(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0141738
(43) 공개일자 2016년12월09일

(51) 국제특허분류(Int. Cl.)
G06F 21/35 (2013.01) *A61B 5/00* (2006.01)
A61B 5/024 (2006.01) *A61B 5/11* (2006.01)
G06F 1/16 (2006.01) *G06F 21/32* (2013.01)
G06F 21/34 (2013.01) *G06F 3/0346* (2013.01)
H04L 29/06 (2006.01) *H04W 12/06* (2009.01)
(52) CPC특허분류
G06F 21/35 (2013.01)
A61B 5/02438 (2013.01)
(21) 출원번호 10-2016-7027365
(22) 출원일자(국제) 2015년03월31일
심사청구일자 없음
(85) 번역문제출일자 2016년09월30일
(86) 국제출원번호 PCT/US2015/023719
(87) 국제공개번호 WO 2015/153688
국제공개일자 2015년10월08일
(30) 우선권주장
61/975,684 2014년04월04일 미국(US)
14/444,620 2014년07월28일 미국(US)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
야콥슨, 비요른 마르쿠스
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인 남앤드남

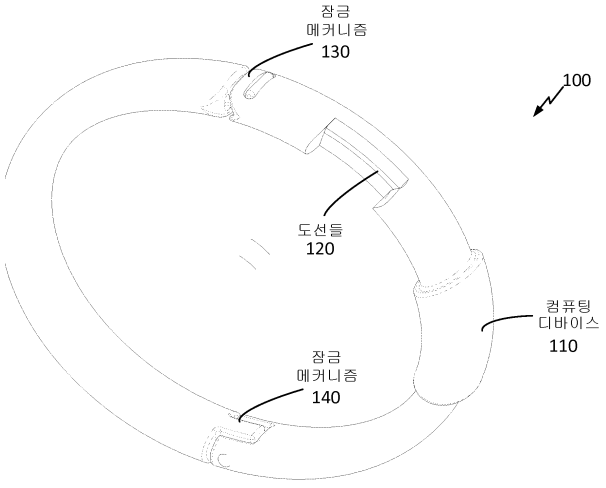
전체 청구항 수 : 총 30 항

(54) 발명의 명칭 **웨어러블 아이덴티티 관리기를 가능하게 하는 방법 및 장치**

(57) 요 약

웨어러블 아이덴티티 관리기 시스템 쪽으로 향해진 다양한 양상들이 개시된다. 제 1 양상에서, 웨어러블 아이덴티티 관리기 디바이스가 사용자에 의해 착용되어 있는지 여부를 기초로 사용자와 웨어러블 아이덴티티 관리기 디바이스 간의 연관 상태가 확인되고, 웨어러블 아이덴티티 관리기 디바이스의 움직임과 연관된 모션 데이터가 모니터링된다. 다음에, 모션 데이터를 포함하는 인증 데이터가 연관 상태를 기초로 송신된다. 다른 양상에서, 웨어러블 아이덴티티 관리기 디바이스가 사용자에 의해 착용되어 있는지 여부를 기초로 사용자와 웨어러블 아이덴티티 관리기 디바이스 간의 연관 상태가 또 결정된다. 그러나 여기서 웨어러블 아이덴티티 관리기 디바이스는 페어링 디바이스와 페어링되고, 페어링 디바이스를 통해 사용자 인증을 가능하게 하기 위해 연관 상태를 기초로 페어링 디바이스에 인증 데이터가 송신된다.

대 표 도 - 도1



(52) CPC특허분류
A61B 5/1116 (2013.01)
A61B 5/681 (2013.01)
A61B 5/6844 (2013.01)
G06F 1/163 (2013.01)
G06F 21/32 (2013.01)
G06F 21/34 (2013.01)
G06F 3/0346 (2013.01)
H04L 63/0853 (2013.01)
H04W 12/06 (2013.01)

명 세 서

청구범위

청구항 1

웨어러블 아이덴티티 관리기 디바이스로서,

메모리; 및

상기 메모리에 통신 가능하게 연결된 프로세서를 포함하며,

상기 프로세서는,

상기 웨어러블 아이덴티티 관리기 디바이스가 착용되어 있는지 여부에 부분적으로 기초하여 사용자와 상기 웨어러블 아이덴티티 관리기 디바이스 간의 연관 상태를 결정하고;

상기 웨어러블 아이덴티티 관리기 디바이스를 페어링 디바이스와 페어링하고 - 상기 페어링 디바이스는 상기 웨어러블 아이덴티티 관리기 디바이스가 착용되어 있는지 여부를 기초로 상기 웨어러블 아이덴티티 관리기 디바이스에 대한 프록시로서 동작하도록 구성됨 -; 그리고

상기 웨어러블 아이덴티티 관리기 디바이스가 착용되어 있는지 여부를 기초로 상기 웨어러블 아이덴티티 관리기 디바이스로부터 상기 페어링 디바이스로 인증 데이터를 송신하도록 구성되고,

상기 인증 데이터는 상기 페어링 디바이스를 통해 외부 디바이스 상에서 사용자 인증을 가능하게 하는,

웨어러블 아이덴티티 관리기 디바이스.

청구항 2

제 1 항에 있어서,

상기 프로세서는,

상기 웨어러블 아이덴티티 관리기 디바이스의 움직임과 연관된 모션 데이터를 모니터링하여 수집하도록 추가로 구성되고,

상기 인증 데이터는 수집된 모션 데이터를 포함하는,

웨어러블 아이덴티티 관리기 디바이스.

청구항 3

제 1 항에 있어서,

상기 프로세서는 연관 프로시저를 통해 상기 웨어러블 아이덴티티 관리기 디바이스를 상기 사용자와 연관시키도록 구성되고,

상기 연관 상태는 상기 연관 프로시저의 결과를 기초로 하는,

웨어러블 아이덴티티 관리기 디바이스.

청구항 4

제 2 항에 있어서,

상기 모션 데이터는 상기 웨어러블 아이덴티티 관리기 디바이스가 가로지르는 정의된 경로를 포함하는,

웨어러블 아이덴티티 관리기 디바이스.

청구항 5

제 1 항에 있어서,

상기 프로세서는 자이로, 글로벌 포지셔닝 시스템(GPS: global positioning system) 디바이스, 터치 감응 센서 또는 마이크로폰 중 적어도 하나로부터 센서 데이터를 리트리브하도록 추가로 구성되며,

상기 인증 데이터는 상기 센서 데이터를 더 포함하는,

웨어러블 아이덴티티 관리기 디바이스.

청구항 6

제 1 항에 있어서,

상기 프로세서는 걸쇠 센서, 압력 센서, 온도 센서, 펄스 센서, 모션 센서 또는 스트레치 센서 중 적어도 하나로부터 리트리브된 데이터를 기초로 상기 웨어러블 아이덴티티 관리기 디바이스가 착용되어 있는지 여부를 추론하도록 추가로 구성되는,

웨어러블 아이덴티티 관리기 디바이스.

청구항 7

제 1 항에 있어서,

상기 프로세서는,

인증 요청을 수신하고;

크리덴셜을 제공하며; 그리고

상기 인증 요청을 기초로 상기 크리덴셜을 송신하도록 추가로 구성되는,

웨어러블 아이덴티티 관리기 디바이스.

청구항 8

제 1 항에 있어서,

상기 프로세서는,

인증 요청을 수신하고;

상기 인증 요청과 연관된 보안 레벨을 확인하고; 그리고

상기 보안 레벨을 기초로 상기 인증 데이터를 송신하도록 추가로 구성되는,

웨어러블 아이덴티티 관리기 디바이스.

청구항 9

하나 또는 그보다 많은 명령들이 저장된 비-일시적 기계 판독 가능 저장 매체로서,

상기 하나 또는 그보다 많은 명령들은 적어도 하나의 프로세서에 의해 실행될 때 상기 적어도 하나의 프로세서로 하여금,

사용자와 웨어러블 아이덴티티 관리기 디바이스 사이의 연관 상태를 확인하게 하고 - 상기 연관 상태는 상기 웨어러블 아이덴티티 관리기 디바이스가 착용되어 있는지 여부에 적어도 부분적으로 기초하여 확인됨 -;

상기 웨어러블 아이덴티티 관리기 디바이스를 페어링 디바이스와 페어링하게 하고 - 상기 페어링 디바이스는 상기 웨어러블 아이덴티티 관리기 디바이스가 착용되어 있는지 여부를 기초로 상기 웨어러블 아이덴티티 관리기 디바이스에 대한 프록시로서 동작하도록 구성됨 -; 그리고

상기 웨어러블 아이덴티티 관리기 디바이스가 착용되어 있는지 여부를 기초로 상기 웨어러블 아이덴티티 관리기 디바이스로부터 상기 페어링 디바이스로 인증 데이터를 송신하게 하며,

상기 인증 데이터는 상기 페어링 디바이스를 통해 외부 디바이스 상에서 사용자 인증을 가능하게 하는,

비-일시적 기계 판독 가능 저장 매체.

청구항 10

제 9 항에 있어서,

상기 하나 또는 그보다 많은 명령들은 상기 적어도 하나의 프로세서로 하여금,

상기 웨어러블 아이덴티티 관리기 디바이스의 움직임과 연관된 모션 데이터를 모니터링하여 수집하게 하기 위한 명령들을 더 포함하며,

상기 인증 데이터는 수집된 모션 데이터를 포함하는,

비-일시적 기계 판독 가능 저장 매체.

청구항 11

제 9 항에 있어서,

상기 하나 또는 그보다 많은 명령들은 상기 적어도 하나의 프로세서로 하여금, 연관 프로시저를 통해 상기 웨어러블 아이덴티티 관리기 디바이스를 상기 사용자와 연관시키게 하기 위한 명령들을 더 포함하며,

상기 연관 상태는 상기 연관 프로시저의 결과를 기초로 하는,

비-일시적 기계 판독 가능 저장 매체.

청구항 12

제 11 항에 있어서,

상기 연관 프로시저는 국소 저장된 비밀번호를 연관 디바이스로부터 수신된 비밀번호와 매칭시키는 것을 포함하는,

비-일시적 기계 판독 가능 저장 매체.

청구항 13

제 11 항에 있어서,

상기 연관 프로시저는 상기 웨어러블 아이덴티티 관리기 디바이스의 연관 움직임을 연관 디바이스의 움직임에 대응하는 수신된 데이터와 매칭시키는 것을 포함하는,

비-일시적 기계 판독 가능 저장 매체.

청구항 14

제 9 항에 있어서,

상기 하나 또는 그보다 많은 명령들은 상기 적어도 하나의 프로세서로 하여금,

인증 요청을 수신하게 하고; 그리고

상기 인증 요청으로부터 외삽된 실행 콘텍스트 또는 사용자 동작 중 적어도 하나를 기초로 크리덴셜을 제공하게 하기 위한 명령들을 더 포함하는,

비-일시적 기계 판독 가능 저장 매체.

청구항 15

제 9 항에 있어서,

상기 하나 또는 그보다 많은 명령들은 상기 적어도 하나의 프로세서로 하여금,

인증 요청을 수신하게 하고;

상기 인증 요청과 연관된 보안 레벨을 확인하게 하고; 그리고

상기 보안 레벨을 기초로 상기 인증 데이터를 제공하게 하기 위한 명령들을 더 포함하는,

비-일시적 기계 판독 가능 저장 매체.

청구항 16

제 15 항에 있어서,

상기 보안 레벨은 사용자 선호 설정, 실행 콘텍스트, 또는 하나 또는 그보다 많은 이력 실행 콘텍스트들 중 적어도 하나에 따라 확인되는,

비-일시적 기계 판독 가능 저장 매체.

청구항 17

무선 통신을 가능하게 하기 위한 방법으로서,

사용자와 웨어러블 아이덴티티 관리기 디바이스 사이의 연관 상태를 결정하는 단계 - 상기 결정하는 단계는 상기 웨어러블 아이덴티티 관리기 디바이스가 착용되어 있는지 여부를 결정하는 단계를 포함함 -;

상기 웨어러블 아이덴티티 관리기 디바이스를 페어링 디바이스와 페어링하는 단계; 및

상기 웨어러블 아이덴티티 관리기 디바이스가 착용되어 있는지 여부를 기초로 상기 웨어러블 아이덴티티 관리기 디바이스로부터 상기 페어링 디바이스로 인증 데이터를 송신하는 단계를 포함하며,

상기 인증 데이터는 상기 페어링 디바이스를 통해 외부 디바이스 상에서 사용자 인증을 가능하게 하는,

무선 통신을 가능하게 하기 위한 방법.

청구항 18

제 17 항에 있어서,

상기 웨어러블 아이덴티티 관리기 디바이스의 움직임과 연관된 모션 데이터를 모니터링하는 단계를 더 포함하며,

상기 인증 데이터는 상기 모션 데이터를 포함하는,

무선 통신을 가능하게 하기 위한 방법.

청구항 19

제 17 항에 있어서,

연관 프로시저를 통해 상기 웨어러블 아이덴티티 관리기 디바이스를 상기 사용자와 연관시키는 단계를 더 포함하며,

상기 연관 상태는 상기 연관 프로시저의 결과를 기초로 하는,

무선 통신을 가능하게 하기 위한 방법.

청구항 20

제 19 항에 있어서,

상기 연관 프로시저는 국소 저장된 비밀번호를 연관 디바이스로부터 수신된 비밀번호와 매칭시키는 것을 포함하는,

무선 통신을 가능하게 하기 위한 방법.

청구항 21

제 19 항에 있어서,

상기 연관 프로시저는 상기 웨어러블 아이덴티티 관리기 디바이스의 연관 움직임을 연관 디바이스의 움직임에 대응하는 수신된 데이터와 매칭시키는 것을 포함하는,

무선 통신을 가능하게 하기 위한 방법.

청구항 22

제 17 항에 있어서,

사용자와 연관된 크리덴셜을 저장하는 단계; 및

인증 요청에 응답하여 상기 페어링 디바이스에 상기 크리덴셜을 제공하는 단계를 더 포함하는,

무선 통신을 가능하게 하기 위한 방법.

청구항 23

제 22 항에 있어서,

상기 인증 요청과 연관된 보안 레벨을 확인하는 단계; 및

상기 보안 레벨을 기초로 상기 페어링 디바이스에 송신되는 상기 크리덴셜의 양을 제한하는 단계를 더 포함하는,

무선 통신을 가능하게 하기 위한 방법.

청구항 24

웨어러블 아이덴티티 관리기 디바이스로서,

사용자와 상기 웨어러블 아이덴티티 관리기 디바이스 사이의 연관 상태를 결정하기 위한 수단 – 상기 연관 상태는 상기 웨어러블 아이덴티티 관리기 디바이스가 착용되어 있는지 여부에 적어도 부분적으로 기초하여 확인됨 –;

상기 웨어러블 아이덴티티 관리기 디바이스를 페어링 디바이스와 페어링하기 위한 수단 – 상기 페어링 디바이스는 상기 웨어러블 아이덴티티 관리기 디바이스가 착용되어 있는지 여부를 기초로 상기 웨어러블 아이덴티티 관리기 디바이스에 대한 프록시로서 동작하도록 구성됨 –; 및

상기 웨어러블 아이덴티티 관리기 디바이스가 착용되어 있는지 여부를 기초로 상기 웨어러블 아이덴티티 관리기 디바이스로부터 상기 페어링 디바이스로 인증 데이터를 송신하기 위한 수단을 포함하며,

상기 인증 데이터는 상기 페어링 디바이스를 통해 외부 디바이스 상에서 사용자 인증을 가능하게 하는,

웨어러블 아이덴티티 관리기 디바이스.

청구항 25

제 24 항에 있어서,

상기 웨어러블 아이덴티티 관리기 디바이스의 움직임과 연관된 모션 데이터를 모니터링하기 위한 수단을 더 포함하며,

상기 인증 데이터는 상기 모션 데이터를 포함하는,

웨어러블 아이덴티티 관리기 디바이스.

청구항 26

제 25 항에 있어서,

상기 모션 데이터는 상기 웨어러블 아이덴티티 관리기 디바이스가 가로지르는 정의된 경로를 포함하는,

웨어러블 아이덴티티 관리기 디바이스.

청구항 27

제 25 항에 있어서,

상기 모니터링하기 위한 수단은 자이로, 터치 감응 센서 또는 마이크로폰 중 적어도 하나로부터 센서 데이터를

리트리브하기 위한 수단을 더 포함하며,

상기 인증 데이터는 상기 센서 데이터를 더 포함하는,

웨어러블 아이덴티티 관리기 디바이스.

청구항 28

제 24 항에 있어서,

상기 결정하기 위한 수단은 걸쇠 센서, 압력 센서, 온도 센서 또는 스트레치 센서 중 적어도 하나로부터 리트리브된 데이터를 기초로 상기 웨어러블 아이덴티티 관리기 디바이스가 착용되어 있는지 여부를 추론하기 위한 수단을 더 포함하는,

웨어러블 아이덴티티 관리기 디바이스.

청구항 29

제 24 항에 있어서,

인증 요청을 수신하기 위한 수단; 및

상기 인증 요청과 연관된 보안 레벨을 확인하기 위한 수단을 더 포함하며,

상기 송신하기 위한 수단은 상기 보안 레벨을 기초로 상기 페어링 디바이스에 상기 인증 데이터를 송신하기 위한 수단을 포함하는,

웨어러블 아이덴티티 관리기 디바이스.

청구항 30

제 29 항에 있어서,

상기 확인하기 위한 수단은 복수의 가능한 보안 레벨들로부터 상기 보안 레벨을 선택하기 위한 수단을 포함하는,

웨어러블 아이덴티티 관리기 디바이스.

발명의 설명

기 술 분 야

[0001] [0001] 본 출원은 2014년 7월 28일자 출원된 미국 특허출원 제14/444,620호, 및 2014년 4월 4일자 출원된 미국 가특허출원 제61/975,684호에 대한 우선권 및 그 이익을 주장하며, 이 출원들의 전체 내용은 이로써 인용에 의해 포함된다.

[0002] [0002] 본 개시의 양상들은 일반적으로 무선 통신 시스템들에 관한 것으로, 보다 구체적으로는 사용자 인증을 가능하게 하는 웨어러블 아이덴티티 관리기 시스템에 관한 것이다.

배 경 기 술

[0003] [0003] 사용자 인증은 장애물 및 부정 행위 위험의 증가하는 소스이다. 일반적인 소비자들은 다수의 서비스들에 동일한 또는 매우 유사한 비밀번호를 사용하는데, 이는 침해들이 야기하는 부정 행위에 대한 노출을 증가시킨다. 많은 사용자들은 비밀번호들을 입력하는 어려움들로 인해, 모바일 디바이스들 상에서 비밀번호들을 필요로 하는 서비스들의 사용에 저항한다. 비밀번호 관리기들이 사용될 수 있지만, 이들은 편리한 부정 행위(즉, 디바이스 소유자와 가까운 사용자들에 의해 시작된 악용 거래들)에 대한 노출을 증가시키고 디바이스 분실과 연관된 위험들을 증가시킨다. 마찬가지로, 개인 식별 번호(PIN: personal identification number)들 및 다른 형태의 메모리 기반 인증은 비슷한 문제들을 제기한다.

발명의 내용

[0004] [0004] 다음은 본 개시의 하나 또는 그보다 많은 양상들의 기본적인 이해를 제공하기 위해 이러한 양상들의 간

단한 요약을 제시한다. 이 요약은 본 개시의 고려되는 모든 특징들의 포괄적인 개요가 아니며, 본 개시의 모든 양상들의 주요 또는 핵심 엘리먼트들을 식별하지도, 본 개시의 임의의 또는 모든 양상들의 범위를 기술하지도 않는 것으로 의도된다. 그 유일한 목적은 본 개시의 하나 또는 그보다 많은 양상들의 일부 개념들을 뒤에 제시되는 보다 상세한 설명에 대한 서론으로서 간단한 형태로 제시하는 것이다.

[0005] [0005] 본 개시의 양상들은 사용자 인증을 가능하게 하는 웨어러블 아이덴티티 관리기 시스템 쪽으로 향해진 방법들, 장치들, 컴퓨터 프로그램 물건들 및 처리 시스템들을 제공한다. 한 양상에서, 본 개시는 거래들을 가능하게 하기 위한 방법을 제공하며, 이는 웨어러블 아이덴티티 관리기 디바이스가 착용되어 있는지 여부를 기초로 사용자와 웨어러블 아이덴티티 관리기 디바이스 간의 연관 상태를 결정하는 단계를 포함한다. 이 방법은 웨어러블 아이덴티티 관리기 디바이스를 페어링 디바이스와 페어링하는 단계, 및 페어링 디바이스를 통해 사용자 인증을 가능하게 하기 위해 연관 상태를 기초로 페어링 디바이스에 인증 데이터를 송신하는 단계를 더 포함한다.

[0006] [0006] 다른 양상에서, 거래들을 가능하게 하도록 구성된 웨어러블 아이덴티티 관리기 디바이스가 개시된다. 웨어러블 아이덴티티 관리기는 검출기 컴포넌트, 결정 컴포넌트 및 송신 컴포넌트를 포함한다. 여기서, 검출기 컴포넌트는 웨어러블 아이덴티티 관리기 디바이스가 착용되어 있는지 여부를 기초로 사용자와 웨어러블 아이덴티티 관리기 디바이스 간의 연관 상태를 결정하도록 구성되는 반면, 결정 컴포넌트는 웨어러블 아이덴티티 관리기 디바이스의 움직임과 연관된 모션 데이터를 모니터링하도록 구성된 센서 컴포넌트를 통해 사용자 인증의 결정을 가능하게 하도록 구성된다. 송신 컴포넌트는 다음에, 인증 데이터가 모션 데이터를 포함하도록, 연관 상태를 기초로 인증 데이터를 송신하도록 구성된다.

[0007] [0007] 추가 양상에서, 거래들을 가능하게 하도록 구성된 다른 웨어러블 아이덴티티 관리기 디바이스가 개시된다. 여기서, 디바이스는 웨어러블 아이덴티티 관리기 디바이스가 착용되어 있는지 여부를 기초로 사용자와 웨어러블 아이덴티티 관리기 디바이스 간의 연관 상태를 결정하기 위한 수단, 및 웨어러블 아이덴티티 관리기 디바이스를 페어링 디바이스와 페어링하기 위한 수단을 포함한다. 웨어러블 아이덴티티 관리기 디바이스는 인증 데이터가 페어링 디바이스를 통해 사용자 인증을 가능하도록, 연관 상태를 기초로 페어링 디바이스에 인증 데이터를 송신하기 위한 수단을 더 포함한다.

[0008] [0008] 또 다른 양상에서, 저장된 하나 또는 그보다 많은 명령들을 통해 거래들을 가능하게 하도록 구성된 비-일시적 기계 판독 가능 저장 매체가 개시된다. 여기서, 적어도 하나의 프로세서에 의해 실행될 때, 하나 또는 그보다 많은 명령들은 적어도 하나의 프로세서로 하여금 다양한 동작들을 수행하게 한다. 동작들은 웨어러블 아이덴티티 관리기 디바이스가 착용되어 있는지 여부를 기초로 사용자와 웨어러블 아이덴티티 관리기 디바이스 간의 연관 상태를 확인하는 동작, 및 웨어러블 아이덴티티 관리기 디바이스의 움직임과 연관된 모션 데이터를 모니터링하는 동작을 포함한다. 동작들은 인증 데이터가 모션 데이터를 포함하도록, 연관 상태를 기초로 인증 데이터를 송신하는 동작을 더 포함한다.

[0009] [0009] 이러한 그리고 다른 개시되는 양상들은 이어지는 상세한 설명의 검토시 더 충분히 이해될 것이다. 본 발명의 다른 양상들, 특징들 및 실시예들은 첨부 도면들과 함께 본 발명의 특정한 예시적인 양상들의 다음 설명의 검토시, 해당 기술분야에서 통상의 지식을 가진 자들에게 명백해질 것이다. 본 발명의 특징들은 아래 특정 양상들 및 도면들과 관련하여 논의될 수 있지만, 본 발명의 모든 양상들은 본 명세서에서 논의되는 유리한 특징들 중 하나 또는 그보다 많은 특징을 포함할 수 있다. 즉, 하나 또는 그보다 많은 양상들은 어떤 유리한 특징들을 갖는 것으로 논의될 수 있지만, 이러한 특징들 중 하나 또는 그보다 많은 특징은 또한 본 명세서에서 논의되는 본 발명의 다양한 실시예들에 따라 사용될 수도 있다. 유사한 방식으로, 예시적인 양상들은 뒤에 디바이스, 시스템 또는 방법 양상들로서 논의될 수 있지만, 이러한 예시적인 양상들은 다양한 디바이스들, 시스템들 및 방법들로 구현될 수 있다고 이해되어야 한다.

도면의 간단한 설명

[0010] [0010] 도 1은 본 개시의 한 양상에 따른 예시적인 웨어러블 아이덴티티 관리기 디바이스의 개략도이다.

[0011] [0011] 도 2는 잠금 및 잠금 해제 구성인 예시적인 웨어러블 아이덴티티 관리기 디바이스를 예시하는 개략도이다.

[0012] [0012] 도 3은 본 명세서의 한 양상에 따라 웨어러블 아이덴티티 관리기 디바이스를 통해 사용자의 인증을 가능하게 하는 예시적인 환경을 예시한다.

[0013] [0013] 도 4는 본 개시의 일부 양상들에 따라 웨어러블 아이덴티티 관리기 디바이스의 이용을 가능하게 하기 위

한 예시적인 프로세스를 예시하는 흐름도이다.

[0014] 도 5는 본 개시의 한 양상에 따라 페어링 디바이스와 페어링된 예시적인 웨어러블 아이덴티티 관리기 디바이스의 개략도이다.

[0015] 도 6은 본 개시의 일부 양상들에 따라 처리 시스템을 이용하는 웨어러블 아이덴티티 관리기 디바이스의 일례를 예시하는 블록도이다.

[0016] 도 7은 본 개시의 한 양상에 따른 예시적인 검출기 컴포넌트들을 예시하는 블록도이다.

[0017] 도 8은 본 개시의 일부 양상들에 따라 웨어러블 아이덴티티 관리기 디바이스와 사용자의 연관을 가능하게 하기 위한 예시적인 프로세스를 예시하는 흐름도이다.

[0018] 도 9는 본 개시의 일부 양상들에 따라 웨어러블 아이덴티티 관리기 디바이스로부터 사용자의 연관 해제를 가능하게 하기 위한 예시적인 프로세스를 예시하는 흐름도이다.

[0019] 도 10은 본 개시의 한 양상에 따른 예시적인 결정 컴포넌트들을 예시하는 블록도이다.

[0020] 도 11은 본 개시의 일부 양상들에 따라 센서 데이터가 사용자 인증을 가능하게 하는데 이용되는 예시적인 프로세스를 예시하는 흐름도이다.

[0021] 도 12는 본 개시의 일부 양상들에 따라 페어링 디바이스가 사용자 인증을 가능하게 하는데 이용되는 예시적인 프로세스를 예시하는 흐름도이다.

[0022] 도 13은 본 개시의 일부 양상들에 따라 사용자 인증을 가능하게 하기 위해 확인된 보안 레벨에 따라 크리덴셜들이 송신되는 예시적인 프로세스를 예시하는 흐름도이다.

[0023] 도 14는 본 개시의 한 양상에 따라 아이덴티티 관리기와 스테이션 간의 예시적인 근접도 검증을 예시하는 개략도이다.

[0024] 도 15는 본 개시의 한 양상에 따라 아이덴티티 관리기와 스테이션 간의 예시적인 암시적 확약 및 명시적 확인 프로토콜을 예시하는 개략도이다.

[0025] 도 16은 본 개시의 한 양상에 따라 판매 시점 단말에서의 예시적인 사용자 인증을 예시하는 제 1 개략도이다.

[0026] 도 17은 본 개시의 한 양상에 따라 판매 시점 단말에서의 예시적인 사용자 인증을 예시하는 제 2 개략도이다.

[0027] 도 18은 본 명세서에서 설명되는 다양한 실시예들이 구현될 수 있는 한정적이지 않은 예시적인 네트워크화된 환경들을 나타내는 블록도이다.

[0028] 도 19는 본 명세서에서 설명되는 다양한 실시예들의 하나 또는 그보다 많은 양상들이 구현될 수 있는 한정적이지 않은 예시적인 컴퓨팅 시스템 또는 운영 환경을 나타내는 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0011] 개요

[0012] [0029] 배경기술에서 논의한 바와 같이, 종래의 사용자 인증 메커니즘들의 다양한 한계들 때문에, 사용자들은 잠재적 부정 행위로부터 자신들을 보호하기 위해 종종 무선 기반 인증 거래들을 바람직하지 않게 금한다. 본 명세서에 개시된 양상들은 사용자들이 웨어러블 아이덴티티 관리기 디바이스를 착용하고 있는지 여부를 기초로 사용자들을 인증하는 인증 인프라구조를 제공함으로써 이러한 한계들을 극복하는 쪽에 향해져 있다. 즉, 사용자들이 웨어러블 아이덴티티 관리기 디바이스와 자신들을 연관시킬 수 있게 하는 양상들이 개시되는데, 여기서 웨어러블 아이덴티티 관리기 디바이스는 웨어러블 아이덴티티 관리기 디바이스가 사용자에 의해 계속해서 착용되어 있는 한 다른 디바이스에 대한 사용자의 무선 인증을 가능하게 하도록 구성된다.

[0013] 예시적인 웨어러블 아이덴티티 관리기 디바이스

[0014] [0030] 다음에 도 1을 참조하면, 본 개시의 한 양상에 따라 예시적인 웨어러블 아이덴티티 관리기 디바이스가 제공된다. 예시된 바와 같이, 웨어러블 아이덴티티 관리기 디바이스(100)는 제 1 잠금 메커니즘(130) 및 제 2 잠금 메커니즘(140)을 포함하는 웨어러블 팔찌로서 구성된다. 웨어러블 아이덴티티 관리기 디바이스(100)는 또

한 컴퓨팅 디바이스(110) 및 도선들(120)을 포함하며, 여기서 컴퓨팅 디바이스(110)는 도선들(120) 사이의 접속이 파손되었는지 여부를 검출하도록 구성된다. 즉, 도 2에 예시된 바와 같이, 웨어러블 아이덴티티 관리기 디바이스(100)는 잠금 메커니즘(130)을 통해 사용자에게 부착 가능함이 고려되는데, 여기서 잠긴 구성(200)은 도선들(120) 사이에 닫힌 회로를 생성하고, 잠금 해제 구성(205)은 도선들(120) 사이의 회로를 차단한다. 더욱이, 컴퓨팅 디바이스(110)는 도선들(120) 간의 접속이 차단되는지(즉, 잠금 해제 구성(205)) 아니면 닫히는지(즉, 잠금 구성(200))에 따라 웨어러블 아이덴티티 관리기 디바이스(100)가 사용자에 의해 착용되어 있는지 여부를 검출할 것임이 고려된다.

[0015] [0031] 아래 더 상세히 논의되는 바와 같이, 웨어러블 아이덴티티 관리기 디바이스(100)가 다른 디바이스들에 대한 사용자의 인증을 가능하게 할 수 있는 것은 우선 웨어러블 아이덴티티 관리기 디바이스(100)와 사용자 간의 연관을 필요로 할 수도 있다. 예컨대, 웨어러블 아이덴티티 관리기 디바이스(100)를 사용자의 손목에 부착할 때, 사용자는 웨어러블 아이덴티티 관리기 디바이스(100)에 대해 사용자의 아이덴티티를 확인하도록 (예를 들어, 컴퓨팅 디바이스(110) 상의 사용자 인터페이스를 통해 또는 웨어러블 아이덴티티 관리기 디바이스(100)에 페어링된 다른 디바이스를 통해) 비밀번호를 입력할 것이 요구될 수도 있다. 사용자의 아이덴티티 확인시, 웨어러블 아이덴티티 관리기 디바이스(100)는 다음에, 잠금 메커니즘(130)이 잠긴 구성을 유지하는 한, 다른 엔티티들(예를 들어, 판매 시점 디바이스들, 도로 요금소들, 금융 기관 웹사이트들 등)에 인증 데이터를 무선으로 송신함으로써 그러한 엔티티들에 대한 다음 사용자 인증들을 가능하게 할 수 있음이 고려된다. 그렇지 않으면, 컴퓨팅 디바이스(110)가 잠금 메커니즘(130)이 풀렸다고 검출한다면, 컴퓨팅 디바이스(110)는 사용자가 더는 웨어러블 아이덴티티 관리기 디바이스(100)를 착용하고 있지 않다고 추론할 것이며, 따라서 사용자가 웨어러블 아이덴티티 관리기 디바이스(100)와 다시 연관할 때까지 인증 데이터를 송신하지 않을 것이다.

[0016] [0032] 대안적인 구현들에서는, 잠금 메커니즘을 사용하기보다는, 다양한 다른 디바이스들 중 임의의 디바이스가 사용자에 의해 웨어러블 아이덴티티 관리기 디바이스(100)가 착용되어 있는지 여부를 검출하는데 사용될 수도 있다. 예컨대, 웨어러블 아이덴티티 관리기 디바이스는 펄스 센서를 더 포함할 수도 있다. 여기서, 펄스 센서가 미리 결정된 양의 시간(예를 들어, 30초) 동안 신호를 검출하지 않았다면, 웨어러블 아이덴티티 관리기 디바이스(100)는 사용자가 더는 디바이스를 착용하고 있지 않다고 추론할 수도 있다. 펄스가 다시 검출되자마자, 웨어러블 아이덴티티 관리기 디바이스(100)는 이 디바이스가 착용되어 있을 가능성이 높다고 추론할 수 있으며, 이는 디바이스를 아이덴티티 획득 모드에 다시 들어가게 한다. 아이덴티티 획득 모드가 시작된 후, 일정 부분의 시간, 예컨대 1분 동안 검출된 어떠한 통신도 없다면, 디바이스는 연관 해제 모드로 돌아갈 수도 있고, 또는 아이덴티티 획득 모드에서 프록시들로서 사용되는 디바이스들을 웨이크업하도록 신호를 전송할 수도 있다.

[0017] [0033] 웨어러블 아이덴티티 관리기 디바이스(100)가 착용되어 있는지 여부를 결정하기 위해 가속도계 센서가 또한 사용될 수 있다. 이러한 구현 내에서는, 적어도 임계량의 시간(예를 들어, 5분) 동안 가속도계에 의해 어떠한 신호도 검출되지 않거나 단지 디바이스가 착용되어 있음을 나타내지 않는 움직임들만이 검출된다면, 웨어러블 아이덴티티 관리기 디바이스(100)는 연관 해제될 것인데, 이는 디바이스가 이전에 나타낸 사용자를 더는 나타내지 않을 것임을 의미한다. 충분히 강한 가속도계 신호가 다시 검출되면, 웨어러블 아이덴티티 관리기 디바이스(100)는 일정량의 시간 동안 또는 아이덴티티가 획득될 때까지 자신을 아이덴티티 획득 모드에 둘 것이다. 자이로(gyros)와 같은 다른 기능적으로 관련된 센서들이 또한 가속도계와 결합하든, 아니면 이에 대한 대안으로서 사용될 수 있다.

[0018] [0034] 웨어러블 아이덴티티 관리기 디바이스(100)가 착용되어 있는지 여부를 결정하기 위해 사용될 수 있는 또 다른 센서는 압력 또는 터치 센서이다. 이러한 센서는 웨어러블 아이덴티티 관리기 디바이스(100)를 신체에 타이트하게 착용하고 있는 사용자들(예를 들어, 꼭 맞는 팔찌, 반지 등)에 대해 특히 바람직할 수도 있다. 일정량의 시간 동안 검출된 어떠한 압력/터치도 없다면, 웨어러블 아이덴티티 관리기 디바이스(100)는 디바이스가 이전에 나타낸 아이덴티티로부터 자신을 연관 해제한다. 압력/터치가 다시 검출되면, 웨어러블 아이덴티티 관리기 디바이스(100)는 아이덴티티 획득 모드로 돌아간다.

[0019] [0035] 스트레치 센서 구현이 또한 고려된다. 예컨대, 웨어러블 아이덴티티 관리기 디바이스(100)가 스트레치 가능 팔찌로서 구성된다면, 웨어러블 아이덴티티 관리기 디바이스(100)는 사용자로부터 제거시 스트레치될 것임이 고려된다. 이에 따라, 웨어러블 아이덴티티 관리기 디바이스(100)는 웨어러블 아이덴티티 관리기 디바이스(100)가 임계 스트레치 메트릭 이상으로 스트레치되었는지 여부를 검출하도록 구성된 스트레치 센서를 포함할 수도 있다. 이러한 구현 내에서, 웨어러블 아이덴티티 관리기 디바이스(100)는 다음에, 스트레치 센서로부터 수신된 데이터를 기초로 연관/연관 해제 프로세스를 트리거하도록 구성될 수도 있다.

[0020] [0036] 센서들은 또한 연관/연관 해제에 대한 사용자의 바람을 표시하는 명시적 사용자 동작을 검출하도록 포함될 수 있다. 여기서는, 의도하지 않은 연관 해제들로부터 보호하기 위해, 연관 해제에 대한 명시적 동작이 연관에 대한 명시적 동작보다 더 의도적일 수도 있다. 예를 들어, 사용자들이 웨어러블 아이덴티티 관리기 디바이스(100)를 착용하고 있는 동안에는 일반적으로 관여할 수 없는 종류의 빠른 스피닝(spinning)을 검출하도록 자이로 센서가 포함될 수도 있으며, 이는 연관 해제를 야기할 것이다. 연관할 필요성을 식별하기 위해 동일한 또는 다른 움직임이 사용될 구성될 수 있다.

[0021] [0037] 웨어러블 아이덴티티 관리기 디바이스(100)는 또한 상태를 변경하려는 바람을 시그널링하도록 구성된 버튼을 포함할 수도 있다. 예를 들어, 10초 동안 이러한 버튼을 누름으로써, 웨어러블 아이덴티티 관리기 디바이스(100)는 연관 해제하도록 구성될 수도 있는 반면, 동일한 버튼을 행에서 3회 누르는 것은 웨어러블 아이덴티티 관리기 디바이스(100)가 아이덴티티를 획득하려고 시도하게 할 수도 있다.

[0022] [0038] 또한, 명시적 사용자 동작들이 암시적 사용자 동작들과 결합할 수도 있음이 고려된다. 예를 들어, 웨어러블 아이덴티티 관리기 디바이스(100)가 (예를 들어, 가속도계 데이터를 통해) 적어도 1분 동안 정지해 있는 것으로 간주되는 동안 10초 동안 버튼이 눌려진다면, 연관 해제가 수행될 수도 있다. 다음에, 펄스 센서가 심장 박동을 검출하는 동안 웨어러블 아이덴티티 관리기 디바이스(100)가 회전되거나 빠르게 흔들린다면, 아이덴티티 획득이 시작될 수도 있다.

[0023] [0039] 이러한 특정 예에서는, 웨어러블 아이덴티티 관리기 디바이스(100)가 팔찌로서 구성된다 하더라도, 다양한 웨어러블 구성들 중 임의의 구성이 고려된다고 인식되어야 한다. 예컨대, 목걸이 형태의 구성이 또한 고려되는데, 여기서 이러한 구성은 두 부분들: 스트링 컴포넌트 및 잠금 컴포넌트를 갖는다. 여기서, 사용자는 자신이 목걸이를 걸고 잠금을 닫으면, 아이덴티티가 선택되어 다른 엔티티들과 연속적인 인증 세션들 동안 이용 가능하게 되는 연관 모드에 들어가는 것이 가능함을 알고 있다. 마찬가지로, 사용자는 자신이 잠금을 열면, 먼저 다른 연관 세션을 통과하지 않고 인증에 목걸이를 사용하는 것이 더는 가능하지 않음을 알고 있다.

[0024] [0040] 추가 예에서, 웨어러블 아이덴티티 관리기 디바이스(100)가 벨트로서 구성된다. 사용자가 버클을 닫는다면, 웨어러블 아이덴티티 관리기 디바이스(100)는 아이덴티티 획득 모드로 설정된다. 더욱이, 벨트와 연관된 가속도계가 1분 동안 어떠한 움직임도 검출하지 않는다면, 웨어러블 아이덴티티 관리기 디바이스(100)는 아이덴티티 연관 해제 모드에 들어간다. 본 개시의 특정 양상에서, 웨어러블 아이덴티티 관리기 디바이스(100)는 슬레이브 디바이스와 함께 마스터 디바이스로서 동작하는 것이 고려된다. 예컨대, 웨어러블 아이덴티티 관리기 디바이스(100)는 벨트가 착용되어 있는지 여부를 결정하도록 구성되며, 벨트가 계속해서 착용되어 있지 않는 한 아이덴티티를 유지하도록 추가로 구성된 벨트일 수도 있다. 슬레이브 디바이스(예를 들어, 링, 스마트 워치, 팔찌 등)는 다음에, 의도를 결정하는데 이용될 수 있으며, 슬레이브 디바이스는 다양한 통신 프로토콜들(예를 들어, 블루투스 LE) 중 임의의 프로토콜을 통해 마스터 디바이스와 통신할 수도 있다. 여기서, 이러한 의도는 마스터 디바이스가 착용되어 있고 이에 따라 사용자와 연관되어 있는 동안 사용자가 슬레이브 디바이스 상에서 명시적 동작을 수행할 것을 요구함으로써 인증될 수도 있다. 예컨대, 의도는 마스터 디바이스가 착용되어 있는 동안 슬레이브 디바이스 상의 버튼을 누름으로써 유효화될 수도 있다. 버튼 유효화가 사실상 실행되었다는 표시를 슬레이브 디바이스로부터 수신하면, 마스터 디바이스는 다음에 다양한 요소들 중 임의의 요소를 기초로 거래를 추가로 인증할 수도 있다. 예컨대, 슬레이브 디바이스로부터 수신되며 버튼 유효화와 연관된 메타데이터(예를 들어, 버튼이 언제 눌려졌는지, 슬레이브 디바이스의 위치 데이터, 슬레이브 디바이스의 모션 데이터 등)가 동기화되거나 아니면 마스터 디바이스 데이터(예를 들어, 마스터 디바이스의 위치 데이터, 마스터 디바이스의 모션 데이터 등)와 비교되어 사용자를 인증할 수 있다.

[0025] [0041] 따라서 일반적으로, 웨어러블 아이덴티티 관리기 디바이스(100)가 전자 회로들을 포함하는, 팔찌들, 스마트 워치들, 반지들, 타투들, 벨트들, 의류 등과 같은 다양한 독립형 웨어러블 아이템들 중 임의의 아이템으로서 구성될 수 있다고 인식되어야 한다. 웨어러블 아이덴티티 관리기 디바이스(100)는 또한 예를 들어, 버튼 크기 배터리로서 구성되며 종래의 배터리들 대신 사용될 수 있다. 웨어러블 아이덴티티 관리기 디바이스(100)는 또한 프린트 가능 스티커들로서 구성되며, 시계들의 뒤판, 목걸이 상의 장식물 등과 같은 다양한 웨어러블 아이템들 중 임의의 아이템 상에 배치될 수 있다. 스티커들 및 패치들의 경우, 뒤판이 제거되면 아이덴티티 획득이 시작될 수 있는 반면, 스티커나 패치가 찢어지는 것으로 인해 회로가 손상되면 연관 해제가 시작될 수 있다.

[0026] [0042] 본 개시의 한 양상에서, 잠재적 도둑들로부터의 다양한 보호들이 쉽게 구현될 수도 있다. 예컨대, 개시된 기술이 널리 알려지면, 절도 미수자들은 그들이 전화 또는 다른 휴대용 디바이스를 포함하는 사람의 가방을 훔쳤고, 이 사람이 웨어러블 아이덴티티 관리기 디바이스를 인증에 사용한다면, 디바이스가 잠길 것임을 알 것

이다. 이는 벗겨지는 웨어러블 아이덴티티 관리기 디바이스를 빌리거나 훔칠 수도 있는 사람들에 의한 웨어러블 아이덴티티 관리기 디바이스의 바람직하지 않은 사용으로부터 보호한다.

[0027] [0043] 다른 예시적인 시나리오에서는, 목걸이가 뜯어질 때 회로가 차단될 것이므로, 희생자의 목에서 목걸이 형태의 웨어러블 아이덴티티 관리기 디바이스를 뜯어내는 것은 사용자 및 사용자의 계정으로부터 웨어러블 아이덴티티 관리기를 자동으로 연관 해제할 것임을 절도 미수자들이 아는 것이 바람직하다. 이는 목걸이를 벗는 것과 동일한 효과를 가질 것이다. 앞서 언급한 바와 같이, 이는 잠금을 포함하여 목걸이 전체에 전도성 도선을 구현함으로써 달성될 수 있다. 그러나 대안으로, 프로세서에서부터 잠금까지, 그리고 그 다음에 뒤로, 다음에 잠금의 다른 부분으로, 그리고 뒤로 이어지는 제 2 회로가 목걸이에 구현된다. 이 제 2 회로가 파손된 적이 있다면, 그것은 목걸이가 벗겨졌다는 표시가 아니라 목걸이가 뜯겨졌다는 표시이며, 이는 경보 신호를 시작하는데 사용될 수 있다. 경보 신호는 보안 회사나 경찰에게 송신될 수 있으며, 웨어러블 아이덴티티 관리기 디바이스와 연관된 임의의 모바일 디바이스에 봉쇄(lock-down) 지시를 전달함으로써, 자원들을 암호화하고 서비스 제공자들에게 경보를 발하는데 사용될 수도 있다. 다음에 자원들은 아래 더 상세히 설명되는 바와 같이, 암호화 키의 백업이 획득된 이후, 나중에만 액세스 가능할 수도 있다.

[0028] [0044] 또 다른 양상에서, 유괴 시나리오가 고려된다. 이러한 시나리오 내에서는, 충분한 동기가 부여된 사람이 사용자로부터 웨어러블 아이덴티티 관리기 디바이스를 연관 해제하지 않고 이를 물리적으로 제거할 수 있도록 웨어러블 아이덴티티 관리기 디바이스를 구성하는 것이 바람직할 것이다. 사실상, 이러한 구성은 웨어러블 아이덴티티 관리기 디바이스의 제거시 그것의 연관 해제를 피하기 위해 유괴범이 희생자를 해치는 것을 고려할 수도 있는 시나리오들에 대해 특히 바람직할 수도 있다. 다시 도 1을 참조하면, 이 문제에 대한 가능한 해결책이 본 명세서에서 개시된다. 즉, 이중 회로 구성이 고려되는데, 여기서는 잠금 메커니즘(130)을 잠금 해제함으로써 도선들(120) 사이의 주 접속이 끊어질 수 있고, 잠금 메커니즘(140)을 잠금 해제함으로써 도선들(120) 사이의 보조 접속이 끊어질 수 있다. 여기서, 잠금 메커니즘(140)을 여는 것에 의해, 사용자가 도선들(120) 사이의 주 접속을 파손하지 않으면서 웨어러블 아이덴티티 관리기 디바이스(100)를 제거할 수 있는데, 이는 웨어러블 아이덴티티 관리기 디바이스(100)와 사용자 간의 연관을 보존한다(이로써 잔인한 공격들에 대한 보안을 제공함). 본 개시의 한 양상에서, 잠금 메커니즘(140)은 잠금 메커니즘(130)보다 열기가 훨씬 더 어렵다. 대안으로, 잠금 메커니즘(140)은 잠금 해제를 허용하지만 이후의 잠금은 허용하지 않도록 설계될 수 있다. 더욱이, 잠금 메커니즘(140)의 개별 컴포넌트들은 서로 옆에 장착될 수 있어, 이들은 하나의 그리고 동일한 물리적 잠금 내에 일정하게 접촉한다. 이렇게, 전체 회로가 종래와 같아 보이는 목걸이, 팔찌 또는 손목시계 밴드에 포함될 수 있어, 2개의 개별 스트랜드(strand)들 또는 2개의 서로 다른 잠금들을 피할 수 있다.

[0029] 예시적인 웨어러블 아이덴티티 인증 시스템

[0030] [0045] 이제 도 3을 참조하면, 본 개시의 한 양상에 따라 웨어러블 아이덴티티 관리기 디바이스를 통해 사용자의 인증을 가능하게 하는 예시적인 환경이 제공된다. 예시된 바와 같이, 환경(300)은 웨어러블 아이덴티티 관리기 디바이스(320)를 포함하는데, 이는 네트워크(310)(예를 들어, 인터넷, 피어 투 피어 네트워크 등)를 통해 페어링 디바이스(330) 및 외부 디바이스(340)에 연결될 수 있다. 여기서, 웨어러블 아이덴티티 관리기 디바이스(320)는 무선 가능 디바이스로서 구성될 수 있음이 고려되며, 여기서 웨어러블 아이덴티티 관리기 디바이스(320)는 일반적으로 본 명세서에서 개시된 웨어러블 아이덴티티 관리기 디바이스들 중 임의의 웨어러블 아이덴티티 관리기 디바이스와 유사하다. 이러한 특정 예의 경우, 웨어러블 아이덴티티 관리기 디바이스(320)가 사용자와 적절히 연관되고 그에 부착된다고 가정하면, 웨어러블 아이덴티티 관리기 디바이스(320)는 외부 디바이스(340)에 인증 데이터를 무선으로 송신함으로써 다양한 타입들의 엔티티들(예를 들어, 판매 시점 디바이스들, 도로 요금소들, 금융 기관 웹사이트들 등) 중 임의의 엔티티에 대응하는 외부 디바이스(340)에 대한 사용자 인증을 가능하게 할 수 있다. 대안으로, 외부 디바이스(340)에 직접 인증 데이터를 송신하기보다는, 웨어러블 아이덴티티 관리기 디바이스(320)는 이러한 인증 데이터를 페어링 디바이스(330)(예를 들어, 스마트폰, 개인용 컴퓨터 등)에 송신하도록 구성될 수 있으며, 여기서 이러한 데이터는 아래 보다 상세히 논의되는 바와 같이, 웨어러블 아이덴티티 관리기 디바이스(320) 및/또는 페어링 디바이스(330)에 상주할 수도 있다.

[0031] 예시적인 웨어러블 아이덴티티 인증 프로세스

[0032] [0046] 다음에 도 4를 참조하면, 본 개시의 한 양상에 따라 웨어러블 아이덴티티 관리기 디바이스의 이용을 가능하게 하기 위한 예시적인 프로세스를 예시하는 흐름도가 제공된다. 예시된 바와 같이, 프로세스(400)는 본 명세서의 한 양상에 따라 다양한 타입들의 컴퓨팅 디바이스들(예를 들어, 웨어러블 아이덴티티 관리기 디바이스(320), 페어링 디바이스(330) 및/또는 외부 엔티티(340)) 중 임의의 디바이스 내에서 수행될 수 있는 일련의 동

작들을 포함한다. 예컨대, 일련의 동작들을 구현하기 위해 프로세스를 이용하여 컴퓨터 판독 가능 저장 매체 상에 저장된 컴퓨터 실행 가능 명령들을 실행함으로써 프로세서(400)가 구현될 수 있다. 다른 양상에서, 적어도 하나의 컴퓨터로 하여금 프로세스(400)의 동작들을 구현하게 하기 위한 코드를 포함하는 컴퓨터 판독 가능 저장 매체가 고려된다.

[0033] [0047] 예시된 바와 같이, 프로세스(400)는 웨어러블 아이덴티티 관리기 디바이스에 사용자의 아이덴티티를 확인해 주도록 사용자가 웨어러블 아이덴티티 관리 디바이스와 연관되는 동작(410)에서 시작된다. 이러한 연관 프로세스는 웨어러블 아이덴티티 관리 디바이스가 사용자의 손목 둘레나, 사용자의 목 둘레에 배치되거나, 아니면 사용자에게 착용되거나 사용자와 물리적으로 연관될 때 시작될 수 있다. 더욱이, 웨어러블 아이덴티티 관리기 디바이스는 이것이 예를 들어, 걸쇠, 잠금 또는 버클이 닫힘으로써 사용자에게 잠재적으로 착용되게 되는 상황을 검출한다. 반대로, 웨어러블 아이덴티티 관리기 디바이스가 벗겨질 때(예를 들어, 걸쇠, 잠금 또는 버클을 개방함으로써 사용자의 손목이나 목으로부터 웨어러블 아이덴티티 관리기 다비이스를 제거할 때) 연관 해제 프로세스가 시작된다.

[0034] [0048] 이전에 언급한 바와 같이, 웨어러블 아이덴티티 관리기 디바이스는 이것이 닫힐 때(즉, 웨어러블 아이덴티티 관리기 디바이스가 잠긴 구성인 동안 도선들의 내부 회로가 닫힐 때) 일정한 전기 접촉을 제공하는 잠금 메커니즘을 포함할 수 있다. 더욱이, 잠금이 열리자마자, 회로는 파손된다. 이는 언제 웨어러블 아이덴티티 관리기 디바이스가 사용자에 의해 잠재적으로 착용되게 되는지- 즉, 언제 걸쇠가 닫히는지 - 그리고 언제 이것이 사용자로부터 제거되고 있는지 - 즉, 언제 걸쇠가 열리는지 -를 검출하는데 사용된다. 잠금을 짧게 열었다가 이를 닫는 동안 웨어러블 아이덴티티 관리기를 계속해서 착용하는 것이 가능한 것처럼, 웨어러블 아이덴티티 관리기를 착용하지 않고 걸쇠는 닫는 것이 가능하지만, 그렇더라도 잠금은 웨어러블 아이덴티티 관리기 디바이스가 언제 상태들을 - 잠재적으로 착용된 상태에서 착용되지 않을 것 같은 상태로 - 변경하고 있는지를 결정하는 것을 가능하게 할 수 있다. 잠금이 닫힐 때 접속을 개선하도록 자성 컴포넌트를 갖는 잠금; 또는 대안으로, 나사를 돌림으로써 열리고 닫히는 나사 잠금을 사용하는 것이 또한 가능한데, 여기서 나사 부분은 전기를 전도하는 물질로 만들어진다.

[0035] [0049] 대안적인 구현에서, 걸쇠는 자석 및 자기장의 변화들을 검출하는 회로를 포함하는데, 걸쇠가 닫히면 자기장이 발생한다. 해당 기술분야에서 통상의 지식을 가진 자는 또 다른 변형들이 예상된다고 인식할 것이며, 여기서 잠금 또는 걸쇠가 열려 있거나 열리게 되는 것 그리고/또는 닫혀 있거나 닫히게 되는 것을 검출한다. 다른 대안적인 접근 방식들은 웨어러블 아이덴티티 관리기 디바이스가 언제 사용자와 물리적으로 연관되어 있고 그리고/또는 연관 해제되어 있는지를 결정하도록 구성된 센서들을 포함한다. 가능한 구현들은 압력 센서들, 온도 센서들, 심박 센서들, 및 사람에게 가능성 있는 근접도를 결정하는데 사용될 수 있는 비슷한 타입들의 센서들을 사용하는 것을 포함한다.

[0036] [0050] 웨어러블 아이덴티티 관리기 디바이스를 사용자의 손목에 부착하면, 사용자는 다양한 방식들 중 임의의 방식으로 연관 프로세스를 완료할 수 있다. 예컨대, 사용자는 웨어러블 아이덴티티 관리기 디바이스 상의 사용자 인터페이스를 통해 비밀번호를 입력하도록 요구될 수도 있다. 그러나 웨어러블 아이덴티티 관리기 디바이스가 사용자 인터페이스를 갖지 않는다면, 동작(420)에서 사용자 인터페이스를 갖지 않는 페어링 디바이스에 웨어러블 아이덴티티 관리기 디바이스를 페어링함으로써 연관이 완료될 수 있다. 이러한 페어링 프로세스는 예를 들어, 모바일 디바이스, 개인용 컴퓨터, 스크린을 가진 한 쌍의 유리들, 또는 스크린, 키보드, 프린터, 버튼, 마이크로폰, 스피커, 판매 시점 디바이스 또는 도어락을 제어하는 컴퓨터와 같은 사용자 입력/출력(I/O: input/output) 메커니즘, 또는 이러한 사용자 I/O 컴포넌트들의 결합을 가진 다른 디바이스를 포함하는 다양한 타입들의 디바이스들 중 임의의 디바이스와 웨어러블 아이덴티티 관리기 디바이스를 연관시킬 수 있다. 단순히 하기 위해, 이러한 디바이스는 아래에서 간혹 "페어링 디바이스" 및/또는 "연관 디바이스"로 지칭된다.

[0037] [0051] 프로세스(400)는 거래를 위해 사용자가 인증되는 동작(430)에서 끝난다. 본 개시의 특정 양상에서, 이러한 인증 프로세스는 사용자 동작에 의해 가능해짐이 고려된다. 예컨대, 인증 프로세스가 시작되면, 웨어러블 아이덴티티 관리기 디바이스는 내장 라디오 송신기들을 사용하여 연관된 페어링 디바이스와 통신할 수 있다. 웨어러블 아이덴티티 관리기 디바이스가 다수의 디바이스들과 페어링되었다면, 예를 들어, 사용자 의도 표시 또는 근접도를 기초로 하나가 선택된다. 예를 들어, 도 5에 예시된 바와 같이, 이러한 의도는 웨어러블 아이덴티티 관리기 디바이스(500)와 페어링 디바이스(510) 둘 다 동기화된 방식으로 이동시키는 것을 포함할 수도 있다. 다른 고려되는 표시들은 웨어러블 아이덴티티 관리기 디바이스(500)와 페어링 디바이스(510)를 함께 탭하는 것, 이들을 매우 가까이 배치하는 것 등을 포함할 수도 있다. 일단 페어링 디바이스가 선택되었다면, 페어링 디바이스에 의해 방사되는 신호; 예컨대 촉각 피드백, 이미지의 디스플레이, 또는 사운드의 발산을 통해 페어링 확

정이 사용자에게 전달될 수도 있다.

[0038] [0052] 본 개시의 다른 양상에서, 비밀번호 관리기의 연결이 고려되며, 여기서 이러한 연결은 앞서 설명한 바와 같이, 웨어러블 아이덴티티 관리기 디바이스가 페어링 디바이스를 선택한 이후에 수행될 수도 있다. 한 구현에서, 페어링 디바이스는 비밀번호 관리기를 포함하며, 페어링 디바이스의 선택은 웨어러블 아이덴티티 관리기 디바이스로부터 페어링 디바이스로 잠금 해제 신호가 전송되게 하는데, 그 후 비밀번호 관리기는 인증의 콘텍스트를 결정하여, 적용 가능한 경우에는 콘텍스트와 연관된 사용자 아이덴티티 및 크리덴셜의 검색을 수행한다. 예를 들어, 콘텍스트는 연관된 도메인을 포함하는, 금융 서비스 제공자에 대한 로그인 화면을 포함할 수도 있다. 비밀번호 관리기는 적어도 하나의 사용자 프로파일을 포함하는데, 여기서 사용자 프로파일은 (집에 있는 사용자; 일을 하고 있는 사용자 등과 같은) 하나의 사용자 또는 하나의 페르소나와 연관된다. 웨어러블 아이덴티티 관리기 디바이스와 연관된 아이덴티티를 기초로, 하나 또는 그보다 많은 사용자 프로파일들이 선택되고, 지리적 위치, 사용자 입력, 네트워크 식별자들 등과 같은 콘텍스트 정보를 기초로, 선택된 하나 또는 그보다 많은 사용자 프로파일들 중의 추가 선택이 수행된다. 다음에, 비밀번호 관리기는 로그인 화면의 도메인과 같은 콘텍스트를 기초로, 어떤 계정이 선택되어야 하는지를 결정한다. 대안으로, 사용자는 페어링 디바이스와 연관된 사용자 인터페이스를 사용하여 이를 선택한다.

[0039] [0053] 계정이 선택되었다면, 연관된 사용자명과 크리덴셜이 로그인 또는 다른 인증 거래를 수행하는데 사용된다. 크리덴셜의 일례는 비밀번호이고; 다른 예는 개인 식별 번호(PIN)이고; 다른 예는 암호화 키이며; 또 다른 예는 힌트 질문(challenge question)들 및 연관된 답변들의 수집이다. 예시적인 구현에서는, 로그인 세션이 완료된 후, 세션은 다른 연산 엔티티, 예컨대 데스크톱 컴퓨터, 도어락 또는 판매 시점 디바이스로 전달되고, 여기서 사용자가 세션을 완료하고 로그아웃을 시작한다. 다른 구현에서, 세션은 전달 없이 페어링 디바이스 상에서 완료된다.

[0040] [0054] 대안으로, 웨어러블 아이덴티티 관리기 디바이스는 비밀번호 관리기를 포함하며, 앞서 설명한 바와 같이 로그인을 수행한다. 이후, 세션은 선택적으로 다른 연산 디바이스로 전달되고, 또는 어떤 경우들에는 크리덴셜 또는 잠금 해제 신호가 웨어러블 아이덴티티 관리기 디바이스로부터 페어링 디바이스로 전달된다.

[0041] [0055] 또 다른 양상에서, 웨어러블 아이덴티티 관리기 디바이스는 페어링 디바이스 대신 도어락 또는 판매 시점 레지스터와 같은 등록된 스테이션으로 전달한다. 이러한 구현 내에서, 등록된 스테이션은 웨어러블 아이덴티티 관리기 디바이스와 페어링된 연산 디바이스와 연관된다. 잠금 해제 신호는 재전송 공격(replay attack)들을 차단하도록; 신호들의 발생기, 예컨대 의사 랜덤 시퀀스 발생기 또는 이러한 함수의 근사치에 의해 발생되는 비트들의 시퀀스를 포함할 수도 있다. 동일한 시퀀스 또는 그것의 선택된 부분들이 웨어러블 아이덴티티 관리기 디바이스 및 등록된 스테이션과 연관된 검증기에 의해 발생될 수도 있다. 인증 토큰과 검증기를 어떻게 동기화하는지는 해당 기술분야에 잘 알려져 있으며, 이러한 기술들은 웨어러블 아이덴티티 관리기 디바이스와 등록된 스테이션과 연관된 검증기를 동기화하는데 사용될 수 있다.

[0042] [0056] 서로 다른 타입들의 승인을 시그널링하기 위한 서로 다른 사용자 관여의 사용이 또한 고려된다. 예컨대, 제 1 타입의 사용자 관여는 전혀 관여하지 않는 것이다. 이것의 제 1 예는 사용자가 회사 건물에 허용되기 전에 사용자의 아이덴티티가 결정되는 기업 시나리오이다. 제 2 예는 사용자가 자신의 차를 유료 도로로 운전할 때 통행료들에 대한 것이다. 여기서, 요금소는 사용자가 접근할 때 사용자의 전화와 연락을 설정하고 있으며, 사용자의 전화가 사용자의 웨어러블 아이덴티티 관리기 디바이스와 상호 작용하여 사용자의 아이덴티티를 확인한다. 다음에, 사용자가 액세스에 대해 과금되어야 하는 도로의 정확한 구간을 결정하기 위해 사용자가 유료 도로를 벗어날 때 동일한 프로세스가 수행될 수 있다. 사용자가 웨어러블 아이덴티티 관리기 디바이스, 전화기 또는 다른 것을 갖지 않는다면, 프로토콜이 성공적으로 완료되지 않는다. 그러면, 대안적인 방식으로, 예를 들면 자동차 번호판에 대해 찍힌 사진을 사용하여 적절한 사용자에게 과금함으로써 요금이 청구될 수 있다.

[0043] [0057] 제 2 타입의 사용자 관여는 로그인을 시그널링하는 것이다. 예컨대, 도 5에 예시된 것과 같이, 페어링 디바이스와 웨어러블 아이덴티티 관리기 디바이스를 동시에 움직이게 하는 것이 사용될 수 있다. 여기서, 사용자는 페어링 디바이스와 웨어러블 아이덴티티 관리기 디바이스 모두에 대해 충분히 강한 모션이 등록될 때까지 계속해서 모션들을 해야 할 수도 있으며, 이러한 두 모션들은 서로 강력하게 상관한다고 결정되었다. 로그인과 연관된 예시적인 모션은 수평 스와이프(swipe)인데, 이는 일부 전화기들이 현재 어떻게 잠금 해제되는지를 흉내낸다.

[0044] [0058] 제 3 타입의 사용자 관여는 구매 승인을 시그널링하는 것이다. 일례는 손으로 미리 정해진 위-아래-위

흔들기 뒤에, 페어링 디바이스 상의 승인 버튼을 누르는 것이다. 사용자들에게 서로 다른 타입들의 동작들의 차이를 분명히 보여주는 것을 돕고, 어디가 유리한지의 확인들을 생성하는 것을 돕고, 이것이 명시적 확인을 기록하는 것보다 더 중요한 경우에 사용자 경험을 단순화하는 것을 돕기 위한 서로 다른 사용자 관여 타입들의 사용을 포함하여 추가 타입들의 사용자 관여가 추가될 수 있다. 지불과 연관된 다른 예시적인 모션은 수직 스와이프인데, 이는 신용 카드를 읽히는 것을 흉내낸다.

[0045] [0059] 본 개시의 추가 양상에서, 웨어러블 아이덴티티 관리기 디바이스는 자원들을 복호화하는데 사용되는 키들을 제공할 수 있다. 예를 들어, 사용자는 디바이스가 움직이지 않거나 갑작스러운 이벤트가 발생할 때, 예컨대 디바이스가 특이한 가속을 경험할 때 사용자의 디바이스의 전체 메모리 계층 구조를 자동으로 암호화되게 하는 것을 택할 수도 있다. 다른 사용자는 디바이스가 꺼질 때 또는 임계량의 시간을 초과하는 기간 동안 디바이스가 사용되지 않을 때만 메일 폴더 및 주소록과 같은 선택된 부분들만이 자동으로 암호화되게 하는 것을 택할 수도 있다. 암호화된 메모리 영역들에 액세스하기 위한 유일한 방법은 웨어러블 아이덴티티 관리기 디바이스에 의해 유지되며 제어된 조건들 하에서만 해제되는 키로 그러한 영역들을 복호화하는 것일 수도 있다. 예컨대, 잠금 해제될 디바이스가 그 존재 안에 있을 때만, 그리고 사용자가 디바이스의 잠금 해제에 특정된 흔들기(waving) 모션을 수행하는 경우에만 키가 해제되는 규칙이 구현될 수도 있다. 이는 도난 및 원치 않는 사용으로부터 페어링 디바이스들을 보호한다.

[0046] [0060] 웨어러블 아이덴티티 관리기 디바이스는 이것이 사용되는 처음에는 장기 액세스 크리덴셜에 연관될 수도 있다고 인식되어야 하는데, 여기서 이러한 크리덴셜은 웨어러블 아이덴티티 관리기 내에 저장될 수도 있다. 웨어러블 아이덴티티 관리기 디바이스가 페어링 디바이스와 연관될 때, 페어링 디바이스의 사용자는 장기 액세스 크리덴셜을 입력하는데, 이는 웨어러블 아이덴티티 관리기 디바이스에 (예를 들어, 일반적으로 블루투스, 근접장 또는 WiFi의 보안 동작 모드들에 의해 제공되는 것과 같은 보안 접속을 통해) 전송된다. 송신된 크리덴셜은 저장된 크리덴셜과 비교되며, 이들이 매칭하는지 여부가 결정된다. 매칭이 존재한다면, 웨어러블 아이덴티티 관리기 디바이스는 자신을 페어링 디바이스와 연관시키라는 요청을 수락한다. 웨어러블 아이덴티티 관리기 디바이스는 선택적으로 다수의 독립적인 장기 액세스 크리덴셜들을 저장하는데, 이러한 크리덴셜들은 서로 다른 사용자들과 연관되고; 크리덴셜들의 대응하는 페르소나 또는 저장된 세트가 이러한 장기 크리덴셜들 중 하나를 사용한 정확한 인증에 의해 액세스 가능해진다. 비밀번호, PIN 또는 비슷한 크리덴셜이 장기 크리덴셜로서 사용될 수 있다. 대안으로, 생체 인식 인증을 지원하도록 생체 인식 템플릿이 저장될 수 있다. 성공적인 연관 이후, 그러나 대응하는 연관 해제 이전에, 사용자는 다른 프로파일 및 연관된 장기 크리덴셜을 추가하도록; 또는 장기 크리덴셜을 수정하거나 삭제하도록 페어링 디바이스로부터 웨어러블 아이덴티티 관리기 디바이스로 커맨드를 전송할 수 있다.

[0047] [0061] 본 개시의 또 다른 양상에서, 웨어러블 아이덴티티 관리기 디바이스와 연관된 하드웨어는 생체 인식 센서, 예컨대 지문 센서, 사용자의 음성을 식별하는데 사용되는 마이크로폰, 또는 다른 이러한 센서를 포함한다. 일반적인 상업적 전개에서는, 동작 속도와 에러율들의 감소 사이의 균형(tradeoff)은 흔히 상대적으로 낮은 보안 및 높은 센서 비용을 야기하는 반면, 설명되는 개시는 빈번한 사용자 인증을 요구하는 것이 아니라, 웨어러블 아이덴티티 관리기 디바이스가 사용자와 연관되고 있는 연관 단계에서만 요구할 것이다. 따라서 생체 인식 센서 판독과 저장된 템플릿 사이의 맞춤에 대해 훨씬 더 높은 요건들을 두는 것이 가능하다. 그 결과, 여전히 우수한 유용성을 유지하면서, 에러율이나 생체 인식 하드웨어의 비용, 또는 둘 다를 감소시킬 수 있는데, 사용자가 인증할 필요가 있을 때는 사용자가 웨어러블 아이덴티티 관리기 디바이스를 착용하기 시작할 때뿐이다 사용자가 동작하는데 눈 깜짝할 시간보다 더 오래 걸린다면, 규칙적인 생체 인식 인증이 바람직하지 않을 수도 있는 반면, 일반적인 사용자는 이러한 콘텍스트에서 훨씬 더 많은 수반되는 인증을 용인할 수도 있다. 이는 연관이 덜 빈번하므로, 그리고 이는 일반적으로, 사용자가 거래의 완료와 같은 목표에 도달하기 위해 서두르는 시점에 수행되지 않기 때문 둘 다이다. 동일한 이유로, 설명한 생체 인식 방법 대신, 복잡한 지식 기반 또는 리콜 기반 인증 방법을 사용하는 것이 용인될 수도 있는데, 따라서 이는 증가된 보안, 또는 일반적인 비밀번호들이 하는 것보다 더 높은 리콜 레이트들을 갖는 인증 방법들의 선택을 허용한다.

[0048] [0062] 다른 고려되는 구현에서, 웨어러블 아이덴티티 관리기 디바이스는 사용자 아이덴티티 대신 계정 또는 필명과 연관되거나, 본 명세서의 다른 구현들에 대해 설명한 것과 같이 사용자 동작들에 의해 지출되거나 커밋(commit)되는 자금들의 표현을 전달한다.

[0049] 예시적인 하드웨어 구현

[0050] [0063] 다음에 도 6을 참조하면, 처리 시스템(614)을 이용하는 웨어러블 아이덴티티 관리기 디바이스(600)에 대

한 예시적인 하드웨어 구현을 예시하는 개념도가 제공되며, 여기서 웨어러블 아이덴티티 관리기 디바이스(600)는 예를 들어, 도 1 - 도 5를 참조로 논의한 웨어러블 아이덴티티 관리기 디바이스들 중 임의의 웨어러블 아이덴티티 관리기 디바이스를 포함하는 임의의 무선 가능 디바이스 내에 구현될 수도 있다. 본 개시의 다양한 양상들에 따르면, 엘리먼트나 엘리먼트의 임의의 부분 또는 엘리먼트들의 임의의 결합은 하나 또는 그보다 많은 프로세서들(604)을 포함하는 처리 시스템(614)으로 구현될 수 있다. 프로세서들(604)의 예들은 마이크로프로세서들, 마이크로컨트롤러들, 디지털 신호 프로세서(DSP: digital signal processor)들, 필드 프로그래밍 가능한 게이트 어레이(FPGA: field programmable gate array)들, 프로그래밍 가능한 로직 디바이스(PLD: programmable logic device)들, 상태 머신들, 게이티드(gated) 로직, 이산 하드웨어 회로들, 및 본 개시 전반에 걸쳐 설명되는 다양한 기능을 수행하도록 구성된 다른 적당한 하드웨어를 포함한다. 즉, 웨어러블 아이덴티티 관리기 디바이스(600)에서 이용되는 것과 같은 프로세서(604)는 아래 설명되며 도 6에 예시된 프로세스들 중 임의의 하나 또는 그보다 많은 프로세스를 구현하는 데 사용될 수도 있다.

[0051] [0064] 이 예에서, 처리 시스템(614)은 일반적으로 버스(602)로 제시된 버스 아키텍처로 구현될 수도 있다. 버스(602)는 처리 시스템(614)의 특정 애플리케이션 및 전체 설계 제약들에 따라, 서비스 지향 아키텍처(SOA: service oriented architecture) 버스를 포함하여 많은 수의 상호 접속 버스들 및 브리지들을 포함할 수 있다. 버스(602)는 (일반적으로 프로세서(604)로 표현되는) 하나 또는 그보다 많은 프로세서들, 메모리(605) 및 (일반적으로 컴퓨터 판독 가능 매체(606)로 표현되는) 컴퓨터 판독 가능 매체들을 포함하는 다양한 회로들을 서로 링크한다. 버스(602)는 또한, 해당 기술분야에 잘 알려져 있고 이에 따라 더는 설명되지 않을, 타이밍 소스들, 주변 장치들, 전압 조정기들 및 전력 관리 회로들과 같은 다양한 다른 회로들을 링크할 수도 있다. 버스 인터페이스(608)는 버스(602)와 트랜시버(610) 사이에 인터페이스를 제공한다. 트랜시버(610)는 송신 매체를 통해 다양한 다른 장치와 통신하기 위한 수단을 제공한다. 장치의 특성에 따라, 사용자 인터페이스(612)(예를 들어, 키패드, 디스플레이, 스피커, 마이크로폰, 조이스틱)가 또한 제공될 수도 있다.

[0052] [0065] 본 개시의 한 양상에서, 컴퓨터 판독 가능 매체(606)는 도시된 바와 같이, 웨어러블 아이덴티티 관리기 디바이스를 통해 사용자의 인증을 가능하게 하기 위한 다양한 명령들(606a 및/또는 606b)을 포함하도록 구성된다. 비슷한 양상에서, 이러한 인증은 도시된 바와 같이, 회로들(620 및/또는 630) 중 임의의 회로에 프로세서(604)를 연결함으로써 하드웨어를 통해 대신 구현될 수 있다. 더욱이, 인증은 명령들(606a 및/또는 606b)의 임의의 결합뿐만 아니라 회로들(620 및/또는 630)의 임의의 결합에 의해서도 수행될 수 있음이 고려된다. 본 개시의 특정 양상에서, 명령들(606a) 및 회로(620)는 웨어러블 아이덴티티 관리기 디바이스(600)가 사용자에 의해 착용되어 있는지 여부를 기초로 사용자와 웨어러블 아이덴티티 관리기 디바이스(600) 간의 연관 상태를 결정하도록 구성된 검출기 컴포넌트 쪽으로 향해져 있는 반면, 명령들(606b) 및 회로(630)는 사용자 인증의 결정을 가능하게 하도록 구성된 결정 컴포넌트 쪽으로 향해져 있다.

[0053] [0066] 이를 위해, 웨어러블 아이덴티티 관리기 디바이스(600)는 다양한 방식들 중 임의의 방식으로 사용자 인증들을 가능하게 하도록 구성될 수도 있다고 인식되어야 한다. 제 1 양상에서, 이러한 인증은 웨어러블 아이덴티티 관리기 디바이스(600)에 의해 추적된 모션 데이터를 이용하여 사용자의 아이덴티티를 검증(예를 들어, 사용자의 손을 흔들어 자동 판매기 거래를 검증) 하는 것을 포함한다. 이러한 특정 구현의 경우, 명령들(606b) 및/또는 회로(630)는 웨어러블 아이덴티티 관리기 디바이스(600)의 움직임과 연관된 모션 데이터를 모니터링하도록 구성된 센서 컴포넌트를 더 포함할 수도 있다. 트랜시버 컴포넌트(610)는 다음에, 다른 인증 데이터(예를 들어, 지불 정보)와 함께 연관 상태를 기초로 모션 데이터를 (예를 들어, 자동 판매기에) 송신하도록 구성될 수도 있다.

[0054] [0067] 제 2 양상에서, 사용자 인증은 페어링 디바이스를 통해(예를 들어, 페어링 디바이스(330)를 통해) 고려된다. 여기서, 이러한 페어링 디바이스는 프록시 디바이스로서의 역할을 할 수도 있음이 고려되며, 여기서 웨어러블 아이덴티티 관리기 디바이스(600)에 의해 페어링 디바이스에 제공되는 인증 데이터는 외부 디바이스(예를 들어, PoS 단말)에 의해 페어링 디바이스를 통해 요청되는 사용자 인증을 가능하게 한다. 이러한 구현의 경우, 명령들(606b) 및/또는 회로(630)는 웨어러블 아이덴티티 관리기 디바이스(600)를 페어링 디바이스와 페어링하도록 구성된 페어링 컴포넌트를 더 포함할 수도 있다. 트랜시버 컴포넌트(610)는 다음에, 연관 상태를 기초로 인증 데이터(예를 들어, 지불 정보)를 페어링 디바이스에 송신하도록 구성될 수도 있다.

[0055] [0068] 도 6의 나머지 엘리먼트들을 다시 참조하면, 프로세서(604)는 컴퓨터 판독 가능 매체(606) 상에 저장된 소프트웨어의 실행을 비롯하여 버스(602)의 관리 및 일반적인 처리를 담당한다고 인식되어야 한다. 소프트웨어는 프로세서(604)에 의해 실행될 때, 처리 시스템(614)으로 하여금, 임의의 특정 장치에 대해 아래에 설명되는 다양한 기능들을 수행하게 한다. 컴퓨터 판독 가능 매체(606)는 또한 소프트웨어 실행시 프로세서(604)에 의해

조작되는 데이터를 저장하기 위해 사용될 수도 있다.

[0056] [0069] 처리 시스템의 하나 또는 그보다 많은 프로세서들(604)은 소프트웨어를 실행할 수 있다. 소프트웨어는, 소프트웨어, 펌웨어, 미들웨어, 마이크로코드, 하드웨어 기술 언어 또는 다른 식으로 지칭되든지 간에, 명령들, 명령 세트들, 코드, 코드 세그먼트들, 프로그램 코드, 프로그램들, 서브프로그램들, 소프트웨어 모듈들, 애플리케이션들, 소프트웨어 애플리케이션들, 소프트웨어 패키지들, 루틴들, 서브루틴들, 객체들, 실행 파일(executable)들, 실행 스레드들, 프로시저들, 함수들 등을 의미하는 것으로 광범위하게 해석될 것이다. 소프트웨어는 컴퓨터 판독 가능 매체(606) 상에 상주할 수 있다. 컴퓨터 판독 가능 매체(606)는 비-일시적 컴퓨터 판독 가능 매체일 수 있다. 비-일시적 컴퓨터 판독 가능 매체는 예로서, 자기 저장 디바이스(예를 들어, 하드 디스크, 플로피 디스크, 자기 스트립), 광 디스크(예를 들어, 콤팩트 디스크(CD: compact disc) 또는 디지털 다기능 디스크(DVD: digital versatile disc)), 스마트카드, 플래시 메모리 디바이스(예를 들어, 카드, 스틱 또는 키 드라이브), 랜덤 액세스 메모리(RAM: random access memory), 판독 전용 메모리(ROM: read only memory), 프로그래밍 가능한 ROM(PROM: programmable ROM), 소거 가능한 PROM(EPROM: erasable PROM), 전기적으로 소거 가능한 PROM(EEPROM: electrically erasable PROM), 레지스터, 착탈식 디스크, 및 컴퓨터에 의해 액세스 및 판독될 수 있는 소프트웨어 및/또는 명령들을 저장하기 위한 임의의 다른 적당한 매체를 포함한다. 컴퓨터 판독 가능 매체는 또한 예로서, 반송파, 송신선, 및 컴퓨터에 의해 액세스 및 판독될 수 있는 소프트웨어 및/또는 명령들을 송신하기 위한 임의의 다른 적당한 매체를 포함할 수도 있다. 컴퓨터 판독 가능 매체(606)는 처리 시스템(614) 내에 상주하거나, 처리 시스템(614) 외부에 있을 수도 있고, 또는 처리 시스템(614)을 포함하는 다수의 엔티티들에 걸쳐 분산될 수도 있다. 컴퓨터 판독 가능 매체(606)는 컴퓨터 프로그램 물건으로 구현될 수 있다. 예로서, 컴퓨터 프로그램 물건은 패키징 재료들에 컴퓨터 판독 가능 매체를 포함할 수 있다. 해당 기술분야에서 통상의 지식을 가진 자들은 전체 시스템에 부과된 전체 설계 제약들 및 특정 애플리케이션에 따라 본 개시 전반에 제시된 설명되는 기능을 어떻게 최상으로 구현할지를 인식할 것이다.

[0057] [0070] 다음에 도 7을 참조하면, 검출기 회로(620) 및 검출기 명령들(606a) 각각은 복수의 서브컴포넌트들 중 임의의 서브컴포넌트를 통해 웨어러블 아이덴티티 관리기 디바이스(600)와 사용자의 연관 상태 확인을 가능하게 할 수 있다고 인식되어야 한다. 예컨대, 검출기 회로(620)는 연관 하위 회로(710) 및 연관 해제 하위 회로(720)를 포함할 수 있는 반면, 검출기 명령들(606a)은 연관 명령들(712) 및 연관 해제 명령들(722)을 포함할 수 있다. 여기서, 연관 하위 회로(710) 및 연관 명령들(712)은 연관 프로시저를 통해 사용자를 웨어러블 아이덴티티 관리기 디바이스(600)와 처음에 연관시키는 쪽으로 향해져 있다. 이러한 연관 프로시저는 웨어러블 아이덴티티 관리기 디바이스(600)를 통해 직접(예를 들어, 사용자 인터페이스를 통해) 또는 연관 디바이스를 통해(예를 들어, 페어링 디바이스(330)를 통해 수행될 수 있음이 고려된다. 본 개시의 특정 양상에서, 연관 하위 회로(710) 및/또는 연관 명령들(712)은 웨어러블 아이덴티티 관리기 디바이스(600) 및/또는 연관 디바이스를 통해 사용자에 의해 입력된 비밀번호와 국소 저장된 비밀번호를 매칭시키도록 구성될 수도 있다. 본 개시의 다른 양상에서, 연관 하위 회로(710) 및/또는 연관 명령들(712)은 웨어러블 아이덴티티 관리기 디바이스(600)의 연관 움직임에 대응하는 데이터를 연관 디바이스의 움직임에 대응하는, 연관 디바이스로부터 수신된 데이터와 매칭시키도록 구성될 수도 있다. 대안으로, 웨어러블 아이덴티티 관리기 디바이스(600)의 움직임을 연관 디바이스의 움직임과 비교하기보다는, 웨어러블 아이덴티티 관리기 디바이스(600)의 움직임은 미리 결정된 연관 움직임(예를 들어, 웨어러블 아이덴티티 관리기 디바이스(600)를 좌우로 흔드는 것)에 대응하는 내부적으로 저장된 데이터와 비교될 수 있다.

[0058] [0071] 다음에 도 8을 참조하면, 웨어러블 아이덴티티 관리기 디바이스와 사용자의 연관을 가능하게 하기 위한 예시적인 프로세스(800)를 예시하는 흐름도가 제공된다. 본 개시의 한 양상에서, 프로시저(800)는 웨어러블 아이덴티티 관리기 디바이스(600)에 의해 연관 하위 회로(710) 및/또는 연관 명령들(712)을 통해 수행될 수 있음이 고려된다. 프로시저(800)는 연관 디바이스가 필요한지 여부를 웨어러블 아이덴티티 관리기 디바이스(600)가 결정하는 동작(810)에서 시작된다.

[0059] [0072] 연관 디바이스 없이 사용자를 연관시키기 위한 여러 가지 구현들이 고려된다고 인식되어야 한다. 예컨대, 연관 디바이스가 필요하지/요구되지 않는다면, 프로시저(800)는 연관 데이터에 대해 위해 사용자 활동이 모니터링되는 동작(815)으로 진행한다. 이를 위해, 이러한 연관 데이터는 예를 들어, (예를 들면, 키보드를 통해 입력되는) 비밀번호 입력, (예를 들면, 마이크로폰을 통해 수신되는) 음성 커맨드 및/또는 (예를 들면, 가속도계에 의해 추적되는) 움직임을 포함하는 사용자 동작과 연관된 다양한 타입들의 데이터 중 임의의 데이터를 포함할 수도 있다고 인식되어야 한다. 동작(825)에서 연관 데이터가 수신된다면, 프로시저(800)는 연관 데이터가 분석되는(예를 들어, 입력된 비밀번호를 내부적으로 저장된 비밀번호와 비교하는) 동작(840)으로 진행한다. 다

음에, 프로시저(800)는 분석을 기초로(예를 들어, 입력된 비밀번호가 내부적으로 저장된 비밀번호와 매칭하는지 여부를 기초로) 연관 상태가 결정되는 동작(850)에서 끝난다.

[0060] [0073] 그러나 많은 경우들에, 연관 디바이스는 사실상 필요하다/요구된다. 예를 들어, 웨어러블 아이덴티티 관리기 디바이스(600)는 비밀번호를 입력할 사용자 인터페이스가 없을 수도 있기 때문에, 사용자 인터페이스를 갖는 연관 디바이스의 이용이 필요할 수도 있다. 웨어러블 아이덴티티 관리기 디바이스(600)가 사용자 인터페이스를 포함한다 하더라도, 이러한 인터페이스의 형태 요소는 비밀번호 입력을 번거롭게 할 수 있다.

[0061] [0074] 다시 프로시저(800)를 참조하면, 동작(810)에서 연관 디바이스가 이에 따라 사실상 필요하다면/요구된다면, 웨어러블 아이덴티티 관리기 디바이스(600)는 연관 디바이스와 접속이 설정되는 동작(820)으로 진행한다. 여기서, 이러한 접속은 (예를 들어, 블루투스 접속을 통한) 무선 접속 또는 (예를 들어, 범용 직렬 버스 접속을 통한) 유선 접속일 수도 있다고 인식되어야 한다. 일단 접속된다면, 웨어러블 아이덴티티 관리기 디바이스(600)는 다음에 동작(830)에서 연관 디바이스로부터 연관 데이터의 수신을 시작할 수 있는데, 연관 데이터는 (예를 들어, 수신된 비밀번호를 내부적으로 저장된 비밀번호와 비교하여) 동작(840)에서 분석된다. 다음에, 프로시저(800)는 분석을 기초로(예를 들어, 수신된 비밀번호가 내부적으로 저장된 비밀번호와 매칭하는지 여부를 기초로) 연관 상태가 결정되는 동작(850)에서 끝난다.

[0062] [0075] 또한, 보다 안전한 연관 프로시저를 필요로 하는 인증들(예를 들어, 임계량을 초과하는 구매들, 민감한 이메일 계정들 등)의 경우, 웨어러블 아이덴티티 관리기 디바이스(600)와 연관 디바이스 모두를 통해 확인되는 데이터를 이용하는 것이 바람직할 수도 있다. 예컨대, 도 5를 참조로 논의한 웨어러블 아이덴티티 관리기 디바이스(500)와 비슷하게, 연관 프로시저는 연관 디바이스와 웨어러블 아이덴티티 관리기 디바이스(600)를 동시에 움직이게 하는 것을 포함할 수도 있는데, 여기서 동작(830)에서 수신된 연관 데이터는 웨어러블 아이덴티티 관리기 디바이스(600)와 연관 디바이스 둘 다로부터의 모션 데이터를 포함한다. 동작(840)에서, 연관 디바이스와 웨어러블 아이덴티티 관리기 디바이스(600)의 각각의 움직임은 다음에 이러한 모션 데이터를 기초로 비교된다. 움직임들이 (예를 들어, 시간 및 가로지르는 경로에 있어) 실질적으로 비슷하다고 여겨진다면, 사용자는 다음에 동작(850)에서 웨어러블 아이덴티티 관리기 디바이스(600)에 연관된다.

[0063] [0076] 다시 도 7을 참조하면, 예시된 바와 같이, 검출기 회로(620)는 연관 해제 하위 회로(720)를 더 포함할 수 있는 반면, 검출기 명령들(606a)은 연관 해제 명령들(722)을 더 포함할 수도 있다. 여기서, 연관 해제 하위 회로(720) 및 연관 해제 명령들(722)은 웨어러블 아이덴티티 관리기 디바이스(600)가 더는 사용자에 의해 착용되어 있지 않다는 검출시 웨어러블 아이덴티티 관리기 디바이스(600)로부터 사용자를 연관 해제시키는 쪽으로 향해져 있다. 본 개시의 특정 양상에서, 웨어러블 아이덴티티 관리기 디바이스(600)는 하나 또는 그보다 많은 센서 컴포넌트들에 연결될 수 있는데, 여기서 연관 해제 하위 회로(720) 및/또는 연관 해제 명령들(722)은 이러한 센서들로부터 리트리브된 데이터를 기초로 웨어러블 아이덴티티 관리기 디바이스(600)가 착용되어 있는지 여부를 추론하도록 구성될 수도 있다. 이를 위해, 예를 들면, (예를 들어, 웨어러블 아이덴티티 관리기 디바이스(100)와 같은 팔찌가 언제 풀렸는지를 검출하기 위한 걸쇠 센서), (예를 들어, 반지와 손가락 사이의 압력을 검출하기 위한) 압력 센서, (예를 들어, 체온을 검출하기 위한) 온도 센서, (예를 들어, 심장 박동을 검출하기 위한) 펄스 센서 또는 (예를 들어, 스트레치 가능 팔찌가 언제 스트레치되었는지를 검출하기 위한) 스트레치 센서를 포함하여, 다양한 타입들의 센서 컴포넌트들 중 임의의 하나 또는 그보다 많은 센서 컴포넌트가 사용될 수도 있다고 인식되어야 한다.

[0064] [0077] 다음에 도 9를 참조하면, 웨어러블 아이덴티티 관리기 디바이스로부터 사용자의 연관 해제를 가능하게 하기 위한 예시적인 프로세스(900)를 예시하는 흐름도가 제공된다. 본 개시의 한 양상에서, 프로시저(900)는 웨어러블 아이덴티티 관리기 디바이스(600)에 의해 연관 해제 하위 회로(720) 및/또는 연관 해제 명령들(722)을 통해 수행될 수 있음이 고려된다. 프로시저(900)는 웨어러블 아이덴티티 관리기 디바이스(600)가 자신이 연관된 상태임을 결정하는 동작(910)에서 시작된다. 웨어러블 아이덴티티 관리기 디바이스(600)가 연관된 상태에 들어간다면, 프로시저(900)는 웨어러블 아이덴티티 관리기 디바이스(600)에 연결된 연관 해제 센서들이 모니터링되는 동작(920)으로 진행한다. 여기서는, 이전에 언급한 바와 같이, 이러한 모니터링은 예를 들어, 걸쇠 센서, 압력 센서, 온도 센서, 펄스 센서 또는 스트레치 센서를 포함하는 다양한 타입들의 센터들 중 하나 또는 그보다 많은 센서로부터 데이터를 리트리브하는 것을 포함할 수도 있다. 이를 위해, 사용자에 의해 착용되는 웨어러블 아이덴티티 관리기 디바이스(600)와 일치하는 임계값들이 특정 연관 해제 센서들(예를 들어, 임계 압력 값, 임계 온도 값 등)에 할당될 수 있으며, 여기서 웨어러블 아이덴티티 관리기 디바이스(600)가 착용되어 있는지 여부에 관한 추론들은 수신된 센서 값들을 이러한 임계치들과 비교하는 것을 기초로 한다. 동작(930)에서, 웨어러블 아이덴티티 관리기 디바이스(600)는 다음에, 연관 해제 센서들 중 임의의 센서가 트리거되었는지 여부

를 결정한다. 연관 해제 센서가 사실상 트리거되었다면, 프로세스(900)는 웨어러블 아이덴티티 관리기 디바이스(600)가 사용자로부터 연관 해제되는 동작(940)에서 끝난다. 그렇지 않고 연관 해제 센서가 트리거되지 않는다면, 프로세스(900)는 연관 해제 센서들이 계속해서 모니터링되는 동작(920)으로 루프백한다.

[0065] [0078] 다음에 도 10을 참조하면, 결정 회로(630) 및 결정 명령들(606b) 각각은 복수의 서브컴포넌트들 중 임의의 서브컴포넌트를 통해 사용자 인증의 결정을 가능하게 할 수 있다고 인식되어야 한다. 예컨대, 결정 회로(630)는 센서 하위 회로(1010), 페어링 하위 회로(1020), 크리덴셜 관리기 하위 회로(1030) 및 보안 하위 회로(1040)를 포함할 수 있는 반면, 결정 명령들(606b)은 센서 명령들(1012), 페어링 명령들(1022), 크리덴셜 관리기 명령들(1032) 및 보안 명령들(1042)을 포함할 수 있다. 앞서 언급한 바와 같이, 웨어러블 아이덴티티 관리기 디바이스(600)가 가로지르는 경로에 대응하는 모션 데이터가 사용자를 인증(예를 들어, 사용자의 손을 흔들어 자동 판매기 거래를 검증)하는데 이용될 수도 있다. 여기서, 센서 하위 회로(1010) 및/또는 센서 명령들(1012)은 복수의 모션 센서 디바이스들(예를 들어, 가속도계, 자이로 등) 중 임의의 모션 센서 디바이스를 통해 이러한 모션 데이터를 모니터링하도록 구성될 수도 있다.

[0066] [0079] 추가 양상에서, 웨어러블 아이덴티티 관리기 디바이스(600)는 또한 다른 타입들의 데이터를 이용하여 사용자를 인증하도록 구성될 수도 있음이 고려된다. 예컨대, 웨어러블 아이덴티티 관리기 디바이스(600)가 겪는 움직임에 대응하는 모션 데이터에 추가하여, 센서 하위 회로(1010) 및/또는 센서 명령들(1012)은 웨어러블 아이덴티티 관리기 디바이스(600)에 연결된 하나 또는 그보다 많은 다른 컴포넌트들로부터 데이터를 리트리브하도록 구성될 수도 있다. 이러한 컴포넌트들은 예컨대, (예를 들어, 인증이 사용자의 손을 흔들고 있는 동안 터치스크린 버튼을 누르는 것을 포함할 수도 있는) 버튼, (예를 들어, 인증이 사용자가 흔들고 있는 동안 사용자의 위치를 확인하는 것을 포함할 수도 있는) 글로벌 포지셔닝 시스템(GPS: global positioning system) 디바이스, 또는 (예를 들어, 인증이 사용자의 손을 흔들고 있는 동안 음성 커맨드를 말하는 것을 포함할 수도 있는) 마이크로폰을 포함할 수도 있다. 따라서 웨어러블 아이덴티티 관리기 디바이스(600)에 의해 제공되는 인증 데이터는 이러한 또는 다른 컴포넌트들 중 임의의 컴포넌트로부터의 센서 데이터를 포함할 수도 있는데, 여기서 이러한 인증 데이터는 요청 디바이스(예를 들어, PoS 단말, 페어링 디바이스 등)에 대한 사용자의 아이덴티티 검증을 가능하게 한다.

[0067] [0080] 다음에 도 11을 참조하면, 사용자 인증을 가능하게 하기 위해 센서 데이터가 이용되는 예시적인 프로세스(1100)를 예시하는 흐름도가 제공된다. 본 개시의 한 양상에서, 프로시저(1100)는 웨어러블 아이덴티티 관리기 디바이스(600)에 의해 수행될 수 있음이 고려된다. 프로시저(1100)는 웨어러블 아이덴티티 관리기 디바이스(600)가 인증 요청을 수신하는 동작(1110)에서 시작된다. 여기서, 이러한 요청은 요청 엔티티(예를 들어, PoS 단말)로부터 직접 또는 프록시 디바이스(예를 들어, 페어링 디바이스)를 통해 요청 엔티티로부터 간접적으로 수신될 수도 있음이 고려된다. 인증 요청의 수신시, 프로시저(1100)는 웨어러블 아이덴티티 관리기 디바이스(600)가 사용자와 연관되는지 여부를 결정하기 위한 동작(1120)으로 진행한다. 웨어러블 아이덴티티 관리기 디바이스(600)가 사용자와 연관되지 않는다면, 프로시저(1100)는 동작(1125)에서 인증 요청이 거부되는 것으로 끝난다. 대안으로, 요청을 거부하기보다는, 웨어러블 아이덴티티 관리기 디바이스(600)는 연관된 상태인 동안에는 단지 인증 요청들을 수신하도록 구성될 수도 있다.

[0068] [0081] 그러나 웨어러블 아이덴티티 관리기 디바이스(600)가 사실상 사용자와 연관된다면, 프로시저(1100)는 인증 요청이 분석되는 동작(1130)으로 진행한다. 요청을 분석함으로써, 웨어러블 아이덴티티 관리기 디바이스(600)는 동작(1140)에서 요청과 연관된 다양한 인증 파라미터들을 확인할 수 있다. 동작(1150)에서, 웨어러블 아이덴티티 관리기 디바이스(600)는 다음에, 동작(1140)에서 확인된 특정 인증 파라미터들에 대응하는 센서 데이터를 리트리브한다. 예컨대, 하나의 인증 요청은 단지 상하 움직임에 대응하는 모션 데이터를 필요로 할 수도 있는 반면, 다른 인증 요청은 상하 움직임 + 음성 커맨드에 대응하는 모션 데이터를 필요로 할 수도 있다. 웨어러벌 아이덴티티 관리기 디바이스(600)는 다음에, 동작(1160)에서 요청 엔티티에 인증 데이터를 송신하며, 여기서 인증 데이터는 모션 데이터를 포함한다.

[0069] [0082] 다시 도 10을 참조하면, 예시된 바와 같이, 결정 회로(630)는 페어링 하위 회로(1020)를 더 포함할 수 있는 반면, 결정 명령들(606b)은 페어링 명령들(1022)을 더 포함할 수 있다. 여기서, 페어링 하위 회로(1020) 및 페어링 명령들(1022)은 웨어러블 아이덴티티 관리기 디바이스(600)를 페어링 디바이스(예를 들어, 페어링 디바이스(330))와 페어링하는 쪽으로 향해져 있다. 더욱이, 페어링 하위 회로(1020) 및/또는 페어링 명령들(1022)은 웨어러블 아이덴티티 관리기 디바이스(600)가 페어링된 디바이스를 통해 시작된 사용자 거래를 인증하는데 사용될 수 있게 이러한 페어링을 가능하게 하도록 구성될 수도 있음이 고려된다.

[0070] [0083] 다음에 도 12를 참조하면, 사용자 인증을 가능하게 하기 위해 페어링 디바이스가 이용되는 예시적인 프로세스(1200)를 예시하는 흐름도가 제공된다. 본 개시의 한 양상에서, 프로시저(1200)는 웨어러블 아이덴티티 관리기 디바이스(600)에 의해 수행될 수 있음이 고려된다. 프로시저(1200)는 웨어러블 아이덴티티 관리기 디바이스(600)가 페어링 디바이스와 페어링되는 동작(1210)에서 시작된다. 다음에, 동작(1220)에서, 웨어러블 아이덴티티 관리기 디바이스(600)는 페어링 디바이스를 통해 요청 엔티티로부터 인증 요청을 수신한다. 예컨대, 거래가 온라인 구매라면, 요청 엔티티는 온라인 소매업체인 반면, 페어링된 디바이스는 브라우저 애플리케이션(예를 들어, 랩톱, 스마트폰 등)을 실행하는 디바이스이다. 인증 요청의 수신시, 프로시저(1200)는 웨어러블 아이덴티티 관리기 디바이스(600)가 사용자와 연관되는지 여부를 결정하기 위한 동작(1230)으로 진행한다. 웨어러블 아이덴티티 관리기 디바이스(600)가 사용자와 연관되지 않는다면, 프로시저(1200)는 동작(1235)에서 인증 요청이 거부되는 것으로 끝난다.

[0071] [0084] 그러나 웨어러블 아이덴티티 관리기 디바이스(600)가 사실상 사용자와 연관된다면, 프로시저(1200)는 요청과 연관된 다양한 인증 파라미터들이 확인되는 동작(1240)으로 진행한다. 동작(1250)에서, 웨어러블 아이덴티티 관리기 디바이스(600)는 다음에, 동작(1240)에서 확인된 특정 인증 파라미터들에 대응하는 인증 데이터를 리트리브한다. 웨어러벌 아이덴티티 관리기 디바이스(600)는 다음에, 동작(1260)에서 페어링 디바이스에 인증 데이터를 송신하며, 여기서 이러한 송신은 요청 엔티티에 대해 사용자를 인증하기 위해 페어링 디바이스를 통해 개인 정보가 수동으로 입력될 필요성을 없앤다.

[0072] [0085] 또 도 10을 참조하면, 예시된 바와 같이, 결정 회로(630)는 크리덴셜 관리기 하위 회로(1030) 및 보안 하위 회로(1040)를 더 포함할 수 있는 반면, 결정 명령들(606b)은 크리덴셜 관리기 명령들(1032) 및 보안 명령들(1042)을 더 포함할 수 있다. 여기서, 크리덴셜 관리기 하위 회로(1030) 및 크리덴셜 관리기 명령들(1032)은 사용자와 연관된 크리덴셜의 제공 쪽으로 향해져 있는 반면, 보안 하위 회로(1040) 및 보안 명령들(1042)은 인증 요청과 연관된 보안 레벨의 확인 쪽으로 향해져 있다. 더욱이, 웨어러블 아이덴티티 관리기 디바이스(600)는 크리덴셜 관리기 하위 회로(1030), 크리덴셜 관리기 명령들(1032), 보안 하위 회로(1040) 및/또는 보안 명령들(1042)의 임의의 결합을 이용하여, 인증 요청으로부터 확인된 보안 레벨을 기초로 요청 엔티티에 제공된 사용자 크리덴셜들의 양을 제한하도록 구성될 수도 있음이 고려된다. 본 개시의 특정 양상에서, 크리덴셜들은 인증 요청으로부터 외삽된 실행 콘텍스트 또는 사용자 동작 중 적어도 하나를 기초로 제공되는 반면, 보안 레벨은 사용자 선호 설정, 실행 콘텍스트, 또는 하나 또는 그보다 많은 이력 실행 콘텍스트들 중 적어도 하나에 따라 확인된다. 더욱이, 아래 보다 상세히 논의되는 바와 같이, 보안 레벨은 복수의 가능한 보안 레벨들로부터 선택될 수 있다.

[0073] [0086] 다음에 도 13을 참조하면, 사용자 인증을 가능하게 하기 위해 확인된 보안 레벨에 따라 크리덴셜들이 송신되는 예시적인 프로세스(1300)를 예시하는 흐름도가 제공된다. 본 개시의 한 양상에서, 프로시저(1300)는 웨어러블 아이덴티티 관리기 디바이스(600)에 의해 수행될 수 있음이 고려된다. 프로시저(1300)는 웨어러블 아이덴티티 관리기 디바이스(600)가 인증 요청을 수신하는 동작(1310)에서 시작된다. 인증 요청의 수신시, 프로시저(1300)는 웨어러블 아이덴티티 관리기 디바이스(600)가 사용자와 연관되는지 여부를 결정하기 위한 동작(1320)으로 진행한다. 웨어러블 아이덴티티 관리기 디바이스(600)가 사용자와 연관되지 않는다면, 프로시저(1300)는 동작(1325)에서 인증 요청이 거부되는 것으로 끝난다.

[0074] [0087] 그러나 웨어러블 아이덴티티 관리기 디바이스(600)가 사실상 사용자와 연관된다면, 프로시저(1300)는 인증 요청이 분석되는 동작(1330)으로 진행한다. 요청을 분석함으로써, 웨어러블 아이덴티티 관리기 디바이스(600)는 동작(1340)에서 요청과 연관된 적절한 보안 레벨을 선택할 수 있다. 이전에 언급한 바와 같이, 이러한 보안 레벨은 복수의 가능한 보안 레벨들로부터 선택될 수 있고, 여기서 선택은 다양한 요소들(예를 들어, 사용자 선호 설정, 실행 콘텍스트 및/또는 하나 또는 그보다 많은 이력 실행 콘텍스트들 등) 중 임의의 요소에 좌우될 수 있다. 동작(1350)에서, 웨어러블 아이덴티티 관리기 디바이스(600)는 다음에, 동작(1340)에서 선택된 보안 레벨에 따라 크리덴셜들을 리트리브한다. 프로시저(1300)는 다음에, 웨어러블 아이덴티티 관리기 디바이스(600)가 보안 레벨을 기초로 요청 엔티티에 크리덴셜들을 송신하는 동작(1360)에서 끝난다.

[0075] 예시적인 보안 레벨들

[0076] [0088] 개시된 웨어러블 아이덴티티 인프라구조는 다양한 보안 레벨들 중 임의의 보안 레벨을 가능하게 할 수 있다고 인식되어야 한다. 그러나 특정 양상에서는, 3개의 예시적인 보안 레벨들: 근접도 검증, 암시적 확약 및 명시적 확인이 고려된다. 이러한 3개의 보안 레벨들 각각, 그리고 대응하는 페어링 방법이 아래에 논의되는데, 여기서 페어링 방법들은 스테이션과 웨어러블 아이덴티티 관리기 디바이스 간의 프로토콜들의 콘텍스트 내에서

설명된다.

[0077] [0089] 이 예에서, 근접도 검증은 단순히, 액세스 특권들을 갖는 아이덴티티와 연관된 아이덴티티 관리기가 사용자와 상호 작용하는 객체(예를 들어, 전화기, 마우스 등) 주변에 있음을 검증하는 것에 의존하기 때문에, 근접도 검증은 3개의 보안 레벨들 중 가장 낮은 것으로 여겨진다. 페어링에 대해, 스테이션— 전화기든, 마우스든, 문고리든, 판매 시점 단말 등이든 —은 웨어러블 아이덴티티 관리기 디바이스에 웨이크업 신호를 송신할 수 있으며, 웨어러블 아이덴티티 관리기 디바이스는 웨어러블 아이덴티티 관리기 디바이스와 연관된 아이덴티티의 표현을 포함하는 확인 응답으로 응답한다. 이러한 표현은 정적 고유 식별자, 필명, 롤링 코드로부터의 출력, 또는 암호화 토큰일 수도 있다.

[0078] [0090] 다음에 도 14를 참조하면, 웨어러블 아이덴티티 관리기와 스테이션 간의 예시적인 근접도 기반 검증을 예시하는 개략도가 제공된다. 최저 보안 레벨에서는, 거래를 진행하기에 근접도 검증이 충분함이 고려된다. 특정 구현에서, 스테이션은 아이덴티티 관리기에 의해 수신되는 웨이크업 신호를 송신하여, 아이덴티티 관리기가 아이덴티티 주장(assertion)으로 응답하게 한다. 웨이크업 신호는 아이덴티티 관리기에 의해 유지되는 화이트리스트와 비교되는 스테이션의 아이덴티티의 표시자를 포함할 수 있다. 매칭이 존재한다면, 아이덴티티 주장은 스테이션과 연관된 키 그리고 스테이션으로 송신된 암호문을 사용하여 암호화된다. 여기서, 스테이션이 아이덴티티 관리기가 그 이전 아이덴티티로부터 연관 해제되었는지 여부를 알지 못하기 때문에 — 전용 채널에도 불구하고 — 단순히 평문 확인 응답으로부터 아이덴티티를 추론하는 것은 불가능하다는 점이 주목되어야 한다.

[0079] [0091] 3개의 보안 레벨들 중에서, 암시적 확약은 중간 레벨로 여겨진다. 암시적 확약은 근접도 검증을 통과한 아이덴티티 관리기와 연관된 사용자에 대해 타당해 보이는 사용자 의도를 결정하는 것에 의존한다. 이는 가속도계 데이터를 암시적 사용자 동작들(예를 들어, 그렇게 하도록 요청되지 않아도 사용자가 취하고 있는 동작들)에 대응하는 데이터와 비교함으로써 얻어질 수 있다. 이러한 동작들의 예들은 스크린을 탭하여 애플리케이션 또는 자원을 선택하는 것, 랩톱 키보드 상에서 타이핑하는 것, 그리고 문고리를 돌리는 것을 포함한다. 페어링에 대해, 암시적 확약은 2개의 신호들(예를 들어, 2개의 가속도계 자취들, 하나의 가속도계 자취와 연관된 클릭 타이밍 신호 등)의 비교를 필요로 한다. 이러한 비교는 아이덴티티 관리기에 의해 실행될 수도 있고 — 이는 어떤 의미에서는, 그 사용자를 정확히 나타내는 것을 담당함 —, 결과는 앞서 설명한 바와 같이, 아이덴티티 관리기와 연관된 아이덴티티의 표현과 함께 스테이션으로 전달될 수도 있다.

[0080] [0092] 동작의 명시적 사용자 확인으로부터 가장 높은 보안 레벨이 얻어지는데, 여기서 사용자의 아이덴티티 관리기는 또한 근접도 검증을 통과했다. 명시적 확인의 두 가지 예들은 사용자가 전화기를 (스마트 팔찌를 착용하는데 사용되는 손으로) 흔드는 것, 그리고 판매 시점 단말의 스크린 상에 서명하는 것인데, 여기서 검출된 스크린 움직임들 또는 스타일러스 가속도계 데이터가 아이덴티티 관리기에 의해 생성된 가속도계 데이터와 비교된다. 페어링에 관해 암시적 확약과 명시적 확인 사이의 차이점은 앞서 설명한 두 신호들의 비교로부터 얻어진 매칭과 연관된 확실성에 대부분 있다. 즉, 명시적 확인의 경우, 더 많은 양의 신호가 비교되어야 한다. 신호들의 비교의 한 가지 실제 구현은 가능성 있는 엔트로피의 양을 결정하는 엔트로피 미터의 단순한 형태, 지속적인 배경 움직임에 대한 조정, 및 비교를 수행하기 전 충분한 양의 신호 수집을 포함한다. 대안으로, 두 신호들은 확인이 생성되어 송신되는 시점인 충분한 합의가 있을 때까지 (윈도잉 방법을 사용하여) 비교될 수 있다.

[0081] [0093] 특정 양상에서, 보안 레벨은 작업의 타입 또는 작업의 듀레이션을 선택함으로써 원하는 레벨로 조정될 수 있음이 고려된다. 여기서는, 움직임에 대해 추가 요건들을 두는 것을 제외하면, 암시적 확약 프로토콜과 실질적으로 비슷한 프로토콜이 사용될 수 있다. 다음에 도 15를 참조하면, 암시적 확약과 명시적 확인에 대한 예시적인 접근 방식이 제공된다. 스테이션이 웨이크업 신호를 전송함으로써 시작된다. 아이덴티티 관리기가 웨이크업 신호를 수신하자마자, 아이덴티티 관리기는 움직임들(m_1)을 측정한다. 동시에, 스테이션은 움직임들(m_2)을 측정한다. 웨이크업 신호의 시간 기간(T) 내에, 스테이션은 측정된 움직임들(m_2) 및 그 공개키(P)에 대한 커밋(commitment)을 송신한다. 커밋은 m_2, P 그리고 스테이션이 임으로 선택한 숫자(r)에 암호화 해시 함수를 적용함으로써 계산될 수 있다. 웨이크업 신호로부터 시간(T)이 경과한 후, 스테이션은 값들(m_2; P; r)을 누설한다. 아이덴티티 관리기는 3개의 요소들을 검증한다: (1) 웨이크업 신호의 시간(T) 내에 커밋이 수신되었음; (2) 커밋이 누설된 값들에 대응함; 그리고 (3) 움직임들(m_1, m_2)이 서로 충분히 잘 매칭함. 명시적 확인의 경우, 움직임들이 추가 요건들을 충족함이 또한 검증된다. 이러한 조건들 모두 충족된다면, 아이덴티티 관리기는 공개키(P)를 사용하여 암호화된 아이덴티티 주장을 준비하고 결과적인 암호문을 스테이션으로 송신한다.

[0082] [0094] 많은 PoS 거래들의 경우, 사용자 서명을 요구하는 것이 원하는 명시적 확인일 수도 있다는 점이 주목된

다. 즉, PoS 거래에 대한 사용자 인증은 아이덴티티 관리기에 의해 생성된 가속도계 데이터와 검출된 PoS 스크린 움직임들 또는 스타일러스 가속도계 데이터와의 앞서 언급한 매칭을 필요로 할 수도 있다. 다음에 도 16 - 도 17을 참조하면, 웨어러블 아이덴티티 관리기 디바이스에 의해 가능해지는 PoS 거래의 예시적인 서명 인증이 제공된다. 도 16 - 도 17에 예시된 바와 같이, 이러한 인증은 웨어러블 아이덴티티 관리기 디바이스(1600)를 착용하고 있는 동안 스타일러스(1612)로 판매 시점 터치스크린(1610) 상에 사용자가 자신의 서명을 사인할 것을 요구할 수도 있다. 도 16에서는, 예컨대, 사용자의 서명의 초기 스트로크들이 도시되는데, 여기서는 웨어러블 아이덴티티 관리기 디바이스(1600)에 의해 생성된 가속도계 데이터가 판매 시점 터치스크린(1610)에 의해 캡처된 초기 스트로크들 및/또는 스타일러스(1612)의 움직임들에 대응하는 가속도계 데이터와 매칭된다. 더욱이, 웨어러블 아이덴티티 관리기 디바이스(1600)가 가로지르는 검출된 경로가 판매 시점 터치스크린(1610) 및/또는 스타일러스(1612)에 의해 검출된 것과 같은 서명 스트로크에 대응하는 신호들과 일치하는지 여부에 대한 결정이 이루어진다.

[0083] [0095] 일부 구현들에서는, 웨어러블 아이덴티티 관리기 디바이스(1600)가 가로지르는 경로 및 이러한 신호들의 동시 발생 검출이 요구될 수도 있다. 예컨대, 도 17에 예시된 바와 같이, 사용자가 자신의 이름을 서명할 때 웨어러블 아이덴티티 관리기 디바이스(1600)가 가로지르는 경로는 실질적으로 수평일 수도 있는데, 여기서 이러한 경로는 사용자가 자신의 이름을 서명하기 시작하는 시점(t_1)에서부터 사용자가 자신의 서명을 마치는 시점(t_2)까지 추적된다. 여기서, t_1에서부터 t_2까지의 웨어러블 아이덴티티 관리기 디바이스(1600)의 실질적으로 수평 경로는 t_1에서부터 t_2까지 판매 시점 터치스크린(1610)에 의해 캡처된 서명 스트로크들 및/또는 t_1에서부터 t_2까지의 서명과 일치하는 스타일러스(16112)의 움직임들에 대응하는 가속도계 데이터와 매칭될 수도 있다. PoS 지불의 인증은 다음에, 이러한 매칭이 미리 결정된 신뢰도 내에 있는지 여부를 확인하는 것에 의해 적어도 부분적으로 기초할 수도 있다.

[0084] [0096] 본 명세서에 개시된 양상들에 따른 PoS 거래들의 다양한 예시적인 인증들이 이제 설명된다. 제 1 예에서는, 사용자가 자신의 주로 사용하는 손의 손목에 웨어러블 아이덴티티 관리기 디바이스를 착용하고 있으며, 여기서 웨어러블 아이덴티티 관리기 디바이스는 사용자와 이전에 연관되었고, 따라서 사용자의 아이덴티티의 표현을 이미 저장했다고 가정된다. 이 예의 경우, PoS 단말은 연관된 스타일러스를 갖는 스크린, 및 스크린 상에서 스타일러스의 시간 기반 자취를 기록하는데 사용되는 소프트웨어를 포함하는 레거시 단말이다. PoS 단말은 또한 네트워크에 접속되며, 무선 라디오 송신기를 포함한다. 여기서, 사용자는 스타일러스를 집어드는 것으로 시작하며, 이를 스크린에 가깝게 놓는다. 이 결과, 무선 라디오 송신기를 사용하여 관여(engage) 신호가 송신되며, 이는 웨어러블 아이덴티티 관리기 디바이스에 의해 수신된다. 웨어러블 아이덴티티 관리기 디바이스는 다음에 식별과 연관된 동작 모드에 들어간다.

[0085] [0097] 다음에, 사용자는 PoS 단말 스크린 상의 박스에 자신의 이름을 서명하도록 유도된다. 동시에, 식별과 연관된 동작 모드에 들어간 웨어러블 아이덴티티 관리기 디바이스는 웨어러블 아이덴티티 관리기 디바이스의 움직임을 (예를 들어, 가속도계 데이터를 통해) 기록하는데, 이는 시간-공간 시리즈의 형태로 임시로 저장된다. 다음에, PoS 단말 상의 소프트웨어가 스크린 상의 스타일러스의 시간 기반 자취의 함수를 계산하고, 이를 무선 라디오 송신기를 사용하여 웨어러블 아이덴티티 관리기 디바이스에 송신한다.

[0086] [0098] 웨어러블 아이덴티티 관리기 디바이스는 다음에, 시간-공간 시리즈와 시간 기반 자취 사이의 비교를 기초로, 이들이 미리 결정된 신뢰도 내에 서로 대응하는지 여부에 대한 결정을 한다. 두 엘리먼트들이 서로 비교된다고 결정된다면, 웨어러블 아이덴티티 관리기 디바이스는 '성공' 상태에 들어간다. 그렇지 않으면, 웨어러블 아이덴티티 관리기 디바이스는 어떤 임계량의 시간 동안 동일하나 상태를 유지하여, 잠재적으로 추가 신호들을 수신하고 추가 비교들을 수행한다. 웨어러블 아이덴티티 관리기 디바이스 성공 상태에 들어가지 않고 시간 임계치에 도달한다면, 웨어러블 아이덴티티 관리기 디바이스는 사용자가 스타일러스를 집어들기 전에 있었던 상태로 돌아간다.

[0087] [0099] 웨어러블 아이덴티티 관리기 디바이스가 성공 상태에 들어간다면, 웨어러블 아이덴티티 관리기 디바이스는 PoS 단말과 연관된 라디오 송신기에 성공 신호를 전달한다. 예시적인 구현에서, 이 신호는 사용자와 연관되는 금융 자원들의 하나 또는 그보다 많은 선택들과 연관된 정보를 포함한다. 적어도 2개의 선택들이 이용 가능하다면, PoS 스크린은 이들을 사용자에게 디스플레이하는데 사용되며, 이는 사용자가 자신의 선호 소스를 선택하게 한다. 대안으로, 이러한 정보는 다른 저장소로부터 수신된다.

[0088] [00100] 성공 신호는 아이덴티티 정보, 그리고 바람직하게는 사용자 아이덴티티 또는 웨어러블 아이덴티티 관리

기 디바이스와 연관된 필명과 같이 도용되거나 재현될 수 없는 아이덴티티 주장, 그리고 사용 번호나 시간을 추가로 포함할 수도 있다고 고려된다. 이 예에서, 거래량 및 선택된 금융 소스를 표시하는 정보가 아이덴티티 정보와 함께 백엔드 엔티티에 송신된다. 백엔드는 다음에, 어떤 사용자에게 얼마의 양을 그리고 어떤 금융 자원으로부터 청구되어야 하는지를 결정한다.

[0089] [00101] 제 2 예시적인 사용 시나리오에서, 제 1 예에 관해 앞서 개시한 많은 초기 파라미터들이 다시 가정된다. 즉, 사용자가 자신의 주로 사용하는 손의 손목에 웨어러블 아이덴티티 관리기 디바이스를 착용하고 있으며, 여기서 웨어러블 아이덴티티 관리기 디바이스는 사용자와 이전에 연관되었고, 따라서 사용자의 아이덴티티의 표현을 이미 저장했다고 가정된다. PoS 단말은 다시 네트워크에 접속되며, 연관된 스타일러스를 갖는 스크린, 스크린 상에서 스타일러스의 시간 기반 자취를 기록하는데 사용되는 소프트웨어, 그리고 무선 라디오 송신기를 포함한다. 사용자가 PoS 스크린에 가깝게 스타일러스를 배치하면, 관여 신호가 다시 웨어러블 아이덴티티 관리기 디바이스에 송신되며, 이는 웨어러블 아이덴티티 관리기 디바이스가 식별과 연관된 동작 모드에 들어가게 한다.

[0090] [00102] 이 예에서, 스타일러스는 가속도계를 사용하여 자신의 움직임을 결정하는데, 여기서 이러한 가속도계 데이터를 포함하는 신호는 다음에 식별과 연관된 모드로 동작하고 있는 웨어러블 아이덴티티 관리기 디바이스에 전송된다. 그러나 웨어러블 아이덴티티 관리기 디바이스는 또한 가속도계를 포함하는데, 이는 수신된 스타일러스 가속도계 신호와 비교되는 움직임 기반 신호를 발생시킨다. 이들이 웨어러블 아이덴티티 관리기 디바이스가 식별 모드에 들어간 후 일정 시간 임계치 이전에 서로 대응한다고 결정된다면, 웨어러블 아이덴티티 관리기 디바이스는 성공 상태에 들어간다. 다음에 시스템은 앞서 제 1 예에서 설명한 동일한 프로시저에 따라 진행한다.

[0091] [00103] 제 3 예에서, 자동 판매기 시나리오가 고려된다. 제 1 예 및 제 2 예와 비슷하게, 사용자가 자신의 주로 사용하는 손의 손목에 웨어러블 아이덴티티 관리기 디바이스를 착용하고 있으며, 여기서 웨어러블 아이덴티티 관리기 디바이스는 사용자와 이전에 연관되었고, 따라서 사용자의 아이덴티티의 표현을 이미 저장했다고 또 가정된다. 웨어러블 아이덴티티 관리기 디바이스는 가속도계를 추가로 포함할 수 있는데, 이는 웨어러블 아이덴티티 관리기 디바이스가 가로지르는 경로들을 추적하여 기록하는데 사용될 수 있다.

[0092] [00104] 이 예에서, 자동 판매기는 사용자 선택을 검출하는 사용자 인터페이스, 그리고 사용자가 자동 판매기에 접근할 때 관여 신호를 전송하도록 구성된 라디오 송신기를 갖는다. 이러한 관여 신호는 다음에 웨어러블 아이덴티티 관리기 디바이스에 의해 수신되며, 이는 웨어러블 아이덴티티 관리기 디바이스가 식별 모드에 들어가게 한다. 자동 판매기는 다음에 사용자 선택을 검출하고, 상호 작용을 특성화하는 신호, 예컨대 관여하게 되는 버튼 또는 레버와 연관된 가속 데이터 및 타이밍을 웨어러블 아이덴티티 관리기 디바이스에 송신한다. 종래의 판매 시점 디바이스는 또한 이러한 단순화된 사용자 경험 접근 방식을 사용할 수 있는데, 물론 여기서 사용자는 단순히 예를 들어, 거래를 마무리하기 위해 클릭 또는 흔들어야 한다.

[0093] [00105] 상호 작용을 특성화하는 신호의 수신시, 이러한 특정 거래에 사용자를 인증하기 위해, 웨어러블 아이덴티티 관리기 디바이스는 수신된 신호를 웨어러블 아이덴티티 관리기 디바이스가 가로지르는 경로에 대응하는 내부적으로 저장된 가속도계 데이터와 비교한다. 웨어러블 아이덴티티 관리기 디바이스가 식별 모드에 들어간 시점 이후 일정 시간 임계치 이전에 검출된 이러한 대응 관계가 존재한다면, 웨어러블 아이덴티티 관리기 디바이스는 성공 상태에 들어간다.

[0094] [00106] 웨어러블 아이덴티티 관리기 디바이스가 성공 상태에 들어간다면, 웨어러블 아이덴티티 관리기 디바이스는 자동 판매기의 라디오 송신기에 성공 신호를 전달한다. 이러한 성공 신호는 아이덴티티 정보, 그리고 바람직하게는 사용자 아이덴티티 또는 웨어러블 아이덴티티 관리기 디바이스와 연관된 필명과 같이 도용되거나 재현될 수 없는 아이덴티티 주장, 그리고 사용 번호나 시간을 추가로 포함할 수도 있다고 고려된다. 이 예에서, 거래량 및 선택된 금융 소스를 표시하는 정보가 자동 판매기에 의해 아이덴티티 정보와 함께 백엔드 엔티티에 송신된다. 백엔드는 다음에, 어떤 사용자에게 얼마의 양을 그리고 어떤 금융 자원으로부터 청구되어야 하는지를 결정한다.

[0095] 예시적인 이득들

[0096] [00107] 해당 기술분야에서 통상의 지식을 가진 자는 본 명세서에서 개시되는 양상들을 구현함으로써 다양한 이득들이 달성될 수 있다고 쉽게 인식할 것이다. 예시적인 이득들의 완전하지 않은 리스트가 아래에 제공된다.

[0097] [00108] 제 1 예시적인 이득은 사용자들이 임의의 크리덴셜들을 (가능하게는, 사용자들의 아이덴티티 관리기들이 사용자들과 연관될 때 이들에 대해 인증하기 위한 것 외에는) 사용하는 버릇이 있지 않을 것이므로, 사용자

들이 피싱 공격들로부터 보호된다는 점이다. 아이덴티티 관리기가 인증을 요청한 스테이션으로 어떠한 종래 크리덴셜들을 전달하지 않을 것이므로, 사용자들이 또한 이러한 공격들로부터 보호될 것이다.

[0098] [00109] 다른 예시적인 이득은 사용자들이 악성 코드로부터 – 어느 정도까지는 – 보호된다는 점이다. 이는 아이덴티티 관리기와 그 주변들 사이의 매우 제한적인 인터페이스가 아이덴티티 관리기가 손상되는 것을 매우 어렵게 하기 때문이다. 특히, 사용자들은 그들의 아이덴티티 관리기들에 임의의 소프트웨어를 설치할 가능성이 낮기 때문에, 전체 등급의 취약성들이 회피된다.

[0099] [00110] 본 명세서에서 개시되는 양상들의 추가 이득은 약한 크리덴셜들에 관한 것이다. 즉, 크리덴셜들은 단지 연관 단계에만 사용되기 때문에, 크리덴셜들의 품질은 별로 문제가 되지 않는다. 이는 타깃화된 아이덴티티 관리기에 대해 물리적 액세스하는 사람들에 대해 약한 크리덴셜들의 잠재적 사용을 제한한다.

[0100] [00111] 또한, 아이덴티티 관리기 또는 연관된 프록시가 비밀번호 관리기로서 작동한다면, 이는 또한 아이덴티티 관리기와 직접 호환 가능하지 않은 사이트들에서 비밀번호들을 관리하는 작업으로부터 사용자를 해방시켜준다. 잠재적 악성 코드 공격들에 대한 연관된 솔루션의 노출은 어떤 엔티티가 비밀번호 관리기로서 작동하는지, 그리고 이것이 전화기라면, 비밀번호가 안전한 실행 환경에서 실행되는지 여부에 다른 무엇보다도 더 좌우된다.

[0101] [00112] 사용자들은 또한 사이트 침해들에 대해 어떤 높아진 보안을 얻을 수 있다. 예컨대, 아이덴티티 관리기들에 의해 송신된 거래 토큰들은 도난당한다면 쓸모가 없다. 예를 들어, 롤링 코드의 출력은 디지털 서명들을 기초로 암호화 토큰들이 하는 것과 같이 이러한 이득들을 제공한다.

[0102] 예시적인 웨어러블 아이덴티티 인증 사용 시나리오들

[0103] [00113] 제 1 예시적인 사용 시나리오에서, 사용자는 앞서 설명한 바와 같은 웨어러블 아이덴티티 관리기 디바이스의 팔찌 구성, 및 2개의 전화기들– 사용자가 일을 위해 주로 사용하는 것 하나, 그리고 사용자가 주로 개인 업무를 위해 사용하는 다른 하나 –을 갖는다. 두 전화기 모두 인증 프로세스에 사용되는 소프트웨어가 설치되어 있다: 업무 전화는 사용자의 고용주에 의해 마스터 데이터 관리(MDM: master data management) 애플리케이션이 설치되고, 가정용 개인 전화는 애플리케이션 스토어로부터 사용자에 의해 개인용 애플리케이션이 다운로드된다. MDM 애플리케이션과 개인용 애플리케이션 모두 사용자와 연관된 암호화된 사용자 프로파일 파일을 다운로드함으로써, 그리고 전화기와 팔찌 사이의 연관 프로세스에 사용되는 크리덴셜을 등록함으로써 구성되었다. 업무용 전화의 경우, 이 크리덴셜은 업무용 전화 상의 지문 센서와 연관된 생체 인식 템플릿이다. 개인용 전화의 경우, 이는 비밀번호이다. 이러한 크리덴셜들 둘 다 안전하나 방식으로 저장된다(예를 들어, 보안 저장소에, 또는 해시되어 저장됨).

[0104] [00114] 일반적인 아침에, 사용자는 일어나서 샤워한 다음 자신의 팔찌를 찰 것이다. 사용자가 팔찌의 걸쇠를 잠그면, 팔찌의 웨어러블 아이덴티티 관리기가 자동으로 연관 단계에 들어간다. 이는 사용자가 전화기의 무선 거리 내에 도달할 때 사용자의 개인용 전화를 웨이크업할 것이며, 무선 거리는 1미터 약간 미만일 수도 있다. 개인용 전화는 팔찌의 웨어러블 아이덴티티 관리기에 의해 방사되는 저전력 블루투스 신호를 검출하고, 이것이 이전에 블루투스 페어링되어 접속을 생성한 유닛에 대한 것이라고 결정한다. 블루투스 접속이 설정된 후, 전화기의 화면은 예를 들어, "Alice의 팔찌에 접속함" 메시지를 디스플레이하고, 직후에 "Alice의 팔찌에 대한 비밀번호를 입력하세요"라고 하는 텍스트를 디스플레이할 수도 있다. 다음에, 사용자는 자신의 개인용 전화기의 화면 상의 작은 박스에 자신의 비밀번호를 타이핑한다. 이는 비밀번호를 해시하고 해시된 비밀번호를 팔찌 및 전화기의 연관과 연관된 이전에 저장된 비밀번호와 비교함으로써 전화기에 의해 검증된다. 다음에 사용자는 자신이 팔찌를 착용하고 있는 손으로 전화기를 흔든다. 전화기의 가속도계가 가속도계 출력으로부터 신호 다이제스트를 계산하고 이를 팔찌에 – 그러나 사용자가 이전에 입력한 비밀번호가 정확한 경우에만 – 전송한다. 전화기는 또한 이것이 팔찌의 웨어러블 아이덴티티 관리기에 대한 사용자의 비밀번호라는 표시를 송신한다. 이러한 모든 통신은 블루투스 접속과 연관된 대칭 암호화를 사용하여 안전하게 된다. 팔찌의 가속도계는 또한 모션을 기초로 신호를 발생시키며, 팔찌의 웨어러블 아이덴티티 관리기가 전화기로부터 수신된 다이제스트를 발생된 신호와 비교하여, 이들이 서로 대응한다면, 웨어러블 아이덴티티 관리기는 연관을 수락하여, 이것이 현재 사용자에 의해 착용되어 있음을 저장한다(이는 전화기에 의해 웨어러블 아이덴티티 관리기에 전달되었음).

[0105] [00115] 아침 식사 후, 사용자가 자신의 개인용 전화 상에서 자신의 이메일을 확인하기 위해 로그인하길 원한다. 사용자는 이메일 애플리케이션을 시작하는데, 이는 인증을 필요로 한다고 표시한다(사용자가 그 애플리케이션이 사용되지 않을 때 이를 잠금 모드로 설정했기 때문에, 액세스하기 위해 인증을 필요로 함). 사용자가 자신의 팔찌를 착용하고 있기 때문에, 사용자는 자신이 자신의 이메일에 액세스하기 위해 사용해야 할 PIN을

입력할 필요가 없다. 대신, 사용자는 팔찌가 있는 손을 사용하여 전화기를 천천히 흔든다. 사용자의 메일 리더 애플리케이션은 무엇보다도, 사용자의 팔찌의 웨어러블 아이덴티티 관리기와 연관된 인증 라이브러리를 사용하는데, 이는 웨어러블 아이덴티티 관리기와 통신 세션을 시작하고, 웨어러블 아이덴티티 관리기는 자신이 사용자에 의해 착용되어 있음을 보안 채널을 통해 전화기에 전달한다. 인증 라이브러리는 메일 애플리케이션을 잠금 해제하는데, 이는 사용자가 자신의 이메일을 읽을 수 있게 한다.

[0106] [00116] 나중에, 사용자가 자신의 은행 계좌에 액세스하길 원하고, 자신의 은행과 연관된 뱅킹 애플리케이션을 시작한다. 뱅킹 애플리케이션은 사용자의 개인용 전화기 상에서 실행되며, 또한 앞서 설명한 인증 라이브러리를 사용한다. 뱅킹 애플리케이션이 시작되면, 이는 로그인을 요구한다. 그러면 사용자는 자신의 전화기를 천천히 흔들고, 사용자의 팔찌의 웨어러블 아이덴티티 관리기와 세션이 시작된다. 앞서 설명한 것과 비슷하게, 웨어러블 아이덴티티 관리기는 개인용 전화기에 신호를 송신하며, 여기서 이 신호는 애플리케이션 라이브러리와 연관된 코드에 의해 처리된다. 애플리케이션 라이브러리는 비밀번호 관리기의 애플리케이션 프로그래밍 인터페이스(API: application programming interface)를 호출하여, 사용자가 전화기를 사용하고 있음을 표시한다. 비밀번호 관리기는 사용자의 은행에 대한 액세스인 호의 콘텍스트를 결정하고, 사용자 이름들 및 크리덴셜들을 저장하는데 사용되는 보안 저장소로부터 사용자의 사용자명 및 비밀번호를 검색한다. 이들은 뱅킹 애플리케이션에 입력되며, 뱅킹 애플리케이션은 이들의 수신시 이들을 사용자의 은행에서 이미 시작된 보안 소켓 계층(SSL: secure sockets layer) 세션을 통해 전달한다. 사용자의 은행은 이것이 정확한 로그인임을 검증하고, 계좌에 대한 액세스를 허용하여, 사용자의 개인용 전화기 상의 뱅킹 애플리케이션과 통신한다.

[0107] [00117] 나중에, 사용자가 로그아웃하고, 그 다음 출근하러 지하철로 향한다. 떠나기 전에, 사용자는 자신의 업무용 전화를 잡아챈다. 사용자의 달력을 체크하기 위해 전화기에 로그인하는 대신에, 사용자는 자신이 팔찌를 착용하고 있는 손으로 업무용 전화기를 천천히 흔든다. 업무용 전화는 또한 웨어러블 아이덴티티 관리기와 이미 페어링되어 있으며, 이와 블루투스 세션을 시작한다. 팔찌가 개인용 전화기와 이미 연관되었고, 그렇게 함으로써 팔찌가 사용자에 의해 착용되어 있음이 각인되었기 때문에, 사용자의 개인용 전화기와 팔찌의 웨어러블 아이덴티티 관리기 사이의 앞서 설명한 연관은 불필요하다. 웨어러블 아이덴티티 관리기는 이 사실을 업무용 전화기에 전달하고, 다음에 그 전화기는 자동으로 잠금 해제된다(PIN이 불필요함).

[0108] [00118] 사용자가 자신의 스케줄을 확인하고 자신이 지하철을 타기 전에 커피 마실 시간이 있음을 인식한다. 사용자는 자신의 인근 카페에 가서 커피를 주문하고 자신의 손을 흔들어 인증한다. 사용자의 팔찌는 판매 시점 컴퓨터와 블루투스 접속을 설정하고, 이는 사용자가 저장된 돈이 있음을 검증하고, 자신의 신용 카드로 $3을 자동으로 청구한다.

[0109] [00119] 사용자의 커피를 구입한 후, 사용자는 지하철로 걸어간다. 사용자가 개찰구들을 통과할 때, 사용자는 개찰구들을 통과하기 위해 자신의 손을 흔들 필요가 없고, 이에 토큰을 공급하거나 등록된 팔찌를 착용할 필요가 있다. 여기서, 사용자가 자신의 팔찌를 등록했다고 가정된다. 개찰구가 사용자를 통과하도록 허용하기 전에, 개찰구는 사용자의 팔찌와의 접속을 시작하고, 암호화된 채널을 통해 전송된 식별 값을 획득하는데, 여기서 이 값은 사용자의 계정과 연관된다. 사용자의 잔고가 자동 리필에 대한 임계치(사용자는 이를 $10로 설정함)를 초과하기 때문에, 사용자의 신용 카드로 어떠한 청구도 필요하지 않고, 사용자의 잔고는 단순히 지하철 요금의 양만큼 감소된다.

[0110] [00120] 30분 후에, 사용자가 직장에 도착한다. 사용자의 사무실에서, 회전식 문이 사용자의 팔찌의 웨어러블 아이덴티티 관리기에 대한 접속을 생성하고, 사용자가 등록된 고용인이라고 결정한 다음, 사용자를 들여보낸다. 사용자가 자신의 책상에 앉으면, 사용자의 컴퓨터가 WiFi를 통해 사용자의 업무용 전화에 대한 접속을 설정하고, 이는 결국 사용자의 팔찌의 웨어러블 아이덴티티 관리기에 대한 접속을 설정한다. 사용자의 전화기의 비밀번호 관리기가 내장 가속도계에 의해 발생된 신호와 전화기로부터 수신하는 가속기 신호를 비교한 후 비밀번호 관리기가 웨어러블 아이덴티티 관리기에 의해 잠금 해제된다. 물론, 본질적으로 동일한 것 외에도, 이들은 또한 어떤 움직임 – 이 경우에는, 짧은 흔들림을 표시해야 한다. 사용자의 전화기의 비밀번호 관리기가 사용자의 컴퓨터를 잠금 해제하며, 사용자는 비밀번호로 로그인할 필요가 없다.

[0111] [00121] 웨어러블 아이덴티티 관리기의 이러한 사용들 중 일부에서는, 흔들림이 요구되었고, 다른 사용들에서는 그렇지 않았다는 점이 주목되어야 한다. 이는 소프트웨어가 웨어러블 아이덴티티 관리기에 대한 접속을 함으로써 결정되며, 가속도계 신호가 전달되거나, 어떠한 흔들림도 요구되지 않는다는 표시가 전달된다. 단지 페어링된 디바이스들만이 웨어러블 아이덴티티 관리기에 의해 허용되기 때문에, 악성 디바이스가 잘못된 신호를 전달하는 것이 가능하지 않다. 또한, 사용자의 웨어러블 아이덴티티 관리기에 의해 비슷한 흔들림 동작이 등록되지

않기 때문에, 사용자의 은행 계좌에 액세스하길 원하는 누군가가 이들의 전화기들을 흔드는 것도 가능하지 않다. 이런 식으로, 사용자는 하루종일 어떠한 크리덴셜들도 입력할 필요가 없다. 사용자가 집에 오면, 사용자는 팔찌를 벗는데, 팔찌는 이제 팔찌가 임의의 인증에 관여하게 되기 전에 다시 사용자와 연관될 필요가 있는 상태에 자동으로 자신을 놓고 있다. 따라서 사용자가 친구를 보러 나가는 동안 사용자의 집에 침입하는 절도범은 – 절도범이 또한 사용자의 전화기들 중 하나를 훔친다 하더라도, 절도범이 연관 프로세스를 성공적으로 거치는 사용자로서 인증할 수 없기 때문에 – 사용자의 계정들에 대한 액세스를 사용할 수 없다.

[0112] [00122] 제 2 예시적인 사용 시나리오에서는, 사용자가 손목 밴드가 언제 열리거나 닫히는지를 검출하는 웨어러블 아이덴티티 관리기 디바이스의 시계 구성을 방금 구입했다. 사용자가 처음으로 손목 밴드를 닫을 때, 웨어러블 디바이스 관리기는 자신을 구성 상태에 놓는다. 사용자는 시계 제조사의 웹사이트로부터 안내서 애플리케이션을 다운로드하고, 이를 자신의 전화기 상에 설치한다. 사용자가 애플리케이션을 시작하면, 애플리케이션은 사용자가 시계에 대한 이름을 입력하고 비밀번호를 선택하여 자신의 시계를 자신의 전화기에 연관시킬 것을 요구한다. (사용자의 전화기는 생체 인식 센서를 갖지 않는다.) 이렇게 한 후, 사용자의 전화기와 연관된 웨어러블 아이덴티티 관리기는 사용자가 입력한 정보와 연관되며, 로그인에 사용될 수 있다.

[0113] [00123] 사용자가 그날 이후 자신의 전화기를 사용하여 온라인 옥션 사이트에 방문하면, 사용자의 전화기 상의 인증 라이브러리가 사용자가 비밀번호 관리기에 등록되지 않은 장소에 로그인하고 있다고 결정하고, 사용자가 비밀번호 관리기에 저장된 이러한 사용자 이름과 비밀번호를 원한다면, 사용자에게 사용자가 자신의 전화기를 착용하고 있는 손목의 손을 사용하여 자신의 전화기를 흔들 것을 요청한다. 사용자는 이러한 아이디어를 좋아하며, 자신의 손을 흔든다. 다음에 사용자가 옥션 사이트를 방문할 때, 사용자는 자신의 사용자 이름과 비밀번호를 사용하여 로그인할 필요가 없는데, 이들 둘 다 사용자의 전화기의 비밀번호 관리기에 의해 자동 채움될 것이고 사용자가 로그인될 것이기 때문이다.

[0114] [00124] 그러나 사용자는 또한 자신의 랩톱을 사용하여 다양한 계정들에 로그인한다. 사용자가 자신의 랩톱 브라우저에 브라우저 플러그인을 다운로드한다. 브라우저 플러그인은 사용자에게 사용자의 전화기를 랩톱 컴퓨터에 페어링하도록 요청하는데, 사용자는 이를 표준 블루투스 페어링 프로토콜을 사용하여 수행한다. 다음에, 브라우저 플러그인은 사용자의 전화기 상의 비밀번호 관리기와 연관된 저장소를 복사하기 위한 허가를 요청한다. 사용자는 브라우저 플러그인에 이러한 허가를 하지 않는다. 플러그인은 다음에 사용자의 전화기 상의 비밀번호 관리기를 사용할 것을 요청하는데, 사용자가 이에 동의한다. 그 결과, 사용자의 전화기 상의 비밀번호 관리기는 필요할 때 사용자의 랩톱과 페어링하도록 구성된다.

[0115] [00125] 사용자가 자신의 랩톱 상에서 옥션 사이트를 방문하면, 사용자의 랩톱 상의 루틴은 이것이 로그인 세션이라고 결정하고, 사용자의 전화기와 전화기 상의 비밀번호 관리기에 대한 접속을 설정한다. 비밀번호 관리기는 이것이 이 도메인에 대해 저장된 사용자 이름 및 크리덴셜을 갖는다고 결정하고, 사용자의 시계의 웨어러블 아이덴티티 관리기와의 접속을 시작한다. 사용자가 자신의 손을 천천히 흔들고, 웨어러블 아이덴티티 관리기는 내장된 가속도계를 사용하여, 전화기로부터 수신된 신호가 자신이 스스로 발생시킨 신호와 매칭한다고 결정한다. 이 결과, 그리고 이전에 설명한 것에 대해 비슷한 방식으로, 사용자의 전화기의 비밀번호 관리기는 랩톱 상에서 옥션 사이트에 대해 비밀번호를 사용하기 위한 허가를 얻는다. 그 결과, 사용자 이름과 크리덴셜이 보안 접속을 통해 랩톱으로 전달되거나, 대안으로는 옥션 사이트에 대한 세션을 시작하는데 사용되는데, 여기서 이러한 세션은 다음에 랩톱으로 넘겨지고, 사용자가 로그인된다.

[0116] [00126] 사용자가 나중에 자신의 은행 웹사이트에 방문하여 자신의 랩톱 상에서 로그인하면, 사용자가 설치한 브라우저 플러그인에서의 루틴은 사용자가 로그인하고 있다고 결정한다. 이는 사용자의 전화기 상의 비밀번호 저장소에 사용자 이름 및 크리덴셜을 추가하기 위한 요청을 디스플레이하고 있다. 이는 사용자의 컴퓨터의 스크린 상에 디스플레이된다. 사용자는 이 요청을 승인하고, 자신의 전화기를 흔들어 자신의 전화기 상의 비밀번호 관리기에 사용자의 랩톱으로부터 이에 전송된 사용자 이름 및 크리덴셜들을 전달한다.

[0117] [00127] 이러한 시나리오에서, 이전 사용자(이하, "Alice")와 현재 사용자(이하, "Bob")가 친구들이고, Alice는 간혹 Bob의 랩톱을 사용한다. 사용자가 자신의 랩톱을 사용하여 사이트를 방문하거나, 로그인을 필요로 하는 애플리케이션을 사용할 때, Bob의 랩톱은 자신이 연관된 어떤 전화기들이 존재하는지를 결정할 것이다. Alice가 그녀와 Bob이 둘 다 사용하는 옥션 사이트를 방문할 때, Bob의 랩톱은 Alice와 Bob의 전화기들 둘 다 존재한다고 결정하고, 둘 다와 세션들을 설정하여 로그인을 완료한다. Bob이 랩톱을 사용하는 것이 아니라, Alice가 사용하고 있기 때문에, 그녀가 컴퓨터 상에서 로그인 화면을 볼 때 자신의 전화기를 집어든다. 그녀는 그녀가 자신의 웨어러블 아이덴티티 관리기와 연관되는 팔찌를 착용하고 있는 손목의 손으로 이를 흔들고, 따라서 그녀

의 전화기는 인증이 완료되었음을 표시하는 신호를 얻고, 이는 자신의 비밀번호 관리기 루틴에 관여하여 Bob의 랩톱 상에서 Alice를 로그인한다.

[0118] [00128] Bob은 또한 다른 사용자인 Cindy와 친구들인데, Cindy는 간혹 Bob의 전화기를 사용한다. Bob의 전화기는 Bob의 프로파일 및 Cindy의 프로파일을 모두 포함하는 비밀번호 관리기를 갖는다. Cindy가 Bob의 전화기를 사용하여 또는 Bob의 전화기에 접속된 컴퓨터를 사용하여 자원에 액세스하면, Bob의 전화기 상의 비밀번호 관리기는 Bob의 또는 프로파일을 선택할지 아니면 Cindy의 프로파일을 선택할지를 결정하고, Cindy의 시계와 페어링되는 Bob의 전화기가 Cindy의 시계로부터 확인 신호를 수신한 후 Cindy의 프로파일로 결정한다. 이 신호는 Bob의 전화기와 Cindy의 시계 상에서 발새애된 가속도계 신호들을 비교함으로써 생성된다.

[0119] [00129] 어느 날, Cindy가 Bob에게 정말 화가 나서, Bob의 전화기로부터의 신호들을 승인하지 않도록 자신의 시계를 구성한다. 그녀는 그녀 자신의 전화기를 사용하여 이를 수행하는데, 그 전화기는 그녀의 시계와 페어링되었고 시계의 마스터 디바이스이다. Bob은 그가 원한다 하더라도 그녀의 시계에 대한 구성을 변경할 수 없는데, 이는 그의 전화기가 그녀의 시계의 마스터가 아니라 단지 그에 연관되기 때문이다. 다음날, Cindy가 자신의 마음을 바꾸고 그녀의 시계를 Bob의 전화기와의 세션들을 다시 허용하도록 재구성한다. 그러나 Bob은 또한 그의 비밀번호 관리기와 연관된 저장소로부터 그녀의 프로파일들을 제거하도록 그의 전화기를 재구성했으므로, Cindy는 그의 전화기를 사용하여 인증들을 수행할 수 없다. 그녀는 그에게 그녀의 프로파일을 다시 추가할 것을 요청하고, 그는 동의한다. 그는 자신의 시계의 웨어러블 아이덴티티 관리기를 사용하여 그의 손의 흔들림으로 그의 전화기에 대해 인증한 다음, Cindy가 그녀의 프로파일을 추가하도록 승인한다. 그녀는 그녀가 사용하는 클라우드 저장소로부터 그녀의 암호화된 프로파일을 다운로드하고 이를 추가한다. 클라우드 저장소는 다운로드를 요청하고 있는 사람이 Cindy임을 아는데, 이는 저장소가 Cindy의 시계로부터 발생하며 사용자가 Cindy가 자신의 프로파일을 추가하도록 승인한 후 Bob의 시계로 전달되는 암호화된 요청을 포함하는 요청을 Bob의 전화기로부터 수신하기 때문이다. 그녀는 자신의 손에 전화기를 갖고, 이를 흔들며, 클라우드 저장소 위치의 정보와 함께 암호화된 요청이 Bob의 전화기 상의 비밀번호 관리기에 의해 수신되어 사용된다. Cindy는 이제 다시 Bob의 전화기를 사용할 수 있다.

[0120] [00130] Cindy가 몇 주 후에 태블릿 컴퓨터를 사면, 그녀는 이를 자신의 전화기에 페어링하고, Bob의 전화기에 대해 이것이 어떻게 수행되었는지와 비슷하게, 흔들기를 사용하여 자신의 새로운 태블릿의 비밀번호 관리기를 클라우드 저장소로부터 자신의 프로파일의 암호화된 사본을 다운로드하도록 승인한다. 암호화는 이러한 경우들 둘 다, 엿듣는 사람이 데이터를 학습하는 것을 차단하고, SSL과 같은 기술을 사용한다.

[0121] [00131] 제 3 예시적인 사용 시나리오에서, Dave는 이것이 가속도계를 갖지 않는다는 점을 제외하면, 팔찌들과 비슷한 기능을 갖는 시계 및 이전에 설명한 시계들을 갖는다. 대신 이는 Dave가 요청에 동의한다면 그가 누를 수 있는 버튼을 갖는다. Dave가 그의 전화기를 시계와 페어링할 때, 전화기와 시계는 이들의 스크린 상에 번호를 디스플레이하고, Dave는 이들을 비교하여 이들이 서로 대응함을 확실히 한다. 이들이 대응하기 때문에, 그는 버튼을 눌러 승인하고, 이들은 서로 연관되게 된다.

[0122] [00132] 이후, Dave가 자신의 전화기를 벗으면, 전화기는 다시 연관될 필요가 있는 상태로 되돌아간다. Dave는 다시 페어링을 하고, 이는 전화기와 다시 한 번 연관된다. 그는 다음에 그의 전화기를 사용하여 사이트에 로그인하길 원하는데, 이는 Dave의 전화기에 요청을 전송한다. Dave의 전화기 상에 메시지가 디스플레이되어, 그에게 버튼을 누름으로써 로그인 요청을 승인하거나, 그가 요청을 승인하길 원하지 않는다면 버튼을 누르지 않고 3초 동안 단순히 대기하도록 요청한다. Dave가 버튼을 누르고, 그의 시계가 전화기에 신호를 전송하는데, 신호는 비밀번호 관리기에 전달될 때 적절하나 사용자 이름과 크리덴셜들의 검색을 시작하고, 사이트에 대한 Dave의 로그인이 이어진다.

[0123] [00133] 이후에, Dave에게는 웨어러블 아이덴티티 관리기를 갖는 목걸이가 주어진다. 이는 바로 Dave의 전화기처럼 가속도계를 갖는다. 이들을 페어링하기 위해, Dave는 단순히 목걸이를 걸고 자신의 손에 전화기— 그가 목걸이를 그와 연관시키기 위해 사용하고 있는 전화기 —를 갖고 걷는다. 목걸이는 Dave가 전화기를 흔드는 것이 아니라 단순히 그의 손에 전화기를 갖고 걷는다는 점을 제외하면, Alice의 팔찌가 그녀의 전화기와 연관되는 것과 같은 방식으로 목걸이 자체를 전화기와 연관시킨다. 전화기의 그리고 목걸이의 가속도계 출력이 비교되며, 이들이 서로 대응한다는 결정이 이루어지는데, 그 후 목걸이가 Dave와 연관된다. 나중에, Dave는 그의 목걸이를 아이덴티티의 소스로서 사용하여 구매를 수행하길 원한다. 그는 자신의 전화기의 스크린 상에서 "구매 승인" 버튼을 누르고 몇 걸음 걷거나 앞뒤로 천천히 흔들어, 웨어러블 아이덴티티 관리기 및 비밀번호 관리기가 이것이 "구매 승인" 버튼을 누른 동일한 사람에 의해 사용됨을 검증하게 한다.

[0124] [00134] Dave의 목걸이의 경우, 이러한 비교는 그의 전화기에서 수행되는데, 목걸이는 착용자의 아이덴티티 정보를 저장하고 언제 목걸이가 벗겨져, 목걸이가 인증을 수행하기 위해 계정과 다시 한 번 연관될 필요가 있는 상태에 놓여질 수 있는지를 검출하는데만 사용되는 여분의 소형 배터리를 갖기 때문이다.

[0125] 목걸이의 라디오 송신기는 마치 라디오 주파수 식별(RFID: radio frequency identification) 토큰과 같은 신호들의 수신 및 송신 모두를 위한 배경 라디오 신호들에 의해 전력이 공급된다.

[0126] [00135] 잠깐 동안 목걸이를 착용한 후, Dave는 목걸이를 Alice에게 빌려주는데, Alice는 이를 그녀의 전화기와 연관시키고 그녀의 팔찌 대신 이를 사용한다. Alice가 이를 Dave에게 돌려주면, 목걸이는 Dave가 이를 착용할 때 자신을 Dave 및 그의 전화기와 연관시킨다.

[0127] [00136] 제 4 예시적인 사용 시나리오에서, 본 명세서에서 개시되는 양상들은 종래의 로그인 프로세스를 대체하도록 구현된다. 전화기와 같은 모바일 디바이스 상에서, 사용자는 단순히 전화기를 웨이크업함으로써(예를 들어, 이를 집어들어, 그 스크린을 터치하거나 버튼을 누름으로써) 로그인 프로세스를 시작할 수 있다. 프로세스는 또한 사용자가 애플리케이션을 시작하거나 애플리케이션에 의해 참조되는 자원에 액세스하도록 시도함으로써 시작될 수도 있다. 예시적인 자원들은 사용자 주소록들; 이메일들; (가장 최근에 걸려온 전화 통화들의 리스트와 같은) 사용 로그 파일들; 사진들 또는 사진들의 디렉토리들; 및 장거리 전화들을 거는 능력이다. 데스크톱 또는 랩톱은 비슷한 방식으로 액세스될 수 있는데, 여기서는 마우스, 마우스 패드 또는 키보드가 확약 또는 확인을 얻는데 사용될 데이터를 수집하는 역할을 맡는다.

[0128] [00137] 서로 다른 자원들은 또한 서로 다른 보안 레벨들과 연관될 수 있는데 – 예를 들어, 사용자는 전화기를 잠금 해제하기 위한 중간 보안 레벨; (전화기가 일단 웨이크업되면) 그 이메일 리더에 액세스하기 위한 낮은 보안 레벨; 그러나 사용 로그들에 대한 액세스를 얻기 위한 높은 보안 레벨을 필요로 할 수도 있다. 다음에, 동일한 사용자가 자신의 업무용 컴퓨터에 로그인하기 위해서는 높은 보안 레벨을, 그러나 자신의 집 컴퓨터에 로그인하기 위해서는 중간 보안 레벨만을 필요로 할 수도 있는데, 이는 첫 번째 장소에서는 소그룹의 사람들에 의해서만 액세스 가능하기 때문이다. 사용자 또는 그의 고용주는 또한 서로 다른 타입들의 액세스에 서로 다른 보안 레벨들을 할당할 수도 있다.

[0129] [00138] 아이덴티티 관리기 또는 연관된 프록시가 아이덴티티 관리기 기술과 호환 가능하지 않은 사이트들에 대한 비밀번호 관리기로서 작동하는 특별한 로그인 케이스가 또한 고려된다. 여기서, 로그인 세션은 가능하게 하는 디바이스에 세션 비밀들을 노출시키지 않으면서 이러한 디바이스들 중 하나에 의해 완화될 수도 있다.

[0130] [00139] 제 5 예시적인 사용 시나리오에서, 본 명세서에서 개시되는 양상들은 온라인 지불이든 판매 시점 지불이든, 지불을 가능하게 하도록 구현된다. 온라인 지불을 수행하기 위해, 사용자는 체크아웃 버튼을 클릭함으로써 지불 프로세스를 시작할 수 있다. 낮은 그리고 중간 위험 구매들을 위해, 이것으로 충분할 수도 있는데, 이는 중간 보안 레벨을 제공하기 때문이다. 그러나 고위험 구매들의 경우, 명시적 확인이 대신 요구될 수도 있다. 여기서, 많은 요소들이 거래의 위험 레벨, 예컨대 값; 상품의 타입; 사용자의 구매들의 이력; 및 구매가 시작되는 위치에 영향을 줄 수도 있다. 요구되는 보안 레벨은 사용자, 상품, 금융 기관, 또는 이들의 결합에 의해 선택될 수도 있다. 예를 들어, 사용자는 최소 보안 레벨에 대한 자신의 선호도들을 설정할 수도 있지만, 이들은 상인 또는 금융 기관에 의해 설정된 정책에 의해 선택적으로 높아질 수 있다. 판매 시점 거래의 경우, 사용자가 판매 시점 단말 상에 자신의 서명을 기재하고 움직임이 사용자의 아이덴티티 관리기의 움직임과 상관될 때 명시적 확인이 얻어질 수 있다. 이는 (분쟁 거래들에 유용할 수도 있는) 사용자 의도의 보증들을 제공할 뿐만 아니라, 여러 가능한 사용자들 중 어느 사용자가 거래와 연관될지를 식별하는데 도움이 될 수도 있다. 다른 타입들의 지불들– 예컨대, 지하철 요금들의 지불들 –은 근접도 검증보다 더 높은 보안을 필요로 하지 않을 수도 있다.

[0131] [00140] 제 6 예시적인 사용 시나리오에서, 본 명세서에서 개시되는 양상들은 귀속(attribution) 목적들로 구현된다. 이를 위해, 터치스크린과 연관된 가속도계 자취들을 팔찌들의 가속도계 자취들과 비교함으로써, 다수의 사용자들이 동시에 스크린을 터치하는 경우에도 스크린 상에서 사용자 상호 작용들을 귀속시킬 수 있는데, 이는 새로운 타입들의 게임 환경들을 낳는다는 점이 주목된다. 이는 또한 사용자가 2개의 팔찌들을 동시에 착용하는 것이 말이 되는 몇 가지 사용 시나리오들 중 하나일 수도 있다. 게임과 관련하여, 사용자 아이덴티티에 동작들을 귀속시키는 것이 필수적일 수도 있는 것이 아니라, 어떤 형태의 의사 익명성이 더 현실적일 수도 있다.

[0132] 예시적인 네트워크 및 분산 환경들

[0133] [00141] 해당 기술분야에서 통상의 지식을 가진 자는 본 명세서에서 설명한 컴퓨팅 디바이스를 이용하기 위한

다양한 구현들 및 관련 양상들이, 컴퓨터 네트워크의 일부로서 또는 분산 컴퓨팅 환경에서 전개될 수 있고 임의의 종류의 데이터 저장소에 접속될 수 있는 임의의 컴퓨터 또는 다른 클라이언트나 서버 디바이스와 관련하여 구현될 수 있다고 인식할 수 있다. 더욱이, 해당 기술분야에서 통상의 지식을 가진 자는 이러한 양상들이 임의의 수의 메모리 또는 저장 유닛들, 그리고 임의의 수의 저장 유닛들에 걸쳐 발생하는 임의의 수의 애플리케이션들 및 프로세스들을 갖는 임의의 컴퓨터 시스템 또는 환경에서 구현될 수 있다고 인식할 것이다. 이는 원격 또는 로컬 저장소를 갖는, 네트워크 환경 또는 분산 컴퓨팅 환경에서 전개되는 서버 컴퓨터들 및 클라이언트 컴퓨터들을 갖는 환경을 포함하지만 이에 한정된 것은 아니다.

[0134] [00142] 도 18은 예시적인 네트워크 또는 분산 컴퓨팅 환경의 한정적이지 않은 개략도를 제공한다. 분산 컴퓨팅 환경은 컴퓨팅 객체들 또는 디바이스들(1810, 1812 등) 그리고 컴퓨팅 객체들 또는 디바이스들(1820, 1822, 1824, 1826, 1828 등)을 포함하는데, 이들은 애플리케이션들(1830, 1832, 1834, 1836, 1838)로 표현되는 것과 같이, 프로그램들, 방법들, 데이터 저장소들, 프로그래밍 가능 로직 등을 포함할 수 있다. 컴퓨팅 객체들 또는 디바이스들(1810, 1812 등) 그리고 컴퓨팅 객체들 또는 디바이스들(1820, 1822, 1824, 1826, 1828 등)은 개인용 디지털 보조기기(PDA: personal digital assistant)들, 오디오/비디오 디바이스들, 모바일 전화들, MP3 플레이어들, 랩톱들 등과 같은 서로 다른 디바이스들을 포함할 수도 있다고 인식될 수 있다.

[0135] [00143] 각각의 컴퓨팅 객체 또는 디바이스(1810, 1812 등) 그리고 컴퓨팅 객체들 또는 디바이스들(1820, 1822, 1824, 1826, 1828 등)은 통신 네트워크(1840)를 통해 직접적으로 또는 간접적으로 하나 또는 그보다 많은 다른 컴퓨팅 객체들 또는 디바이스들(1810, 1812 등) 그리고 컴퓨팅 객체들 또는 디바이스들(1820, 1822, 1824, 1826, 1828 등)과 통신할 수 있다. 도 18에서 단일 엘리먼트로서 예시되지만, 네트워크(1840)는 도 18의 시스템에 서비스들을 제공하는 다른 컴퓨팅 객체들 및 컴퓨팅 디바이스들을 포함할 수도 있고 그리고/또는 도시되지 않은 다수의 상호 접속된 네트워크들을 나타낼 수도 있다. 각각의 컴퓨팅 객체 또는 디바이스(1810, 1812 등 또는 1820, 1822, 1824, 1826, 1828 등)은 또한 애플리케이션들(1830, 1832, 1834, 1836, 1838)과 같은 애플리케이션을 포함할 수 있는데, 이는 다양한 구현들에 따라 개시된 양상들과의 통신 또는 개시된 양상들의 구현에 적합한 애플리케이션 프로그래밍 인터페이스(API), 또는 다른 객체, 소프트웨어, 펌웨어 및/또는 하드웨어를 이용할 수도 있다.

[0136] [00144] 분산 컴퓨팅 환경들을 지원하는 다양한 시스템들, 컴포넌트들 및 네트워크 구성들이 있다. 예를 들어, 컴퓨팅 시스템은 유선 또는 무선 시스템에 의해, 로컬 네트워크들 또는 넓게 분산된 네트워크들에 의해 서로 접속될 수 있다. 현재, 많은 네트워크들이 인터넷에 연결되며, 이는 넓게 분산된 컴퓨팅에 대한 인프라 구조를 제공하고 많은 서로 다른 네트워크들을 포괄하지만, 다양한 구현들에서 설명한 바와 같이 기술들에 따라 이루어지는 예시적인 통신들에 임의의 네트워크 인프라 구조가 사용될 수 있다.

[0137] [00145] 따라서 네트워크 토폴러지들 및 네트워크 인프라 구조들의 호스트, 예컨대 클라이언트/서버, 피어 투 피어 또는 하이브리드 아키텍처들이 이용될 수 있다. 클라이언트/서버 아키텍처, 특히 네트워크화된 시스템에서, 클라이언트는 보통 다른 컴퓨터, 예를 들어 서버에 의해 제공되는 공유 네트워크 자원들에 액세스하는 컴퓨터이다. 도 18의 예시에서는, 한정적이지 않은 예로서, 상황들에 따라 임의의 컴퓨터가 클라이언트, 서버, 또는 둘 다로 고려될 수 있지만, 컴퓨팅 객체들 또는 디바이스들(1820, 1822, 1824, 1826, 1828 등)이 클라이언트들로서 고려될 수 있고, 컴퓨팅 객체들 또는 디바이스들(1810, 1812 등)은 서버들로서 고려될 수 있는데, 여기서 컴퓨팅 객체들 또는 디바이스들(1810, 1812 등)은 데이터 서비스들, 예컨대 컴퓨팅 객체들 또는 디바이스들(1820, 1822, 1824, 1826, 1828 등)로부터의 데이터 수신, 데이터의 저장, 데이터의 처리, 컴퓨팅 객체들 또는 디바이스들(1820, 1822, 1824, 1826, 1828 등)로의 데이터 송신을 제공한다. 이러한 컴퓨팅 디바이스들 중 임의의 디바이스가 하나 또는 그보다 많은 구현들에 대해 본 명세서에서 설명한 바와 같이 양상들 및 관련 기술들을 연루시킬 수 있는 서비스들 또는 작업들을 요청하거나 데이터를 처리하고 있을 수도 있다.

[0138] [00146] 서버는 일반적으로 인터넷 또는 무선 네트워크 인프라 구조들과 같은 원격 또는 로컬 네트워크를 통해 액세스 가능한 원격 컴퓨터 시스템이다. 클라이언트 프로세스는 제 1 컴퓨터 시스템에서 액티브할 수 있고, 서버 프로세스는 제 2 컴퓨터 시스템에서 액티브할 수 있어, 통신 매체를 통해 서로 통신하여, 분산된 기능을 제공하고 다수의 클라이언트들이 서버의 정보 수집 능력들을 활용할 수 있게 한다. 사용자 프로파일링에 따라 이용되는 임의의 소프트웨어 객체들은 독립형으로 또는 다수의 컴퓨팅 디바이스들이나 객체들에 걸쳐 분산되어 제공될 수 있다.

[0139] [00147] 통신 네트워크/버스(1840)가 예를 들어, 인터넷인 네트워크 환경에서, 컴퓨팅 객체들 또는 디바이스들(1810, 1812 등)은 컴퓨팅 객체들 또는 디바이스들(1820, 1822, 1824, 1826, 1828 등)이 HTTP와 같은 다수의

공지된 프로토콜들 중 임의의 프로토콜을 통해 통신하는 웹 서버들일 수 있다. 언급한 바와 같이, 컴퓨팅 객체들 또는 디바이스들(1810, 1812 등)은 분산 컴퓨팅 환경의 특징일 수도 있으므로, 컴퓨팅 객체들 또는 디바이스들(1820, 1822, 1824, 1826, 1828 등)로서의 역할을 할 수도 있고, 또는 그 반대도 가능하다.

[0140] 예시적인 컴퓨팅 디바이스

[0141] [00148] 언급한 바와 같이, 앞서 언급한 구현들 중 여러 개가 임의의 디바이스에 적용되는데, 여기서는 본 명세서에 개시된 양상들의 구현을 가능하게 하기 위한 컴퓨팅 디바이스를 포함하는 것이 바람직할 수도 있다. 따라서 모든 종류들의 핸드헬드, 휴대용 및 다른 컴퓨팅 디바이스들 및 컴퓨팅 객체들이 본 명세서에서 설명된 다양한 구현들과 관련한 사용을 위해 고려된다고 이해된다. 이에 따라, 도 19에서 아래 설명되는 하기의 범용 원격 컴퓨터는 단지 일례일 뿐이고, 해당 개시의 구현들은 네트워크/버스 상호 운용성 및 상호 작용을 갖는 임의의 클라이언트로 구현될 수도 있다.

[0142] [00149] 필수적이지 않을 수도 있지만, 구현들 중 임의의 구현은 부분적으로는 운영 시스템을 통해, 디바이스 또는 객체에 대한 서비스들의 개발자에 의한 사용을 위해 구현될 수 있고, 그리고/또는 동작 가능한 컴포넌트(들)와 관련하여 동작하는 애플리케이션 소프트웨어 내에 포함될 수 있다. 소프트웨어는 클라이언트 워크스테이션들, 서버들 또는 다른 디바이스들과 같은 하나 또는 그보다 많은 컴퓨터들에 의해 실행되는, 프로그램 모듈들과 같은 컴퓨터 실행 가능 명령들의 일반적인 콘텍스트로 기술될 수도 있다. 해당 기술분야에서 통상의 지식을 가진 자들은 네트워크 상호 작용들이 다양한 컴퓨터 시스템 구성들 및 프로토콜들로 실시될 수도 있다고 인식할 것이다.

[0143] [00150] 따라서 위에서 명확히 한 바와 같이, 컴퓨팅 시스템 환경(1900)이 적당한 컴퓨팅 환경의 단지 일례일 뿐이고 구현들 중 임의의 구현의 사용 또는 기능의 범위에 관해 어떠한 한정도 제안하는 것으로 의도되지 않는다 하더라도, 도 19는 구현들 중 하나 또는 그보다 많은 구현이 구현될 수 있는 적당한 컴퓨팅 시스템 환경(1900)의 일례를 예시한다. 컴퓨팅 환경(1900)은 예시적인 운영 환경(1900)에 예시된 컴포넌트들 중 임의의 하나 또는 이들의 결합과 관련된 어떠한 의존이나 요건도 갖는 것으로 해석되지 않아야 한다.

[0144] [00151] 도 19를 참조하면, 본 명세서에서 하나 또는 그보다 많은 구현들을 구현하기 위한 예시적인 원격 디바이스는 범용 컴퓨팅 디바이스를 핸드헬드 컴퓨터(1910)의 형태로 포함할 수 있다. 핸드헬드 컴퓨터(1910)의 컴포넌트들은 처리 유닛(1920), 시스템 메모리(1930), 그리고 시스템 메모리를 포함하는 다양한 시스템 컴포넌트들을 처리 유닛(1920)에 연결하는 시스템 버스(1921)를 포함할 수도 있지만 이에 한정된 것은 아니다.

[0145] [00152] 컴퓨터(1910)는 일반적으로 다양한 컴퓨터 판독 가능 매체들을 포함하며, 컴퓨터(1910)에 의해 액세스 가능한 임의의 이용 가능 매체들일 수 있다. 시스템 메모리(1930)는 판독 전용 메모리(ROM) 및/또는 랜덤 액세스 메모리(RAM)와 같은 휘발성 및/또는 비휘발성 메모리 형태로 컴퓨터 저장 매체들을 포함할 수도 있다. 한정이 아닌 예로서, 메모리(1930)는 또한 운영 시스템, 애플리케이션 프로그램들 다른 컴퓨터 모듈들 및 프로그램 데이터를 포함할 수도 있다.

[0146] [00153] 사용자는 입력 디바이스들(1940)을 통해 컴퓨터(1910)에 커맨드들 및 정보를 입력할 수 있다. 모니터 또는 다른 타입의 디스플레이 디바이스가 또한 출력 인터페이스(1950)와 같은 인터페이스를 통해 시스템 버스(1921)에 접속된다. 모니터 외에도, 컴퓨터들은 또한 스피커들 및 프린터와 같은 다른 주변 출력 디바이스들을 포함할 수 있으며, 이들은 출력 인터페이스(1950)를 통해 접속될 수 있다.

[0147] [00154] 컴퓨터(1910)는 원격 컴퓨터(1970)와 같은 하나 또는 그보다 많은 다른 원격 컴퓨터들에 대한 논리적 접속들을 사용하여 네트워크 또는 분산 환경에서 작동할 수 있다. 원격 컴퓨터(1970)는 주변 컴퓨터, 서버, 라우터, 네트워크 PC, 피어 디바이스 또는 다른 공통 네트워크 노드, 또는 임의의 다른 원격 매체 소비 또는 송신 디바이스일 수도 있으며, 컴퓨터(1910)에 대해 앞서 설명한 엘리먼트들 중 임의의 엘리먼트 또는 모든 엘리먼트를 포함할 수도 있다. 도 19에 도시된 논리적 접속들은 근거리 네트워크(LAN: local area network) 또는 광역 네트워크(WAN: wide area network)와 같은 네트워크(1971)를 포함하지만, 다른 네트워크들/버스들을 포함할 수도 있다. 이러한 네트워킹 환경들은 가정들, 사무실들, 전사적(enterprise-wide) 컴퓨터 네트워크들, 인트라넷들 및 인터넷에서 아주 흔하다.

[0148] [00155] 앞서 언급한 바와 같이, 다양한 컴퓨팅 디바이스들, 네트워크들 및 광고 아키텍처들과 관련하여 예시적인 구현들이 설명되었지만, 기본 개념들은 본 명세서에서 개시된 양상들을 구현하는 것이 바람직한 임의의 컴퓨팅 디바이스나 시스템 및 임의의 네트워크 시스템에 적용될 수도 있다.

[0149] [00156] 본 명세서에서 설명한 양상들 중 하나 또는 그보다 많은 양상들을 구현하는 다수의 방법들, 예를 들어

적절한 API, 공구 키트, 드라이버 코드, 운영 시스템, 제어, 독립형 또는 다운로드 가능 소프트웨어 객체 등이 있으며, 이는 애플리케이션들이 본 명세서에서 개시된 양상들을 구현할 수 있게 한다. 실시예들은 API(또는 다른 소프트웨어 객체)의 관점으로부터, 그리고 또한 설명된 구현들 중 하나 또는 그보다 많은 구현에 따라 본 명세서에서 개시된 양상들의 구현을 가능하게 하는 소프트웨어 또는 하드웨어 객체로부터도 고려될 수 있다. 본 명세서에서 설명한 다양한 구현들은 완전히 하드웨어에, 부분적으로는 하드웨어에 그리고 부분적으로는 소프트웨어에, 그리고 또한 소프트웨어에도 있는 양상들을 가질 수도 있다.

[0150] [00157] 본 명세서에서 "예시적인"이라는 단어는 일례, 실례 또는 예시로서의 역할을 의미하는데 사용된다. 혼선을 피하기 위해, 본 명세서에서 개시된 요지는 이러한 예들로 한정되지 않는다. 추가로, 본 명세서에서 "예시적인" 것으로서 설명한 어떠한 양상이나 설계도 반드시 다른 양상들 또는 설계들에 비해 선호되거나 유리한 것으로 해석되는 것도 아니고, 해당 기술분야에서 통상의 지식을 가진 자들에게 공지된 대등한 예시적인 구조들 및 기술들을 불가능하게 하는 것으로 여겨지는 것도 아니다. 더욱이, "포함한다," "갖는다," "함유한다"라는 용어들 및 다른 비슷한 단어들이 상세한 설명 또는 청구항들에서 사용되는 정도까지는, 혼선을 피하기 위해, 이러한 용어들은 어떠한 추가 또는 다른 엘리먼트들을 불가능하게 하지 않고 열린 전환어로서 "포함하는"이라는 용어와 비슷한 식으로 포괄적인 것으로 의도된다.

[0151] [00158] 언급한 바와 같이, 본 명세서에서 설명한 다양한 기술들은 하드웨어 또는 소프트웨어와, 또는 적절한 경우에는 이 둘의 결합과 관련하여 구현될 수도 있다. 본 명세서에서 사용된 바와 같이, "컴포넌트," "시스템" 등의 용어들은 마찬가지로 컴퓨터 관련 엔티티, 하드웨어, 하드웨어와 소프트웨어의 결합, 소프트웨어, 또는 실행중인 소프트웨어를 의미하는 것으로 의도된다. 예를 들어, 컴포넌트는 프로세서 상에서 실행되는 프로세스, 프로세서, 객체, 실행 파일(executable), 실행 스레드, 프로그램 및/또는 컴퓨터일 수도 있지만, 이러한 것으로 한정되는 것은 아니다. 예시로서, 컴퓨터 상에서 실행되는 애플리케이션과 컴퓨터 둘 다 컴포넌트일 수 있다. 하나 또는 그보다 많은 컴포넌트들이 프로세스 및/또는 실행 스레드 내에 상주할 수 있으며, 컴포넌트는 하나의 컴퓨터 상에 로컬화될 수도 있고 그리고/또는 2개 또는 그보다 많은 컴퓨터들 사이에 분산될 수도 있다.

[0152] [00159] 앞서 언급한 시스템들은 여러 가지 컴포넌트들 사이의 상호 작용에 관해 설명되었다. 이러한 시스템들 및 컴포넌트들은 그러한 컴포넌트들 또는 지정된 서브컴포넌트들, 지정된 컴포넌트들 또는 서브컴포넌트들 중 일부, 그리고/또는 추가 컴포넌트들을 이들의 다양한 치환들 및 결합들에 따라 포함할 수 있다고 인식될 수 있다. 이러한 컴포넌트들은 또한 상위(parent) 컴포넌트들(계층 구조) 내에 포함되기보다는 다른 컴포넌트들에 통신 가능하게 연결된 컴포넌트들로서 구현될 수 있다. 추가로, 하나 또는 그보다 많은 컴포넌트들이 집성 기능을 제공하는 단일 컴포넌트로 결합되거나 여러 개별 서브컴포넌트들로 분할될 수도 있고, 관리 계층과 같은 임의의 하나 또는 그보다 많은 중간 계층들이 집적 기능을 제공하기 위해 이러한 서브컴포넌트들에 통신 가능하게 연결되도록 제공될 수도 있다는 점이 주목된다. 본 명세서에서 설명한 임의 컴포넌트들은 또한 본 명세서에서 구체적으로 설명되지 않았지만 해당 기술분야에서 통상의 지식을 가진 자들에 의해 일반적으로 공지된 하나 또는 그보다 많은 다른 컴포넌트들과 상호 작용할 수도 있다.

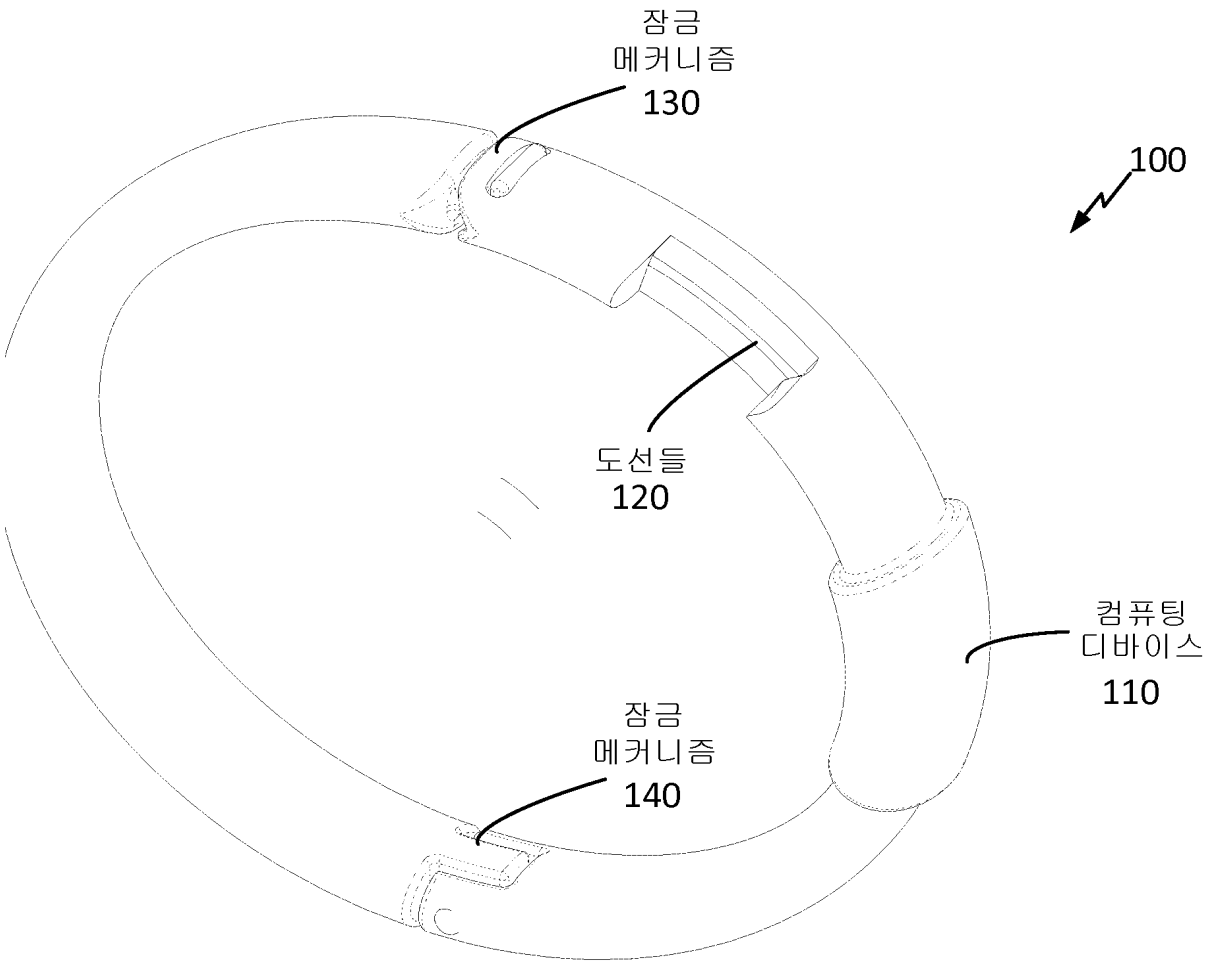
[0153] [00160] 앞서 설명한 예시적인 시스템들의 관점에서, 개시된 요지에 따라 구현될 수 있는 방법들은 다양한 도면들의 흐름도들을 참조로 인식될 수 있다. 설명의 간소화를 위해, 방법들은 일련의 블록들로서 도시 및 설명되지만, 일부 블록들은 다른 순서들로 그리고/또는 본 명세서에서 도시 및 설명된 것들로부터의 다른 블록들과 동시에 발생할 수도 있으므로, 청구 대상은 블록들의 순서로 한정되지 않는다고 이해 및 인식되어야 한다. 흐름도를 통해 비-순차적인 또는 분기형 흐름이 예시되는 경우, 동일한 또는 비슷한 결과를 달성하는 블록들의 다양한 다른 분기들, 흐름 경로들 및 순서들이 구현될 수도 있다고 인식될 수 있다. 더욱이, 이하 설명되는 방법들을 구현하기 위해 예시된 모든 블록들이 요구되지는 않을 수도 있다.

[0154] [00161] 일부 구현들에서는, 클라이언트 측 관점이 예시되지만, 혼선을 피하기 위해 대응하는 서버 관점이 존재하거나 그 반대도 가능하다고 이해되어야 한다. 마찬가지로, 방법이 실시되는 경우, 저장소 그리고 하나 또는 그보다 많은 컴포넌트들을 통해 그 방법을 실시하도록 구성된 적어도 하나의 프로세서를 갖는 대응하는 디바이스가 제공될 수 있다.

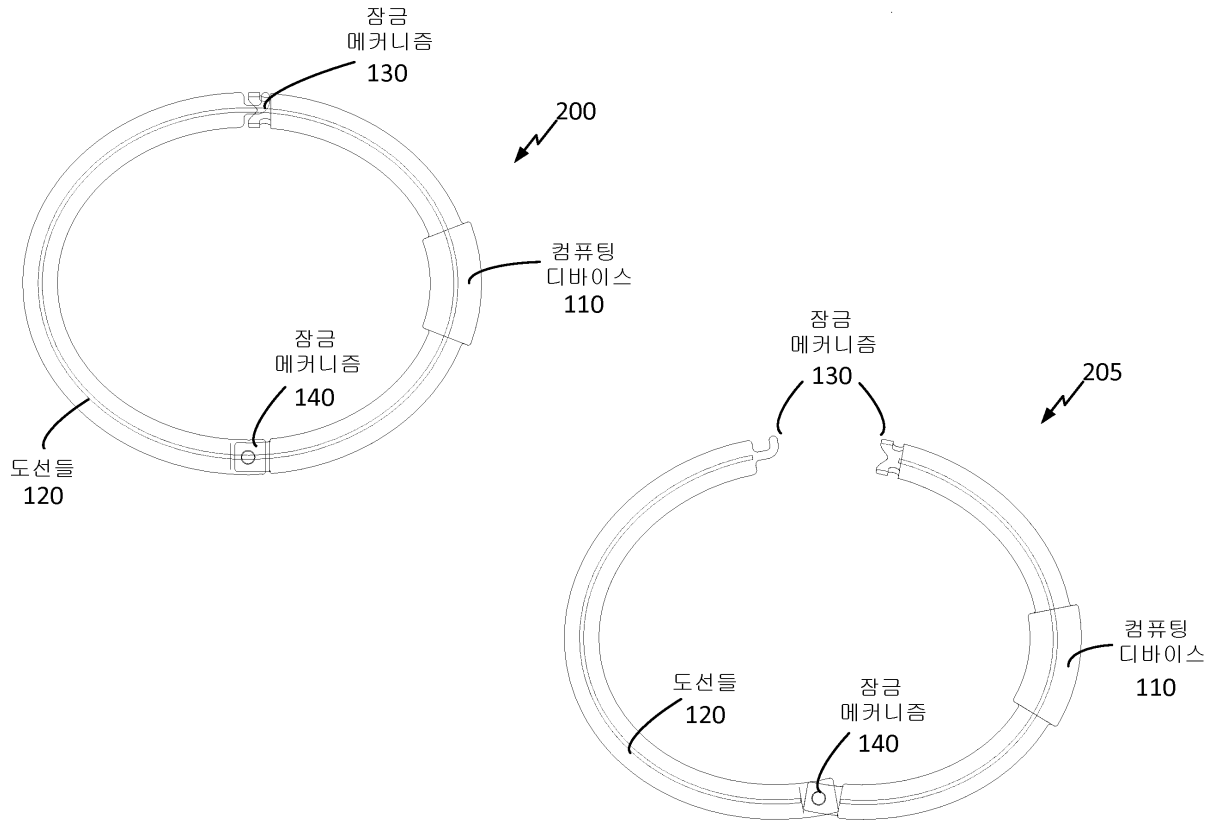
[0155] [00162] 다양한 도면들의 선호되는 구현들과 관련하여 다양한 구현들이 설명되었지만, 다른 비슷한 구현들이 사용될 수도 있고 또는 이로부터 벗어나지 않으면서 동일한 기능을 수행하기 위한 수정들 및 추가들이 설명된 구현들에 대해 이루어질 수도 있다고 이해되어야 한다. 또 추가로, 앞서 설명한 구현들의 하나 또는 그보다 많은 양상들은 복수의 처리 칩들 또는 디바이스들로 또는 이들에 걸쳐 구현될 수도 있고, 저장소는 복수의 디바이스들에 걸쳐 비슷하게 영향이 미칠 수도 있다. 따라서 본 발명은 임의의 단일 구현으로 한정되지 않아야 한다.

도면

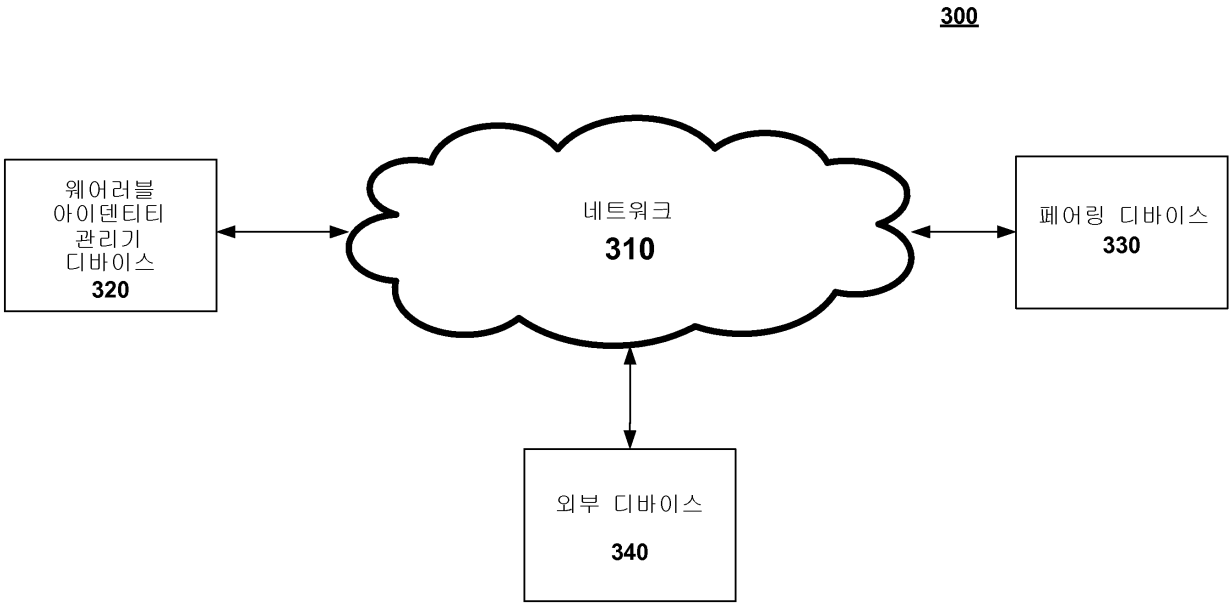
도면1



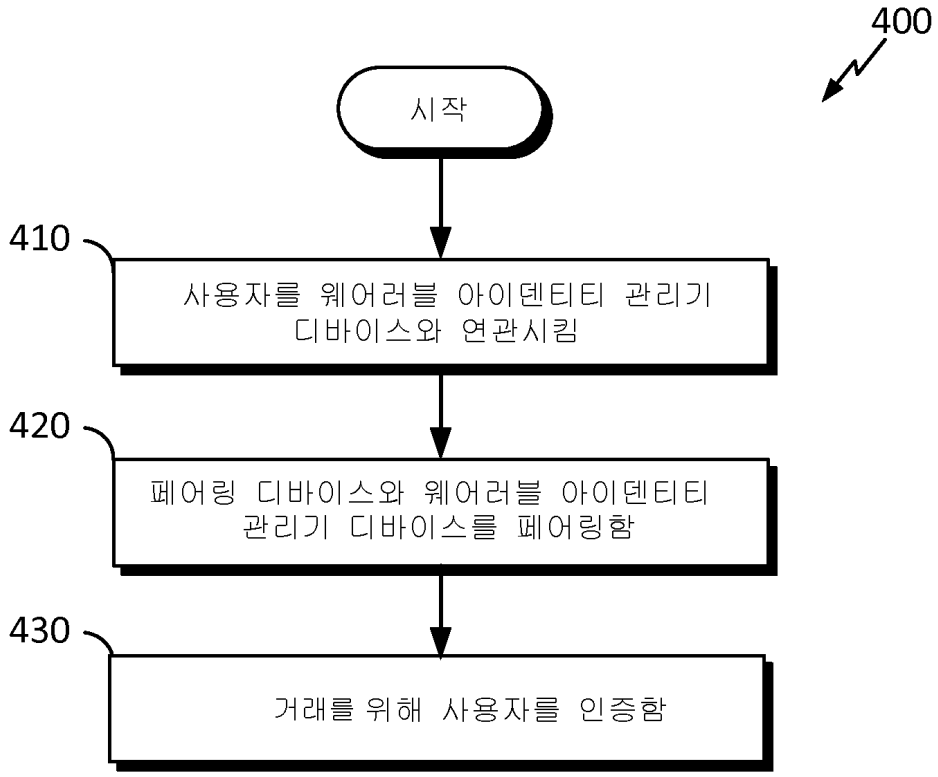
도면2


잠금
메커니즘
130
200
컴퓨팅
디바이스
110
잠금
메커니즘
140
도선들
120
잠금
메커니즘
130
205
컴퓨팅
디바이스
110
도선들
120
잠금
메커니즘
140

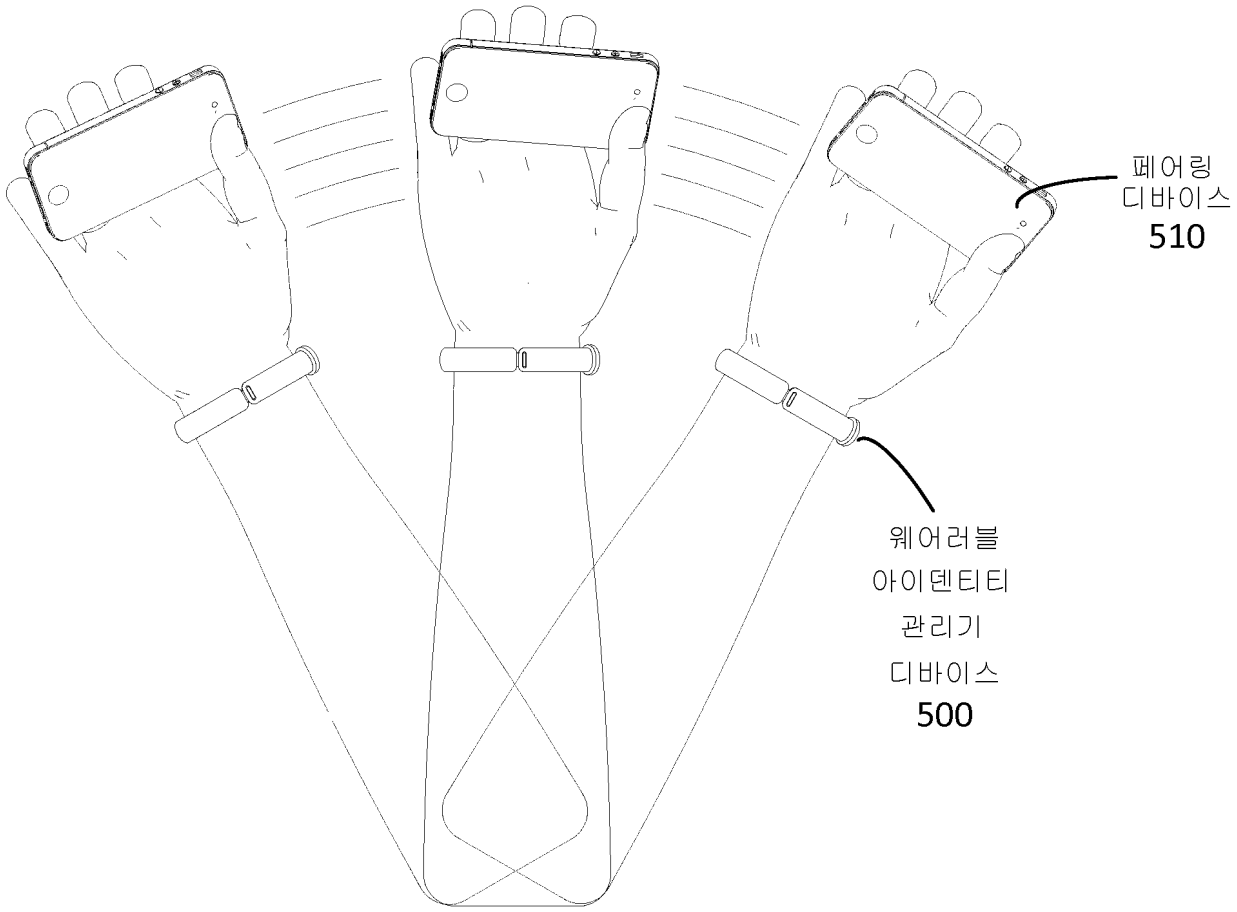
도면3


300
웨어러블
아이덴티티
관리기
디바이스
320
네트워크
310
페어링 디바이스
330
외부 디바이스
340

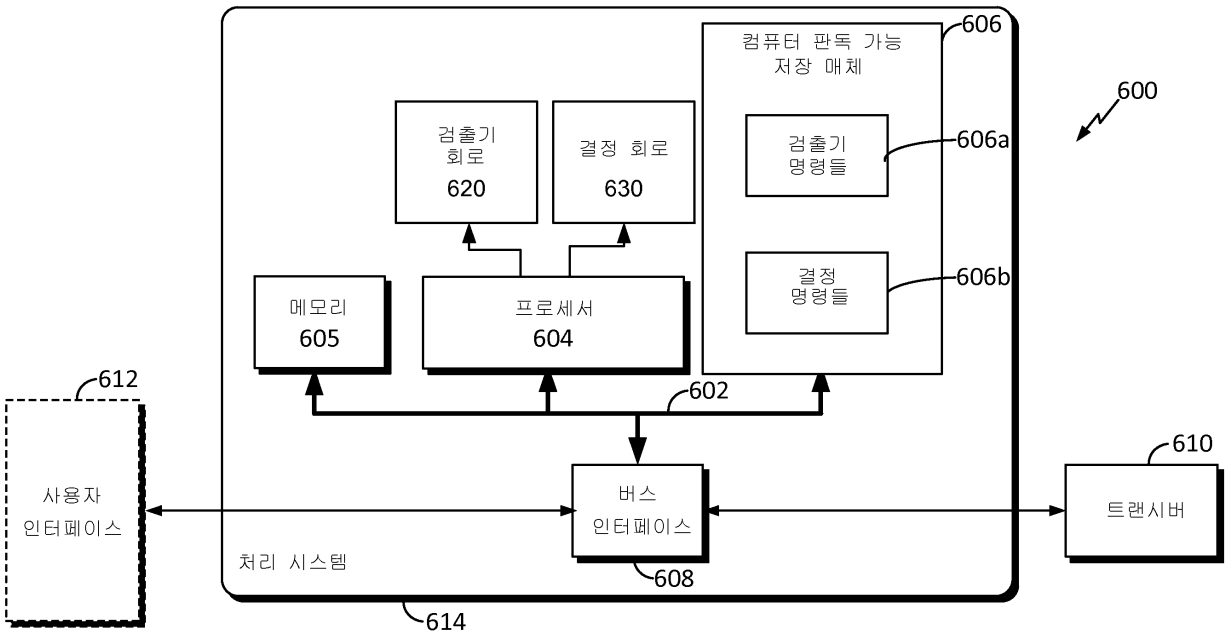
도면4


400
시작
410
사용자를 웨어러블 아이덴티티 관리기 디바이스와 연관시킴
420
페어링 디바이스와 웨어러블 아이덴티티 관리기 디바이스를 페어링함
430
거래를 위해 사용자를 인증함

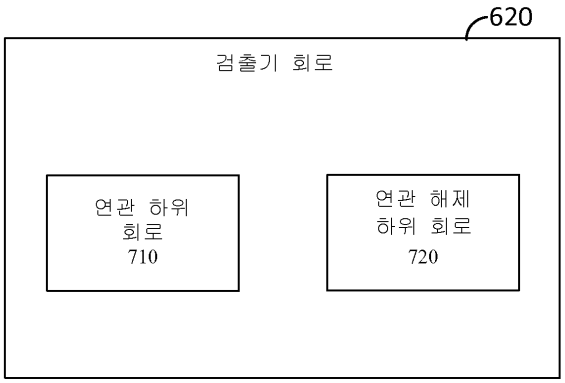
도면5

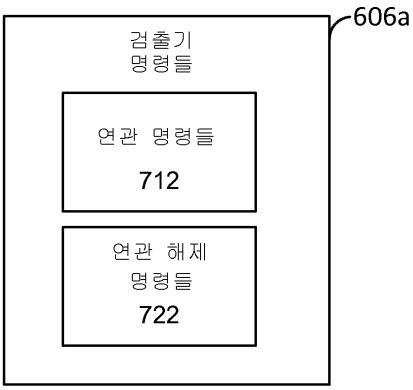

페어링
디바이스
510
웨어러블
아이덴티티
관리기
디바이스
500

도면6

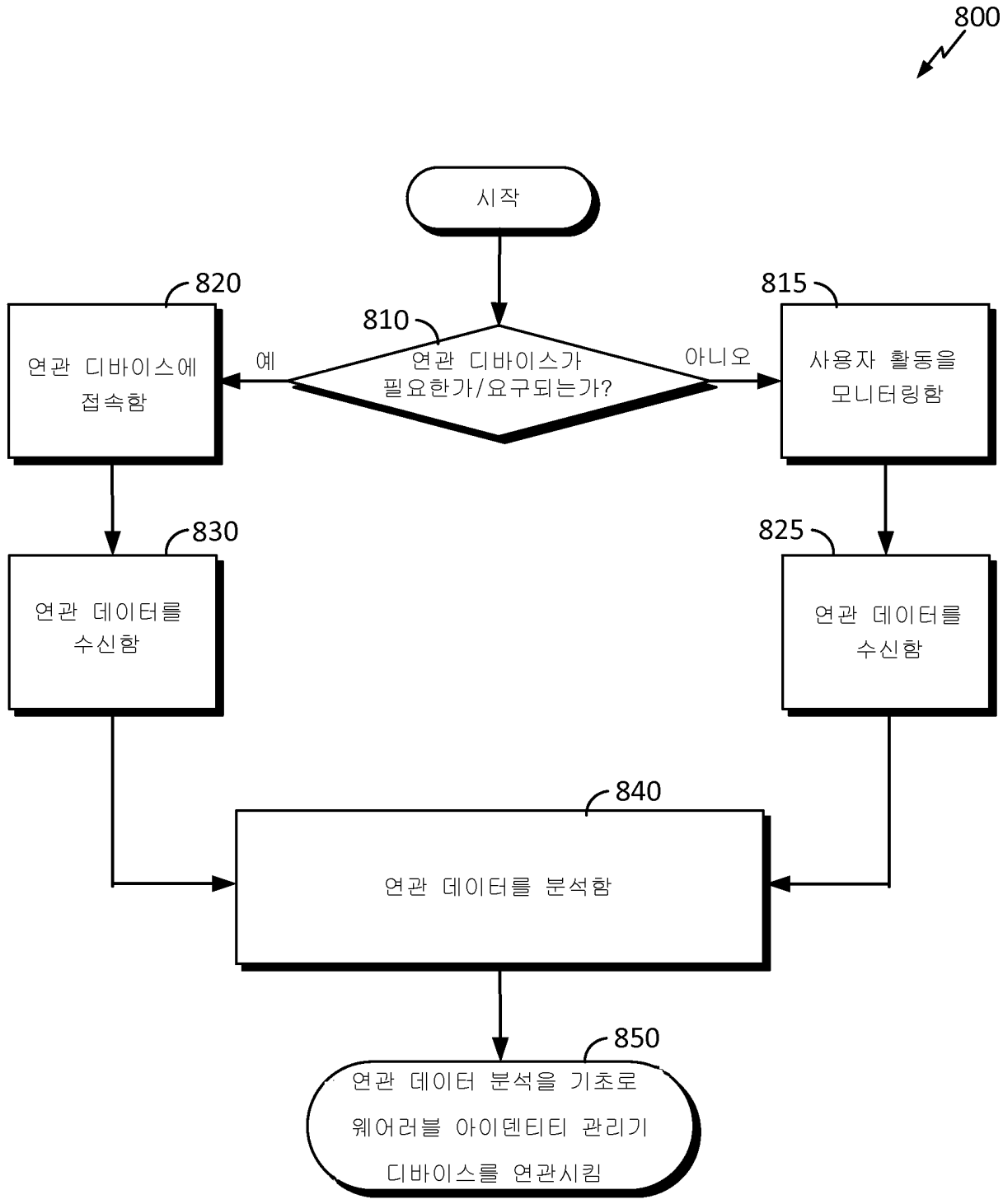

600
606
컴퓨터 판독 가능
저장 매체
606a
검출기
명령들
606b
결정
명령들
검출기
회로
620
결정 회로
630
메모리
605
프로세서
604
602
612
사용자
인터페이스
버스
인터페이스
608
610
트랜시버
처리 시스템
614

도면7

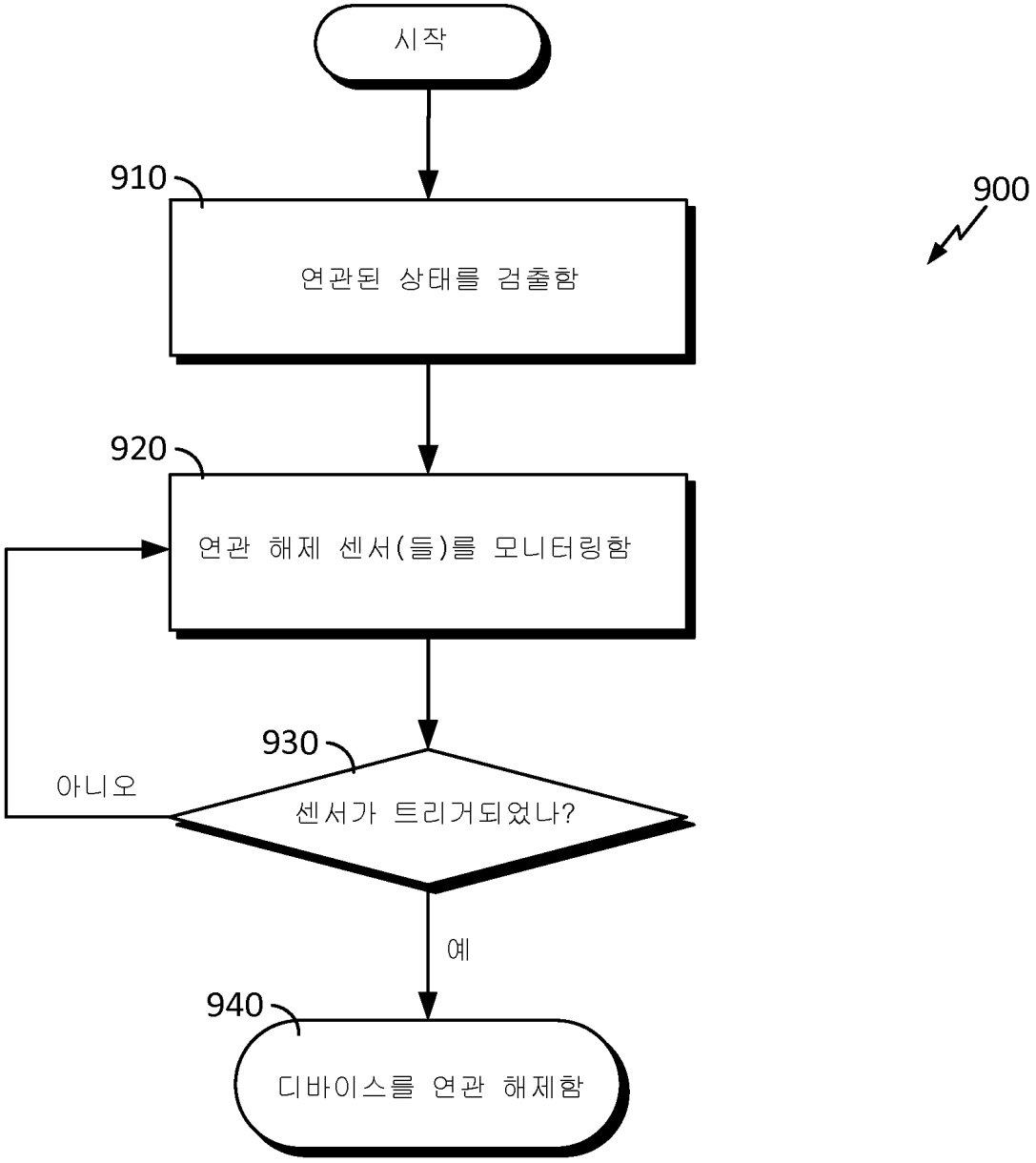

620
검출기 회로
연관 하위 회로
710
연관 해제 하위 회로
720


606a
검출기 명령들
연관 명령들
712
연관 해제 명령들
722

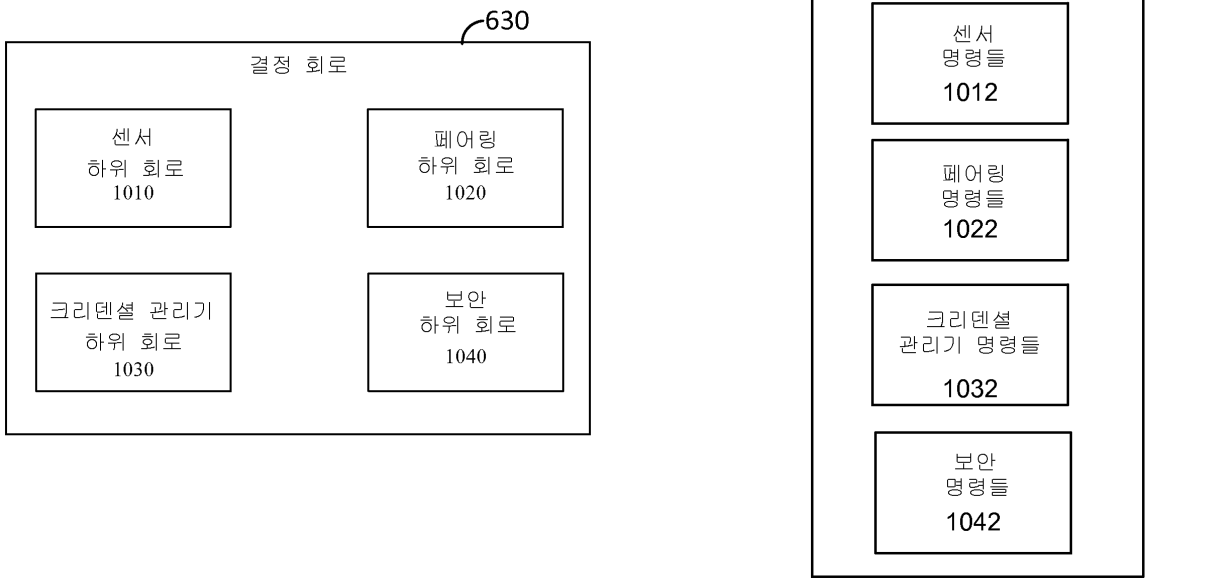
도면8


800
시작
810
연관 디바이스가 필요한가/요구되는가?
예
아니오
820
연관 디바이스에 접속함
815
사용자 활동을 모니터링함
830
연관 데이터를 수신함
825
연관 데이터를 수신함
840
연관 데이터를 분석함
850
연관 데이터 분석을 기초로 웨어러블 아이덴티티 관리기 디바이스를 연관시킴

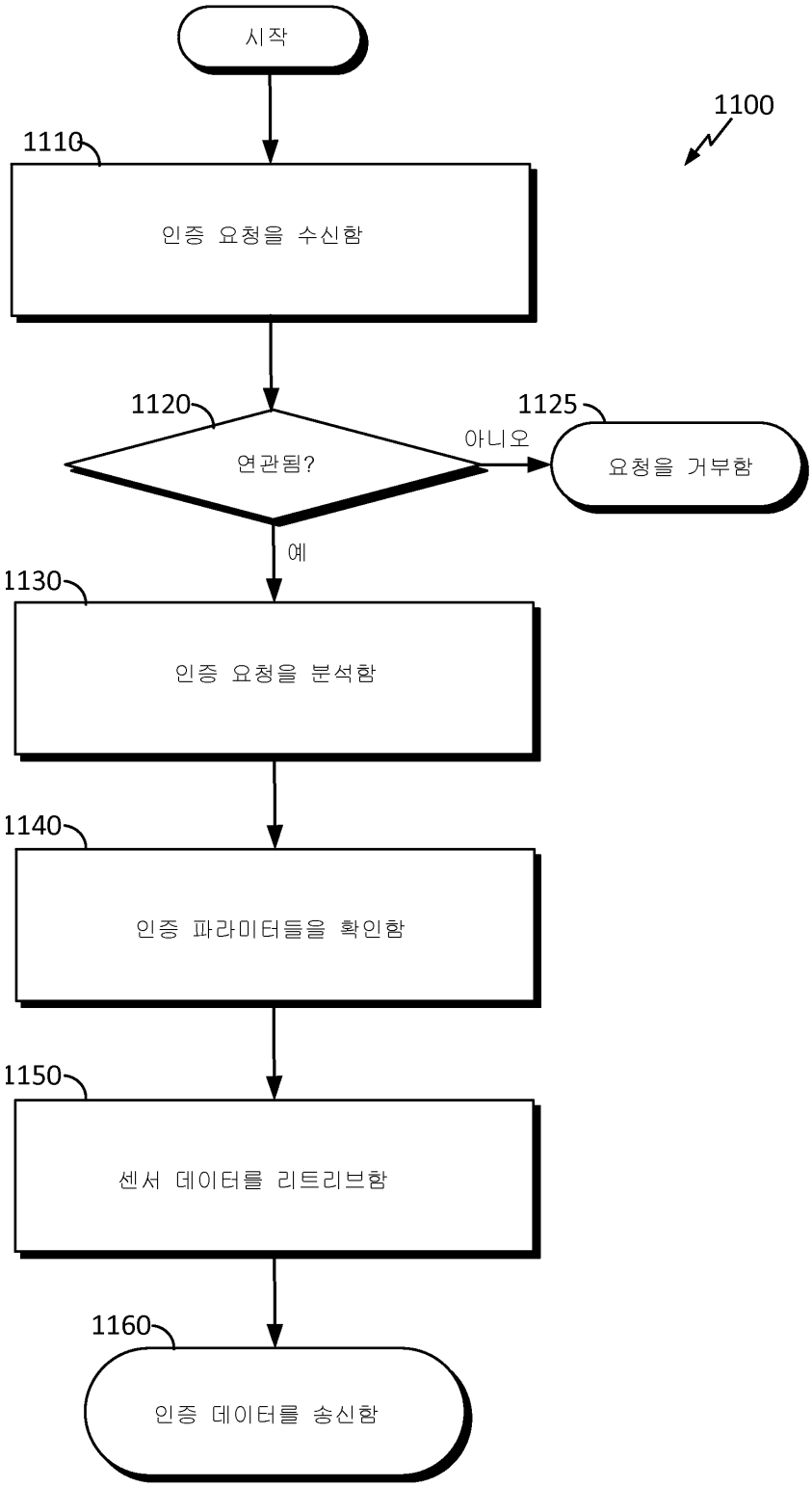
도면9


시작
910
연관된 상태를 검출함
900
920
연관 해제 센서(들)를 모니터링함
930
아니오
센서가 트리거되었나?
예
940
디바이스를 연관 해제함

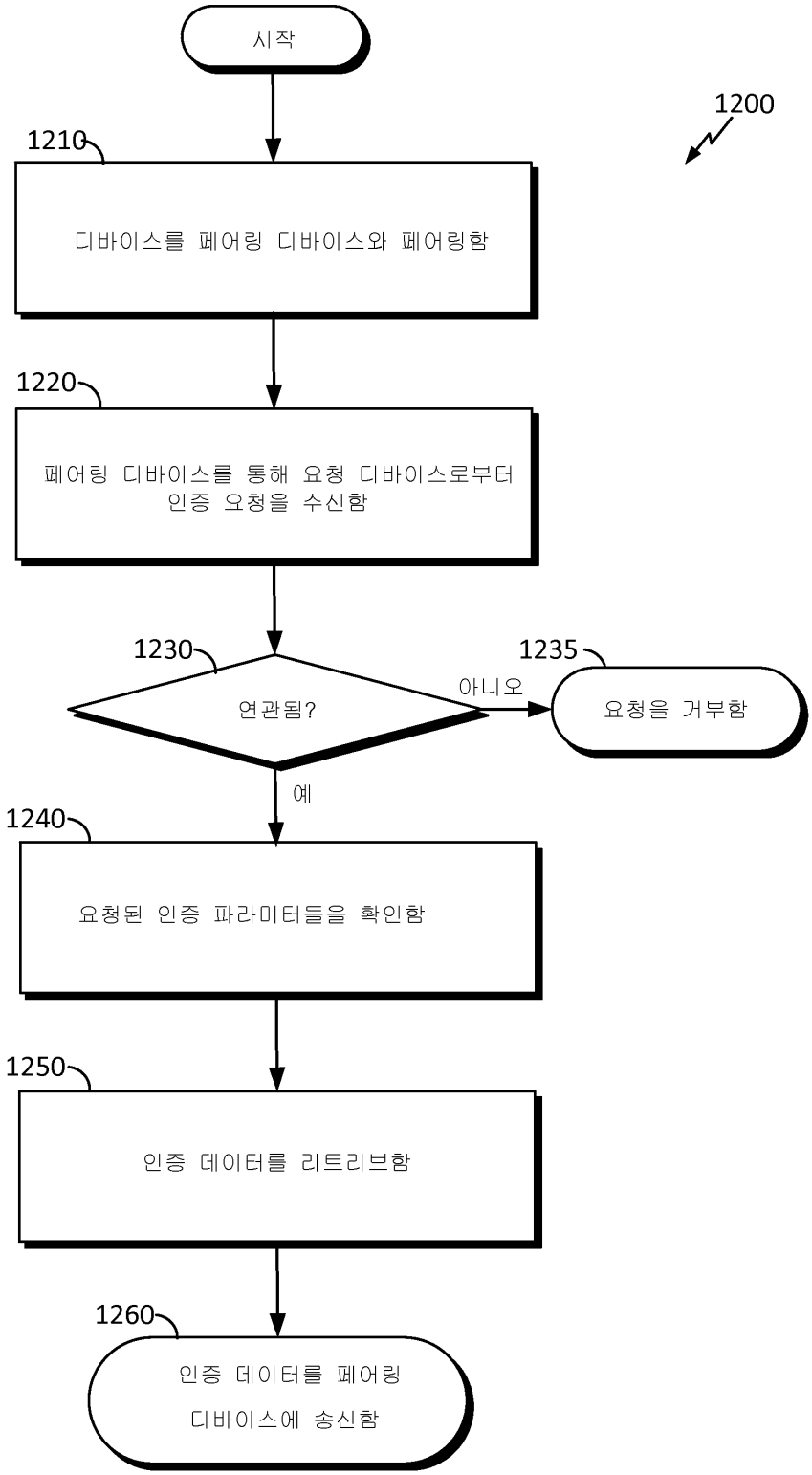
도면10


630
결정 회로
센서
하위 회로
1010
페어링
하위 회로
1020
크리덴셜 관리기
하위 회로
1030
보안
하위 회로
1040
606b
결정 명령들
센서
명령들
1012
페어링
명령들
1022
크리덴셜
관리기 명령들
1032
보안
명령들
1042

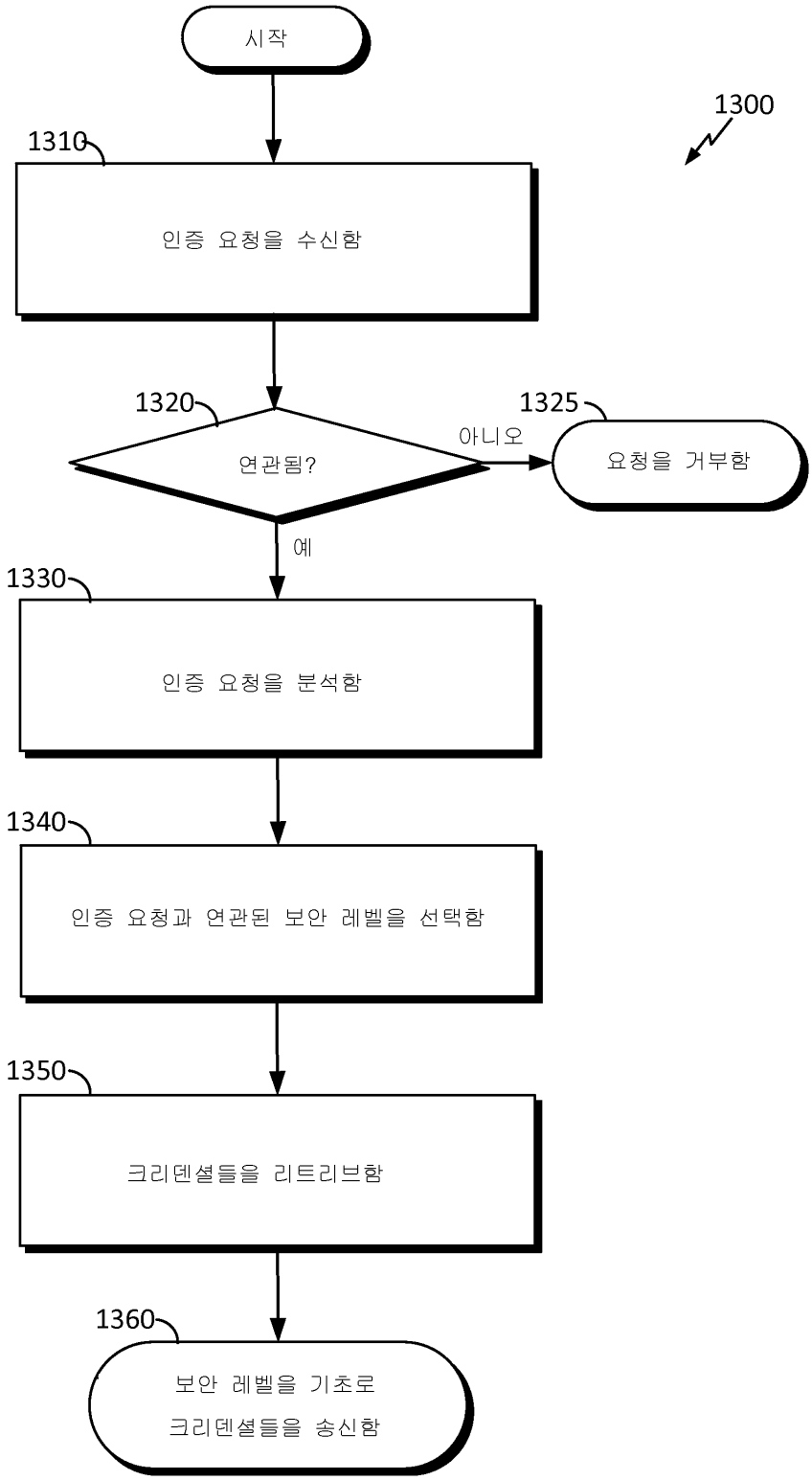
도면11


시작
1100
1110
인증 요청을 수신함
1120
연관됨?
아니오
1125
요청을 거부함
예
1130
인증 요청을 분석함
1140
인증 파라미터들을 확인함
1150
센서 데이터를 리트리브함
1160
인증 데이터를 송신함

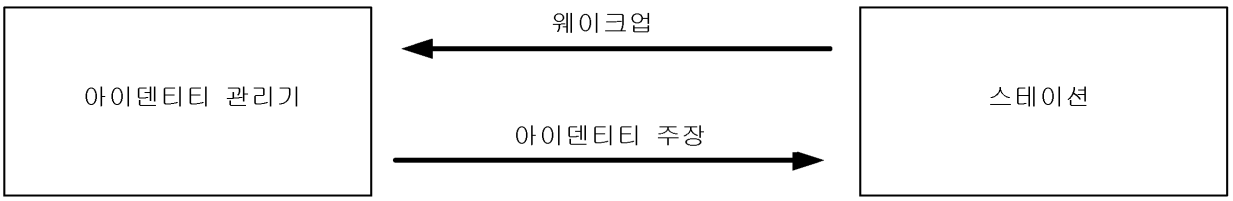
도면12


시작
1200
1210
디바이스를 페어링 디바이스와 페어링함
1220
페어링 디바이스를 통해 요청 디바이스로부터 인증 요청을 수신함
1230
연관됨?
아니오
1235
요청을 거부함
예
1240
요청된 인증 파라미터들을 확인함
1250
인증 데이터를 리트리브함
1260
인증 데이터를 페어링 디바이스에 송신함

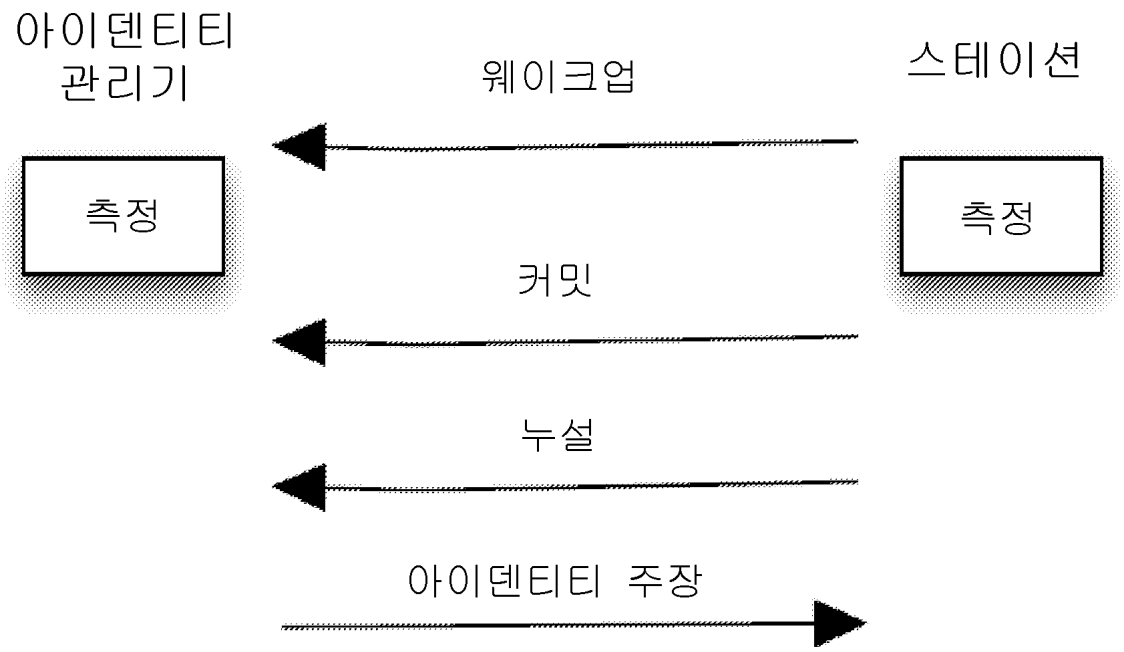
도면13


시작
1300
1310
인증 요청을 수신함
1320
연관됨?
아니오
1325
요청을 거부함
예
1330
인증 요청을 분석함
1340
인증 요청과 연관된 보안 레벨을 선택함
1350
크리덴셜들을 리트리브함
1360
보안 레벨을 기초로
크리덴셜들을 송신함

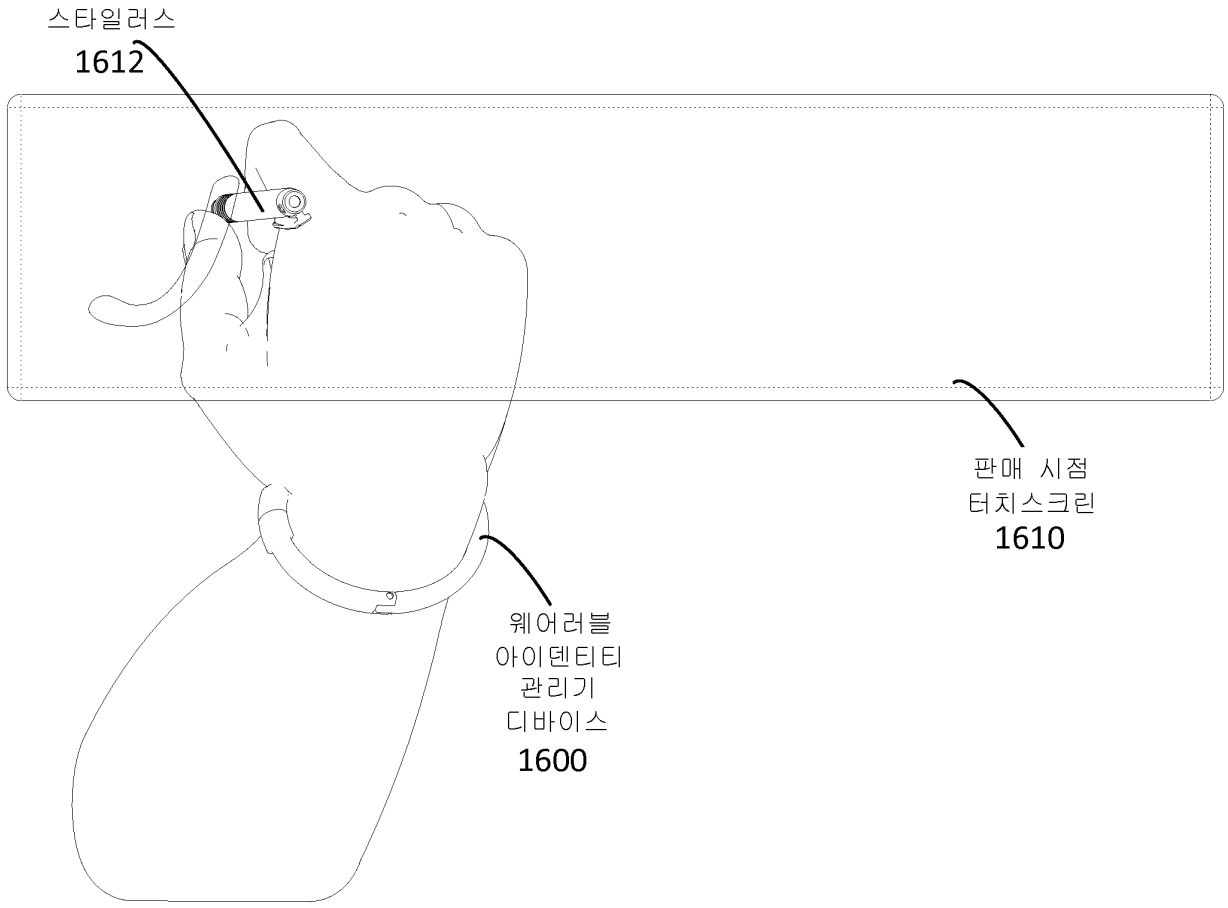
도면14


웨이크업
아이덴티티 관리기
아이덴티티 주장
스테이션

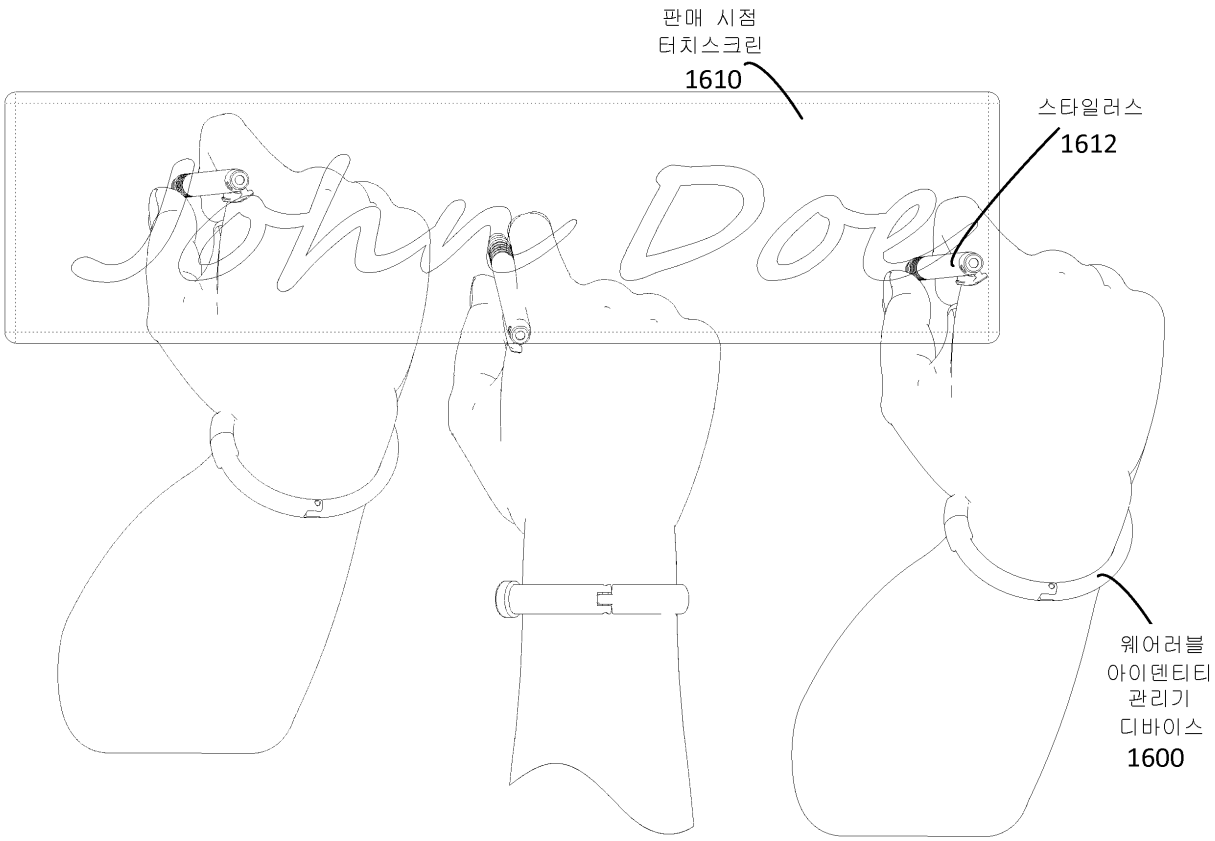
도면15


아이덴티티
관리기
웨이크업
스테이션
측정
측정
커밋
누설
아이덴티티 주장

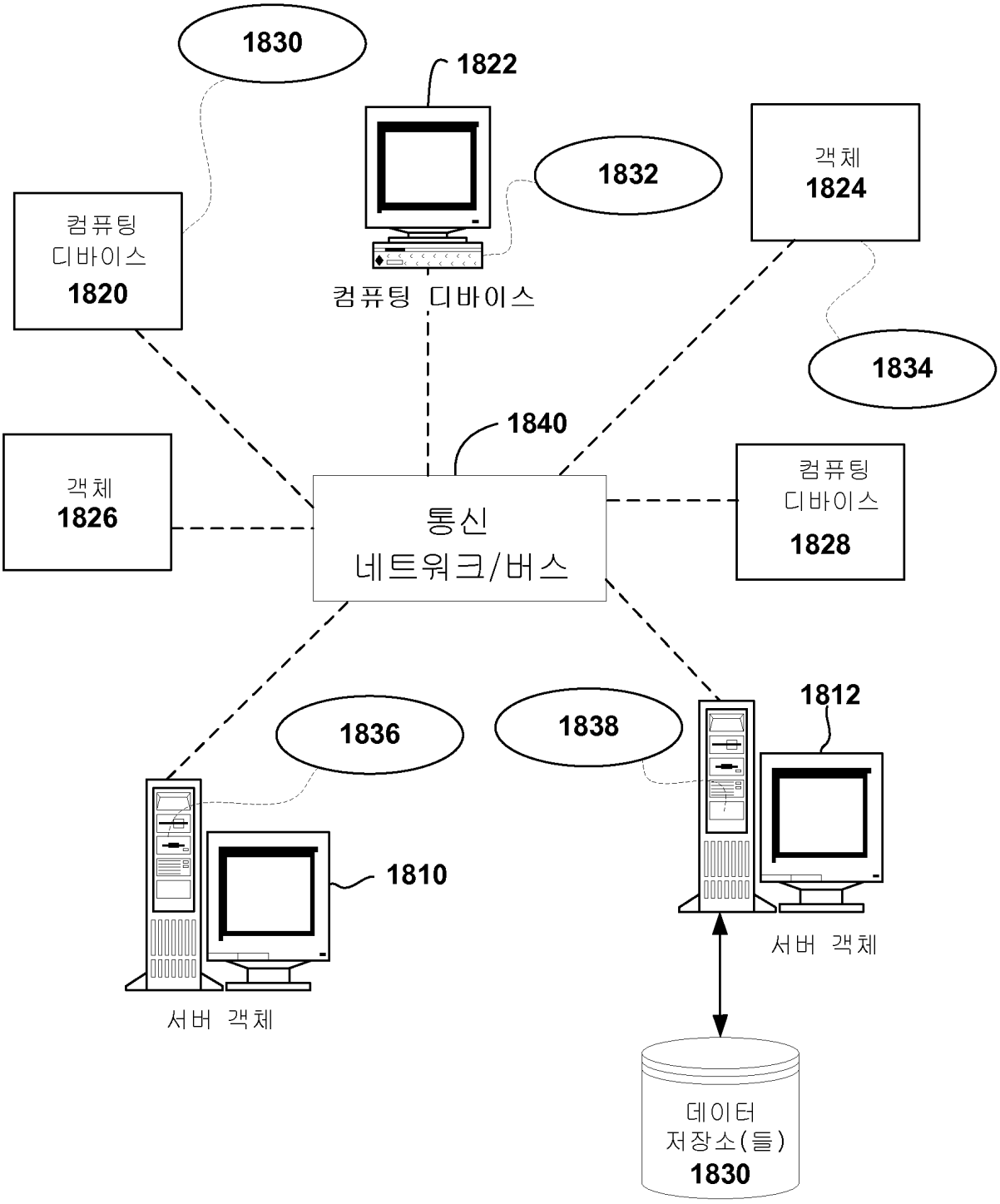
도면16



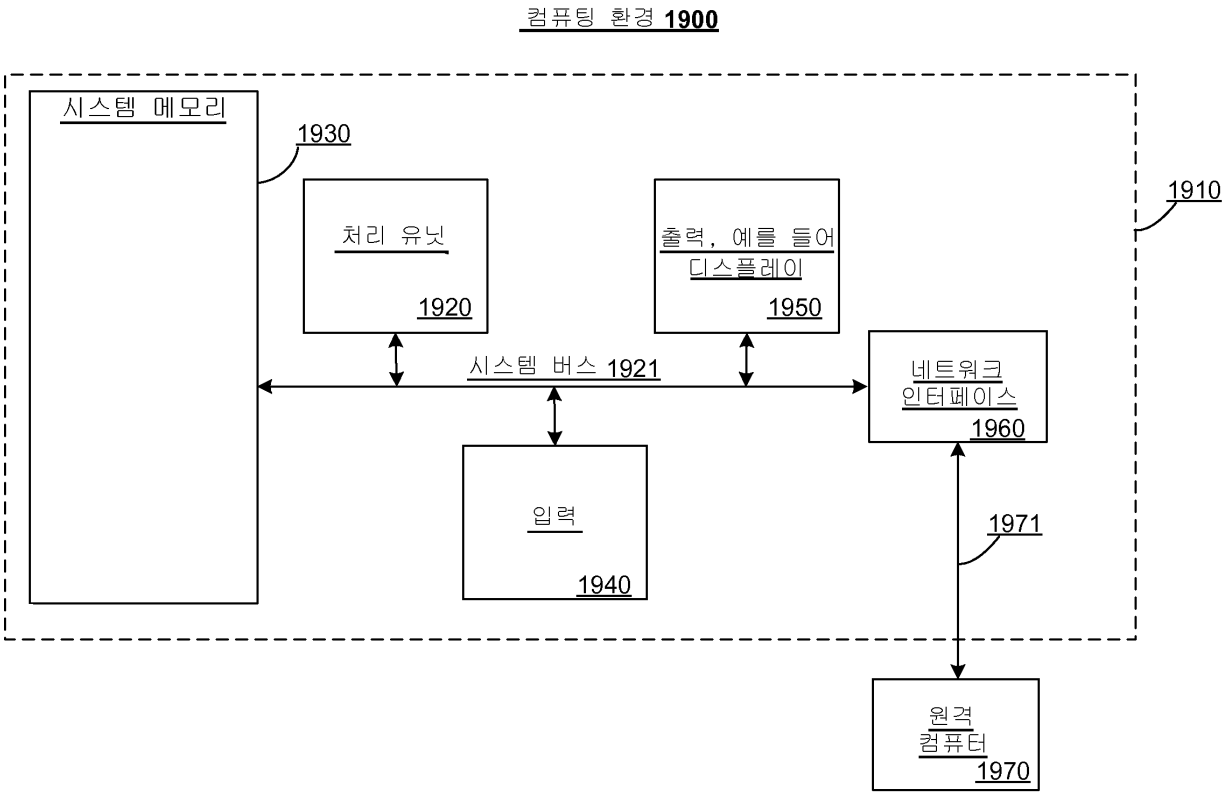
도면17



도면18


1830
1822
1832
객체
1824
컴퓨팅
디바이스
1820
컴퓨팅 디바이스
1834
1840
객체
1826
통신
네트워크/버스
컴퓨팅
디바이스
1828
1836
1838
1812
1810
서버 객체
서버 객체
데이터
저장소(들)
1830

도면19


컴퓨팅 환경 1900
시스템 메모리
1930
처리 유닛
1920
출력, 예를 들어 디스플레이
1950
1910
시스템 버스 1921
네트워크 인터페이스
1960
입력
1940
1971
원격 컴퓨터
1970