되면 데이터가 손상되는 것을 방지하기 위해 미리 정의된 액션이 데이터를 보호하도록 자동적으로 실행된다.

[0016] 상황 기반의 데이터 보호 시스템은, 유저에 의한 의도치 않은 또는 본의 아니게 인가된 액세스를 방지한다. 데이터는 위험한 상황이 식별될 때 침해되는 것이 자동적으로 방지된다.

[0017] 상황 기반의 데이터 보호 시행(enforcement) 및 실행(execution) 아키텍처의 실시형태가 제공된다. 시행 아키텍처는, 데이터 민감 레벨(예를 들면, 레벨 1, 레벨 2, 등등), 데이터 보호 응답(예를 들면, 소프트 삭제(soft delete), 하드 삭제(hard delete), 등등), 위험/트리거 상황(상황 1, 상황 2), 및 이들 엘리먼트 사이의 매핑(예를 들면, 레벨 1 -> 상황 1 -> 소프트 삭제, 이것은 상황 1이 검출되는 경우 레벨 1 컨텐츠가 소프트 삭제되어야 한다는 것을 나타낸다)을 정의하기 위해 사용될 수도 있다. 실행 아키텍처는, 데이터가 보호되는 것을 보장하기 위해 미리 정의된 액션/응답을 활성화하도록 구성된다. "소프트 삭제"와 같은 액션은 복구될 수 있지만, "하드 삭제"는 데이터의 복구에 대한 옵션 없이 데이터를 완전히 삭제한다. 데이터는 또한, 파일 시스템 요청에 응답하여 데이터가 검색되지(retrieved) 않게 하는 것에 의해 숨겨질 수 있다.

[0018] 실시형태에서, 잠재적인 위험한 상황은 임의의 디바이스 상태에서 발생할 수 있고, 유저가 시스템을 이산적으로 통지할 또는 시스템이 상황을 자동적으로 검출할 기술이 제공된다. 상황 기반의 데이터 보호는 다음의 제어 지점 중 임의의 하나 또는 그 조합과 함께 구현될 수 있고 시행될 수 있다:

[0019] 전력 오프 상태의 디바이스: 탬퍼(tamper) 검출을 구현하기 위해 디바이스에 추가적인 칩셋(예를 들면, 추가적인 프로세서, 오퍼레이팅 시스템, 등등)을 포함하는 것에 시행이 달성될 수 있다.

[0020] 부트 업(boot-up) 상태의 디바이스: 미리 정의된 키 인터럽트(예를 들면, 특정한 키 조합, 등등) 또는 다른 미리 결정된 유저 입력이 유저에 의해 제공되지 않는 경우, 디바이스는 데이터 보호 모드로 자동적으로 부팅될 수 있다.

[0021] 유저 로그인 상태의 디바이스: 데이터 보호와 결부되는 유저 계정에 대한, 일반적인 디바이스 로그인 패스워드 이외의 대안적인 패스워드가 입력되는 것을 필요로 할 수도 있다. 유저 로그인 프로세스 동안의 추가적인 입력 및/또는 입력 거동의 존재 또는 부재가 또한 검출될 수도 있고/있거나 데이터 보호를 활성화할지 또는 활성화하지 않을지의 여부를 결정하기 위해 사용될 수 있다.

[0022] 동작 상태의 디바이스:

[0023] ● 디바이스의 물리적 위치가 가능한 위협을 나타낼 수 있다.

[0024] ● 위험한 환경을 식별하기 위해, 특정한 거리 내에서 디바이스를 보고 있는 사람들의 수를 디바이스의 카메라가 검출할 수 있다.

[0025] ● 디바이스는 동작 상태에 있고 보호되지 않을 때 도난 당할 수 있거나 뺏길 수 있고, 디바이스의 유저가 합법적인지의 여부는 유저 인터페이스(user interface; UI) 입력 패턴(예를 들면, 키보드/손가락 터치 면적, 사이즈/마우스 사용 패턴, 등등)에 기초하여 결정될 수도 있다.

[0026] ● 디바이스는 위험을 결정하기 위해 유저의 생체 신호(biometric signal)를 검출하도록 구성될 수도 있다(예를

들면, 로그인 유저가 강압 하에 있고 따라서 데이터 보호가 별개로 시행될 수도 있다).

[0027] 셧다운 상태의 디바이스: 디바이스는 유저 퍼미션(user's permission) 없이 셧다운하도록 강제될 수도 있다. 이 경우, 셧다운 패스워드 또는 다른 미리 결정된 유저 입력이 제공되지 않으면, 디바이스에 의해 저장되어 있는 데이터에 대한 위협이 식별될 수도 있다.

[0028] 예시적인 실시형태에서, 데이터 보호는 디바이스 상의 선택된 데이터에 대해 다음과 같이 구성된다. 하기의 여러 문단에서 사용되는 예시적인 예에서, 디바이스의 유저로부터의 생체 정보는 데이터 보호를 활성화하기 위한 상황적 트리거(contextual trigger)로서 구성된다.

[0029] (A) 보호될 컨텐츠, 상황적 트리거, 및 보호 응답이 정의된다. 예를 들면, 보호될 컨텐츠를 정의하는 파일(들) 및/또는 폴더(들)가 지정된다. 상황적 트리거 및 관련 데이터 보호 정책이 컨텐츠에 대해 설정된다. 생체 정보에 기초한 것들을 비롯하여, 여러 상이한 타입의 상황적 트리거가 선택될 수도 있다. 예를 들면, 데이터 보호 상황은 유저의 물리적 상태(예를 들면, 유저의 심박수, 땀 레벨, 얼굴 표정, 등등)에 결부될 수 있다. 물리적 상태에 대한 일반적이지 않은/비정상적인 동작 값뿐만 아니라, 취할 관련 액션/응답이 정의될 수 있다(예를 들면, 심박수 > 100 bpm -> 민감 컨텐츠 삭제).

[0030] (B) 컨텐츠에 대한 액세스의 상황이 모니터링되고 인식된다. 특정한 상황적 구성에 따라 상황을 검출하는 많은 방식이 존재한다. 예를 들면, 생체 정보와 관련하여, 디바이스는 유저의 물리적 상태의 이상을 검출할 수도 있고 미리 정의된 액션/응답을 트리거할 수도 있다. 센서(온보드 및/또는 디바이스에 대해 원격)가 유저의 다양한 물리적 상태, 예컨대 디바이스로부터의 유저의 거리, 심박수, 땀 레벨, 온도, 혈압, 등등을 모니터링할 수 있다.

[0031] (C) 상황적 트리거가 검출되는 경우, 데이터를 보호하기 위해, 여러 가능한 응답이 취해질 수 있다. 이러한 데이터 보호 응답의 예는 다음 중 하나 이상을 포함하는데, 민감한 것으로 마킹된 데이터가, 복구에 대한 어떠한 옵션도 없이, 디바이스로부터 자동적으로 삭제되는 하드 삭제; 데이터를 바로 덮어쓰기 하지 않고, 데이터에 대한 링크 또는 파일 포인터를 삭제하고 그 링크 또는 파일 포인트를 안전한 위치에 저장하는 것에 의해 민감한 것으로 마킹된 데이터가 보호되는 소프트 삭제; 민감 데이터를 목표로 하는 파일 시스템 데이터 요청이 무시되게 하는 것에 의해 데이터를 숨기는 것; 유저에게 경보(예를 들면, 메시지, 사운드, 시각적 경보, 등등)를 제공하는 것; 파일이 열릴 수 없게 만드는 것; 데이터가 디스플레이되는 열린 창을 닫거나 또는 이러한 창을 다른 창 뒤로 숨기는 것, 등등이다.

[0032] (D) 데이터가 데이터 보호 응답으로서 소프트 삭제되면, 데이터는 나중에 오퍼레이팅 시스템에 의해 복구될 수도 있다. 소프트 삭제는, 예를 들면, 데이터(예를 들면, 파일)에 대한 링크 또는 파일 포인터만을 삭제하는 것을 포함할 수도 있다. 이러한 실시형태에서, 데이터는 보안 저장소로부터 링크 또는 파일 포인터를 복구하는 것에 의해 복구/복원될 수 있다. 하나의 실시형태에서, 데이터의 복원은, 유저가 정확한 패스워드와 올바른 패스워드 입력 상황에서 로그인하는 다음 번(next time)과 같이, 자동적일 수 있다. 대안적으로, 복원은 정확한 패스워드 상황에서 트리거될 수도 있다.

[0033] 다른 실시형태에서, 데이터 보호는 디바이스 상의 선택된 데이터에 대해 다음과 같이 구성된다. 이 실시형태에서, 디바이스의 위치는 데이터 보호를 활성화하기 위한 상황적 트리거로서 구성된다.

[0034] (A) 보호될 컨텐츠, 상황적 트리거, 및 보호 응답이 정의된다. 예를 들면, 보호될 컨텐츠를 정의하는 파일(들) 및/또는 폴더(들)이 지정된다. 상황적 트리거 및 관련 데이터 보호 정책이 컨텐츠에 대해 설정된다. 예컨대 지리적 좌표, 맵, 등등을 사용하는 것에 의해, 지리적 위치가 데이터 보호 상황으로서 설정된다. 예를 들면, 민감 데이터는, 디바이스가 특정 국가에 있을 때 (하드 또는 소프트) 삭제되도록 또는 숨겨지도록 구성될 수도 있다. 상황의 데이터 민감도 레벨, 상황, 및 데이터 보호 응답 사이의 매핑이 구성된다.

[0035] (B) 디바이스의 위치가 결정된다. 예를 들면, GPS(global positioning system), 셀룰러 네트워크(예를 들면, 디바이스가 SIM 카드를 구비하는 경우), HTTP 프록시의 IP(Internet protocol; 인터넷 프로토콜) 어드레스, 등등 중 하나 이상을 사용하여, 디바이스의 현재 위치가 결정될 수 있다. 대안적으로, (예를 들면, 시간에 걸쳐 디바이스를 추적하는 것에 의해 결정되는) 디바이스의 이동 경로에 기초하여 디바이스의 미래 위치가 예상될 수 있다. 디바이스의 미래 위치는 또한, 이용가능한 경우(예를 들면, 약속 장소), 디바이스 상의 유저의 캘린더를 분석하는 것에 결정될 수 있고/있거나, 다른 방식으로 결정될 수 있다.

[0036] (C) 디바이스가 미리 결정된 위치에 있는 것으로 결정되는, 또는 미리 결정된 위치에 곧 있을 것으로 예상되는 경우에, 데이터를 보호하기 위해 여러 가능한 데이터 보호 응답이 시행될 수 있다. 데이터 보호 응답의 예는,

본원의 다른 곳에서 설명되는 또는 다르게는 공지되어 있는 것들, 예컨대 데이터의 경보, 하드 삭제, 소프트 삭제, 숨김을 포함한다.

[0037] (D) 데이터가 데이터 보호 응답으로서 소프트 삭제되면, 데이터는 나중에 오퍼레이팅 시스템에 의해 복구될 수도 있다. 데이터의 이러한 복구는 본원의 다른 곳에서 설명되는 바와 같이 또는 다르게는 공지되어 있는 바와 같이 수행될 수도 있다.

[0038] 데이터 보호 실시형태의 추가 설명이 하기의 하위섹션에서 제공된다. 예를 들면, 바로 다음의 하위섹션은, 데이터에 대한 보호를 구성하기 위한 추가 실시형태를 설명하고, 데이터 보호의 트리거링 및 시행에 대한 추가 실시형태를 설명하는 하위섹션이 후속한다.

[0039] A. 데이터 보호를 구성하기 위한 예시적인 실시형태

[0040] 데이터 보호 시스템은, 실시형태에서, 원하지 않는 액세스로부터 데이터를 보호하도록 다양한 방식으로 구성될 수도 있다. 예를 들면, 도 1은, 예시적인 실시형태에 따른, 컴퓨팅 디바이스(102) 상에 저장되는 데이터를 보호하도록 구성되는 데이터 보호 시스템(136)을 포함하는 데이터 보호 환경(100)의 블록도이다. 도 1에서 도시되는 바와 같이, 데이터 보호 환경(100)은 컴퓨팅 디바이스(102) 및 서버(104)를 포함한다. 컴퓨팅 디바이스(102) 및 서버(104)는 네트워크(106)에 의해 통신 가능하게 커플링될 수도 있다. 데이터 보호 시스템(136)은 컴퓨팅 디바이스(102)에 포함된다. 도 1의 실시형태에서, 데이터 보호 시스템(136)은 유저 인터페이스 모듈(108), 상황적 트리거 모니터(contextual trigger monitor; 110), 데이터 보호 시행기(data protection enactor; 112), 및 스토리지(114)를 포함한다. 또한, 서버(104)는 유저 인터페이스 모듈(128)을 포함한다. 환경(100)의 특징은 다음과 같이 설명된다.

[0041] 도 1에서 도시되는 바와 같이, 데이터 보호 시스템(136)은 컴퓨팅 디바이스(102)에서 구현될 수도 있다. 다른 실시형태에서, 데이터 보호 시스템(136)은 부분적으로 컴퓨팅 디바이스(102)에서 그리고 부분적으로 서버(104)에서 구현될 수도 있다는 것을 유의한다. 예를 들면, 유저 인터페이스 모듈(108), 상황적 트리거 모니터(110), 및 데이터 보호 시행기(112)가 컴퓨팅 디바이스(102)에 포함될 수도 있다. 대안적으로, 유저 인터페이스 모듈(108)은 컴퓨팅 디바이스(102)에 존재하지 않을 수도 있지만, 대신, 서버(104)의 유저 인터페이스 모듈(128)은, 상황적 트리거 모니터(110) 및 데이터 보호 시행기(112)와 함께, 데이터 보호 시스템(136)의 일부일 수도 있다. 다른 실시형태에서, 유저 인터페이스 모듈(108 및 128) 둘 다가 존재할 수도 있거나 데이터 보호 시스템(136)의 일부일 수도 있다.

[0042] 컴퓨팅 디바이스(102)는, 모바일 컴퓨터 또는 모바일 컴퓨팅 디바이스(예를 들면, Microsoft® Surface® 디바이스, 개인 휴대형 정보 단말(personal digital assistant; PDA), 랩탑 컴퓨터, 노트북 컴퓨터, 태블릿 컴퓨터 예컨대 Apple iPad™, 넷북, 등등), 이동 전화(예를 들면, 셀폰, 스마트폰 예컨대 Microsoft Windows® 폰, 애플 아이폰, Google® Android™ 오퍼레이팅 시스템을 구현하는 폰, Palm® 디바이스, Blackberry® 디바이스, 등등), 웨어러블 컴퓨팅 디바이스(예를 들면, 스마트 워치, Google® Glass™와 같은 스마트 글래스를 포함하는 헤드 마운트형 디바이스, 등등), 디지털 카메라, 또는 다른 타입의 모바일 디바이스, 또는 고정식 컴퓨팅 디바이스 예컨대 데스크탑 컴퓨터 또는 PC(personal computer; 퍼스널 컴퓨터)를 포함하는, 임의의 타입의 고정식 또는 모바일 컴퓨팅 디바이스일 수도 있다.

[0043] 스토리지(114)는, (예를 들면, 하드 디스크 드라이브에서의) 자기 디스크, (예를 들면, 광학 디스크 드라이브에서의) 광학 디스크, (예를 들면, 테이프 드라이브에서의) 자기 테이프, 메모리 디바이스 예컨대 RAM 디바이스, ROM 디바이스, 등등, 및/또는 임의의 다른 적절한 타입의 저장 매체/디바이스를 비롯한 데이터를 저장하기에 적합한 임의의 타입의 저장 매체/디바이스 중 하나 이상을 포함할 수도 있다.

[0044] 스토리지(114)에 저장된 것으로 도시되는 데이터(124)는, 하나 이상의 파일, 하나 이상의 폴더, 파일과 폴더의 조합, 및/또는 임의의 다른 타입의 데이터 구조체 및/또는 다수의 데이터를 비롯한 임의의 타입의 데이터일 수도 있다. 데이터(데이터(124))의 단일의 인스턴스가 스토리지(114)에 저장된 것으로 도시되지만, 데이터의 단일의 인스턴스는 도 1에서 예시의 용이성을 위해 도시된다. 데이터의 임의의 수의 인스턴스가 스토리지(114)에 저장될 수도 있고, 각각의 인스턴스는 본원에서 개시되는 바와 같이 구성되는 대응하는 보안 파라미터를 갖는 임의의 사이즈의 하나 이상의 파일 및/또는 폴더이다는 것이 이해되어야 한다.

[0045] 네트워크(106)의 예는, 근거리 통신망(local area network; LAN), 광역 통신망(wide area network; WAN), 개인 영역 네트워크(personal area network; PAN), 및/또는 인터넷과 같은 통신 네트워크의 조합을 포함한다. 네트워크(106)를 통한 통신을 위해, 컴퓨팅 디바이스(102) 및 서버(104) 각각은, 네트워크 인터페이스(예를 들면, 네

트워크 인터페이스 카드(network interface card; NIC), 등등), 유선 또는 무선 인터페이스, 예컨대 IEEE 802.11 무선 LAN(wireless LAN; WLAN) 무선 인터페이스, 와이맥스(Wi-MAX; Worldwide Interoperability for Microwave Access) 인터페이스, 이더넷 인터페이스, USB(Universal Serial Bus) 인터페이스, 셀룰러 네트워크 인터페이스, Bluetooth™ 인터페이스, 등등을 포함할 수도 있다.

[0046] 유저는, 컴퓨팅 디바이스(102)에 의해 저장되어 있는 데이터, 예컨대 스토리지(114)에 저장되어 있는 데이터(124)에 대한 데이터 보호를 구성하기 위해, 컴퓨팅 디바이스(102)에서 유저 인터페이스 모듈(108)과 (존재하는 경우) 상호작용할 수도 있거나, 또는 서버(104)에서 유저 인터페이스 모듈(128)과 (존재하는 경우) 상호작용할 수도 있다. 데이터 보호를 구성하는 유저는 컴퓨팅 디바이스(102)의 소유자 또는 다른 유저, 시스템 관리자(예를 들면, 컴퓨팅 디바이스(102)가 회사의 디바이스인 경우), 또는 다른 사람일 수도 있다.

[0047] 컴퓨팅 디바이스(102)에서의 유저 인터페이스 모듈(108)은, 컴퓨팅 디바이스(102)의 유저가 컴퓨팅 디바이스(102)에 저장되어 있는 데이터에 대한 보호를 구성하기에 편리한 방식으로 존재할 수도 있다. 유저 인터페이스 모듈(108)은 컴퓨팅 디바이스(102) 상에 저장되어 있는 데이터 보호 애플리케이션(예를 들면, 독립형 데스크탑 또는 모바일 애플리케이션, 부분적으로 클라우드 기반인 "앱", 등등)의 일부일 수도 있거나, 컴퓨팅 디바이스(102)의 오퍼레이팅 시스템의 일부일 수도 있거나, 또는 컴퓨팅 디바이스(102)에서 다른 방식으로 존재할 수도 있고 구성될 수도 있다.

[0048] 유저 인터페이스 모듈(108)에 의해 생성되는 유저 인터페이스와 상호작용할 때, 유저는 스토리지(114)에 저장되어 있는 데이터, 예컨대 데이터(124)를 보는 것이 가능하게 될 수도 있고, 데이터 보호 구성을 위해 이러한 데이터를 선택할 수도 있다. 유저는, 데이터(124)에 대한 데이터 보호를 구성하기 위해, 그리고 데이터 보호 구성이 데이터(124)와 관련하여 보안 속성(122)으로서 저장되게 하기 위해 유저 인터페이스와 상호작용할 수도 있다.

[0049] 다른 실시형태에서, 컴퓨팅 디바이스(102)에서 유저 인터페이스 모듈(108)을 구비하지 않는 것이 바람직할 수도 있다. 예를 들면, 컴퓨팅 디바이스(102)를 획득하여 로그인할 수 있는 임의의 사람이 유저 인터페이스(108)에 액세스할 수 있고, 따라서 컴퓨팅 디바이스(102)에 저장되어 있는 데이터에 대한 보호를 구성(제거하는 것을 포함함)할 수 있으면, 보안 약점인 것으로 결정될 수도 있다. 이러한 실시형태에서, 유저 인터페이스 모듈(108)은 컴퓨팅 디바이스(102)에 존재하지 않을 수도 있고, 대신, 유저 인터페이스 모듈(128)은, 컴퓨팅 디바이스(102)에 저장되어 있는 데이터에 대한 보호를 구성하기 위해 사용되도록 서버(104)에 존재할 수도 있다. 예를 들면, 유저 인터페이스 모듈(128)은, 네트워크에서 액세스가 불가능한 서버(102) 상에 설치되는 데이터 보호 애플리케이션(또는 오퍼레이팅 시스템)의 일부일 수도 있거나, 네트워크에서 액세스가 가능한 애플리케이션(예를 들면, 브라우저로 액세스가 가능한 애플리케이션)의 일부일 수도 있거나, 또는 서버(104)에서 다른 방식으로 존재할 수도 있고 구성될 수도 있다.

[0050] 서버(104)의 유저 인터페이스 모듈(128)에 의해 생성되는 유저 인터페이스와 상호작용할 때, 유저는 컴퓨팅 디바이스(102)에 의해 저장되어 있는 데이터, 예컨대 데이터(124)를 네트워크(106)를 통해 보는 것이 가능하게 될 수도 있고, 데이터 보호 구성을 위해 이러한 데이터를 선택하는 것이 가능하게 될 수도 있다. 유저는 데이터(124)에 대한 데이터 보호를 구성하기 위해 유저 인터페이스와 상호작용할 수도 있고, 데이터 보호 구성이 데이터(124)와 관련하여 보안 속성(122)으로서 저장되게 할 수도 있다.

[0051] 유저 인터페이스 모듈(108) 및/또는 유저 인터페이스 모듈(128)은, 실시형태에서, 데이터 보호를 임의의 방식으로 구성하기 위해 사용될 수도 있다. 예를 들면, 한 실시형태에서, 유저 인터페이스 모듈(108) 및/또는 유저 인터페이스 모듈(128)은 도 2에서 예시되는 방식으로 동작할 수도 있다. 도 2는, 예시적인 실시형태에 따른, 저장된 데이터에 대한 보호를 구성하기 위한 프로세스의 플로우차트(200)를 묘사한다. 플로우차트(200)는 도 1과 관련하여 다음과 같이 설명된다. 다음의 설명에 기초하면, 추가적인 구조적 및 동작적 실시형태가 관련 기술분야(들)의 숙련된 자에게는 명백할 것이다.

[0052] 플로우차트(200)는 단계 202로 시작한다. 단계 202에서, 컴퓨팅 디바이스 상에 저장되어 있는 데이터에 데이터 민감도 레벨이 할당되는 것을 가능하게 하는 유저 인터페이스가 제공된다. 예를 들면, 도 1에서 도시되는 바와 같이, 유저 인터페이스 모듈(108)은 (존재하는 경우) 유저 인터페이스(138)를 생성할 수도 있고, 유저 인터페이스 모듈(128)은 (존재하는 경우) 유저 인터페이스(140)를 생성할 수도 있다. 유저 인터페이스(138) 및 유저 인터페이스(140) 각각은, 그래픽 유저 인터페이스, 터치 인터페이스, 음성 제어 인터페이스, 햅틱 인터페이스, 제스쳐 인터페이스, 등등을 비롯한 임의의 수의 유저 인터페이스 엘리먼트를 포함하는 임의의 타입의 유저 인터페이스일 수도 있다.

[0053] 한 실시형태에서, 유저 인터페이스(138) 및/또는 유저 인터페이스(140)는, 컴퓨팅 디바이스(102) 상에 저장되어 있는 데이터, 예컨대 데이터(124)에 데이터 민감도 레벨이 할당되는 것을 가능하게 하기 위해 제공될 수도 있다. 도 1에서 도시되는 바와 같이, 유저 인터페이스(138)는, 제1 데이터 민감도(data sensitivity; DS) 선택기(116)를 포함하고, 유저 인터페이스(140)는 제2 DS 선택기(130)를 포함한다. DS 선택기(116) 및/또는 DS 선택기(130)는, 어떤 것이 존재하는지에 따라, 데이터(124)에 데이터 민감도 레벨을 할당하기 위해 유저의 의해 함께 상호작용될 수도 있다. 예를 들면, DS 선택기(116) 및/또는 DS 선택기(130)는, 체크박스, 토글 스위치, 버튼, 풀다운 메뉴, 다른 유저 인터페이스 엘리먼트와 같은 유저 인터페이스 엘리먼트일 수도 있다. 유저는 데이터(124)에 대한 데이터 민감도를 선택하기 위해 유저 인터페이스 엘리먼트와 상호작용할 수도 있다. 예를 들면, 유저는 선택된 데이터를 민감한 것으로 또는 민감하지 않은 것으로 지정하기 위해 DS 선택기(116) 또는 DS 선택기(130)와 상호작용할 수도 있다. 한 실시형태에서, 유저는 또한, 선택된 데이터를 상이한 정도의 민감도(예를 들면, 민감하지 않음, 적당히 민감함, 아주 민감함, 등등)를 갖는 것으로 지정하기 위해 DS 선택기(116) 또는 DS 선택기(130)와 상호작용할 수도 있다.

[0054] 단계 204에서, 데이터 보호 응답은 유저 인터페이스를 통해 데이터와 관련되도록 선택될 수 있다. 한 실시형태에서, 유저 인터페이스(138) 및/또는 유저 인터페이스(140)는, 컴퓨팅 디바이스(102) 상에 저장되어 있는 데이터, 예컨대 데이터(124)에 데이터 보호 응답이 할당되는 것을 가능하게 하기 위해 제공될 수도 있다. 데이터 보호 응답은, 데이터가 바람직하지 않은 또는 위험한 액세스로 적어도 잠재적으로 위협 받고 있는 것으로 결정되는 경우(예를 들면, 컴퓨팅 디바이스(102)를 둔 곳을 잊어버리고, 컴퓨팅 디바이스(102)가 잠재적으로 도난 당하고, 도난 당한 것이 알려져 있고, 권한 없는 사람에 의해 잠재적으로 액세스되고 있고, 컴퓨팅 디바이스(102)의 유저가 데이터에 액세스하도록 강제되고 있고, 등등)에 데이터와 관련하여 시행될 것이다.

[0055] 도 1에서 도시되는 바와 같이, 유저 인터페이스(138)는 제1 데이터 보호 응답(data protection response; DPR) 선택기(118)를 포함하고, 유저 인터페이스(140)는 제2 DPR 선택기(132)를 포함한다. DPR 선택기(118) 및/또는 DPR 선택기(132)는, 어떤 것이 존재하는지에 따라, 데이터 보호 응답을 데이터(124)에 할당하기 위해 유저에 의해 함께 상호작용될 수도 있다. 예를 들면, DPR 선택기(118) 및/또는 DPR 선택기(132)는 본원에서 개시되는 또는 다르게는 공지되어 있는 임의의 타입의 유저 인터페이스 엘리먼트일 수도 있다. 유저는 데이터(124)에 대한 데이터 보호 응답을 선택하기 위해 유저 인터페이스 엘리먼트와 상호작용할 수도 있다. 데이터(124)에 대한 선택 및 할당을 위해, 다양한 타입의 데이터 보호 응답이 이용가능할 수도 있다.

[0056] 예를 들면, 한 실시형태에서, 플로우차트(200)의 단계 204는 도 3에서 도시되는 프로세스를 포함할 수도 있다. 도 3은, 예시적인 실시형태에 따른, 데이터에 대한 데이터 보호 응답을 선택하기 위한 단계(302)를 묘사한다. 단계 302에서, 데이터 보호 응답은, 소프트 삭제 및 하드 삭제를 포함하는 복수의 데이터 보호 응답으로부터 선택될 수 있다. 따라서, 한 실시형태에서, DPR 선택기(118) 및/또는 DPR 선택기(132)는 데이터 보호 응답의 리스트를 제공할 수도 있고, 데이터 보호 응답 중 하나 이상은 (예를 들면, 풀다운 메뉴, 체크박스, 등등에 의해) 리스트로부터 선택되어 데이터에 할당될 수도 있다. 데이터 보호 응답은 데이터를 하드 삭제하는 것 또는 데이터를 소프트 삭제하는 것을 포함할 수도 있다. 본원에서 더 상세히 논의되는 바와 같이, "하드 삭제"는 데이터를 영구적으로 액세스 불가능하게 만드는 것(예를 들면, 메모리/스토리지에서 데이터를 덮어쓰기 하는 것)을 포함하고, 한편 "소프트 삭제"는, 데이터가 나중의 시간에 복구될 수도 있도록, (예를 들면, 데이터에 대한 링크 또는 파일 포인터를 삭제하는 것에 의해) 데이터를 일시적으로 액세스 불가능하게 만드는 것을 포함한다. 다른 예시적인 데이터 보호 응답은, 데이터에 대한 파일 시스템 요청이 무시되게 하는 것에 의해 데이터를 숨기는 것을 포함할 수도 있다.

[0057] 다른 타입의 데이터 보호 응답이 선택될 수도 있다. 예를 들면, 도 4는, 예시적인 실시형태에 따른, 하나 이상의 상이한 데이터 보호 응답을 선택하기 위한 프로세스의 플로우차트(400)를 묘사한다. 플로우차트(400)의 각각의 단계는 별개의 그리고 독립적인 데이터 보호 응답의 선택을 설명한다. 플로우차트(400)에서 설명되는 데이터 보호 응답 중 임의의 하나 이상은 데이터의 특정한 인스턴스에 선택 및 할당될 수도 있다. 플로우차트(400)는 다음과 같이 설명된다. 다음의 설명에 기초하면, 추가적인 구조적 및 동작적 실시형태가 관련 기술분야(들)의 숙련된 자에게는 명백할 것이다.

[0058] 플로우차트(400)는 단계 402로 시작한다. 단계 402에서, 소프트 삭제 데이터 보호 응답이 선택된다. 전술한 바와 같이, DPR 선택기(118) 및/또는 DPR 선택기(132)는, 데이터에 대한 데이터 보호 응답으로서 할당될 소프트 삭제에 대한 옵션을 제공할 수도 있다. 소프트 삭제에 따르면, 데이터는 컴퓨팅 디바이스(102) 상에서 유저에 의한 시야로부터 은닉된다. 예를 들면, 데이터를 나타내는 파일에 대한 링크 또는 파일 포인터가 삭제될 수도 있고, 링크 또는 파일 포인터는, 가능한 차후의 복구/복원을 위해, 안전한 것으로 생각되는 위치에 저장될 수도

있다.

[0059] 단계 404에서, 하드 삭제 데이터 보호 응답이 선택된다. 전술한 바와 같이, DPR 선택기(118) 및/또는 DPR 선택기(132)는, 데이터에 대한 데이터 보호 응답으로서 할당될 하드 삭제에 대한 옵션을 제공할 수도 있다. 하드 삭제에 따르면, 데이터는, 복구 또는 복원될 수 없는 방식으로 스토리지(예를 들면, 스토리지(114))로부터 삭제된다. 예를 들면, 데이터가 저장되어 있던 저장 위치는 덮어쓰기 될 수도 있다.

[0060] 단계 406에서, 경보 데이터 보호 응답이 선택된다. 한 실시형태에서, DPR 선택기(118) 및/또는 DPR 선택기(132)는, 데이터에 대한 데이터 보호 응답으로서 할당될 경보에 대한 옵션을 제공할 수도 있다. 경보는, 컴퓨팅 디바이스(102)의 권한 소지 유저(예를 들면, 소유자, 시스템 관리자, 등등)에게, 데이터가 인가되지 않은 액세스로 위협 받을 수도 있다는 것을 통지하도록 구성될 수도 있다. 경보는 권한 소지 유저의 전화번호의 주소로 전달/송신될 수도 있거나, 또는, 이메일 메시지, 텍스트 메시지, 소셜 네트워크 메시지, 전화 통화, 비프음 노이즈(beeping noise)(또는 다른 사운드), 등등을 비롯한 다른 형태로 제시될 수도 있다.

[0061] 단계 408에서, 파일이 열리지 않게 하는 데이터 보호 응답이 선택된다. 한 실시형태에서, DPR 선택기(118) 및/또는 DPR 선택기(132)는, 데이터에 대한 데이터 보호 응답으로서, 하나 이상의 파일(데이터를 나타냄)이 열리지 않게 하는 것에 대한 옵션을 제공할 수도 있다. 파일(들)은, 파일(들)을 잠그는 것, 파일(들)에 대한 퍼미션을 (유저의 액세스 권한 위로) 향상시키는 것, 등등을 비롯한 임의의 방식으로, 열리는 않게 될 수도 있다.

[0062] 단계 410에서, 열린 데이터 디스플레이 윈도우가 닫히게 하는 데이터 보호 응답이 선택된다. 한 실시형태에서, DPR 선택기(118) 및/또는 DPR 선택기(132)는, 데이터에 대한 데이터 보호 응답으로서, 데이터를 디스플레이하는 열린 디스플레이 윈도우를 닫는 것에 대한 옵션을 제공할 수도 있다.

[0063] 단계 412에서, 열린 데이터 디스플레이 윈도우가 적어도 하나의 다른 윈도우 뒤로 숨겨지게 하는 데이터 보호 응답이 선택된다. 한 실시형태에서, DPR 선택기(118) 및/또는 DPR 선택기(132)는, 데이터에 대한 데이터 보호 응답으로서, 열린 디스플레이 윈도우를, 하나 이상의 다른 윈도우 뒤에 숨기기 위한 옵션을 제공할 수도 있다. 예를 들면, 데이터 디스플레이 윈도우는, 이미 열려 있는 하나 이상의 다른 윈도우 뒤로 이동할 수도 있거나, 또는 하나 이상의 신규의 윈도우가 데이터 디스플레이 윈도우 앞에서 열릴 수도 있다.

[0064] 본원에서 설명되는 바와 같이, 데이터 보호 응답을 데이터에 할당하도록 DPR 선택기(118) 및/또는 DPR 선택기(132)가 상호작용될 수도 있다는 것을 유의한다. 다른 실시형태에서, 데이터 보호 응답은 데이터 민감도와 사전 관련될 수도 있고, 데이터 민감도 레벨이 특정한 데이터에 할당되는 경우, 관련된 데이터 보호 응답도 또한 그 데이터에 할당된다. 예를 들면, 소프트 삭제는 낮은 데이터 민감도 레벨과 관련될 수도 있고, 하드 삭제는 높은 데이터 민감도 레벨과 관련될 수도 있다. (플로우차트(200)의 단계 202에서) 특정한 데이터에 낮은 민감도 레벨이 할당되면, (단계 204에서) 그 특정한 데이터에 소프트 삭제가 또한 자동적으로 할당된다.

[0065] 도 2를 다시 참조하면, 단계 206에서, 유저 인터페이스를 통해 데이터에 상황적 트리거가 할당될 수 있다. 한 실시형태에서, 유저 인터페이스(138) 및/또는 유저 인터페이스(140)는, 컴퓨팅 디바이스(102) 상에 저장되어 있는 데이터, 예컨대 데이터(124)에 상황적 트리거가 할당되는 것을 가능하게 하기 위해 제공될 수도 있다. 상황적 트리거는, 검출시, 컴퓨팅 디바이스(102)가 인가되지 않은 액세스를 받게 되었거나 또는 인가되지 않은 액세스에 취약하게 되었다는 것을 나타내는 상태 또는 상태의 세트일 수도 있다.

[0066] 도 1에서 도시되는 바와 같이, 유저 인터페이스(138)는 제1 상황적 트리거(contextual trigger; CT) 선택기(120)를 포함하고, 유저 인터페이스(140)는 제2 CT 선택기(134)를 포함한다. CT 선택기(120) 및/또는 CT 선택기(134)는, 어떤 것이 존재하는지에 따라, 상황적 트리거를 설정하기 위해 유저에 의해 함께 상호작용될 수도 있는데, 상황적 트리거의 검출은 데이터 보호 모드가 데이터 보호 시행기(112)에 의해 활성화되게 한다. 예를 들면, CT 선택기(120) 및/또는 CT 선택기(134)는 본원에서 개시되는 또는 다르게는 공지되어 있는 임의의 타입의 유저 인터페이스 엘리먼트일 수도 있다. 유저는 데이터(124)에 대한 상황적 트리거를 선택하기 위해 유저 인터페이스 엘리먼트와 상호작용할 수도 있다. 상황적 트리거의 예는 다음의 것을 포함하지만 이들로 제한되지는 않는데, 권한 없는 유저가 컴퓨팅 디바이스(102)에 근접한 상태에 있다는 것의 감지; 컴퓨팅 디바이스(102)를 개봉하는 것; 디바이스 부트 업, 로그인, 또는 셧다운 동안 소정의 유저 입력 및/또는 유저 입력 거동의 검출된 존재 또는 부재; 유저가 권한 소지 유저가 아니다는 것을 나타내는 컴퓨팅 디바이스(102)의 유저의 감지된 거동이다. 아주 다양한 다른 상황적 트리거도 또한 사용될 수도 있다.

[0067] 전술한 바와 같이, 민감도 레벨, 데이터 보호 응답, 및 상황적 트리거가 데이터(124)에 대한 할당을 위해 선택될 수도 있다. 컴퓨팅 디바이스(102)에서 만들어지는 민감도 레벨, 데이터 보호 응답, 및 상황적 트리거의 선택

은 유저 인터페이스 모듈(108)로부터 보안 속성(122A)으로서 출력된다. 서버(104)에서 만들어지는 민감도 레벨, 데이터 보호 응답, 및 상황적 트리거의 선택은 유저 인터페이스 모듈(128)로부터 보안 속성(122A)으로서 출력되고, 통신 신호에서 네트워크(106)를 통해 컴퓨팅 디바이스(102)로 송신된다. 보안 속성(122A 또는 122B)은 데이터(124)와 관련하여 보안 속성(122)으로서 저장될 수도 있다.

[0068] B. 데이터 보호를 트리거하고 시행하기 위한 예시적인 실시형태

[0069] 데이터 보호 시스템은, 인가되지 않은 액세스로 위협 받는 데이터를 모니터링하기 위해, 그리고 데이터를 보호할 데이터 보호 정책을 시행하기 위해, 다양한 방식으로 구성될 수도 있다. 예를 들면, 도 1과 관련하여 전술한 바와 같이, 컴퓨팅 디바이스(102)의 데이터 보호 시스템(136)은 상황적 트리거 모니터(110) 및 데이터 보호 시행기(112)를 포함한다. 상황적 트리거 모니터(110) 및 데이터 보호 시행기(112)는, 각각, 데이터의 인가되지 않은 액세스를 검출하도록, 그리고 데이터 보호를 시행하도록 구성된다. 상황적 트리거 모니터(110) 및 데이터 보호 시행기(112)가 도 5와 관련하여 다음과 같이 설명된다. 도 5는, 예시적인 실시형태에 따른, 데이터 보호 응답의 시행을 트리거하는 데이터와 관련되는 상황적 트리거를 모니터링하기 위한 프로세스의 플로우차트(500)를 묘사한다. 플로우차트(500), 상황적 트리거 모니터(110) 및 데이터 보호 시행기(112)가 다음과 같이 설명된다. 다음의 설명에 기초하면, 추가적인 구조적 및 동작적 실시형태가 관련 기술분야(들)의 숙련된 자에게는 명백할 것이다.

[0070] 플로우차트(500)는 단계 502로 시작한다. 단계 502에서, 상황적 트리거의 발생이 모니터링된다. 예를 들면, 도 1에서 도시되는 바와 같이, 상황적 트리거 모니터(110)가 데이터(124)와 관련되는 보안 속성(122)의 상황적 트리거(들)를 수신한다. 상황적 트리거 모니터(110)는 보안 속성(122)의 상황적 트리거(들)를, 유저 인터페이스 모듈(108) 및/또는 유저 인터페이스 모듈(128)로부터, 또는 스토리지(114)로부터 직접적으로 수신할 수도 있다. 상황적 트리거 모니터(110)는, 상황적 트리거(들) 중 임의의 것이 검출되었는지를 결정하기 위해 시간에 걸쳐 동작한다. 상황적 트리거가 검출되었다는 것을 상황적 트리거 모니터(110)가 결정하면, 상황적 트리거 모니터(110)는 트리거 통지(126)를 생성하는 것에 의해 데이터 보호 시행기(112)에게 통지한다.

[0071] 단계 504에서, 데이터와 관련되는 데이터 보호 응답은, 상황적 트리거의 발생이 검출될 때, 시행된다. 트리거 통지(126)에 응답하여, 데이터 보호 시행기(112)는, 데이터(124)와 관련되는 보안 속성(122)의 데이터 보호 응답(들)을 시행할 수도 있다. 시행된 데이터 보호 응답은 도 1에서 시행된 액션(142)으로서 예시된다.

[0072] 실시형태에서, 본원에서 언급되는 또는 다르게는 공지되어 있는 임의의 하나 이상의 데이터 보호 응답을, 보안 속성(122)의 데이터 보호 응답이 나타낼 수도 있고, 데이터 보호 시행기(112)가 시행할 수도 있다. 예를 들면, 본원의 교시에 기초하여 관련 기술 분야(들)에서 숙련된 자에게 명백할 임의의 다른 적절한 데이터 보호 응답, 및/또는 플로우차트(400)(도 4)를 참조로 설명되는 그리고 본원의 다른 곳에서 설명되는 데이터 보호 응답 중 임의의 하나 이상을, 데이터 보호 응답이 나타낼 수도 있고 데이터 보호 시행기(112)가 시행할 수도 있다. 따라서, 데이터 보호 시행기(112)는 하나 이상의 데이터 보호 응답을 실행하기 위한 기능성을 포함할 수도 있거나 또는 그 기능성에 액세스할 수도 있다. 예를 들면, 데이터 보호 시행기(112)는, 파일 및/또는 폴더의 소프트 삭제(이것은 파일 암호화, 파일/폴더 이동 및/또는 이름바꾸기, 파일/폴더에 대한 링크 재구성, 등등을 포함할 수도 있음)를 수행할 수 있는 파일 매니저 모듈을 포함할 수도 있거나 그 파일 매니저 모듈에 액세스할 수도 있다. 데이터 보호 시행기(112)는, 경보 메시지를 전송하도록 구성되는 메시징 모듈(예를 들면, 문자 메시지(texting) 툴, 이메일 툴, 인스턴트 메시징 툴, 소셜 네트워크 메시징 툴, 전화 통신 툴, 오디오 툴, 등등)을 포함할 수도 있거나 또는 메시징 모듈에 액세스할 수도 있다 다른 예에서, 데이터 보호 시행기(112)는, 디스플레이된 윈도우 및/또는 열려 있는 윈도우를 재정렬할 수 있는 (예를 들면, OS의) 윈도우 관리 모듈을 포함할 수도 있거나 또는 그 윈도우 관리 모듈에 액세스할 수도 있다. 데이터 보호 시행기(112)는, 본원의 교시에 기초하여 관련 기술 분야(들)에서 숙련된 자에게 명백한 바와 같이, 하나 이상의 데이터 보호 응답을 수행하기 위한 추가적인 및/또는 대안적인 기능성을 가지고 구성될 수도 있다.

[0073] III. 소정 수의 사람이 컴퓨팅 디바이스에 근접하여 위치한다는 결정에 기초한 예시적인 상황적 트리거

[0074] 상황적 트리거 모니터(110)는, 데이터가 인가되지 않은 액세스에 노출되거나 또는 인가되지 않은 액세스로 위협 받는 것을 나타내는 트리거를 모니터링하기 위해 다양한 방식으로 구성될 수도 있다. 예를 들면, 도 6은, 예시적인 실시형태에 따른, 소정 수의 사람이 컴퓨팅 디바이스에 근접하여 위치한다는 결정을 상황적 트리거로서 사용하도록 구성되는 데이터 보호 시스템(600)의 블록도이다. 도 6에서 도시되는 바와 같이, 데이터 보호 시스템(600)은 상황적 트리거 모니터(110) 및 데이터 보호 시행기(112)를 포함한다. 또한, 상황적 트리거 모니터(110)는 다중 유저 인식 로직(multiuser recognition logic; 604) 및 모드 선택 로직(606)을 포함한다. 한 실시형

태에서, 상황적 트리거 모니터(110)는 플로우차트(500)(도 5)의 단계 502를 수행할 수도 있고, 데이터 보호 시행기(112)는 플로우차트(500)의 단계 504를 수행할 수도 있다. 데이터 보호 시스템(600)은 도 1에서 도시되는 데이터 보호 시스템(136)의 대응하는 부분의 예이며, 예시의 용이성을 위해, 시스템(600)의 모든 특징이 도 6에서 도시되는 것은 아니다. 데이터 보호 시스템(600)은 컴퓨팅 디바이스(102)에 포함될 수도 있다. 데이터 보호 시스템(600)은 다음과 같이 설명된다.

[0075] 도 6의 실시형태에서, 상황적 트리거 모니터(110)는, 소정 수의 사람이 컴퓨팅 디바이스에 근접하여 위치한다는 결정을 데이터 보호를 위한 상황적 트리거로서 사용하도록 구성된다. 도 6에서 도시되는 실시형태에 따르면, 하나 이상의 이미지 캡쳐 디바이스(602)가 컴퓨팅 디바이스(102)와 통합되거나 또는 적절한 유선 및/또는 무선 연결을 통해 컴퓨팅 디바이스(102)에 연결될 수도 있다. 이미지 캡쳐 디바이스(들)(602)는 컴퓨팅 디바이스(102) 주위의 하나 이상의 구역의 이미지를 캡쳐하도록 동작한다. 이미지 캡쳐 디바이스(들)(602)는, 예를 들면, 하나 이상의 광 감지 카메라를 포함할 수도 있다. 그러나, 이 예는 제한하는 것으로 의도되지 않으며, 이미지 캡쳐 디바이스(들)(602)는, 거리 센서, 단층 촬영 디바이스, 레이더 디바이스, 초음파 카메라, 또는 등등을 포함하지만 이들로 제한되지는 않는, 2D 이미지, 3D 이미지, 또는 이미지 시퀀스를 캡쳐하는데 적합한 다른 타입의 디바이스를 포함할 수도 있다.

[0076] 이미지 캡쳐 디바이스(들)(602)는, 이미지 데이터(616)의 형태로 표현되는 하나 이상의 이미지를 캡쳐하도록 동작한다. 이러한 이미지 데이터는 다중 인물 인식 로직(multi-person recognition logic; 604)으로 전달된다. 다중 인물 인식 로직(604)은, 컴퓨팅 디바이스(102)에 근접하여 위치한 사람의 수를 결정하기 위해 이미지 데이터(616)를 분석한다. 예를 들면, 다중 인물 인식 로직(604)은, 이미지 데이터(616)에 기초하여 컴퓨팅 디바이스(102)에 근접하여 위치한 다수의 별개의 얼굴을 식별하기 위해, 얼굴 인식 알고리즘을 적용할 수도 있다. 다른 예로서, 다중 인물 인식 로직(604)은, 이미지 데이터(616)에 기초하여 컴퓨팅 디바이스(102)에 근접하여 위치한 다수의 별개의 몸(body)을 식별하기 위해, 몸 인식 알고리즘(body recognition algorithm)을 적용할 수도 있다.

[0077] 한 실시형태에서, 다중 인물 인식 로직(604)은, 컴퓨팅 디바이스(102)의 일정 거리 내의 사람의 수를 결정하기 위해 이미지 데이터(616)를 분석하는 것에 의해, 컴퓨팅 디바이스(102)에 근접하여 위치한 사람의 수를 결정하도록 구성된다. 예를 들면, 컴퓨팅 디바이스(102)의 1 피트, 3 피트, 5 피트, 10 피트 또는 임의의 다른 특정 거리 내에 위치한 사람의 수가 다중 인물 인식 로직(604)에 의해 결정될 수도 있다. 하나의 실시형태에서, 거리는 고정 값(즉, 유저가 구성할 수 없는 값)이다. 대안적인 실시형태에서, 거리는 유저가 구성할 수 있는 값이다. 또한 이러한 실시형태에 따르면, 컴퓨팅 디바이스(102) 또는 서버(104)는, 다중 인물 인식 로직(604)에 의해 사람의 존재가 결정되어야 하는 특정 거리를 유저가 지정할 수 있게 하는 유저 인터페이스를 제공하도록 구성되는 유저 인터페이스 모듈(예를 들면, 컴퓨팅 디바이스(102)의 유저 인터페이스 모듈(108) 또는 서버(104)의 유저 인터페이스 모듈(128))을 포함할 수도 있다.

[0078] 다중 인물 인식 로직(604)이 컴퓨팅 디바이스(102)에 근접하여 위치한 사람의 수를 결정한 이후, 다중 인물 인식 로직(604)은 이러한 정보를 출력(608)으로서 모드 선택 로직(606)으로 전달한다. 모드 선택 로직(606)은, 컴퓨팅 디바이스(102)에 근접하여 위치한 사람의 수를 임계 값에 비교한다. 하나의 실시형태에서, 임계 값은 고정 값(즉, 유저가 구성할 수 없는 값)이다. 대안적인 실시형태에서, 임계 값은 유저가 구성할 수 있는 값이다. 또한 이러한 실시형태에 따르면, 컴퓨팅 디바이스(102) 또는 서버(104)는, 유저가 임계 값을 지정할 수 있게 하는 유저 인터페이스를 제공하도록 구성되는 유저 인터페이스 모듈(예를 들면, 컴퓨팅 디바이스(102)의 유저 인터페이스 모듈(108) 또는 서버(104)의 유저 인터페이스 모듈(128))을 포함할 수도 있다.

[0079] 컴퓨팅 디바이스(102)에 근접하여 위치한 사람의 수를 임계 값에 비교한 결과에 기초하여, 모드 선택 로직(606)은 컴퓨팅 디바이스(102)의 복수의 동작 모드 중 하나를 선택적으로 활성화한다.

[0080] 예를 들면, 하나의 실시형태에서, 모드 선택 로직(606)은 다음과 같이 동작한다. 컴퓨팅 디바이스(102)에 근접하여 위치한 사람의 수가 임계 값을 초과하지 않는다는 것을 모드 선택 로직(606)이 결정하면, 모드 선택 로직(606)은, 컴퓨팅 디바이스(102) 상에 저장되어 있는 민감 데이터 및 비민감 데이터를 유저가 보는 것과 액세스하는 것 둘 다가 가능한 동작의 모드를 활성화한다. 이것은 본질적으로, 데이터 보호 시행기(112)에 의해 어떠한 데이터 보호 조치도 시행되지 않는 일반적인 또는 "열린" 동작 모드를 포함한다.

[0081] 여전히 또한 이 실시형태에 따르면, 컴퓨팅 디바이스(102)에 근접하여 위치한 사람의 수가 임계 값을 초과한다는 것을 모드 선택 로직(606)이 결정하면, 모드 선택 로직(606)은, 컴퓨팅 디바이스(102) 상에 저장되어 있는 비민감 데이터를 유저가 볼 수 있고 액세스할 수 있게 되지만, 컴퓨팅 디바이스(102) 상에 저장되어 있는 민감

데이터를 유저가 볼 수 없게 및/또는 액세스할 수 없게 되는 동작의 모드를 활성화한다. 이것은, 데이터 보호 시행기(112)로 하여금 컴퓨팅 디바이스(102) 상에 저장되어 있는 민감 데이터에 할당되는 다양한 데이터 보호 응답을 구현하게 하는 신호(612)를 데이터 보호 시행기(112)로 전송하는 것을 수반할 수도 있다. 앞서 언급된 바와 같이, 이러한 데이터 보호 응답은, 민감 데이터의 항목을 하드 삭제하는 것, 민감 데이터의 항목을 소프트 삭제하는 것, 민감 데이터의 항목에 대한 파일 시스템 요청이 무시되게 하는 것, 민감 데이터의 항목이 열리거나 닫힐 수 없게 하는 것, 또는 민감 데이터의 항목이 디스플레이되는 윈도우를 숨기는 것을 포함할 수도 있지만 그러나 이들로 제한되지는 않는다.

[0082] 데이터 보호 시행기(112)는, 데이터(124)와 관련되는 보안 속성(122)의 데이터 보호 응답을 시행할 수도 있다. 도 6에서 도시되는 바와 같이, 데이터 보호 시행기(112)는 데이터(124)와 관련되는 보안 속성(122)으로부터 데이터 보호 응답(614)을 수신한다. 데이터 보호 응답(614)은, 데이터(124)에 대해 데이터 보호가 시행되어야 한다는 것을 모드 선택 로직(606)으로부터 수신되는 신호(612)가 나타내는 경우, 데이터 보호 시행기(112)에 의해 수행될 하나 이상의 데이터 보호 응답을 나타낸다.

[0083] 이제, 데이터 보호에 대한 앞선 접근 방식(approach)이 도 7의 플로우차트(700)를 참조로 설명될 것이다. 특히, 도 7은, 예시적인 실시형태에 따른, 컴퓨팅 디바이스에 근접하여 위치한 사람의 결정된 수에 기초하여, 데이터에 대한 데이터 보호 응답을 시행하기 위한 프로세스의 플로우차트(700)를 묘사한다.

[0084] 도 7을 참조하면, 플로우차트(700)의 방법은 단계 702로 시작한다. 단계 702에서, 컴퓨팅 디바이스에 연결되는 또는 컴퓨팅 디바이스와 통합되는 하나 이상의 이미지 캡쳐 디바이스로부터 이미지 데이터가 수신된다. 예를 들면, 전술한 바와 같이, 다중 인물 인식 로직(604)은, 컴퓨팅 디바이스(102)에 연결되는 또는 컴퓨팅 디바이스(102)와 통합되는 이미지 캡쳐 디바이스(들)(602)로부터 이미지 데이터(616)를 수신할 수도 있다.

[0085] 단계 704에서, 이미지 데이터는 컴퓨팅 디바이스에 근접하여 위치한 사람의 수를 결정하도록 분석된다. 예를 들면, 전술한 바와 같이, 다중 인물 인식 로직(604)은, 컴퓨팅 디바이스(102)에 근접하여 위치한 사람의 수를 결정하기 위해 이미지 데이터(616)를 분석할 수도 있다. 다중 인물 인식 로직(604)은, 다수의 별개의 얼굴을 식별하기 위해 이미지 데이터(616)를 분석하는 것에 의해, 다수의 별개의 몸을 식별하기 위해 이미지 데이터(616)를 분석하는 것에 의해, 및/또는 컴퓨팅 디바이스(102)에 근접하여 위치한 다수의 사람을 식별하기 위한 임의의 다른 적절한 이미지 분석 기술을 사용하는 것에 의해, 이 단계를 수행할 수도 있다. 다중 인물 인식 로직(604)은 또한, 컴퓨팅 디바이스(102)의 소정의 유저가 지정한 또는 시스템이 지정한 거리 내의 사람의 수를 결정하기 위해 이미지 데이터(616)를 분석하는 것에 의해, 이 단계를 수행할 수도 있다.

[0086] 단계 706에서, 컴퓨팅 디바이스에 근접하여 위치한 사람의 수가 임계 값을 초과하는지가 결정된다. 예를 들면, 전술한 바와 같이, 다중 인물 인식 로직(604)은, 컴퓨팅 디바이스(102)에 근접하여 위치한 사람의 수가 시스템이 지정하는 또는 유저가 지정하는 임계치를 초과하는지의 여부를 결정할 수도 있다.

[0087] 단계 708에서, 컴퓨팅 디바이스에 근접하여 위치한 사람의 수가 임계 값을 초과하지 않는다는 결정에 응답하여, 열린 동작 모드(open operating mode)가 활성화된다. 예를 들면, 컴퓨팅 디바이스(102)에 근접하여 위치한 사람의 수가 임계 값을 초과하지 않는다는 결정에 응답하여, 모드 선택 로직(606)은 열린 동작 모드가 활성화되게 할 수도 있다. 열린 동작 모드는, 컴퓨팅 디바이스(102) 상에 저장되어 있는 모든 민감 데이터 및 비민감 데이터를 유저가 볼 수 있고 액세스할 수 있는 모드(즉, 데이터 보호 응답이 데이터 보호 시행기(112)에 의해 시행되지 않은 모드)를 포함할 수도 있다. 이 단계가 열린 동작 모드의 "활성화"를 참조하지만, 이 단계는 또한, 임계 값이 초과되지 않는 한 열린 동작 모드에서의 계속된 동작을 망라한다.

[0088] 단계 710에서, 컴퓨팅 디바이스에 근접하여 위치한 사람의 수가 임계 값을 초과한다는 결정에 응답하여, 데이터 보호 동작 모드가 활성화된다. 예를 들면, 컴퓨팅 디바이스(102)에 근접하여 위치한 사람의 수가 임계 값을 초과한다는 결정에 응답하여, 모드 선택 로직(606)은, 데이터 보호 시행기(112)로 하여금 컴퓨팅 디바이스(102)를 데이터 보호 모드로 진입시키게 하는 신호(612)를 데이터 보호 시행기(112)로 전송할 수도 있다. 앞서 설명된 바와 같이, 데이터 보호 모드 동안, 데이터 보호 시행기(112)는, 이러한 민감 데이터를 유저가 볼 수 없게 및/또는 액세스할 수 없게 만들기 위해, 컴퓨팅 디바이스(102) 상에 저장되어 있는 민감 데이터에 할당되는 다양한 데이터 보호 응답을 구현할 수도 있다. 앞서 언급된 바와 같이, 이러한 데이터 보호 응답은, 민감 데이터의 항목을 하드 삭제하는 것, 민감 데이터의 항목을 소프트 삭제하는 것, 민감 데이터의 항목에 대한 파일 시스템 요청이 무시되게 하는 것, 민감 데이터의 항목이 열리거나 닫힐 수 없게 하는 것, 또는 민감 데이터의 항목이 디스플레이되는 윈도우를 숨기는 것을 포함할 수도 있지만 그러나 이들로 제한되지는 않는다.

[0089] 상기에서 논의된 바와 같이, 데이터 보호 동작 모드 동안, 데이터 보호 시행기(112)는 민감 데이터의 선택된 항목(예를 들면, 선택된 파일 및/또는 폴더)이 소프트 삭제되게 할 수도 있다. 이러한 소프트 삭제는, 예를 들면, 민감 데이터의 항목에 대한 링크 또는 파일 포인터의 보안 백업 카피를 (예를 들면, 링크 또는 파일 포인터의 암호화된 카피를 컴퓨팅 디바이스(102) 상에 또는 원격 디바이스 상에 저장하는 것에 의해) 생성하는 것 및 그 다음 링크 또는 파일 포인터에 컴퓨팅 디바이스(102)의 파일 시스템 및/또는 오퍼레이팅 시스템이 액세스할 수 없도록, 이러한 링크 또는 파일 포인터를 삭제하는 것을 포함할 수도 있다. 이러한 실시형태에 따르면, 소프트 삭제된 데이터는, 삭제된 링크 또는 파일 포인터를 보안 백업 카피로부터 컴퓨팅 디바이스(102)로 복원하는 것에 의해 복구될 수도 있다. 하나의 실시형태에서, 도 7의 단계 710의 수행의 결과로서 소프트 삭제되는 민감 데이터는, 나중에, 소프트 삭제된 데이터가 복구되어야 한다는 것을 나타내는 컴퓨팅 디바이스(102)에 대해 소정의 액션을 유저가 후속하여 수행할 때, 복구될 수도 있다.

[0090] IV. 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스에 근접하여 위치하지 않는다는 결정에 기초한 예시적인 상황적 트리거

[0091] 상황적 트리거 모니터(110)는, 데이터가 인가되지 않은 액세스에 노출되거나 또는 인가되지 않은 액세스로 위협받는 것을 나타내는 트리거를 모니터링하기 위해 다양한 방식으로 구성될 수도 있다. 예를 들면, 도 8은, 예시적인 실시형태에 따른, 컴퓨팅 디바이스의 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스에 근접하여 위치하지 않는다는 결정을 상황적 트리거로서 사용하도록 구성되는 데이터 보호 시스템(800)의 일부의 블록도이다. 도 8에서 도시되는 바와 같이, 데이터 보호 시스템(800)은 상황적 트리거 모니터(110) 및 데이터 보호 시행기(112)를 포함한다. 또한, 상황적 트리거 모니터(110)는 유저 인식 로직(804) 및 모드 선택 로직(806)을 포함한다. 한 실시형태에서, 상황적 트리거 모니터(110)는 플로우차트(500)(도 5)의 단계 502를 수행할 수도 있고, 데이터 보호 시행기(112)는 플로우차트(500)의 단계 504를 수행할 수도 있다. 데이터 보호 시스템(800)은 도 1에서 도시되는 데이터 보호 시스템(136)의 대응하는 부분의 예이며, 예시의 용이성을 위해, 시스템(800)의 모든 특징이 도 8에서 도시되는 것은 아니다. 데이터 보호 시스템(800)은 컴퓨팅 디바이스(102)에 포함될 수도 있다. 데이터 보호 시스템(800)은 다음과 같이 설명된다.

[0092] 도 8의 실시형태에서, 상황적 트리거 모니터(110)는, 컴퓨팅 디바이스의 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스에 근접하여 위치하지 않는다는 결정을, 데이터 보호를 위한 상황적 트리거로서 사용하도록 구성된다. 도 8에서 도시되는 실시형태에 따르면, 하나 이상의 이미지 캡쳐 디바이스(802)가 컴퓨팅 디바이스(102)와 통합되거나 또는 적절한 유선 및/또는 무선 연결을 통해 컴퓨팅 디바이스(102)에 연결될 수도 있다. 이미지 캡쳐 디바이스(들)(802)는 컴퓨팅 디바이스(102) 주위의 하나 이상의 구역의 이미지를 캡쳐하도록 동작한다. 이미지 캡쳐 디바이스(들)(802)는, 예를 들면, 하나 이상의 광 감지 카메라를 포함할 수도 있다. 그러나, 이 예는 제한하는 것으로 의도되지 않으며, 이미지 캡쳐 디바이스(들)(802)는, 거리 센서, 단층 촬영 디바이스, 레이더 디바이스, 초음파 카메라, 또는 등등을 포함하지만 이들로 제한되지는 않는, 2D 이미지, 3D 이미지, 또는 이미지 시퀀스를 캡쳐하는데 적합한 다른 타입의 디바이스를 포함할 수도 있다.

[0093] 이미지 캡쳐 디바이스(들)(802)는, 이미지 데이터(816)의 형태로 표현되는 하나 이상의 이미지를 캡쳐하도록 동작한다. 이러한 이미지 데이터는 유저 인식 로직(804)으로 전달된다. 유저 인식 로직(804), 컴퓨팅 디바이스(102)의 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스(102)에 근접하여 위치하는지를 결정하기 위해 이미지 데이터(816)를 분석한다. 예를 들면, 유저 인식 로직(804)은, 이미지 데이터(816)에 기초하여 컴퓨팅 디바이스(102)에 근접하여 위치한 소유자 또는 권한 소지 유저의 얼굴을 식별하기 위해 얼굴 인식 알고리즘을 적용할 수도 있다. 예를 들면, 유저 인식 로직(804)은, 이미지 데이터(816)에 기초하여 컴퓨팅 디바이스(102)에 근접하여 위치한 소유자 또는 권한 소지 유저의 몸을 식별하기 위해 몸 인식 알고리즘을 적용할 수도 있다. 소정의 실시형태에서, 유저 인식 로직(804)은 컴퓨팅 디바이스(102)의 소유자 또는 권한 소지 유저의 얼굴 및/또는 몸을 인식하도록 훈련될 수도 있다.

[0094] 한 실시형태에서, 유저 인식 로직(804)은, 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스(102)의 일정 거리 내에 있는지를 결정하기 위해 이미지 데이터(816)를 분석하는 것에 의해, 컴퓨팅 디바이스(102)의 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스(102)에 근접하여 위치하는지를 결정하도록 구성된다. 예를 들면, 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스(102)의 1 피트, 3 피트, 5 피트, 10 피트 또는 임의의 다른 특정 거리 내에 있는지의 여부가 유저 인식 로직(804)에 의해 결정될 수도 있다. 하나의 실시형태에서, 거리는 고정 값(즉, 유저가 구성할 수 없는 값)이다. 대안적인 실시형태에서, 거리는 유저가 구성할 수 있는 값이다. 또한 이러한 실시형태에 따르면, 컴퓨팅 디바이스(102) 또는 서버(104)는, 유저 인식 로직(804)에 의해 소유자 또는 권한 소지 유저의 존재가 결정되어야 하는 특정 거리를 유저가 지정할 수 있게 하는 유저 인터페이스를 제공하도록 구성되

는 유저 인터페이스 모듈(예를 들면, 컴퓨팅 디바이스(102)의 유저 인터페이스 모듈(108) 또는 서버(104)의 유저 인터페이스 모듈(128))을 포함할 수도 있다.

[0095] 컴퓨팅 디바이스(102)의 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스(102)에 근접하여 위치하는지의 여부를 유저 인식 로직(804)이 결정한 이후, 유저 인식 로직(804)은 이러한 정보를 출력(808)으로서 모드 선택 로직(806)으로 전달한다. 이 정보에 기초하여, 모드 선택 로직(806)은 컴퓨팅 디바이스(102)의 복수의 동작 모드 중 하나를 선택적으로 활성화한다.

[0096] 예를 들면, 하나의 실시형태에서, 모드 선택 로직(806)은 다음과 같이 동작한다. 컴퓨팅 디바이스(102)의 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스(102)에 근접하여 위치한다는 것을 출력(808)이 나타내면, 모드 선택 로직(806)은, 컴퓨팅 디바이스(102) 상에 저장되어 있는 민감 데이터 및 비민감 데이터를 유저가 보는 것과 액세스하는 것 둘 다가 가능한 동작의 모드를 활성화한다. 이것은 본질적으로, 데이터 보호 시행기(112)에 의해 어떠한 데이터 보호 조치도 시행되지 않는 일반적인 또는 "열린" 동작 모드를 포함한다.

[0097] 여전히 또한 이 실시형태에 따르면, 컴퓨팅 디바이스(102)의 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스(102)에 근접하여 위치하지 않는다는 것을 출력(808)이 나타내면, 모드 선택 로직(806)은, 컴퓨팅 디바이스(102) 상에 저장되어 있는 비민감 데이터를 유저가 볼 수 있고 액세스할 수 있지만, 컴퓨팅 디바이스(102) 상에 저장되어 있는 민감 데이터를 유저가 볼 수 없게 및/또는 액세스할 수 없게 되는 동작의 모드를 활성화한다. 이것은, 데이터 보호 시행기(112)로 하여금 컴퓨팅 디바이스(102) 상에 저장되어 있는 민감 데이터에 할당되는 다양한 데이터 보호 응답을 구현하게 하는 신호(812)를 데이터 보호 시행기(112)로 전송하는 것을 수반할 수도 있다. 앞서 언급된 바와 같이, 이러한 데이터 보호 응답은, 민감 데이터의 항목을 하드 삭제하는 것, 민감 데이터의 항목을 소프트 삭제하는 것, 민감 데이터의 항목에 대한 파일 시스템 요청이 무시되게 하는 것, 민감 데이터의 항목이 열리거나 닫힐 수 없게 하는 것, 또는 민감 데이터의 항목이 디스플레이되는 윈도우를 숨기는 것을 포함할 수도 있지만 그러나 이들로 제한되지는 않는다.

[0098] 데이터 보호 시행기(112)는, 데이터(124)와 관련되는 보안 속성(122)의 데이터 보호 응답을 시행할 수도 있다. 도 8에서 도시되는 바와 같이, 데이터 보호 시행기(112)는 데이터(124)와 관련되는 보안 속성(122)으로부터 데이터 보호 응답(814)을 수신한다. 데이터 보호 응답(814)은, 데이터(124)에 대해 데이터 보호가 시행되어야 한다는 것을 모드 선택 로직(806)으로부터 수신되는 신호(812)가 나타내는 경우, 데이터 보호 시행기(112)에 의해 수행될 하나 이상의 데이터 보호 응답을 나타낸다.

[0099] 이제, 데이터 보호에 대한 앞선 접근 방식이 도 9의 플로우차트(900)를 참조로 설명될 것이다. 특히, 도 9는, 예시적인 실시형태에 따른, 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스에 근접하여 위치하지 않는다는 결정에 기초하여 데이터에 대한 데이터 보호 응답을 시행하기 위한 프로세스의 플로우차트(900)를 묘사한다.

[0100] 도 9를 참조하면, 플로우차트(900)의 방법은 단계 902로 시작한다. 단계 902에서, 컴퓨팅 디바이스에 연결되는 또는 컴퓨팅 디바이스와 통합되는 하나 이상의 이미지 캡쳐 디바이스로부터 이미지 데이터가 수신된다. 예를 들면, 전술한 바와 같이, 유저 인식 로직(804)은, 컴퓨팅 디바이스(102)에 연결되는 또는 컴퓨팅 디바이스(102)와 통합되는 이미지 캡쳐 디바이스(들)(802)로부터 이미지 데이터(816)를 수신할 수도 있다.

[0101] 단계 904에서, 이미지 데이터는, 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스에 근접하여 위치하는지의 여부를 결정하도록 분석된다. 예를 들면, 전술한 바와 같이, 유저 인식 로직(804)은, 컴퓨팅 디바이스(102)의 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스(102)에 근접하여 위치하는지를 결정하기 위해 이미지 데이터(816)를 분석할 수도 있다. 유저 인식 로직(804)은, 컴퓨팅 디바이스(102)의 소유자 또는 권한 소지 유저의 얼굴을 식별하거나 인식하기 위해 이미지 데이터(816)를 분석하는 것에 의해, 컴퓨팅 디바이스(102)의 소유자 또는 권한 소지 유저의 몸을 식별하거나 인식하기 위해 이미지 데이터(816)를 분석하는 것에 의해, 및/또는 컴퓨팅 디바이스(102)에 근접하여 위치한 컴퓨팅 디바이스(102)의 소유자 또는 권한 소지 유저를 식별하거나 인식하기 위한 임의의 다른 적절한 이미지 분석 기술을 사용하는 것에 의해, 이 단계를 수행할 수도 있다. 유저 인식 로직(804)은 또한, 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스(102)의 소정의 유저가 지정한 또는 시스템이 지정한 거리 내에 있는지를 결정하기 위해 이미지 데이터(816)를 분석하는 것에 의해, 이 단계를 수행할 수도 있다.

[0102] 단계 906에서, 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스에 근접하여 위치한다는 결정에 응답하여, 열린 동작 모드가 활성화된다. 예를 들면, 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스에 근접하여 위치한다는 것을 결정하는 것에 응답하여, 모드 선택 로직(806)은 열린 동작 모드가 활성화되게 할 수도 있다. 열린 동작 모드는, 컴퓨팅 디바이스(102) 상에 저장되어 있는 모든 민감 데이터 및 비민감 데이터를 유저가 볼 수 있고 액세

스할 수 있는 모드(즉, 데이터 보호 응답이 데이터 보호 시행기(112)에 의해 시행되지 않은 모드)를 포함할 수도 있다. 이 단계가 열린 동작 모드의 "활성화"를 참조하지만, 이 단계는 또한, 임계 값이 초과되지 않는 한 열린 동작 모드에서의 계속된 동작을 망라한다.

[0103] 단계 908에서, 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스에 근접하여 위치하지 않는다는 결정에 응답하여, 데이터 보호 동작 모드가 활성화된다. 예를 들면, 소유자 또는 권한 소지 유저가 컴퓨팅 디바이스(102)에 근접하여 위치하지 않는다는 결정에 응답하여, 모드 선택 로직(806)은, 데이터 보호 시행기(112)로 하여금 컴퓨팅 디바이스(102)를 데이터 보호 모드로 진입시키게 하는 신호(812)를 데이터 보호 시행기(112)로 전송할 수도 있다. 앞서 설명된 바와 같이, 데이터 보호 모드 동안, 데이터 보호 시행기(112)는, 이러한 민감 데이터를 유저가 볼 수 없게 및/또는 액세스할 수 없게 만들기 위해, 컴퓨팅 디바이스(102) 상에 저장되어 있는 민감 데이터에 할당되는 다양한 데이터 보호 응답을 구현할 수도 있다. 앞서 언급된 바와 같이, 이러한 데이터 보호 응답은, 민감 데이터의 항목을 하드 삭제하는 것, 민감 데이터의 항목을 소프트 삭제하는 것, 민감 데이터의 항목에 대한 파일 시스템 요청이 무시되게 하는 것, 민감 데이터의 항목이 열리거나 닫힐 수 없게 하는 것, 또는 민감 데이터의 항목이 디스플레이되는 윈도우를 숨기는 것을 포함할 수도 있지만 그러나 이들로 제한되지는 않는다.

[0104] 상기에서 논의된 바와 같이, 데이터 보호 동작 모드 동안, 데이터 보호 시행기(112)는 민감 데이터의 선택된 항목(예를 들면, 선택된 파일 및/또는 폴더)이 소프트 삭제되게 할 수도 있다. 이러한 소프트 삭제는, 예를 들면, 민감 데이터의 항목에 대한 링크 또는 파일 포인터의 보안 백업 카피를 (예를 들면, 링크 또는 파일 포인터의 암호화된 카피를 컴퓨팅 디바이스(102) 상에 또는 원격 디바이스 상에 저장하는 것에 의해) 생성하는 것 및 그 다음 링크 또는 파일 포인터에 컴퓨팅 디바이스(102)의 파일 시스템 및/또는 오퍼레이팅 시스템이 액세스할 수 없도록, 이러한 링크 또는 파일 포인터를 삭제하는 것을 포함할 수도 있다. 이러한 실시형태에 따르면, 소프트 삭제된 데이터는, 삭제된 링크 또는 파일 포인터를 보안 백업 카피로부터 컴퓨팅 디바이스(102)로 복원하는 것에 의해 복구될 수도 있다. 하나의 실시형태에서, 도 9의 단계 908의 수행의 결과로서 소프트 삭제되는 민감 데이터는, 나중에, 소프트 삭제된 데이터가 복구되어야 한다는 것을 나타내는 컴퓨팅 디바이스(102)에 대해 소정의 액션을 유저가 후속하여 수행할 때, 복구될 수도 있다.

[0105] V. 소정의 유저 제스처의 검출된 존재 또는 부재에 기초한 예시적인 상황적 트리거

[0106] 상황적 트리거 모니터(110)는, 데이터가 인가되지 않은 액세스에 노출되거나 또는 인가되지 않은 액세스로 위협받는 것을 나타내는 트리거를 모니터링하기 위해 다양한 방식으로 구성될 수도 있다. 예를 들면, 도 10은, 소정의 유저 제스처의 검출된 존재 또는 부재를 상황적 트리거로서 사용하도록 구성되는 데이터 보호 시스템(1000)의 일부의 블록도이다. 도 10에서 도시되는 바와 같이, 데이터 보호 시스템(1000)은 상황적 트리거 모니터(110) 및 데이터 보호 시행기(112)를 포함한다. 또한, 상황적 트리거 모니터(110)는 제스처 인식 로직(1004) 및 모드 선택 로직(1006)을 포함한다. 한 실시형태에서, 상황적 트리거 모니터(110)는 플로우차트(500)(도 5)의 단계 502를 수행할 수도 있고, 데이터 보호 시행기(112)는 플로우차트(500)의 단계 504를 수행할 수도 있다. 데이터 보호 시스템(1000)은 도 1에서 도시되는 데이터 보호 시스템(136)의 대응하는 부분의 예이며, 예시의 용이성을 위해, 시스템(1000)의 모든 특징이 도 10에서 도시되는 것은 아니다. 데이터 보호 시스템(1000)은 컴퓨팅 디바이스(102)에 포함될 수도 있다. 데이터 보호 시스템(1000)은 다음과 같이 설명된다.

[0107] 도 10의 실시형태에서, 상황적 트리거 모니터(110)는, 소정의 유저 제스처가 인식되었다는 또는 인식되지 않았다는 결정을, 데이터 보호를 위한 상황적 트리거로서 사용하도록 구성된다. 도 10에서 도시되는 실시형태에 따르면, 하나 이상의 이미지 캡처 디바이스(1002)가 컴퓨팅 디바이스(102)와 통합되거나 또는 적절한 유선 및/또는 무선 연결을 통해 컴퓨팅 디바이스(102)에 연결될 수도 있다. 이미지 캡처 디바이스(들)(1002)는 컴퓨팅 디바이스(102) 주위의 하나 이상의 구역의 이미지를 캡처하도록 동작한다. 이미지 캡처 디바이스(들)(1002)는, 예를 들면, 하나 이상의 광 감지 카메라를 포함할 수도 있다. 그러나, 이 예는 제한하는 것으로 의도되지 않으며, 이미지 캡처 디바이스(들)(1002)는, 거리 센서, 단층 촬영 디바이스, 레이더 디바이스, 초음파 카메라, 또는 등등을 포함하지만 이들로 제한되지는 않는, 2D 이미지, 3D 이미지, 또는 이미지 시퀀스를 캡처하는데 적합한 다른 타입의 디바이스를 포함할 수도 있다.

[0108] 이미지 캡처 디바이스(들)(1002)는, 이미지 데이터(1016)의 형태로 표현되는 하나 이상의 이미지를 캡처하도록 동작한다. 이러한 이미지 데이터는 제스처 인식 로직(1004)으로 전달된다. 제스처 인식 로직(1004)은, 특정한 유저 제스처가 인식되었는지 또는 인식되지 않았는지를 결정하기 위해 이미지 데이터(1016)를 분석한다. 예를 들면, 제스처 인식 로직(1004)은, 특정한 유저 얼굴 제스처, 손 제스처, 팔 제스처, 몸 제스처, 다리 제스처, 및/또는 발 제스처가 인식되었는지 또는 인식되지 않았는지의 여부를 결정하기 위해, 이미지 데이터(1016)를 분

석할 수도 있다. 소정의 실시형태에서, 특정한 유저 제스쳐는 고정된다(즉, 유저가 구성할 수 없는 유저 제스쳐). 대안적인 실시형태에서, 유저 제스쳐는 유저가 선택가능한 또는 유저가 정의할 수 있는 값이다. 또한 이러한 실시형태에 따르면, 컴퓨팅 디바이스(102) 또는 서버(104)는, 유저가 특정한 유저 제스쳐를 선택할 수 있게 하는 유저 인터페이스를 제공하도록 구성되는 유저 인터페이스 모듈(예를 들면, 컴퓨팅 디바이스(102)의 유저 인터페이스 모듈(108) 또는 서버(104)의 유저 인터페이스 모듈(128))을 포함할 수도 있다.

[0109] 특정한 제스쳐가 인식되었는지 또는 인식되지 않았는지의 여부를 제스쳐 인식 로직(1004)이 결정한 이후, 제스쳐 인식 로직(1004)은 이러한 정보를 출력(1008)으로서 모드 선택 로직(1006)으로 전달한다. 이 정보에 기초하여, 모드 선택 로직(1006)은 컴퓨팅 디바이스(102)의 복수의 동작 모드 중 하나를 선택적으로 활성화한다.

[0110] 예를 들면, 하나의 실시형태에서, 모드 선택 로직(1006)은 다음과 같이 동작한다. 특정한 유저 제스쳐가 인식되었다는 것을 출력(1008)이 나타내면, 모드 선택 로직(1006)은, 컴퓨팅 디바이스(102) 상에 저장되어 있는 민감 데이터 및 비민감 데이터를 유저가 보는 것과 액세스하는 것 둘 다가 가능한 동작의 모드를 활성화한다. 이것은 본질적으로, 데이터 보호 시행기(112)에 의해 어떠한 데이터 보호 조치도 시행되지 않는 일반적인 또는 "열린" 동작 모드를 포함한다.

[0111] 여전히 또한 이 실시형태에 따르면, 특정한 유저 제스쳐가 인식되지 않았다는 것을 출력(1008)이 나타내면, 모드 선택 로직(1006)은, 컴퓨팅 디바이스(102) 상에 저장되어 있는 비민감 데이터를 유저가 볼 수 있고 액세스할 수 있지만, 컴퓨팅 디바이스(102) 상에 저장되어 있는 민감 데이터를 유저가 볼 수 없게 및/또는 액세스할 수 없게 되는 동작의 모드를 활성화한다. 이것은, 데이터 보호 시행기(112)로 하여금 컴퓨팅 디바이스(102) 상에 저장되어 있는 민감 데이터에 할당되는 다양한 데이터 보호 응답을 구현하게 하는 신호(1012)를 데이터 보호 시행기(112)로 전송하는 것을 수반할 수도 있다. 앞서 언급된 바와 같이, 이러한 데이터 보호 응답은, 민감 데이터의 항목을 하드 삭제하는 것, 민감 데이터의 항목을 소프트 삭제하는 것, 민감 데이터의 항목에 대한 파일 시스템 요청이 무시되게 하는 것, 민감 데이터의 항목이 열리거나 닫힐 수 없게 하는 것, 또는 민감 데이터의 항목이 디스플레이되는 윈도우를 숨기는 것을 포함할 수도 있지만 그러나 이들로 제한되지는 않는다.

[0112] 대안적인 실시형태에서, 모드 선택 로직(1006)은 다음과 같이 동작한다. 특정한 유저 제스쳐가 인식되지 않았다는 것을 출력(1008)이 나타내면, 모드 선택 로직(1006)은, 컴퓨팅 디바이스(102) 상에 저장되어 있는 민감 데이터 및 비민감 데이터를 유저가 보는 것과 액세스하는 것 둘 다가 가능한 동작의 모드를 활성화한다. 이것은 본질적으로, 데이터 보호 시행기(112)에 의해 어떠한 데이터 보호 조치도 시행되지 않는 일반적인 또는 "열린" 동작 모드를 포함한다.

[0113] 여전히 또한 이 실시형태에 따르면, 특정한 유저 제스쳐가 인식되었다는 것을 출력(1008)이 나타내면, 모드 선택 로직(1006)은, 컴퓨팅 디바이스(102) 상에 저장되어 있는 비민감 데이터를 유저가 볼 수 있고 액세스할 수 있지만, 컴퓨팅 디바이스(102) 상에 저장되어 있는 민감 데이터를 유저가 볼 수 없게 및/또는 액세스할 수 없게 되는 동작의 모드를 활성화한다. 이것은, 데이터 보호 시행기(112)로 하여금 컴퓨팅 디바이스(102) 상에 저장되어 있는 민감 데이터에 할당되는 다양한 데이터 보호 응답을 구현하게 하는 신호(1012)를 데이터 보호 시행기(112)로 전송하는 것을 수반할 수도 있다. 앞서 언급된 바와 같이, 이러한 데이터 보호 응답은, 민감 데이터의 항목을 하드 삭제하는 것, 민감 데이터의 항목을 소프트 삭제하는 것, 민감 데이터의 항목에 대한 파일 시스템 요청이 무시되게 하는 것, 민감 데이터의 항목이 열리거나 닫힐 수 없게 하는 것, 또는 민감 데이터의 항목이 디스플레이되는 윈도우를 숨기는 것을 포함할 수도 있지만 그러나 이들로 제한되지는 않는다.

[0114] 이제, 데이터 보호에 대한 앞선 접근 방식이 도 11의 플로우차트(1100)를 참조로 설명될 것이다. 특히, 도 11은, 예시적인 실시형태에 따른, 유저 제스쳐가 인식되었다는 또는 인식되지 않았다는 결정에 기초하여, 데이터에 대한 데이터 보호 응답을 시행하기 위한 프로세스의 플로우차트(1100)를 묘사한다.

[0115] 도 11을 참조하면, 플로우차트(1100)의 방법은 단계 1102로 시작한다. 단계 1102에서, 컴퓨팅 디바이스에 연결되는 또는 컴퓨팅 디바이스와 통합되는 하나 이상의 이미지 캡쳐 디바이스로부터 이미지 데이터가 수신된다. 예를 들면, 전술한 바와 같이, 제스쳐 인식 로직(1004)은, 컴퓨팅 디바이스(102)에 연결되는 또는 컴퓨팅 디바이스(102)와 통합되는 이미지 캡쳐 디바이스(들)(1102)로부터 이미지 데이터(1016)를 수신할 수도 있다.

[0116] 단계 1104에서, 이미지 데이터는, 특정한 유저 제스쳐가 인식되었는지 또는 인식되지 않았는지를 결정하도록 분석된다. 예를 들면, 전술한 바와 같이, 유저 인식 로직(1004)은, 특정한 유저 제스쳐가 인식되었는지 또는 인식되지 않았는지를 결정하기 위해 이미지 데이터(1016)를 분석할 수도 있다. 제스쳐 인식 로직(1004)은, 특정한 유저 얼굴 제스쳐, 손 제스쳐, 팔 제스쳐, 몸 제스쳐, 다리 제스쳐, 및/또는 발 제스쳐가 인식되었는지 또는 인

식되지 않았는지의 여부를 결정하기 위해, 이미지 데이터(1016)를 분석할 수도 있다.

[0117] 단계 1106에서, 단계 1104 동안 이루어진 결정에 기초하여, 열린 동작 모드 및 데이터 보호 동작 모드 중 하나가 선택적으로 활성화된다. 예를 들면, 단계 1104 동안 이루어진 결정에 기초하여, 모드 선택 로직(1006)은, 선택적으로, 열린 동작 모드가 활성화되게 할 수도 있거나 또는 데이터 보호 모드가 활성화되게 할 수도 있다. 열린 동작 모드는, 컴퓨팅 디바이스(102) 상에 저장되어 있는 모든 민감 데이터 및 비민감 데이터를 유저가 볼 수 있고 액세스할 수 있는 모드(즉, 데이터 보호 응답이 데이터 보호 시행기(112)에 의해 시행되지 않은 모드)를 포함할 수도 있다. 이 단계가 열린 동작 모드의 "활성화"를 참조하지만, 이 단계는 또한, 임계 값이 초과되지 않는 한 열린 동작 모드에서의 계속된 동작을 망라한다. 데이터 보호 동작 모드는, 데이터 보호 시행기(112)가 이러한 민감 데이터를 유저가 볼 수 없게 및/또는 유저가 액세스할 없게 만들기 위해 컴퓨팅 디바이스(102) 상에 저장되어 있는 민감 데이터에 할당되는 다양한 데이터 보호 응답을 구현하는 모드를 포함할 수도 있다. 앞서 언급된 바와 같이, 이러한 데이터 보호 응답은, 민감 데이터의 항목을 하드 삭제하는 것, 민감 데이터의 항목을 소프트 삭제하는 것, 민감 데이터의 항목에 대한 파일 시스템 요청이 무시되게 하는 것, 민감 데이터의 항목이 열리거나 닫힐 수 없게 하는 것, 또는 민감 데이터의 항목이 디스플레이되는 윈도우를 숨기는 것을 포함할 수도 있지만 그러나 이들로 제한되지는 않는다.

[0118] 상기에서 논의된 바와 같이, 데이터 보호 동작 모드 동안, 데이터 보호 시행기(112)는 민감 데이터의 선택된 항목(예를 들면, 선택된 파일 및/또는 폴더)이 소프트 삭제되게 할 수도 있다. 이러한 소프트 삭제는, 예를 들면, 민감 데이터의 항목에 대한 링크 또는 파일 포인터의 보안 백업 카피를 (예를 들면, 링크 또는 파일 포인터의 암호화된 카피를 컴퓨팅 디바이스(102) 상에 또는 원격 디바이스 상에 저장하는 것에 의해) 생성하는 것 및 그 다음 링크 또는 파일 포인터에 컴퓨팅 디바이스(102)의 파일 시스템 및/또는 오퍼레이팅 시스템이 액세스할 수 없도록, 이러한 링크 또는 파일 포인터를 삭제하는 것을 포함할 수도 있다. 이러한 실시형태에 따르면, 소프트 삭제된 데이터는, 삭제된 링크 또는 파일 포인터를 보안 백업 카피로부터 컴퓨팅 디바이스(102)로 복원하는 것에 의해 복구될 수도 있다. 하나의 실시형태에서, 도 11의 단계 1106의 수행의 결과로서 소프트 삭제되는 민감 데이터는, 나중에, 소프트 삭제된 데이터가 복구되어야 한다는 것을 나타내는 컴퓨팅 디바이스(102)에 대해 소정의 액션을 유저가 후속하여 수행할 때, 복구될 수도 있다.

[0119] VI. 예시적인 모바일 및 고정식 디바이스(stationary device) 실시형태

[0120] 도 12는, 도 1을 참조로 전술한 바와 같은 컴퓨팅 디바이스(102)를 구현하기 위해 사용될 수도 있는 예시적인 모바일 디바이스(1202)의 블록도이다. 도 12에서 도시되는 바와 같이, 모바일 디바이스(1202)는 다양한 옵션적인 하드웨어 및 소프트웨어 컴포넌트를 포함한다. 모바일 디바이스(1202)의 임의의 컴포넌트는 임의의 다른 컴포넌트와 통신할 수 있지만, 예시의 용이성을 위해, 모든 연결이 도시되지는 않는다. 모바일 디바이스(1202)는 다양한 컴퓨팅 디바이스(예를 들면, 셀폰, 스마트폰, 핸드헬드 컴퓨터, 개인 휴대 정보 단말(PDA) 등등) 중 임의의 것일 수도 있고, 셀룰러 또는 위성 네트워크와 같은 하나 이상의 이동 통신 네트워크(1204)와의, 또는 근거리 또는 광역 네트워크와의 무선의 양방향 통신을 허용할 수도 있다.

[0121] 예시된 모바일 디바이스(1202)는, 신호 코딩, 데이터 프로세싱, 입출력 프로세싱, 전력 제어, 및/또는 다른 기능과 같은 작업을 수행하기 위한 프로세서 회로(1210)(예를 들면, 신호 프로세서, 마이크로프로세서, ASIC, 또는 다른 제어 및 프로세싱 로직 회로부)를 포함할 수 있다. 오퍼레이팅 시스템(1212)은 모바일 디바이스(1202)의 컴포넌트의 할당과 사용량 및 하나 이상의 애플리케이션 프로그램(1214)("애플리케이션" 또는 "앱"으로 또한 칭해짐)에 대한 지원을 제어할 수 있다. 애플리케이션 프로그램(1214)은 공통 모바일 컴퓨팅 애플리케이션(예를 들면, 이메일, 캘린더, 연락처, 웹 브라우저, 메시징 애플리케이션) 및 임의의 다른 컴퓨팅 애플리케이션(예를 들면, 워드 프로세싱, 매핑, 미디어 플레이어 애플리케이션)을 포함할 수도 있다. 하나의 실시형태에서, 오퍼레이팅 시스템(1212) 또는 애플리케이션 프로그램(1214)은 도 1을 참조로 전술한 바와 같은 데이터 보호 관리 시스템(136), 도 6을 참조로 전술한 바와 같은 데이터 보호 관리 시스템(600), 도 8을 참조로 전술한 바와 같은 데이터 보호 관리 시스템(800), 또는 도 10을 참조로 전술한 바와 같은 데이터 보호 관리 시스템(1000) 중 하나를 포함한다.

[0122] 예시된 모바일 디바이스(1202)는 메모리(1220)를 포함할 수 있다. 메모리(1220)는 비분리식 메모리(non-removable memory; 1222) 및/또는 분리식 메모리(removable memory; 1224)를 포함할 수 있다. 비분리식 메모리(1222)는 RAM, ROM, 플래시 메모리, 하드 디스크, 또는 기타 잘 알려진 메모리 디바이스 또는 기술을 포함할 수 있다. 분리식 메모리(1224)는, 플래시 메모리 또는 GSM 통신 시스템에서 기타 잘 알려져 있는 가입자 식별 모듈(Subscriber Identity Module; SIM) 카드, 또는 "스마트 카드"와 같은 기타 잘 알려진 메모리 디바이스 또는

기술을 포함할 수 있다. 메모리(1220)는 오퍼레이팅 시스템(1212) 및 애플리케이션(1214)을 실행하기 위한 데이터 및/또는 코드를 저장하기 위해 사용될 수 있다. 예시적인 데이터는, 웹페이지, 텍스트, 이미지, 사운드 파일, 비디오 데이터, 또는 하나 이상의 유선 또는 무선 네트워크를 통해 하나 이상의 네트워크 서버 또는 다른 디바이스로 전송될 및/또는 하나 이상의 네트워크 서버 또는 다른 디바이스로부터 수신될 다른 데이터를 포함할 수 있다. 메모리(1220)는 가입자 식별자, 예컨대, 인터내셔널 모바일 가입자 아이덴티티(International Mobile Subscriber Identity; IMSI), 및 기기 식별자, 예컨대 인터내셔널 모바일 기기 식별자(International Mobile Equipment Identifier; IMEI)를 저장하기 위해 사용될 수 있다. 이러한 식별자는 유저 및 기기를 식별하기 위해 네트워크로 송신될 수 있다. 한 실시형태에서, 메모리(1220)는 스토리지(114)를 포함한다.

[0123] 모바일 디바이스(1202)는, 터치 스크린(1232), 마이크(1234), 카메라(1236), 물리적 키보드(1238) 및/또는 트랙볼(1240)과 같은 하나 이상의 입력 디바이스(1230) 및 스피커(1252) 및 디스플레이(1254)와 같은 하나 이상의 출력 디바이스(1250)를 지원할 수 있다. 터치 스크린, 예컨대 터치 스크린(1232)은 입력을 상이한 방식으로 검출할 수 있다. 예를 들면, 용량성 터치 스크린은, 오브젝트(예를 들면, 손가락 끝)가 표면에 걸쳐 흐르는 전류를 왜곡시키거나 방해할 때 터치 입력을 검출한다. 다른 예로서, 터치스크린은, 광학 센서로부터의 빔이 방해될 때 터치 입력을 검출하는 광학 센서를 사용할 수 있다. 스크린의 표면과의 물리적 접촉은, 몇몇 터치 스크린에 의해 검출될 입력에 대해 불필요하다.

[0124] 다른 가능한 출력 디바이스(도시되지 않음)는 압전 또는 다른 햅틱 출력 디바이스를 포함할 수 있다. 몇몇 디바이스는 복수의 입력/출력 기능을 서빙할 수 있다. 예를 들면, 터치 스크린(1232) 및 디스플레이(1254)는 단일의 입력/출력 디바이스에서 결합될 수 있다. 입력 디바이스(1230)는 내츄럴 유저 인터페이스(Natural User Interface; NUI)를 포함할 수 있다.

[0125] 무선 모뎀(들)(1260)은, 기술분야에서 널리 이해되고 있는 바와 같이, 안테나(들)(도시되지 않음)에 커플링될 수 있고 프로세서(1210)와 외부 디바이스 사이의 양방향 통신을 지원할 수 있다. 모뎀(1260)은 일반적으로 나타내어진 것이며 모바일 통신 네트워크(1204)와 통신하기 위한 셀룰러 모뎀(1266) 및/또는 다른 무선 기반 모뎀(예를 들면, 블루투스(1264) 또는 와이파이(1262))을 포함할 수 있다. 무선 모뎀(들)(1260) 중 적어도 하나는, 단일의 셀룰러 네트워크 내에서의, 셀룰러 네트워크 사이에서의, 또는 모바일 디바이스와 공중 교환 전화망(public switched telephone network; PSTN) 사이에서의 데이터 및 음성 통신을 위해, 하나 이상의 셀룰러 네트워크, 예컨대, GSM 네트워크와의 통신을 위해 구성될 수도 있다.

[0126] 모바일 디바이스(1202)는 적어도 하나의 입출력 포트(1280), 전원(1282), 위성 내비게이션 시스템 수신기(1284), 예컨대 GPS(Global Positioning System) 수신기, 가속도계(1286)(뿐만 아니라, 콤파스 및 자이로스코프를 포함하지만 이들로 제한되지는 않는 다른 센서), 및/또는 USB 포트, IEEE 1394(파이어와이어) 포트, 및/또는 RS-232 포트일 수 있는 물리적 커넥터(1290)를 더 포함할 수도 있다. 모바일 디바이스(1202)의 예시된 컴포넌트는, 기술 분야의 숙련된 자에 의해 인식되는 바와 같이, 임의의 컴포넌트가 제거될 수 있고 다른 컴포넌트가 추가될 수 있기 때문에, 필수적이거나 모두 포함되는 것은 아니다.

[0127] 한 실시형태에서, 모바일 디바이스(1202)의 소정의 컴포넌트는, 도 1을 참조로 전술한 바와 같은 데이터 보호 관리 시스템(136), 도 6을 참조로 전술한 바와 같은 데이터 보호 관리 시스템(600), 도 8을 참조로 전술한 바와 같은 데이터 보호 관리 시스템(800), 또는 도 10을 참조로 전술한 바와 같은 데이터 보호 관리 시스템(1000)에 기인하는 동작 중 임의의 것을 수행하도록 구성된다. 전술한 바와 같은 이들 컴포넌트에 기인하는 동작을 수행하기 위한 컴퓨터 프로그램 로직은 메모리(1220)에 저장될 수도 있고 프로세서 회로(1210)에 의해 실행될 수도 있다. 이러한 컴퓨터 프로그램 로직을 실행하는 것에 의해, 프로세서 회로(1210)는, 도 1을 참조로 전술한 바와 같은 데이터 보호 관리 시스템(136), 도 6을 참조로 전술한 바와 같은 데이터 보호 관리 시스템(600), 도 8을 참조로 전술한 바와 같은 데이터 보호 관리 시스템(800), 또는 도 10을 참조로 전술한 바와 같은 데이터 보호 관리 시스템(1000)의 특징 중 임의의 것을 구현하도록 야기될 수도 있다. 또한, 이러한 컴퓨터 프로그램 로직을 실행하는 것에 의해, 프로세서 회로(1210)는, 도 2 내지 도 5, 도 7, 도 9 및 도 11에서 묘사되는 플로우차트 중 임의의 것 또는 전체의 단계 중 임의의 것 또는 전체를 수행하게 될 수도 있다.

[0128] 또한, 도 13은, 본원에서 설명되는 다양한 실시형태를 구현하기 위해 사용될 수도 있는 예시적인 프로세서 기반 컴퓨터 시스템(1300)을 묘사한다. 예를 들면, 컴퓨터 시스템(1300)은 도 1을 참조로 전술한 바와 같은 엔드 유저 컴퓨팅 디바이스(102) 또는 서버(104)를 구현하기 위해 사용될 수도 있다. 컴퓨터 시스템(1300)은 또한, 도 2 내지 도 5, 도 7, 도 9 및 도 11에서 묘사되는 플로우차트 중 임의의 것 또는 전체의 단계 중 임의의 것 또는 전체를 구현하기 위해 사용될 수도 있다. 본원에서 개시되는 컴퓨터 시스템(1300)의 설명은 예시의 목적을 위해

제공되는 것이며, 제한하는 것으로 의도되지는 않는다. 실시형태는, 관련 기술분야(들)의 숙련된 자에게 알려진 바와 같이, 컴퓨터 시스템의 미래의 타입에서 구현될 수도 있다.

[0129] 도 13에서 도시되는 바와 같이, 컴퓨터 시스템(1300)은, 프로세싱 유닛(1302), 시스템 메모리(1304), 및 시스템 메모리(1304)를 포함하는 다양한 시스템 컴포넌트를 프로세싱 유닛(1302)에 커플링하는 버스(1306)를 포함한다. 프로세서 유닛(1302)은, 하나 이상의 물리적 하드웨어 전기 회로 디바이스 엘리먼트 및/또는 집적 회로 디바이스(반도체 재료 칩 또는 다이)에서, 중앙 프로세싱 유닛(central processing unit; CPU), 마이크로컨트롤러, 마이크로프로세서, 및/또는 다른 물리적 하드웨어 프로세서 회로로서 구현되는 전기 및/또는 광학 회로이다. 버스(1306)는, 메모리 버스 또는 메모리 컨트롤러, 주변장치 버스(peripheral bus), 가속 그래픽 포트, 및 다양한 버스 아키텍처 중 임의의 것을 사용하는 프로세서 또는 로컬 버스를 비롯하여, 임의의 여러 타입의 버스 구조 중 하나 이상을 나타낸다. 시스템 메모리(1304)는 리드 온리 메모리(read only memory; "ROM")(1308) 및 랜덤 액세스 메모리(random access memory; "RAM")(1310)를 포함한다. 기본 입력/출력 시스템(basic input/output system; BIOS)(1312)은 ROM(1308)에 저장된다.

[0130] 컴퓨터 시스템(1300)은 다음의 드라이브 중 하나 이상을 또한 구비하는데, 하드 디스크로부터 판독하거나 또는 하드 디스크에 기록하기 위한 하드 디스크 드라이브(1314), 분리식 자기 디스크(1318)로부터 판독하거나 또는 분리식 자기 디스크(1318)에 기록하기 위한 자기 디스크 드라이브(1316), 및 CD ROM, DVD ROM, BLU-RAY™ 디스크 또는 다른 광학 매체와 같은 분리식 광학 디스크(1322)로부터 판독하거나 또는 분리식 광학 디스크(1322)에 기록하기 위한 광학 디스크 드라이브(1320)이다. 하드 디스크 드라이브(1314), 자기 디스크 드라이브(1316), 및 광학 디스크 드라이브(1320)는, 각각, 하드 디스크 드라이브 인터페이스(1324), 자기 디스크 드라이브 인터페이스(1326), 및 광학 드라이브 인터페이스(1328)를 통해 버스(1306)에 의해 연결된다. 드라이브 및 그 관련 컴퓨터 판독가능 매체는, 컴퓨터 판독가능 명령어, 데이터 구조체, 프로그램 모듈, 및 컴퓨터에 대한 다른 데이터의 비휘발성 저장을 제공한다. 하드 디스크, 분리식 자기 디스크, 및 분리식 광학 디스크가 개시되지만, 데이터를 저장하기 위해, 다른 타입의 컴퓨터 판독가능 메모리 디바이스 및 스토리지 구조체, 예컨대 플래시 메모리 카드, 디지털 비디오 디스크, 랜덤 액세스 메모리(RAM), 리드 온리 메모리(ROM), 및 등등이 사용될 수 있다.

[0131] 하드 디스크, 자기 디스크, 광학 디스크, ROM, 또는 RAM 상에 다수의 프로그램 모듈이 저장될 수도 있다. 이들 프로그램은, 오퍼레이팅 시스템(1330), 하나 이상의 애플리케이션 프로그램(1332), 다른 프로그램 모듈(1334), 및 프로그램 데이터(1336)를 포함한다. 다양한 실시형태에 따르면, 프로그램 모듈은, 도 1을 참조로 전술한 바와 같은 데이터 보호 관리 시스템(136), 도 6을 참조로 전술한 바와 같은 데이터 보호 관리 시스템(600), 도 8을 참조로 전술한 바와 같은 데이터 보호 관리 시스템(800), 또는 도 10을 참조로 전술한 바와 같은 데이터 보호 관리 시스템(1000)의 기능 및 특징 중 임의의 것 또는 전체를 수행하기 위해, 프로세싱 유닛(1302)에 의해 실행가능한 컴퓨터 프로그램 로직을 포함할 수도 있다. 프로그램 모듈은 또한, 프로세싱 유닛(1302)에 의한 실행시, 도 2 내지 도 5, 도 7, 도 9 및 도 11의 플로우차트를 참조로 도시되거나 설명되는 단계 또는 동작 중 임의의 것을 수행하는 컴퓨터 프로그램을 포함할 수도 있다.

[0132] 유저는 키보드(1338)와 같은 입력 디바이스 및 포인팅 디바이스(1340)를 통해 커맨드 및 정보를 컴퓨터 시스템(1300)에 입력할 수도 있다. 다른 입력 디바이스(도시되지 않음)는 마이크, 조이스틱, 게임 컨트롤러, 스캐너, 또는 등등을 포함할 수도 있다. 하나의 실시형태에서, (예를 들면, 손가락 또는 스타일러스에 의한 것과 같은) 터치를 이용하여 유저가 터치 스크린 스크린 상의 하나 이상의 포인트에 유저 입력을 제공하는 것을 허용하기 위해, 터치 스크린은 디스플레이(1344)와 연계하여 제공된다. 이들 및 다른 입력 디바이스는, 종종, 버스(1306)에 커플링되는 직렬 포트 인터페이스(1342)를 통해 프로세싱 유닛(1302)에 연결되지만, 그러나 병렬 포트, 게임 포트 또는 범용 직렬 버스(USB)와 같은 다른 인터페이스에 의해 연결될 수도 있다. 이러한 인터페이스는 유선 또는 무선 인터페이스일 수도 있다.

[0133] 비디오 어댑터(1346)와 같은 인터페이스를 통해 디스플레이(1344)가 버스(1306)에 또한 연결된다. 디스플레이 스크린(1344) 외에, 컴퓨터 시스템(1300)은 스피커 및 프린터와 같은 다른 주변 출력 장치(도시되지 않음)를 포함할 수도 있다.

[0134] 컴퓨터 시스템(1300)은, 네트워크 인터페이스 또는 어댑터(1350), 모뎀(1352), 또는 네트워크를 통한 통신을 확립하기 위한 임의의 적절한 수단을 통해, 네트워크(1348)(예를 들면, 근거리 통신망 또는 광역 통신망 예컨대 인터넷)에 연결된다. 내부 또는 외부에 있을 수도 있는 모뎀(1352)은 직렬 포트 인터페이스(1342)를 통해 버스(1306)에 연결된다.

[0135] 본원에서 사용되는 바와 같이, 용어 "컴퓨터 프로그램 매체", "컴퓨터 판독가능 매체", 및 "컴퓨터 판독가능 저

장 매체"는, 일반적으로, 하드 디스크 드라이브(1314)와 관련되는 하드 디스크, 분리식 자기 디스크(1318), 분리식 광학 디스크(1322)와 같은 메모리 디바이스 또는 스토리지 구조체뿐만 아니라, 플래시 메모리 카드, 디지털 비디오 디스크, 랜덤 액세스 메모리(RAM), 리드 온리 메모리(ROM), 및 등등과 같은 다른 메모리 디바이스 또는 스토리지 구조체를 가리키기 위해 사용된다. 이러한 컴퓨터 판독가능 저장 매체는 통신 매체와는 구별되며 겹쳐지지 않는다(통신 매체를 포함하지 않는다). 통신 매체는, 통상적으로, 컴퓨터 판독가능 명령어, 데이터 구조체, 프로그램 모듈, 또는 변조된 데이터 신호, 예컨대 반송파에서의 다른 데이터를 구현할 수도 있다. 용어 "변조된 데이터 신호"는, 자신의 특성 세트 중 하나 이상이 신호에 정보를 인코딩하는 것과 같은 방식으로 설정되거나 변경된 신호를 의미한다. 비제한적인 예로서, 통신 매체는 무선 매체 예컨대 음향, RF, 적외선 및 다른 무선 매체를 포함한다. 실시형태는 또한 이러한 통신 매체를 대상으로 한다.

[0136] 상기에서 언급되는 바와 같이, 컴퓨터 프로그램 및 모듈(애플리케이션 프로그램(1332) 및 다른 프로그램 모듈(1334)을 포함함)은 하드 디스크, 자기 디스크, 광학 디스크, ROM, 또는 RAM 상에 저장될 수도 있다. 이러한 컴퓨터 프로그램은, 네트워크 인터페이스(1350), 직렬 포트 인터페이스(1342), 또는 임의의 다른 인터페이스 타입을 통해 또한 수신될 수도 있다. 이러한 컴퓨터 프로그램은, 애플리케이션에 의해 실행되거나 로딩될 때, 컴퓨터 시스템(1300)이 본원에서 논의되는 본 발명의 실시형태의 특징을 구현하는 것을 가능하게 한다. 따라서, 이러한 컴퓨터 프로그램은 컴퓨터 시스템(1300)의 컨트롤러를 나타낸다.

[0137] 실시형태는 또한, 임의의 컴퓨터 사용가능 매체 상에 저장되는 소프트웨어를 포함하는 컴퓨터 프로그램 제품을 대상으로 한다. 이러한 소프트웨어는, 하나 이상의 데이터 프로세싱 디바이스에서의 실행시, 프로세싱 디바이스(들)로 하여금 본원에서 설명되는 바와 같이 동작하게 한다. 본 발명의 실시형태는, 현재 알려져 있는 또는 미래의 임의의 컴퓨터 사용가능 또는 컴퓨터 판독가능 매체를 활용한다. 컴퓨터 판독가능 매체의 예는, RAM, 하드 드라이브, 플로피 디스크, CD ROM, DVD ROM, 집(zip) 디스크, 테이프, 자기 스토리지 디바이스, 광학 스토리지 디바이스, MEM, 나노 기술 기반의 스토리지 디바이스, 및 등등과 같은 메모리 디바이스 및 스토리지 구조체를 포함하지만, 그러나 이들로 제한되지는 않는다.

[0138] 대안적인 구현예에서, 컴퓨터 시스템(1400)은 하드웨어 로직/전기 회로부 또는 펌웨어로서 구현될 수도 있다. 다른 실시형태에 따르면, 이들 컴포넌트 중 하나 이상은 시스템 온 칩(system-on-chip; SoC)에서 구현될 수도 있다. SoC는, 프로세서(예를 들면, 마이크로컨트롤러, 마이크로프로세서, 디지털 신호 프로세서(digital signal processor; DSP), 등등), 메모리, 하나 이상의 통신 인터페이스, 및/또는 자신의 기능을 수행하기 위한 다른 회로부 및/또는 임베딩된 펌웨어 중 하나 이상을 포함하는 집적 회로 칩을 포함할 수도 있다.

[0139] VII. 예시적인 실시형태

[0140] 실시형태에 따른 시스템은, 적어도 하나의 프로세서 및 적어도 하나의 적어도 하나의 프로세서에 연결되는 하나 이상의 메모리 디바이스를 포함한다. 하나 이상의 메모리 디바이스는 적어도 하나의 프로세서에 의한 실행을 위한 소프트웨어 컴포넌트를 저장한다. 소프트웨어 컴포넌트는 다중 인물 인식 로직 및 모드 선택 로직을 포함한다. 다중 인물 인식 로직은, 컴퓨팅 디바이스에 연결되는 또는 컴퓨팅 디바이스와 통합되는 하나 이상의 이미지 캡쳐 디바이스로부터 이미지 데이터를 수신하도록 그리고 컴퓨팅 디바이스에 근접하여 위치한 사람의 수를 결정하기 위해 이미지 데이터를 분석하도록 구성된다. 모드 선택 로직은, 컴퓨팅 디바이스에 근접하여 위치한 사람의 수가 임계 값을 초과하는지를 결정하도록, 컴퓨팅 디바이스에 근접하여 위치한 사람의 수가 임계 값을 초과하지 않는다는 결정에 응답하여 컴퓨팅 디바이스의 제1 동작 모드를 활성화하도록, 그리고 컴퓨팅 디바이스에 근접하여 위치한 사람의 수가 임계 값을 초과한다는 결정에 응답하여 컴퓨팅 디바이스의 제2 동작 모드를 활성화하도록 구성된다. 컴퓨팅 디바이스의 제1 동작 모드는, 컴퓨팅 디바이스 상에 저장되어 있는 민감 데이터 및 컴퓨팅 디바이스 상에 저장되어 있는 비민감 데이터를 유저가 보는 것과 액세스하는 것 둘 다가 가능한 모드이다. 컴퓨팅 디바이스의 제2 동작 모드는, 컴퓨팅 디바이스 상에 저장되어 있는 비민감 데이터는 유저가 볼 수도 있고 액세스할 수도 있고, 컴퓨팅 디바이스 상에 저장되어 있는 민감 데이터는 유저가 볼 수 없게 되는 것 및 액세스할 수 없게 되는 것 중 하나 이상으로 되는 모드이다.

[0141] 상기 시스템의 하나의 실시형태에서, 하나 이상의 이미지 캡쳐 디바이스는 하나 이상의 카메라를 포함한다.

[0142] 상기 시스템의 다른 실시형태에서, 다중 인물 인식 로직은, 다수의 별개의 얼굴을 식별하기 위해 이미지 데이터를 분석하는 것에 의해, 컴퓨팅 디바이스에 근접하여 위치한 사람의 수를 결정하도록 구성된다.

[0143] 상기 시스템의 또 다른 실시형태에서, 다중 인물 인식 로직은, 다수의 별개의 몸을 식별하기 위해 이미지 데이터를 분석하는 것에 의해, 컴퓨팅 디바이스에 근접하여 위치한 사람의 수를 결정하도록 구성된다.

[0144] 상기 시스템의 또 다른 실시형태에서, 소프트웨어 컴포넌트는, 유저가 임계 값을 지정할 수 있게 하는 유저 인터페이스를 제공하도록 구성되는 유저 인터페이스 모듈을 더 포함한다.

[0145] 상기 시스템의 다른 실시형태에서, 다중 인물 인식 로직은, 컴퓨팅 디바이스의 일정 거리 내의 사람의 수를 결정하기 위해 이미지 데이터를 분석하는 것에 의해, 컴퓨팅 디바이스에 근접하여 위치한 사람의 수를 결정하도록 구성된다. 또한 이러한 실시형태에 따르면, 소프트웨어 컴포넌트는, 유저가 일정 거리를 지정할 수 있게 하는 유저 인터페이스를 제공하도록 구성되는 유저 인터페이스 모듈을 더 포함할 수도 있다.

[0146] 상기 시스템의 또 다른 실시형태에서, 컴퓨팅 디바이스의 제2 동작 모드는, 민감 데이터의 항목을 하드 삭제하는 것, 민감 데이터의 항목을 소프트 삭제하는 것, 민감 데이터의 항목에 대한 파일 시스템 요청이 무시되게 하는 것, 민감 데이터의 항목이 열릴 수 없게 하는 것, 및 데이터의 항목이 디스플레이되는 윈도우를 숨기는 것 중 하나 이상을 수행하는 것에 의해, 민감 데이터 중 적어도 하나의 항목을 유저가 볼 수 없게 또는 액세스할 수 없게 되는 모드이다.

[0147] 실시형태에 따른 컴퓨팅 디바이스 상에 저장되어 있는 민감 데이터를 보호하기 위한 방법으로서, (i) 컴퓨팅 디바이스에 연결되는 또는 컴퓨팅 디바이스와 통합되는 하나 이상의 이미지 캡쳐 디바이스로부터 이미지 데이터를 수신하는 것; (ii) 소유자 또는 권한 소지자(authorized person)가 컴퓨팅 디바이스에 근접하여 위치하는지를 결정하기 위해 이미지 데이터를 분석하는 단계; (iii) 소유자 또는 권한 소지자가 컴퓨팅 디바이스에 근접하여 위치한다는 결정에 응답하여, 컴퓨팅 디바이스 상에 저장되어 있는 민감 데이터 및 컴퓨팅 디바이스 상에 저장되어 있는 비민감 데이터를 유저가 보는 것과 액세스하는 것 둘 다가 가능한 컴퓨팅 디바이스의 제1 동작 모드를 활성화하는 것; 및 (iv) 소유자 또는 권한 소지자가 컴퓨팅 디바이스에 근접하여 위치하지 않는다는 결정에 응답하여, 컴퓨팅 디바이스 상에 저장되어 있는 비민감 데이터는 유저가 볼 수도 있고 액세스할 수도 있고, 컴퓨팅 디바이스 상에 저장되어 있는 민감 데이터는 유저가 볼 수 없게 되는 것 및 액세스할 수 없게 되는 것 중 하나 이상으로 되는 컴퓨팅 디바이스의 제2 동작 모드를 활성화하는 것을 포함한다.

[0148] 상기 방법의 하나의 실시형태에서, 하나 이상의 이미지 캡쳐 디바이스는 하나 이상의 카메라를 포함한다.

[0149] 상기 방법의 다른 실시형태에서, 소유자 또는 권한 소지자가 컴퓨팅 디바이스에 근접하여 위치하는지를 결정하기 위해 이미지 데이터를 분석하는 것은, 소유자 또는 권한 소지자의 얼굴을 식별하기 위해 이미지 데이터를 분석하는 것을 포함한다.

[0150] 상기 방법의 또 다른 실시형태에서, 소유자 또는 권한 소지자가 컴퓨팅 디바이스에 근접하여 위치하는지를 결정하기 위해 이미지 데이터를 분석하는 것은, 소유자 또는 권한 소지자의 몸을 식별하기 위해 이미지 데이터를 분석하는 것을 포함한다.

[0151] 상기 방법의 또 다른 실시형태에서, 소유자 또는 권한 소지자가 컴퓨팅 디바이스에 근접하여 위치하는지를 결정하기 위해 이미지 데이터를 분석하는 것은, 소유자 또는 권한 소지자가 컴퓨팅 디바이스의 일정 거리 내에 있는지를 결정하기 위해 이미지 데이터를 분석하는 것을 포함한다. 또한 이러한 실시형태에 따르면, 방법은 유저가 일정 거리를 지정할 수 있게 하는 유저 인터페이스를 제공하는 것을 더 포함할 수도 있다.

[0152] 상기 방법의 다른 실시형태에서, 컴퓨팅 디바이스의 제2 동작 모드는, 민감 데이터의 항목을 하드 삭제하는 것, 민감 데이터의 항목을 소프트 삭제하는 것, 민감 데이터의 항목에 대한 파일 시스템 요청이 무시되게 하는 것, 민감 데이터의 항목이 열릴 수 없게 하는 것, 및 데이터의 항목이 디스플레이되는 윈도우를 닫거나 또는 숨기는 것 중 하나 이상을 수행하는 것에 의해, 민감 데이터 중 적어도 하나의 항목을 유저가 볼 수 없게 또는 액세스할 수 없게 되는 모드이다.

[0153] 실시형태에 따른 컴퓨터 프로그램 제품은, 적어도 하나의 프로세서에 의한 실행시, 적어도 하나의 프로세서로 하여금 컴퓨팅 디바이스 상에 저장되어 있는 민감 데이터를 보호하기 위한 방법을 수행하게 하는 컴퓨터 프로그램 로직이 기록된 컴퓨터 판독가능 메모리를 포함한다. 방법은, 컴퓨팅 디바이스에 연결되는 또는 컴퓨팅 디바이스와 통합되는 하나 이상의 이미지 캡쳐 디바이스로부터 이미지 데이터를 수신하는 것, 특정한 유저 제스처가 인식되는지의 여부를 결정하기 위해 이미지 데이터를 분석하는 것, 및 결정에 기초하여, 컴퓨팅 디바이스 상에 저장되어 있는 민감 데이터 및 컴퓨팅 디바이스 상에 저장되어 있는 비민감 데이터를 유저가 보는 것과 액세스하는 것 둘 다가 가능한 컴퓨팅 디바이스의 제1 동작 모드 및 컴퓨팅 디바이스 상에 저장되어 있는 비민감 데이터는 유저가 볼 수도 있고 액세스할 수도 있고, 컴퓨팅 디바이스 상에 저장되어 있는 민감 데이터는 유저가 볼 수 없게 되는 것 및 액세스할 수 없게 되는 것 중 하나 이상으로 되는 컴퓨팅 디바이스의 제2 동작 모드 중 하나를 선택적으로 활성화하는 것을 포함한다.

[0154] 상기 컴퓨터 프로그램 제품의 하나의 실시형태에서, 하나 이상의 이미지 캡쳐 디바이스는 하나 이상의 카메라를 포함한다.

[0155] 상기 컴퓨터 프로그램 제품의 다른 실시형태에서, 특정한 제스쳐는, 얼굴 제스쳐, 손 제스쳐, 팔 제스쳐, 몸 제스쳐, 다리 제스쳐, 및 발 제스쳐 중 하나 이상을 포함한다.

[0156] 상기 컴퓨터 프로그램 제품의 또 다른 실시형태에서, 방법은, 유저가 특정한 제스쳐를 지정할 수 있게 하는 유저 인터페이스를 제공하는 것을 더 포함한다.

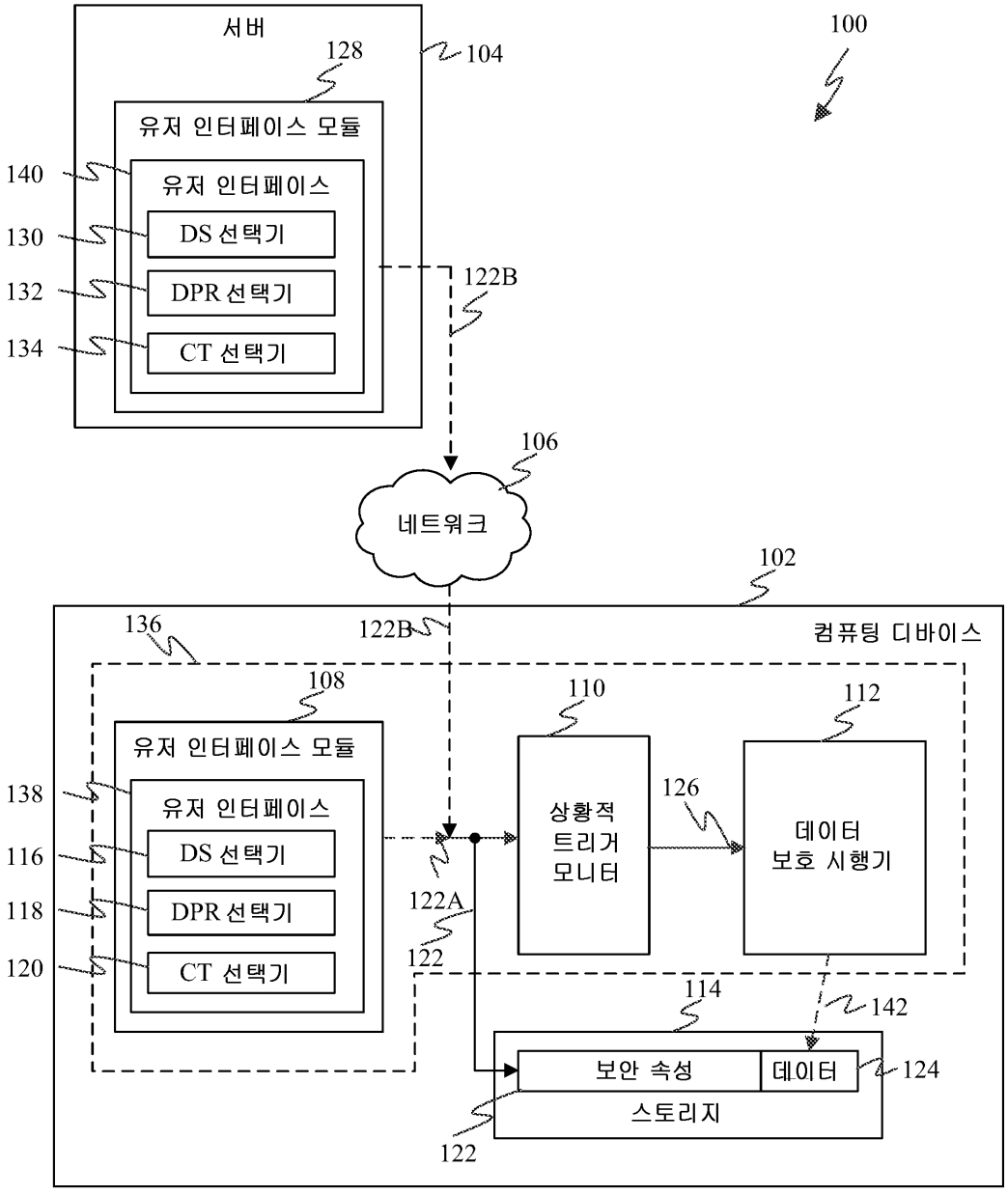
[0157] 상기 컴퓨터 프로그램 제품의 또 다른 실시형태에서, 컴퓨팅 디바이스의 제2 동작 모드는, 민감 데이터의 항목을 하드 삭제하는 것, 민감 데이터의 항목을 소프트 삭제하는 것, 민감 데이터의 항목에 대한 파일 시스템 요청이 무시되게 하는 것, 민감 데이터의 항목이 열릴 수 없게 하는 것, 및 데이터의 항목이 디스플레이되는 윈도우를 숨기는 것 중 하나 이상을 수행하는 것에 의해, 민감 데이터 중 적어도 하나의 항목을 유저가 볼 수 없게 또는 액세스할 수 없게 되는 모드이다.

[0158] VIII. 결론

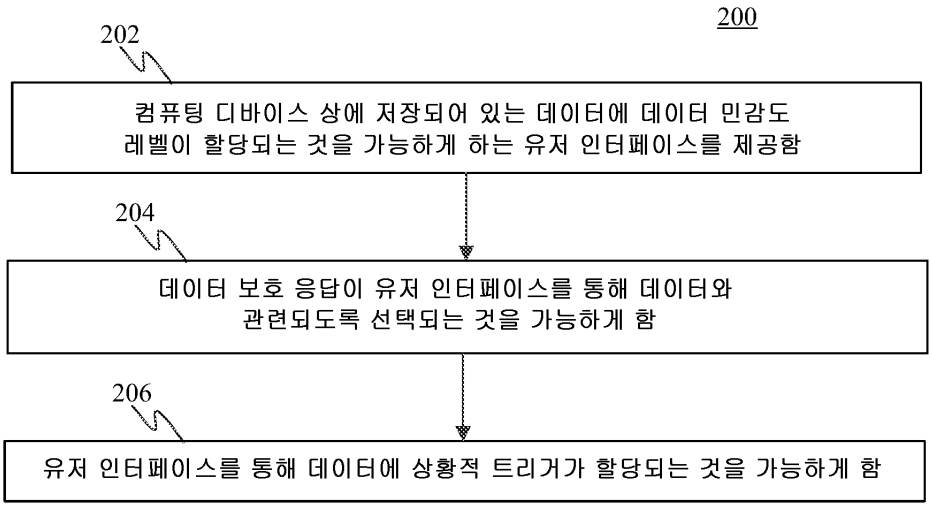
[0159] 본 발명의 다양한 실시형태가 상기에서 설명되었지만, 다양한 실시형태는 단지 예로서 제시된 것이며 제한은 아니다는 것이 이해되어야 한다. 첨부의 청구범위에서 정의되는 바와 같은 본 발명의 취지와 범위를 벗어나지 않으면서, 형태 및 상세에서의 다양한 변경이 이루어질 수도 있다는 것이 관련 기술분야(들)의 숙련된 자에 의해 이해될 것이다. 따라서, 본 발명의 폭과 범위는 상기 설명된 예시적인 실시형태 중 임의의 것에 의해 제한되어야 하는 것이 아니라, 오로지 하기의 청구범위 및 그 균등물에 따라 정의되어야 한다.

도면

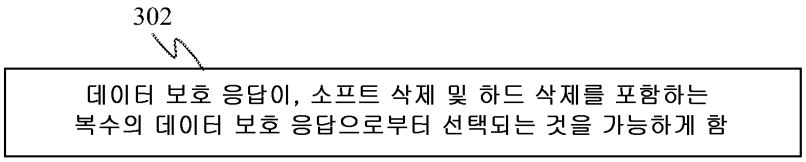
도면1


서버
128
104
100
유저 인터페이스 모듈
140
유저 인터페이스
130
DS 선택기
132
DPR 선택기
134
CT 선택기
122B
106
네트워크
102
136
122B
컴퓨팅 디바이스
108
110
112
유저 인터페이스 모듈
138
유저 인터페이스
126
상황적
트리거
모니터
데이터
보호 시행기
116
DS 선택기
118
DPR 선택기
122A
120
CT 선택기
122
114
142
보안 속성
데이터
124
스토리지
122

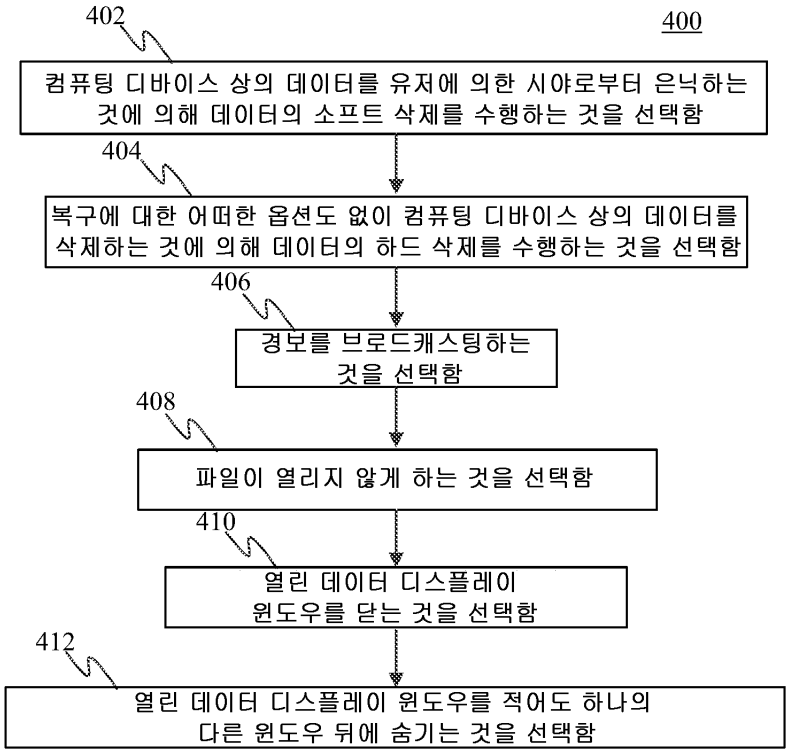
도면2


200
202
컴퓨팅 디바이스 상에 저장되어 있는 데이터에 데이터 민감도 레벨이 할당되는 것을 가능하게 하는 유저 인터페이스를 제공함
204
데이터 보호 응답이 유저 인터페이스를 통해 데이터와 관련되도록 선택되는 것을 가능하게 함
206
유저 인터페이스를 통해 데이터에 상황적 트리거가 할당되는 것을 가능하게 함

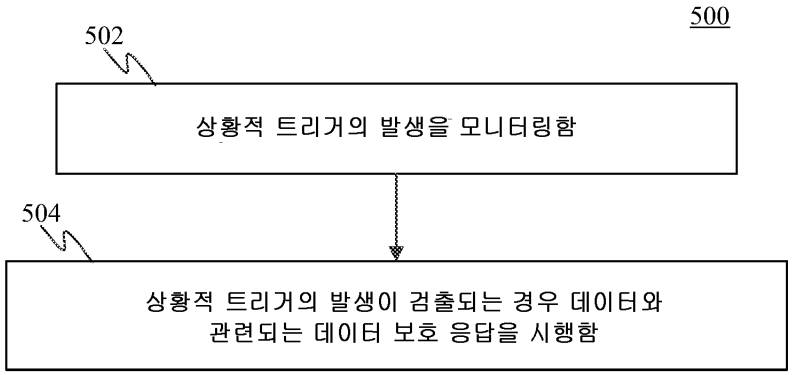
도면3


302
데이터 보호 응답이, 소프트 삭제 및 하드 삭제를 포함하는 복수의 데이터 보호 응답으로부터 선택되는 것을 가능하게 함

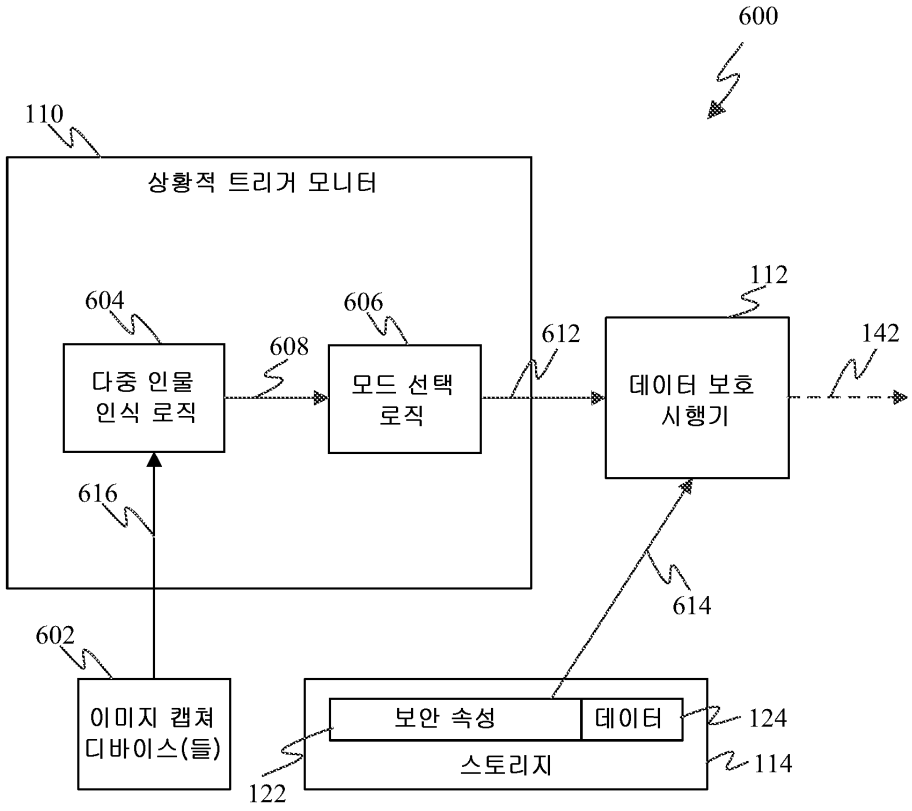
도면4


400
402
컴퓨팅 디바이스 상의 데이터를 유저에 의한 시야로부터 은닉하는 것에 의해 데이터의 소프트 삭제를 수행하는 것을 선택함
404
복구에 대한 어떠한 옵션도 없이 컴퓨팅 디바이스 상의 데이터를 삭제하는 것에 의해 데이터의 하드 삭제를 수행하는 것을 선택함
406
경보를 브로드캐스팅하는 것을 선택함
408
파일이 열리지 않게 하는 것을 선택함
410
열린 데이터 디스플레이 윈도우를 닫는 것을 선택함
412
열린 데이터 디스플레이 윈도우를 적어도 하나의 다른 윈도우 뒤에 숨기는 것을 선택함

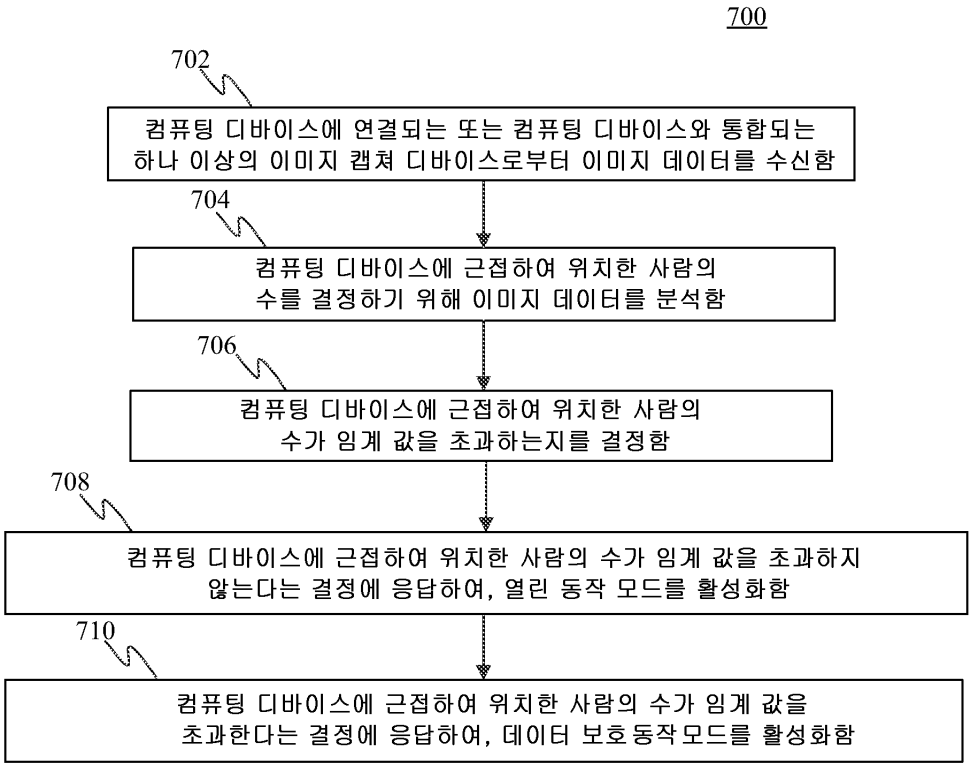
도면5


500
502
상황적 트리거의 발생을 모니터링함
504
상황적 트리거의 발생이 검출되는 경우 데이터와
관련되는 데이터 보호 응답을 시행함

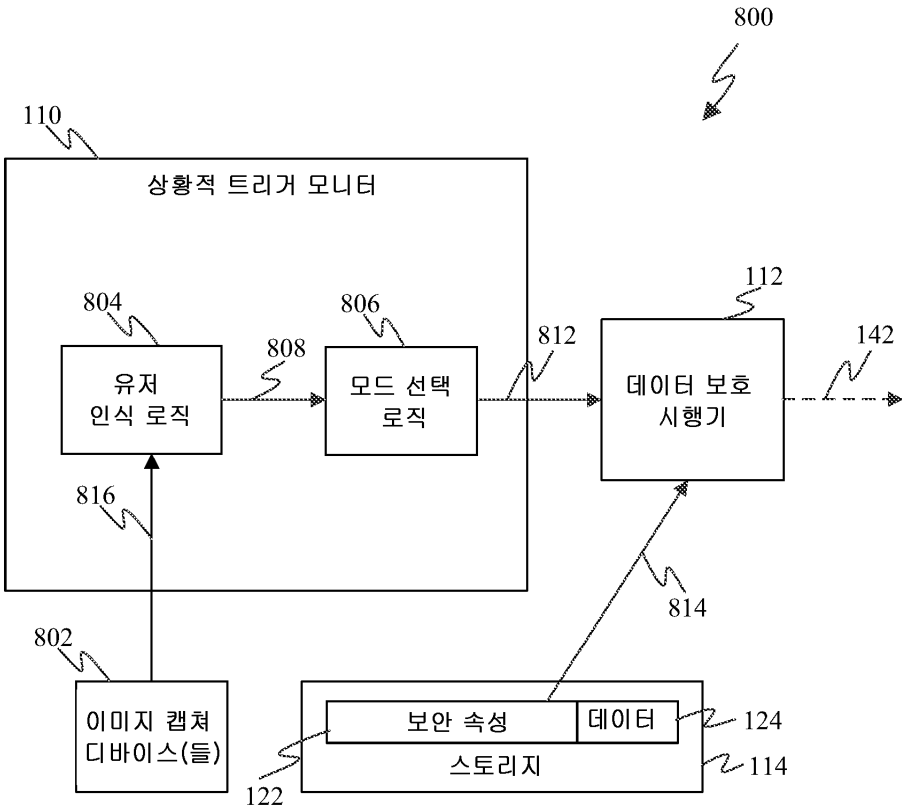
도면6


600
110
상황적 트리거 모니터
604
606
608
612
112
142
다중 인물
인식 로직
모드 선택
로직
데이터 보호
시행기
616
614
602
이미지 캡쳐
디바이스(들)
보안 속성
데이터
124
스토리지
114
122

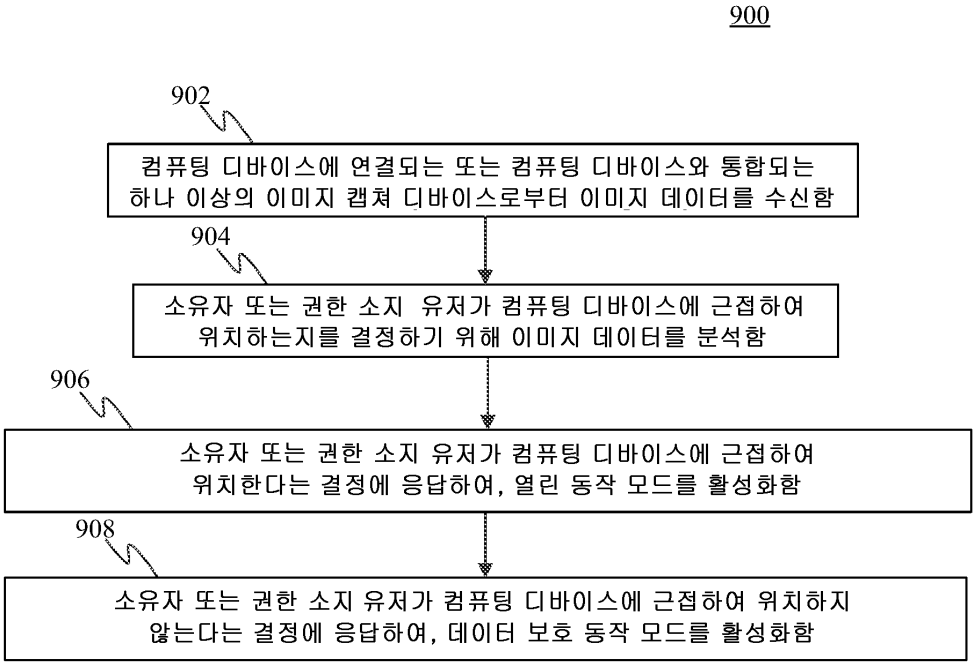
도면7


700
702
컴퓨팅 디바이스에 연결되는 또는 컴퓨팅 디바이스와 통합되는 하나 이상의 이미지 캡쳐 디바이스로부터 이미지 데이터를 수신함
704
컴퓨팅 디바이스에 근접하여 위치한 사람의 수를 결정하기 위해 이미지 데이터를 분석함
706
컴퓨팅 디바이스에 근접하여 위치한 사람의 수가 임계 값을 초과하는지를 결정함
708
컴퓨팅 디바이스에 근접하여 위치한 사람의 수가 임계 값을 초과하지 않는다는 결정에 응답하여, 열린 동작 모드를 활성화함
710
컴퓨팅 디바이스에 근접하여 위치한 사람의 수가 임계 값을 초과한다는 결정에 응답하여, 데이터 보호동작모드를 활성화함

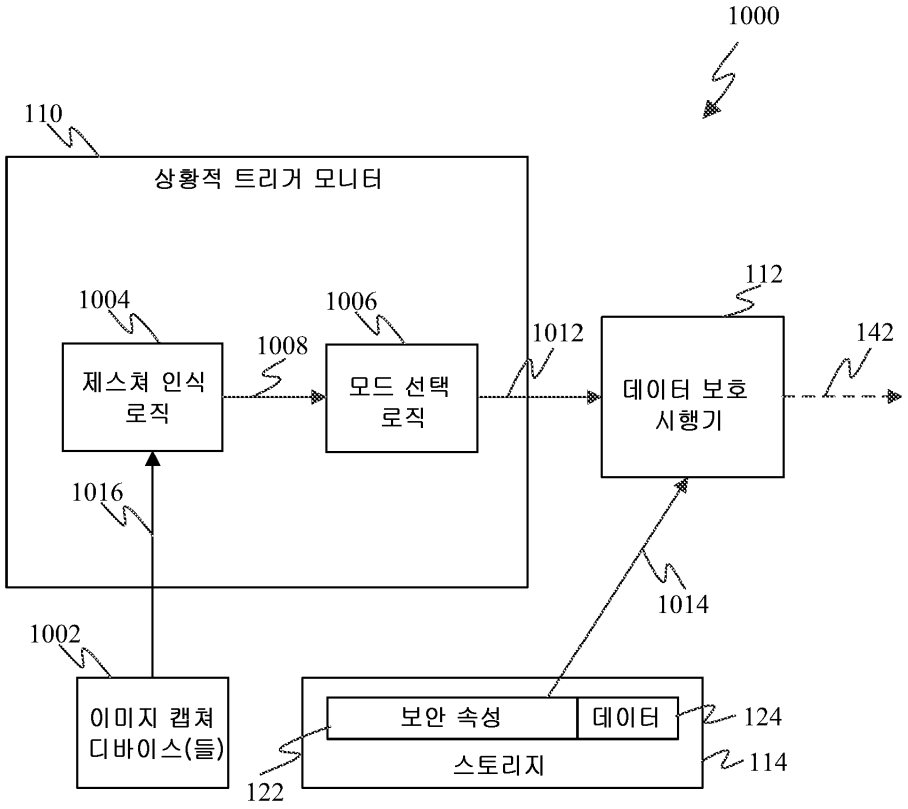
도면8


800
110
상황적 트리거 모니터
804
유저 인식 로직
806
모드 선택 로직
808
812
112
데이터 보호 시행기
142
816
814
802
이미지 캡쳐 디바이스(들)
보안 속성
데이터
124
스토리지
114
122

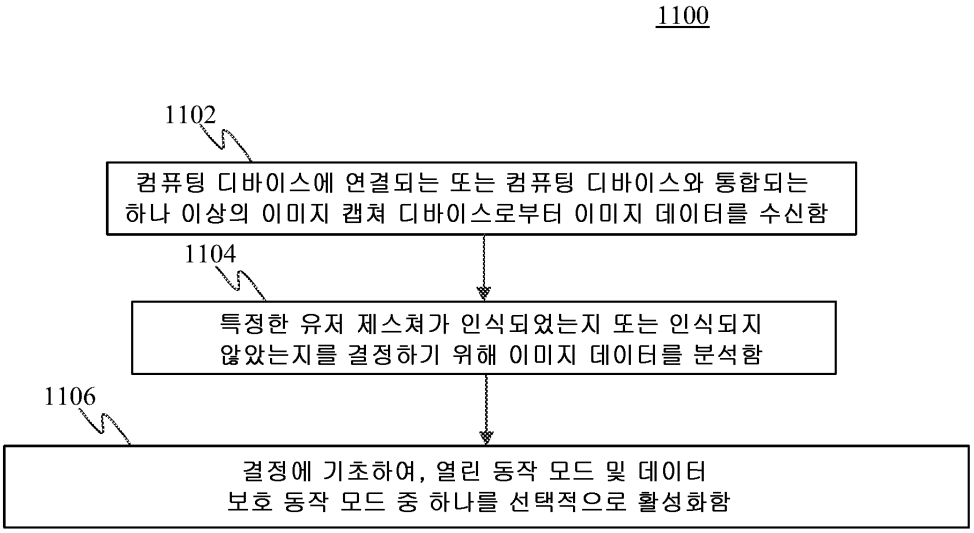
도면9


900
902
컴퓨팅 디바이스에 연결되는 또는 컴퓨팅 디바이스와 통합되는 하나 이상의 이미지 캡쳐 디바이스로부터 이미지 데이터를 수신함
904
소유자 또는 권한 소지 유저가 컴퓨팅 디바이스에 근접하여 위치하는지를 결정하기 위해 이미지 데이터를 분석함
906
소유자 또는 권한 소지 유저가 컴퓨팅 디바이스에 근접하여 위치한다는 결정에 응답하여, 열린 동작 모드를 활성화함
908
소유자 또는 권한 소지 유저가 컴퓨팅 디바이스에 근접하여 위치하지 않는다는 결정에 응답하여, 데이터 보호 동작 모드를 활성화함

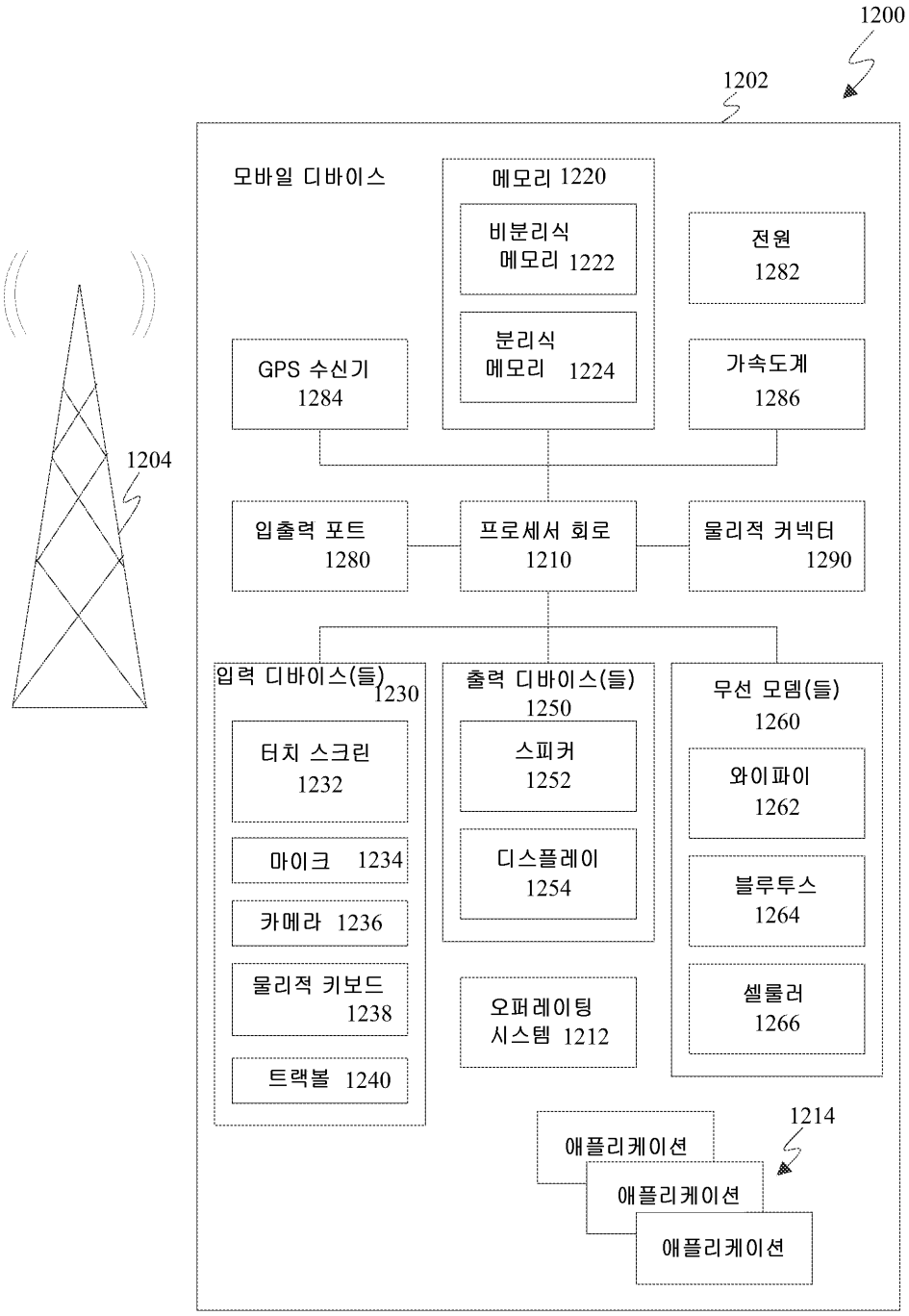
도면10


1000
110
상황적 트리거 모니터
1004
제스쳐 인식 로직
1006
모드 선택 로직
1008
1012
112
데이터 보호 시행기
142
1016
1014
1002
이미지 캡쳐 디바이스(들)
보안 속성
데이터
124
스토리지
114
122

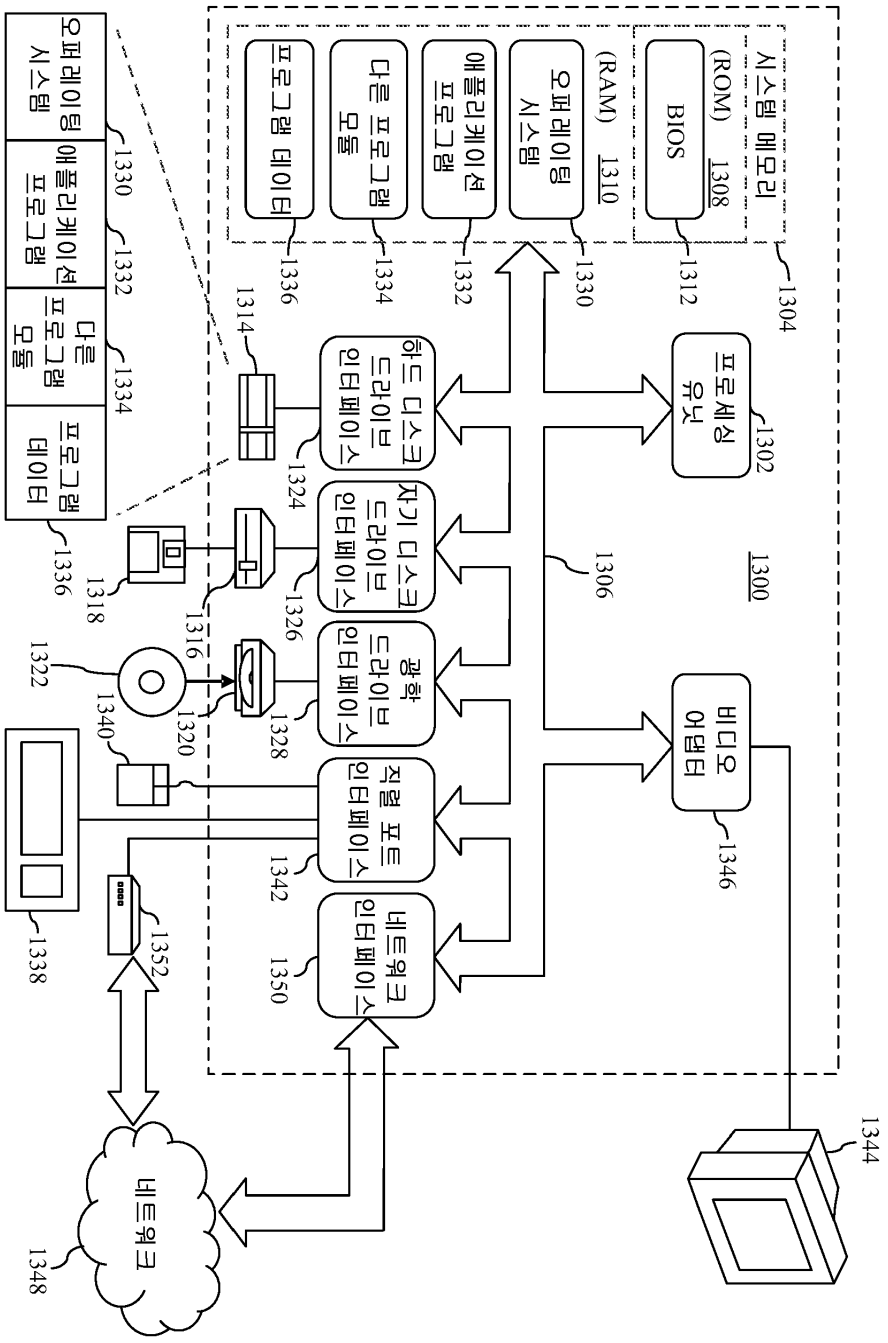
도면11


1100
1102
컴퓨팅 디바이스에 연결되는 또는 컴퓨팅 디바이스와 통합되는
하나 이상의 이미지 캡쳐 디바이스로부터 이미지 데이터를 수신함
1104
특정한 유저 제스쳐가 인식되었는지 또는 인식되지
않았는지를 결정하기 위해 이미지 데이터를 분석함
1106
결정에 기초하여, 열린 동작 모드 및 데이터
보호 동작 모드 중 하나를 선택적으로 활성화함

도면12


1200
1202
모바일 디바이스
메모리 1220
비분리식 메모리 1222
분리식 메모리 1224
전원 1282
GPS 수신기 1284
가속도계 1286
1204
입출력 포트 1280
프로세서 회로 1210
물리적 커넥터 1290
입력 디바이스(들) 1230
터치 스크린 1232
마이크 1234
카메라 1236
물리적 키보드 1238
트랙볼 1240
출력 디바이스(들) 1250
스피커 1252
디스플레이 1254
오퍼레이팅 시스템 1212
무선 모뎀(들) 1260
와이파이 1262
블루투스 1264
셀룰러 1266
1214
애플리케이션
애플리케이션
애플리케이션

도면13


시스템 메모리
(ROM) 1308
BIOS
1312
(RAM) 1310
오퍼레이팅 시스템
애플리케이션 프로그램
다른 프로그램 모듈
프로그램 데이터
1304
1330
1332
1334
1336
프로세싱 유닛
1302
1300
1306
하드 디스크 드라이브 인터페이스
자기 디스크 드라이브 인터페이스
광학 드라이브 인터페이스
직렬 포트 인터페이스
네트워크 인터페이스
비디오 어댑터
1346
1344
1314
1324
1326
1328
1342
1350
1352
1316
1318
1320
1322
1340
1338
네트워크
1348
오퍼레이팅 시스템
애플리케이션 프로그램
다른 프로그램 모듈
프로그램 데이터
1330
1332
1334
1336