



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0140372
(43) 공개일자 2017년12월20일

- | | |
|---|--|
| <p>(51) 국제특허분류(Int. Cl.)
H04W 4/08 (2009.01) H04L 29/08 (2006.01)
H04L 9/32 (2006.01) H04W 12/06 (2009.01)</p> <p>(52) CPC특허분류
H04W 4/08 (2013.01)
H04L 67/1044 (2013.01)</p> <p>(21) 출원번호 10-2017-7034263</p> <p>(22) 출원일자(국제) 2016년03월31일
심사청구일자 2017년11월28일</p> <p>(85) 번역문제출일자 2017년11월27일</p> <p>(86) 국제출원번호 PCT/US2016/025440</p> <p>(87) 국제공개번호 WO 2016/195799
국제공개일자 2016년12월08일</p> <p>(30) 우선권주장
62/168,893 2015년05월31일 미국(US)
(뒷면에 계속)</p> | <p>(71) 출원인
애플 인크.
미합중국 95014 캘리포니아 쿠퍼티노 인피니트 루프 1</p> <p>(72) 발명자
아들러, 미첼, 디.
미국 95014 캘리포니아주 쿠퍼티노 인피니트 루프 1
브라우어, 마이클
미국 95014 캘리포니아주 쿠퍼티노 인피니트 루프 1
(뒷면에 계속)</p> <p>(74) 대리인
장덕순, 백만기</p> |
|---|--|

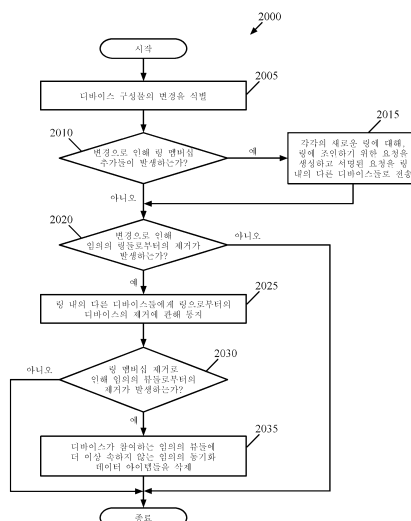
전체 청구항 수 : 총 23 항

(54) 발명의 명칭 디바이스들에 대한 동적 그룹 멤버십

(57) 요약

일부 실시예들은 디바이스들의 상이한 그룹들의 정의들을 식별하는 제 1 디바이스에 대한 방법을 제공하고, 디바이스들 각각은 디바이스가 멤버일 것을 필요로 하는 속성들의 세트에 의해 정의된다. 방법은 그룹 내에서의 멤버십에 대해 디바이스가 적격할 때를 판정하기 위해 제1 디바이스의 속성들을 모니터링한다. 디바이스가 멤버가 아닌 제1 그룹 내에서의 멤버십에 대해 제1 디바이스가 적격할 때, 방법은, 제1 그룹의 멤버인 적어도 하나의 다른 디바이스로, 적어도 디바이스의 개인 키로 서명되는 제1 그룹 내에서의 멤버십을 위한 신청서를 전송한다. 제1 디바이스가 멤버인 제2 그룹 내에서의 멤버십에 대해 제1 디바이스가 부적격하게 될 때, 방법은 제2 그룹으로부터 디바이스를 제거하고 제2 그룹의 멤버들인 다른 디바이스들에게 통지한다.

대표도 - 도20



(52) CPC특허분류

H04L 67/1095 (2013.01)

H04L 9/3255 (2013.01)

H04L 9/3268 (2013.01)

H04W 12/06 (2013.01)

(72) 발명자

월리, 앤드류, 알.

미국 95014 캘리포니아주 쿠퍼티노 인피니트 루프
1

헐리, 존, 씨.

미국 95014 캘리포니아주 쿠퍼티노 인피니트 루프
1

머피, 리차드, 에프.

미국 95014 캘리포니아주 쿠퍼티노 인피니트 루프
1

핀켈스타인, 데이빗, 피.

미국 95014 캘리포니아주 쿠퍼티노 인피니트 루프
1

(30) 우선권주장

62/172,127 2015년06월07일 미국(US)

14/872,022 2015년09월30일 미국(US)

명세서

청구범위

청구항 1

제1 디바이스의 적어도 하나의 프로세싱 유닛에 의한 실행을 위한 프로그램을 저장하는 기계 판독가능 매체로서, 상기 프로그램은,

디바이스들의 상이한 그룹들의 정의들을 식별하기 위한 - 디바이스들의 각각의 그룹은 디바이스가 상기 그룹의 멤버가 되는 데 필요한 속성들의 세트에 의해 정의됨 -;

상기 그룹들 중 하나의 그룹 내에서의 멤버십에 대해 상기 제1 디바이스가 적격할 때를 판정하기 위해 상기 제1 디바이스의 속성들을 모니터링하기 위한;

상기 제1 디바이스가 멤버가 아닌 제1 그룹 내에서의 멤버십에 대해 상기 제1 디바이스가 적격할 때, 상기 제1 그룹의 멤버인 적어도 하나의 다른 디바이스로, 적어도 상기 제1 디바이스의 개인 키(private key)로 서명되는 상기 제1 그룹 내에서의 멤버십을 위한 신청서를 전송하기 위한; 그리고

상기 제1 디바이스가 멤버인 제2 그룹 내에서의 멤버십에 대해 상기 제1 디바이스가 부적격하게 될 때, 상기 제2 그룹으로부터 상기 제1 디바이스를 제거하고 상기 제2 그룹의 멤버들인 다른 디바이스들에게 통지하기 위한 명령어들의 세트들을 포함하는, 기계 판독가능 매체.

청구항 2

제1항에 있어서, 상기 제1 그룹 내에서의 멤버십은 특정 개인 키의 지식을 필요로 하고, 상기 신청서를 전송하기 위한 명령어들의 세트는,

상기 제1 그룹 내에서의 멤버십에 필요한 상기 특정 개인 키로 상기 제1 디바이스의 공개 키(public key) 및 신청 시간에 서명하여 제1 서명을 생성하기 위한;

상기 제1 서명을 상기 제1 디바이스의 아이덴티티(identity)로 패키징하기 위한;

상기 제1 디바이스의 개인 키로 상기 제1 디바이스의 상기 아이덴티티에 서명하여 제2 서명을 생성하기 위한; 그리고

상기 제2 서명을 상기 제1 그룹의 멤버들인 상기 다른 디바이스들로 전송하기 위한 명령어들의 세트들을 포함하는, 기계 판독가능 매체.

청구항 3

제1항에 있어서, 상기 프로그램은, 상기 제1 그룹의 멤버인 상기 다른 디바이스들 중 하나로부터, 상기 제1 디바이스가 상기 제1 그룹의 멤버로서 수용된다는 통지를 수신하기 위한 명령어들의 세트를 추가로 포함하고, 상기 통지는 상기 제1 디바이스를 포함하는 상기 그룹의 멤버들을 리스팅하는, 상기 다른 디바이스에 의해 서명된 메시지를 포함하는, 기계 판독가능 매체.

청구항 4

제1항에 있어서, 상기 제1 디바이스는 복수의 상이한 그룹들의 멤버인, 기계 판독가능 매체.

청구항 5

제1항에 있어서, 상기 그룹들 중 하나의 특정 그룹은 디바이스들이 상기 그룹에 조인(join)하기 위해 특정 운영 체제를 가질 것을 필요로 하는, 기계 판독가능 매체.

청구항 6

제1항에 있어서, 상기 그룹들 중 하나의 특정 그룹은 사용자가 상기 그룹의 멤버로서 확립되는 디바이스에 대해서 새로운 디바이스를 검증할 것을 필요로 하는, 기계 판독가능 매체.

청구항 7

제1항에 있어서, 상기 그룹들 중 하나의 특정 그룹은 디바이스들이 상기 그룹에 조인하기 위해 적어도 특정된 길이의 패스코드로 보호될 것을 필요로 하는, 기계 판독가능 매체.

청구항 8

제1항에 있어서, 상기 프로그램은,

제2 디바이스로부터, 상기 제1 디바이스가 멤버인 제3 그룹 내에서의 멤버십을 위한 신청서를 수신하기 위한;

상기 제2 디바이스가 상기 제3 그룹 내에서의 멤버십을 위한 조건들을 충족시키는지를 검증하기 위한; 그리고

상기 제2 디바이스가 상기 조건들을 충족시킬 때, 상기 제3 그룹의 멤버들인 상기 다른 디바이스들에게 상기 제2 디바이스가 상기 제3 그룹의 멤버라는 것을 특정하는 통지를 전송하기 위한 명령어들의 세트들을 추가로 포함하는, 기계 판독가능 매체.

청구항 9

제8항에 있어서, 상기 제2 디바이스가 상기 제3 그룹 내에서의 멤버십을 위한 조건들을 충족시키는지를 검증하기 위한 명령어들의 세트는, 상기 제3 그룹 내에서의 멤버십을 위해 소유가 필요한 개인 키에 의해 요청이 서명되어 있는지를 검증하기 위한 명령어들의 세트를 포함하는, 기계 판독가능 매체.

청구항 10

제8항에 있어서, 상기 제2 디바이스가 상기 제3 그룹 내에서의 멤버십을 위한 조건들을 충족시키는지를 검증하기 위한 명령어들의 세트는, 사용자에게 상기 제2 디바이스를 제3 그룹 내에서 허용하도록 프롬프트하기 위한 명령어들의 세트를 포함하는, 기계 판독가능 매체.

청구항 11

제1항에 있어서, 상기 멤버십을 위한 신청서는 상기 제1 그룹의 멤버들인 모든 디바이스들로 전송되는, 기계 판독가능 매체.

청구항 12

제1항에 있어서, 상기 멤버십을 위한 신청서는 상기 제1 그룹의 멤버들인 디바이스들의 서브세트로만 전송되는, 기계 판독가능 매체.

청구항 13

전자 디바이스로서,

한 세트의 프로세싱 유닛들; 및

제1 디바이스의 프로세싱 유닛들 중 적어도 하나에 의한 실행을 위한 프로그램을 저장하는 기계 판독가능 매체를 포함하고, 상기 프로그램은,

디바이스들의 상이한 그룹들의 정의들을 식별하기 위한 - 디바이스들의 각각의 그룹은 디바이스가 상기 그룹의 멤버가 되는 데 필요한 속성들의 세트에 의해 정의됨 -;

상기 그룹들 중 하나의 그룹 내에서의 멤버십에 대해 상기 전자 디바이스가 적격할 때를 판정하기 위해 상기 전자 디바이스의 속성들을 모니터링하기 위한;

상기 전자 디바이스가 멤버가 아닌 제1 그룹 내에서의 멤버십에 대해 상기 전자 디바이스가 적격할 때, 상기 제1 그룹의 멤버인 적어도 하나의 다른 디바이스로, 적어도 상기 전자 디바이스의 개인 키로 서명되는 상기 제1 그룹 내에서의 멤버십을 위한 신청서를 전송하기 위한; 그리고

상기 전자 디바이스가 멤버인 제2 그룹 내에서의 멤버십에 대해 상기 전자 디바이스가 부적격하게 될 때, 상기 제2 그룹으로부터 상기 전자 디바이스를 제거하고 상기 제2 그룹의 멤버들인 다른 디바이스들에게 통지하기 위한 명령어들의 세트들을 포함하는, 전자 디바이스.

청구항 14

제13항에 있어서, 상기 제1 그룹은 특정 개인 키의 지식을 필요로 하고, 상기 신청서를 전송하기 위한 명령어들의 세트는,

상기 제1 그룹 내에서의 멤버십에 필요한 상기 특정 개인 키로 상기 전자 디바이스의 공개 키 및 신청 시간에 서명하여 제1 서명을 생성하기 위한;

상기 제1 서명을 상기 전자 디바이스의 아이덴티티로 패키징하기 위한;

상기 전자 디바이스의 개인 키로 상기 전자 디바이스의 상기 아이덴티티에 서명하여 제2 서명을 생성하기 위한; 그리고

상기 제2 서명을 상기 제1 그룹의 멤버들인 상기 다른 디바이스들로 전송하기 위한 명령어들의 세트들을 포함하는, 전자 디바이스.

청구항 15

제13항에 있어서, 상기 프로그램은, 상기 제1 그룹의 멤버인 상기 다른 디바이스들 중 하나로부터, 상기 전자 디바이스가 상기 제1 그룹의 멤버로서 수용된다는 통지를 수신하기 위한 명령어들의 세트를 추가로 포함하고, 상기 통지는 상기 전자 디바이스를 포함하는 상기 그룹의 멤버들을 리스팅하는, 상기 다른 디바이스에 의해 서명된 메시지를 포함하는, 전자 디바이스.

청구항 16

제13항에 있어서, 상기 전자 디바이스는 제1 디바이스이고, 상기 프로그램은,

제2 디바이스로부터, 상기 제1 디바이스가 멤버인 제3 그룹 내에서의 멤버십을 위한 신청서를 수신하기 위한;

상기 제2 디바이스가 상기 제3 그룹 내에서의 멤버십을 위한 조건들을 충족시키는지 검증하기 위한; 그리고

상기 제2 디바이스가 상기 조건들을 충족시킬 때, 상기 제3 그룹의 멤버들인 상기 다른 디바이스들에게 상기 제2 디바이스가 상기 제3 그룹의 멤버라는 것을 특정하는 통지를 전송하기 위한 명령어들의 세트들을 추가로 포함하는, 전자 디바이스.

청구항 17

제16항에 있어서, 상기 제2 디바이스가 상기 제3 그룹 내에서의 멤버십을 위한 조건들을 충족시키는지 검증하기 위한 명령어들의 세트는, 상기 제3 그룹 내에서의 멤버십을 위해 소유가 필요한 개인 키에 의해 요청이 서명되어 있는지를 검증하기 위한 명령어들의 세트를 포함하는, 전자 디바이스.

청구항 18

제16항에 있어서, 상기 제2 디바이스가 상기 제3 그룹 내에서의 멤버십을 위한 조건들을 충족시키는지 검증하기 위한 명령어들의 세트는, 사용자에게 상기 제2 디바이스를 상기 제3 그룹 내에서 허용하도록 프롬프트하기 위한 명령어들의 세트를 포함하는, 전자 디바이스.

청구항 19

제1 디바이스에 대한 방법으로서,

디바이스들의 상이한 그룹들의 정의들을 식별하는 단계 - 디바이스들의 각각의 그룹은 디바이스가 상기 그룹의 멤버가 되는 데 필요한 속성들의 세트에 의해 정의됨 -;

상기 그룹들 중 하나의 그룹 내에서의 멤버십에 대해 상기 제1 디바이스가 적격할 때를 판정하기 위해 상기 제1 디바이스의 속성들을 모니터링하는 단계; 및

상기 제1 디바이스가 멤버가 아닌 제1 그룹 내에서의 멤버십에 대해 상기 제1 디바이스가 적격할 때, 상기 제1 그룹의 멤버인 적어도 하나의 다른 디바이스로, 적어도 상기 제1 디바이스의 개인 키로 서명되는 상기 제1 그룹 내에서의 멤버십을 위한 신청서를 전송하는 단계를 포함하고,

상기 제1 디바이스가 멤버인 제2 그룹 내에서의 멤버십에 대해 상기 제1 디바이스가 부적격하게 될 때, 상기 제

1 디바이스는 상기 제2 그룹으로부터 자신을 제거하고 상기 제2 그룹의 멤버들인 다른 디바이스들에게 통지하는, 방법.

청구항 20

제19항에 있어서, 상기 제1 그룹 내에서의 멤버십은 특정 개인 키의 지식을 필요로 하고, 상기 신청서를 전송하는 단계는,

상기 제1 그룹 내에서의 멤버십에 필요한 상기 특정 개인 키로 상기 제1 디바이스의 공개 키 및 신청 시간에 서명하여 제1 서명을 생성하는 단계;

상기 제1 서명을 상기 제1 디바이스의 아이덴티티로 패키징하는 단계;

상기 제1 디바이스의 개인 키로 상기 제1 디바이스의 상기 아이덴티티에 서명하여 제2 서명을 생성하는 단계; 및

상기 제2 서명을 상기 제1 그룹의 멤버들인 상기 다른 디바이스들로 전송하는 단계를 포함하는, 방법.

청구항 21

제19항에 있어서, 상기 제1 디바이스는 복수의 상이한 그룹들의 멤버인, 방법.

청구항 22

제19항에 있어서, 상기 멤버십을 위한 신청서는 상기 제1 그룹의 멤버들인 모든 디바이스들로 전송되는, 방법.

청구항 23

제19항에 있어서, 상기 멤버십을 위한 신청서는 상기 제1 그룹의 멤버들인 디바이스들의 서브세트로만 전송되는, 방법.

발명의 설명

배경 기술

[0001]

증첩되는 기능을 가진 다수의 디바이스들을 소유한 사용자가 점점 더 보편화되고 있다. 스마트폰들, 태블릿들, 및 컴퓨터들은 모두 웹에 액세스하고, 사용자가 사진들 등을 프로세싱하게 하고, 사용자들은 여러 개의 그러한 디바이스들을 가지려는 경향이 있다. 따라서, 디바이스들 사이에서 데이터를 공유하고 다수의 디바이스들 상의 데이터로의 액세스를 갖기는 원하는 사용자도 또한 점점 더 보편화되고 있다. 사용자들은, 통상적으로, 플래시 메모리 스틱들, 이메일 등과 같이, 디바이스들 사이에서 데이터를 전송하기 위한 모든 종류의 상이한 기법들을 사용할 수 있다. 사용자의 디바이스들 사이에서 데이터를 자동으로 공유하기 위한 더 효율적인 기법들이 요망된다.

발명의 내용

[0002]

일부 실시예들은 한 세트의 관련 전자 디바이스들 사이에서 데이터 아이템들을 동기화시키기 위한 방법을 제공한다. 구체적으로, 일부 실시예들은, 디바이스들이 검증 서브그룹들에 대한 멤버십 조건들을 만족시키는 경우에 디바이스들이 조인(join)할 수 있는 검증 서브그룹들을 정의하고, 검증 서브그룹들을 사용하여 디바이스들이 참여하는 동기화 서브그룹들을 정의한다. 일부 실시예들에서, 상이한 동기화 서브그룹들은 동기화 서브그룹들에 참여하는 디바이스들이 동기화 프로세스들을 통해 서로 공유하는 상이한 타입들의 데이터 아이템들을 정의한다.

[0003]

일부 실시예들에서, 관련 전자 디바이스들의 세트는 사용자가 제3자 서비스와(예컨대, 사용자의 특정 클라우드 서비스 계정과) 연관시키는 모든 디바이스들을 포함한다. 클라우드 서비스 계정 패스워드의 지식은, 일부 실시예들의 검증 서브그룹들 중 적어도 하나의 검증 서브그룹 내에서의 멤버십을 위한 조건으로서의 역할을 하지만, 일부 실시예들은 다양한 디바이스들이 조인할 수 있는 추가적인 검증 서브그룹들을 정의한다. 상이한 실시예들은, 디바이스가 특정 운영 체제를 가지며 특정 레벨의 패스워드 강도를 가지며 보안 프로세서 또는 다른 디바이스 구성 속성들을 갖는다는 조건들을 포함한, 그러한 추가적인 검증 서브그룹들에 조인하기 위한 상이한 세트들의 조건들을 정의한다. 일부 실시예들은, 디바이스가 특정 검증 서브그룹에 조인하기 위해 특정 암호화 시크릿

(secret)의 소유(예컨대, 기업에 의해 정의된 검증 서브그룹에 조인하기 위해 기업 프로파일이 제공된 키의 소유)를 증명하는 것, 또는 사용자가 검증 서브그룹에서 이미 확립된 디바이스 상에서 새로운 디바이스의 멤버십을 검증할 것을 필요로 한다. 또한, 일부 검증 서브그룹들은 새로운 디바이스가 대역 외 프로세스를 통해(예컨대, 검증을 위해 제3자를 사용하는 것에 의해) 확립된 디바이스에 대한 자신의 속성을 검증할 것을 필요로 할 수 있다.

[0004] 디바이스가 검증 서브그룹에 조인하기 위해, 일부 실시예들은 디바이스가 서브그룹에 조인하기 위한 요청에 서명할 것 및 검증 서브그룹에 이미 있는 디바이스들 중 하나에 의해 승인된 요청을 가질 것을 필요로 한다. 예를 들어, 일부 실시예들에서, 디바이스가 암호화 시크릿의 소유를 필요로 하는 검증 서브그룹에 대한 조건들을 충족시킬 때, 디바이스는 (i) (다른 디바이스들과 이미 공유된) 그의 공개 키(public key) 및 서브그룹으로의 신청 날짜/시간에 암호화 시크릿으로부터 생성된 개인 키(private key)로 서명하고, (ii) 이러한 서명을 검증 서브그룹에 조인하는 데 사용되는 그의 아이덴티티(identity)로 패키징하고, (iii) 아이덴티티에 그 자신의 개인 키로 서명한다. 이어서, 이러한 서명은 서브그룹에 조인하기 위한 요청으로서 검증 서브그룹 내의 다른 디바이스들로 전송된다. 다른 디바이스들 중 하나가 요청 디바이스가 서브그룹에 조인하기 위한 모든 조건들을 충족시키는지 검증할 때, 확립된 디바이스는, 추가되는 새로운 디바이스를 포함하는, 검증 서브그룹 내의 다른 디바이스들에게 통지한다. 일부 실시예들에서, 이러한 통지는, 새로운 디바이스를 포함하는, 검증 서브그룹 내의 멤버들의 리스트를 포함한다.

[0005] 일부 실시예들에서, 디바이스들은 다수의 검증 서브그룹들의 멤버들일 수 있다. 또한, 디바이스들은 디바이스들이 새롭게 조건들을 충족시키도록 또는 더 이상 다양한 검증 서브그룹들의 조건들을 충족시키지 않도록 디바이스들의 속성들이 변경될 때 그러한 검증 서브그룹들 안팎으로 동적으로 이동할 수 있다. 디바이스의 속성들이 변경되어(예컨대, 특정 암호화 시크릿을 포함하는 프로파일이 디바이스 상에 설치되는 것, 사용자가 디바이스 패스코드 길이를 변경하는 것 등) 디바이스가 검증 서브그룹에 대해 적격하게 될 때, 디바이스는, 전송된 바와 같이, 검증 서브그룹 내에서의 멤버십을 위한 요청을 생성 및 전송한다. 다른 한편으로, 디바이스의 속성들이 변경되어 디바이스가 현재 멤버인 검증 서브그룹 내에서의 멤버십을 위한 조건들을 디바이스가 더 이상 충족시키지 못할 때, 디바이스는 그것이 더 이상 서브그룹의 멤버이어서는 안 된다는 것을 검출하고, 이러한 통지를 서브그룹의 멤버들인 다른 디바이스들로 송신한다.

[0006] 일부 실시예들에서, 검증 서브그룹들은 디바이스 상에 저장된 어느 데이터 아이템들이 다른 디바이스들과 동기화되어야 하는지를 판정하기 위해 디바이스들을 동기화 서브그룹들로 조직화하는 데 사용된다. 일부 실시예들에서, 동기화 서브그룹들은 (i) 디바이스가 동기화 서브그룹에 참여하기 위한 조건들의 세트 및 (ii) 동기화 서브그룹에 참여하는 디바이스들 사이에서 동기화되는 데이터 아이템의 타입에 의해 정의된다. 일부 실시예들에서, 동기화 서브그룹들에 대한 조건들의 세트는 하나 이상의 검증 서브그룹들 내에서의 멤버십이다. 예를 들어, 제1 동기화 서브그룹에의 참여를 위한 조건들은 제1 검증 서브그룹 내에서의 멤버십일 수 있는 한편, 제2 동기화 서브그룹에의 참여를 위한 조건들은 제2 및 제3 검증 서브그룹들 양측 모두 내에서의 멤버십일 수 있다.

[0007] 동기화 서브그룹들은 관련 디바이스들의 세트가 데이터 아이템들을 서로 동기화시키는 것을 가능하게 하는 데 사용된다. 다양한 실시예들에서, 이러한 동기화된 데이터 아이템들은 온라인 계정들(예컨대, 금융 서비스 웹사이트들, 온라인 포럼 사이트들, 미디어 콘텐츠 제공자들, 온라인 소매 사이트들 등)에 대한 사용자명들 및 패스워드들, 암호화 키들 및/또는 시크릿들(즉, 키들이 생성될 수 있는 데이터), 네트워크(예컨대, Wi-Fi 네트워크) 패스워드들, 노트들, 사진들, 문서들 및 다른 파일들 등 중의 일부 또는 전부를 포함한다. 디바이스들 중 하나가 (예컨대, 새로운 패스워드의 사용자 입력, 새로운 사진의 импорт(import) 또는 다운로드 등으로부터) 동기화 데이터 아이템들의 세트에 추가시킬 새로운 데이터 아이템을 수신할 때, 일부 실시예들의 디바이스는 데이터를 하나 이상의 동기화 서브그룹들에 속하는 것으로서 동적으로 태깅한다. 예를 들어, 데이터가 생성된 애플리케이션(예컨대, Wi-Fi 네트워크들/패스워드들 대 온라인 계정 사용자명들/패스워드들), 사용자명/계정이 액세스를 얻는 웹사이트의 타입(예컨대, 금융 웹사이트 대 비금융 웹사이트), 데이터가 기업과 관련되는지 아닌지의 여부 등에 기초하여 데이터가 태깅될 수 있다.

[0008] 특정 동기화 서브그룹에 속하는 데이터 아이템들은 특정 동기화 서브그룹에 참여하는 디바이스들 사이에서 동기화된다. 일부 실시예들에서, 각각의 쌍의 디바이스들은 데이터 아이템들을 전송하는 데 사용하기 위해 이들 자신들 사이에 (예컨대, 오프-더-레코드(Off-the-Record, OTR) 메시징 프로토콜을 사용하여) 보안 채널을 생성한다. 상이한 실시예들에서, 이러한 보안 채널은 수신 디바이스가 잠금해제될 때에도 일시적인 저장을 허용하는 중앙집중형 서비스(예컨대, 양측 모두의 디바이스들이 로그인되는 클라우드 서비스 계정을 위한 저장소)를 통과시킬 수 있다. 그러나, 일부 실시예들에서, 보안 채널의 사용은 중간자 공격(man-in-the-middle attack)들에

대해 이러한 통신들을 보호한다. 다른 실시예들은 (예컨대, 블루투스 접속을 통해) 직접 피어-투-피어 접속들을 사용한다.

[0009] 제1 디바이스가 그의 데이터 아이템들을 제2 디바이스와 동기화시켜야 하는 것으로 판정할 때, 제1 디바이스는 제1 및 제2 디바이스들 양측 모두가 참여하는 동기화 서브그룹들을 식별한다. 각각의 그러한 서브그룹에 대해, 이어서 제1 디바이스는 그것이 저장하고 (i) 제2 디바이스로 아직 전송되지 않았고 (ii) 제2 디바이스가 참여하는 동기화 서브그룹들에 속하는 모든 동기화 데이터 아이템들을 식별한다. 동기화 서브그룹들이 보안 채널에 대한 임의의 추가적인 요건들을 부과하지 않는 한, 제1 디바이스는 식별된 동기화 데이터 아이템들을 보안 채널을 통해 제2 디바이스로 전송한다. 동기화 서브그룹이 보안 채널에 추가적인 요건들을 부과할 때(예컨대, 검증 서브그룹 내에서의 멤버십에 필요한 암호화 키로 데이터 아이템들을 암호화하는 것), 제1 디바이스는 다수의 상이한 보안 채널들을 사용하여 데이터 아이템들의 세트를 제2 디바이스와 동기화시킬 수 있다. 제2 디바이스는 또한 그의 데이터 아이템들을 제1 디바이스와 동기화시키기 위한 유사한 세트의 동작들을 수행한다.

[0010] 디바이스들이 검증 서브그룹들에 동적으로 조인하고 그들을 이탈하므로, 이는 디바이스들이 동기화 서브그룹들에 조인하고 그들을 이탈하게 할 수 있다. 예를 들어, 특정 동기화 서브그룹이 디바이스가 제1 및 제2 검증 서브그룹들의 멤버일 것을 필요로 하는 경우, 이어서 디바이스가 제1 검증 서브그룹 내에서의 그의 멤버십을 상실한 경우, 디바이스는 제2 검증 서브그룹 내에서의 멤버십을 유지하는 경우에도 더 이상 특정 동기화 서브그룹에 참여하는 것이 불가능할 것이다. 일부 실시예들에서, 디바이스가 더 이상 특정 동기화 서브그룹에 참여하기에 적격하지 않을 때, 디바이스는, 디바이스가 여전히 참여하는 다른 동기화 서브그룹들에 또한 속하는 데이터 아이템들을 제외하고는, 그 특정 동기화 서브그룹에 속하는 모든 데이터 아이템들을 제거한다(또는 디바이스가 이러한 데이터 아이템들을 제거해야 하는지 여부를 판정하도록 사용자에게 프롬프트한다).

[0011] 앞선 개요는 본 발명의 일부 실시예들에 대한 간단한 소개로서의 역할을 하는 것으로 의도된다. 이는 본 문헌에 개시된 모든 발명의 요지의 소개 또는 개괄이 되는 것으로 의도되지 않는다. 다음의 상세한 설명 및 상세한 설명에서 참조되는 도면들은 개요에서 기술된 실시예들, 나아가 다른 실시예들도 더 기술한다. 이에 따라, 본 문헌에 의해 기술된 실시예들 모두를 이해하기 위해서는 개요, 상세한 설명, 및 도면의 완전한 리뷰가 필요하다. 더욱이, 청구된 요지들은 요지들의 사상으로부터 벗어남이 없이 다른 특정 형태들로 구체화될 수 있기 때문에, 청구된 요지들은 개요, 상세한 설명, 및 도면들에서의 예시적인 상세 사항들에 의해 제한되는 것이 아니라, 오히려 첨부된 청구범위에 의해 한정되어야 한다.

도면의 간단한 설명

[0012] 본 발명의 신규한 특징들이 첨부된 청구범위에 제시된다. 그러나, 설명의 목적을 위해, 본 발명의 여러 개의 실시예들이 다음의 도면들에서 제시된다.

도 1은 단일 사용자가 소유할 수 있는 6개의 전자 디바이스들의 예를 도시한다.

도 2는 디바이스가 사용자의 클라우드 서비스 계정 패스워드들을 알고 있다는 단일 기준만을 갖는 제1 링을 도시한다.

도 3은 멤버십을 위해 (i) 디바이스가 iOS 운영 체제를 실행하고 있을 것 및 (ii) 사용자가 디바이스를 링 내에서 승인할 것을 필요로 하는 제2 링을 도시한다.

도 4는 멤버십을 위해 (i) 디바이스가 (패스코드/패스워드 강도에 대한 프록시로서의 역할을 하는) 적어도 12개의 문자들을 갖는 패스코드/패스워드를 가질 것 및 (ii) 사용자가 디바이스를 링 내에서 승인할 것을 필요로 하는 제3 링을 도시한다.

도 5는 멤버십을 위해 디바이스가 (i) 기업 프로파일 구성물(enterprise profile configuration)이 설치되어 있을 것 및 (ii) 클라우드 서비스 패스워드를 알고 있을 것을 필요로 하는 제4 링을 도시한다.

도 6은 멤버십을 위해 (i) 디바이스가 패스워드를 가질 것 및 (ii) 대역 외 프로세스를 이용하여 디바이스가 진품 애플(Apple) 디바이스로서 검증될 것을 필요로 하는 제5 링을 도시한다.

도 7 내지 도 9는 도 1의 디바이스들의 세트에 대한 상이한 뷰들의 예들을 도시하는데, 이때 각각의 뷰는 도 2 내지 도 6의 링들 중 하나 이상의 링 내에서의 멤버십에 기초하여 정의된다.

도 10은 디바이스들을 검증 서브그룹들(링들) 및 동기화 서브그룹들(뷰들)로 그룹화하는 것을 가능하게 하기 위한 일부 실시예들의 디바이스(1000)의 소프트웨어 아키텍처를 개념적으로 도시한다.

도 11은 링 내에서의 멤버십을 요청하기 위한 일부 실시예들의 프로세스(1100)를 개념적으로 도시한다.

도 12는 디바이스를 링 내에서 허용할지 여부를 판정하기 위한 일부 실시예들의 프로세스(1200)를 개념적으로 도시한다.

도 13은 제1 디바이스가 링에 조인할 것을 요청하고 제2 디바이스에 의해 승인되는 것을 개념적으로 도시한다.

도 14는 디바이스가, 시크릿 암호화 키의 소유뿐만 아니라 중앙 기관을 통한 디바이스 속성의 검증을 필요로 하는 링에 조인하는 것을 개념적으로 도시한다.

도 15는 제1 디바이스로부터의 키체인 데이터를 제2 디바이스와 동기화시키기 위한 일부 실시예들의 프로세스(1500)를 개념적으로 도시한다.

도 16은 제1 디바이스에 의한 동기화를 위한 새로운 데이터 아이템의 수신을 도시한다.

도 17은 제1 디바이스로부터의 도 16으로부터의 새로운 데이터 아이템의 제2 디바이스와의 동기화를 도시한다.

도 18 및 도 19는 키들 및 데이터 필드들의 트리에 저장된 데이터에 액세스하기 위해 애플리케이션 특정 개인 키가 사용되는 데이터 보호 구조체를 도시하는데, 이는 궁극적으로 애플리케이션 데이터 자체로의 액세스를 허용한다.

도 20은 디바이스의 링 멤버십 그리고, 그에 후속하여, 그의 뷰 참여를 동적으로 수정하기 위한 일부 실시예들의 프로세스를 개념적으로 도시한다.

도 21a 및 도 21b는 디바이스들 중 하나가 링으로부터 제거되도록 그의 패스워드가 변경될 때의 도 16 및 도 17로부터의 디바이스들을 도시한다.

도 22는 일부 실시예들이 구현되는 모바일 컴퓨팅 디바이스의 아키텍처의 예를 도시한다.

도 23은 본 발명의 일부 실시예들이 구현되는 전자 시스템의 다른 예를 개념적으로 도시한다.

발명을 실시하기 위한 구체적인 내용

[0013] 본 발명에 대한 다음의 상세한 설명에서는, 본 발명의 다수의 상세 사항들, 예들, 및 실시예들이 제시 및 기술된다. 그러나, 본 발명이 제시된 실시예들로 제한되지 않고 본 발명이 논의되는 구체적인 상세 사항들 및 예들 중 일부가 없이 실시될 수 있음은 명백하고 당업자에게 자명할 것이다.

[0014] 일부 실시예들은 한 세트의 관련 전자 디바이스들 사이에서 데이터 아이템들을 동기화시키기 위한 방법을 제공한다. 구체적으로, 일부 실시예들은 디바이스들이 검증 서브그룹들에 대한 멤버십 요건들을 만족시키는 경우에 디바이스들이 조인할 수 있는 검증 서브그룹들을 정의하고, 검증 서브그룹들을 사용하여 디바이스들이 참여하는 동기화 서브그룹들을 정의한다. 일부 실시예들에서, 상이한 동기화 서브그룹들은 동기화 서브그룹들에 참여하는 디바이스들이 동기화 프로세스들을 통해 서로 공유하는 상이한 타입들의 데이터 아이템들을 정의한다.

[0015] 일부 실시예들에서, 관련 전자 디바이스들의 세트는 사용자가 제3자 서비스와(예컨대, 사용자의 특정 클라우드 서비스 계정과) 연관시키는 모든 디바이스들을 포함한다. 클라우드 서비스 계정 패스워드의 지식은, 일부 실시예들의 검증 서브그룹들(또한 본 명세서에서 링들이라고도 지칭됨) 중 적어도 하나의 검증 서브그룹 내에서의 멤버십을 위한 요건으로서의 역할을 하지만, 일부 실시예들은 다양한 디바이스들이 조인할 수 있는 추가적인 링들을 정의한다. 일부 경우들에서, 사용자가 다수의 스마트폰들, 스마트워치들, 태블릿들, 랩톱 컴퓨터들, 데스크톱 컴퓨터들, 미디어 플레이어들 등을 소유 또는 사용할 수 있고, 그 모두는 사용자의 클라우드 서비스 계정에 로그인되며 상이한 속성들을 갖는다.

[0016] 상이한 실시예들은, 디바이스가 특정 운영 체제를 가지며 특정 레벨의 패스워드 강도를 가지며 특정 하드웨어(예컨대, 애플 시큐어 엔클레이브 프로세서(Apple Secure Enclave Processor)와 같은 보안 프로세싱 유닛) 또는 다른 디바이스 구성 속성들을 갖는다는 요건들을 포함한, 그러한 추가적인 링들에 조인하기 위한 상이한 세트들의 요건들을 정의한다. 일부 실시예들은, 디바이스가 특정 링에 조인하기 위해 특정 암호화 시크릿의 소유(예컨대, 기업에 의해 정의된 링에 조인하기 위해 기업 프로파일이 제공된 키의 소유)를 증명하는 것, 또는 사용자가 링에 이미 확립된 디바이스 상에서 새로운 디바이스의 멤버십을 검증할 것을 필요로 한다. 또한, 일부 링들은 새로운 디바이스가 대역 외 프로세스를 통해(예컨대, 검증을 위해 제3자를 사용하는 것에 의해) 확립된 디바이스에 대한 자신의 속성을 검증할 것을 필요로 할 수 있는데, 이때 링은 디바이스가 링에 조인한 특정 시간에

서의 속성의 지속적인 증명서로서의 역할을 한다.

- [0017] 디바이스가 링에 조인하기 위해, 일부 실시예들은 디바이스가 링에 조인하기 위한 요청에 서명할 것 및 링에 이미 있는 디바이스들 중 하나에 의해 승인된 요청을 가질 것을 필요로 한다. 예를 들어, 일부 실시예들에서, 디바이스가 암호화 시크릿의 소유를 필요로 하는 링에 대한 요건들을 충족시킬 때, 디바이스는 (i) (다른 디바이스들과 이미 공유된) 그의 공개 키 및 링으로의 신청 날짜/시간에 암호화 시크릿으로부터 생성된 개인 키로 서명하고, (ii) 이러한 서명을 링에 조인하는 데 사용되는 그의 아이덴티티로 패키징하고, (iii) 아이덴티티에 그 자신의 개인 키로 서명한다. 이어서, 이러한 서명은 링에 조인하기 위한 요청으로서 링 내의 다른 디바이스들로 전송된다. 다른 디바이스들 중 하나가 요청 디바이스가 링에 조인하기 위한 모든 요건들을 충족시키는지를 검증할 때, 확립된 디바이스는, 추가되는 새로운 디바이스를 포함하는, 링 내의 다른 디바이스들에게 통지한다. 일부 실시예들에서, 이러한 통지는, 새로운 디바이스를 현재 포함하는, 링의 멤버들의 리스트를 포함한다.
- [0018] 일부 실시예들에서, 디바이스들은 다수의 링들의 멤버들일 수 있다. 또한, 디바이스들은 디바이스들이 새롭게 요건들을 충족시키도록 또는 더 이상 다양한 링들의 요건들을 충족시키지 않도록 디바이스들의 속성들이 변경될 때 그러한 링들 안팎으로 동적으로 이동할 수 있다. 디바이스의 속성들이 변경되어(예컨대, 특정 암호화 시크릿을 포함하는 프로파일의 디바이스 상에 설치되는 것, 사용자가 디바이스 패스코드 길이를 변경하는 것 등) 디바이스가 링에 대해 적격하게 될 때, 디바이스는, 전송된 바와 같이, 링 내에서의 멤버십을 위한 요청을 생성 및 전송한다. 다른 한편으로, 디바이스의 속성들이 변경되어 디바이스가 현재 멤버인 링 내에서의 멤버십을 위한 요건들을 디바이스가 더 이상 충족시키지 못할 때, 디바이스는 그것이 더 이상 링의 멤버이어서는 안 된다는 것을 검출하고, 이러한 통지를 링의 멤버들인 다른 디바이스들로 송신한다.
- [0019] 일부 실시예들에서, 링들은 디바이스 상에 저장된 어느 데이터 아이템들이 다른 디바이스들과 동기화되어야 하는지를 판정하기 위해 디바이스들을 동기화 서브그룹들(또한 본 명세서에서 뷰들로도 지칭됨)로 조직화하는 데 사용된다. 일부 실시예들에서, 뷰들은 (i) 디바이스가 뷰에 참여하기 위한 요건들의 세트 및 (ii) 뷰에 참여하는 디바이스들 사이에서 동기화되는 데이터 아이템의 타입에 의해 정의된다. 일부 실시예들에서, 뷰들에 대한 요건들의 세트는 하나 이상의 링들 내에서의 멤버십이다. 예를 들어, 제1 뷰에의 참여를 위한 요건들은 제1 링 내에서의 멤버십일 수 있는 한편, 제2 뷰에의 참여를 위한 요건들은 제2 및 제3 링들 양측 모두 내에서의 멤버십일 수 있다.
- [0020] 뷰들은 관련 디바이스들의 세트가 데이터 아이템들을 서로 동기화시키는 것을 가능하게 하는 데 사용된다. 다양한 실시예들에서, 이러한 동기화된 데이터 아이템들은 온라인 계정들(예컨대, 금융 서비스 웹사이트들, 온라인 포럼 사이트들, 미디어 콘텐츠 제공자들, 온라인 소매 사이트들 등)에 대한 사용자명들 및 패스워드들, 암호화 키들 및/또는 시크릿들(즉, 키들이 생성될 수 있는 데이터), 네트워크(예컨대, Wi-Fi 네트워크) 패스워드들, 노트들, 사진들, 문서들 및 다른 파일들 등 중의 일부 또는 전부를 포함한다. 디바이스들 중 하나가 (예컨대, 새로운 패스워드의 사용자 입력, 새로운 사진의 импорт 또는 다운로드 등으로부터) 동기화 데이터 아이템들의 세트에 추가시킬 새로운 데이터 아이템을 수신할 때, 일부 실시예들의 디바이스는 데이터를 하나 이상의 뷰들에 속하는 것으로서 동적으로 태깅한다. 예를 들어, 데이터가 내부에 생성된 애플리케이션(예컨대, Wi-Fi 네트워크들/패스워드들 대 온라인 계정 사용자명들/패스워드들), 사용자명/계정이 액세스를 얻는 웹사이트의 타입(예컨대, 금융 웹사이트 대 비금융 웹사이트), 데이터가 기업과 관련되는지 아닌지의 여부 등에 기초하여 데이터가 태깅될 수 있다.
- [0021] 특정 뷰에 속하는 데이터 아이템들은 특정 뷰에 참여하는 디바이스들 사이에서 동기화된다. 일부 실시예들에서, 각각의 쌍의 디바이스들은 데이터 아이템들을 전송하는 데 사용하기 위해 그 자신들 사이에 (예컨대, 오프-더-레코드(OTR) 메시징 프로토콜을 이용하여) 보안 채널을 생성한다. 상이한 실시예들에서, 이러한 보안 채널은 수신 디바이스가 잠금해제될 때에도 일시적인 저장을 허용하는 중앙집중형 서비스(예컨대, 양측 모두의 디바이스들이 로그인되는 클라우드 서비스 계정을 위한 저장소)를 통과시킬 수 있다. 그러나, 일부 실시예들에서, 보안 채널의 사용은 중간자 공격들에 대해 이러한 통신들을 보호한다. 다른 실시예들은 (예컨대, 블루투스 접속을 통해) 직접 피어-투-피어 접속들을 사용한다. 키체인에 대한 데이터 아이템들의 동기화는 미국 특허 공개 제2014/0281540호에 보다 상세히 기술되어 있다.
- [0022] 제1 디바이스가 (예컨대, 사용자 입력, 특정 기간 경과 등에 기초하여) 그의 데이터 아이템들을 제2 디바이스와 동기화시켜야 하는 것으로 판정할 때, 제1 디바이스는 제1 및 제2 디바이스들 양측 모두가 참여하는 뷰들을 식별한다. 각각의 그러한 뷰에 대해, 이어서 제1 디바이스는 그것이 저장하고 (i) 제2 디바이스로 아직 전송되지 않았고 (ii) 제2 디바이스가 참여하는 뷰들에 속하는 모든 동기화 데이터 아이템들을 식별한다. 뷰들이 보안

채널에 대한 임의의 추가적인 요건들을 부과하지 않는 한, 제1 디바이스는 식별된 동기화 데이터 아이템들을 보안 채널을 통해 제2 디바이스로 전송한다. 부가 보안 채널에 추가적인 요건들을 부과할 때(예컨대, 검증 서브 그룹 내에서의 멤버십에 필요한 암호화 키로 데이터 아이템들을 암호화하는 것), 제1 디바이스는 다수의 상이한 보안 채널들을 사용하여 데이터 아이템들의 세트를 제2 디바이스와 동기화시킬 수 있다. 제2 디바이스는 또한 그의 데이터 아이템들을 제1 디바이스와 동기화시키기 위한 유사한 세트의 동작들을 수행한다.

[0023] 디바이스들이 링들에 동적으로 조인하고 그들을 이탈하므로, 이는 디바이스들이 뷰들에 조인하고 그들을 이탈하게 할 수 있다. 예를 들어, 특정 뷰가 디바이스가 제1 및 제2 링들의 멤버일 것을 필요로 하는 경우, 이어서 디바이스가 제1 링 내에서의 그의 멤버십을 상실한 경우, 디바이스는 제2 링 내에서의 멤버십을 유지하는 경우에도 더 이상 특정 뷰에 참여하는 것이 불가능할 것이다. 일부 실시예들에서, 디바이스가 더 이상 특정 뷰에 참여하기에 적격하지 않을 때, 디바이스는, 디바이스가 여전히 참여하는 다른 뷰들에 또한 속하는 데이터 아이템들을 제외하고는, 그 특정 뷰에 속하는 모든 데이터 아이템들을 제거한다(또는 디바이스가 이러한 데이터 아이템들을 제거해야 하는지 여부를 판정하도록 사용자에게 프롬프트한다).

[0024] 상기는 일부 실시예들의 데이터 동기화 시스템의 예들을 기술한 것이다. 여러 개의 더 상세한 예들이 하기에 기술된다. 섹션 I은 디바이스들의 그룹, 및 디바이스들에 대해 정의될 수 있는 링들 및 뷰들의 예들을 기술한다. 다음으로, 섹션 II는 링들 및 뷰들을 가능하게 하기 위한 일부 실시예들의 디바이스 아키텍처를 기술한다. 이어서, 섹션 III은 일부 실시예들의 링 조인 프로세스를 기술하는 한편, 섹션 IV는 상이한 뷰들에 대한 데이터의 동기화를 기술한다. 이어서, 섹션 V는 일부 실시예들에서 링 상태를 동적으로 평가하는 것 및 뷰 참여에 대한 결과들을 기술한다. 마지막으로, 섹션 VI는 본 발명의 일부 실시예들이 구현되는 전자 시스템을 기술한다.

[0025] I. 링 및 뷰 예들

[0026] 전술된 바와 같이, 일부 실시예들은 디바이스들의 정적 또는 동적 속성들에 기초하여 디바이스들이 조인할 수 있는 디바이스들의 그룹에 대한 링들을 정의한다. 이러한 링들은, 다양한 실시예들에서, 디바이스들의 제조자들, 제3자 개발자들, 또는 사용자들 자신에 의해 정의될 수 있다. 예를 들어, 여러 상이한 타입들의 사용자 디바이스들(그 중 임의의 수의 사용자 디바이스를 단일 사용자가 소유할 수 있다)을 판매하는 제조자는 링 정의들을 디바이스 운영 체제들에 통합시킬 수 있다. 다른 한편으로, 제3자 개발자들 또는 사용자들은, 그들이 유용하다고 알게 된 추가적인 링들을 제안할 수 있고, 일부 또는 모든 디바이스들에 대해 링들을 설계할 수 있다. 일부 실시예들에서, 제조자는 사용자들이 그들의 개인용 디바이스들에 대한 링들을 임의로 정의하게 하는 프레임워크를 디바이스들에게 제공하는데, 이때 그 프레임워크는 임의로 정의된 링들을 기능적 링 정의들로 변환하는 능력을 갖는다.

[0027] 디바이스 제조자들, 제3자 개발자들, 또는 사용자들은 또한 전술된 바와 같이 링 멤버십들에 기초하여 디바이스들을 뷰들로 조직화할 수 있다. 즉, 디바이스가 하나 이상의 링들의 멤버인지 여부에 따라 특정 뷰에의 디바이스의 참여가 정의될 수 있다. 일부 실시예들에서, 뷰들은 또한 링 멤버십 이외의 디바이스 속성들을 참조하여 정의될 수 있는 반면, 다른 실시예들은 뷰들을 링 멤버십들에 기초한 정의들로 제한한다. 일부 실시예들에서, 링 멤버십 기준을 정의하는 것에 더하여, 사용자는 특정 뷰에 대해 어떤 데이터가 공유되는지뿐만 아니라 그 특정 뷰에 참여하기 위해(즉, 특정된 데이터를 다른 디바이스들과 동기화시키기 위해) 디바이스가 어느 링들에 속해야 하는지의 양측 모두를 정의하는 능력을 갖는다.

[0028] 도 1은 단일 사용자가 소유할 수 있는 6개의 전자 디바이스들(105 내지 130)의 예를 도시한다. 도시된 바와 같이, 이러한 6개의 전자 디바이스들은 제1 스마트폰(105), 제2 스마트폰(110), 태블릿(115), 랩톱 컴퓨터(120), 스트리밍 비디오 셋톱 박스(125), 및 데스크톱 컴퓨터(130)를 포함한다. 이러한 경우, 제1 폰(105) 및 랩톱(120)은 사용자의 작업 디바이스들인 한편, 다른 4개의 디바이스들(110, 115, 125, 130)은 사용자의 개인 소유 디바이스들이다. 이러한 디바이스들 각각은 상이한 속성들을 가지며, 그 중 일부가 이 도면에 도시되어 있다.

[0029] 구체적으로, (예컨대, 아이폰(iPhone) 6일 수 있는) 제1 스마트폰(105)은 (i)(사용자가 그 디바이스 상의 클라우드 서비스 계정에 로그인했기 때문에) 사용자의 클라우드 서비스 계정 패스워드를 알고 있고, (ii) 빌트인 지문 스캐너를 가지며, (iii) iOS 운영 체제를 실행하고, (iv) 폰을 분실한 경우에 사용자가 폰에게 그의 메모리를 와이프(wipe)하도록 원격으로 지시하게 하는 원격 와이프 특징이 인에이블되게 하고, (v) 적어도 12개의 문자들의 길이인, 디바이스를 잠금해제하기 위한 패스코드를 가지며, (vi) 기업 구성물이 설치되어 있다. 따라서, 지문 스캐너, 긴 잠금해제 패스코드, 및 원격 와이프 특징 모두는 그 디바이스가 보안 디바이스임을 나타낸다. 또한, 일부 실시예들의 기업 구성물의 설치는 디바이스에 특정 암호화 시크릿을 제공하여 공개/개인 키 쌍의 생성을 가능하게 한다.

- [0030] (예컨대, 이전 아이폰일 수 있는) 제2 스마트폰(110)은 (i) 사용자의 클라우드 서비스 계정 패스워드를 알고 있고, (ii) iOS 운영 체제를 실행하고, (iii) 원격 와이프 특성이 인에이블되게 하고, (iv) 디바이스를 잠금해제하기 위한 4문자 패스코드를 갖는다. 보다 짧은 패스코드를 가지며 지문 스캐너가 없는 이러한 스마트폰(110)은 여전히 상당히 안전하지만, 제1 스마트폰(105)보다 덜 안전하다.
- [0031] 태블릿(115)(예컨대, 아이패드(iPad))은 (i) 사용자의 클라우드 서비스 계정 패스워드를 알고 있고, (ii) iOS 운영 체제를 실행하고, (iii) 디바이스를 잠금해제하기 위한 4문자 패스코드를 갖는다. 랩톱(120)(예컨대, 맥북(MacBook))은 (i) 사용자의 클라우드 서비스 계정 패스워드를 알고 있고, (ii) 맥 OS X 운영 체제를 실행하고, (iii) 디바이스를 잠금해제하기 위한 12문자 패스코드를 가지며, (iv) 기업 구성물이 설치되어 있다. 스트리밍 비디오 셋톱 박스(125)(예컨대, 애플 TV)는 사용자의 클라우드 서비스 계정 패스워드만을 알고 있다. 마지막으로, 홈 데스크톱(130)(예컨대, 아이맥(iMac))은 (i) 사용자의 클라우드 서비스 계정 패스워드를 알고 있고, (ii) 맥 OS X 운영 체제를 실행하고, (iii) 잠금해제하기 위한 12문자 패스코드를 갖는다.
- [0032] 다양한 디바이스들(105 내지 130)에 대해 리스팅된 이러한 속성들은 링 멤버십 기준의 몇 가지 예들(예컨대, 사용자가 클라우드 서비스 계정에 로그인했는지 여부, 디바이스의 운영 체제, 패스코드 강도, 다른 보안 특징들, 기업 구성물을 통한 암호화 시크릿의 존재 등)을 표현한다. 당업자는 링에 대한 멤버십 적격성을 판정하기 위해 많은 다른 기준이 사용될 수 있다는 것을 인식할 것이다. 도시되는 바와 같이, 이러한 기준 중 일부는 디바이스의 속성들이 아니다. 예를 들어, 일부 실시예들은 링 멤버십 기준으로서 디바이스 상에서 동작하는 애플리케이션들의 속성들(예컨대, 애플리케이션이 설치되는지 여부, 애플리케이션이 디바이스 상에 설정되는 방법 등)을 사용한다. 또한, 일부 실시예들은, 사용자가 링에 이미 확립된 다른 디바이스 상에서 디바이스를 승인하는 것, 사용자가 확립된 디바이스에 의해 제공된 코드를 요청 디바이스 상에 입력하는 것 등과 같은, 링에 조인하기 위한 특정 사용자 액션들을 필요로 한다. 또한, 일부 링 멤버십 기준은 제3자 검증을 필요로 한다. 예를 들어, 일부 실시예들은 디바이스가 유효한 iOS 디바이스라는 제3자 증명서를 필요로 한다. 다른 한편으로, 일부 링 멤버십 기준은 (예컨대, 디바이스 패스코드가 적어도 특정 길이인) 멤버십을 요청하는 디바이스에 의해 단순히 어서트(assert)되어야 한다.
- [0033] 도 2 내지 도 6은 디바이스들(105 내지 130)에 대한 일부 실시예들의 다양한 링들의 예들을 제공한다. 도 2는 디바이스가 사용자의 클라우드 서비스 계정 패스워드들을 알고 있다는 단일 기준만을 갖는 제1 링(200)을 도시한다. 일부 실시예들은, 사용자가 클라우드 서비스 계정으로 그 디바이스를 로그인하는 한, 이러한 링을 사용하여 사용자가 소유하는 디바이스들 모두가 링에 함께 조인하게 한다. 일부 실시예들에서, 새로운 디바이스들이 결정적 공개/개인 키 생성 알고리즘을 사용하여 계정 패스워드에 기초하여 개인 키를 생성하는 것 및 (이미 링에 있는 임의의 디바이스에 의해 검증될 수 있는) 이러한 개인 키를 사용하여 링 멤버십을 위한 신청서에 서명하는 것에 의해 링에 신청할 수 있다. 그에 따라, 모든 디바이스들(105 내지 130)은 제1 링(200)의 멤버들이다.
- [0034] 도 3은 멤버십을 위해 (i) 디바이스가 iOS 운영 체제를 실행하고 있는 것 및 (ii) 사용자가 디바이스를 링 내에서 승인할 것을 필요로 하는 제2 링(300)을 도시한다. 따라서, 어떠한 iOS 디바이스(즉, 랜덤한 사용자의 스마트폰)도 링에 조인할 수 없고; 그 대신에, 확립된 디바이스의 사용자는 디바이스를 링 내에서 조인하는 것을 승인해야 한다. 사용자 승인이 비-사용자 디바이스들이 조인하는 것을 방지하기 위한 보안 메커니즘의 예를 제공하지만, 일부 실시예들은 모든 링들에 대해 클라우드 서비스 계정 패스워드(또는 다른 암호화 시크릿)의 지식을 필요로 하여, 사용자가 다른 사용자의 디바이스가 사용자의 실제 디바이스들을 갖는 링 내에서 우연히 허용하게 하는 것을 방지한다. 일부 실시예들에서, 디바이스는 링 조인 절차의 일부로서 그것이 iOS 디바이스임을 어서트하고; 이어서, 디바이스가 사용자에게 속한다는 것뿐만 아니라, 디바이스가 링 멤버십 신청서에서 주장하는 대로 iOS라는 것을 승인하기 위한 프롬프트(예컨대, "An iPhone wishes to join your iOS Device Ring; Please verify that this is your iPhone"라고 판독되는 프롬프트, 또는 이와 유사한 정보)가 사용자에게 제시된다. 다른 실시예들에서, 디바이스는 제3자(예컨대, 디바이스 제조자)를 이용하여 디바이스가 주장된 바와 같은 iOS 디바이스인지를 검증할 것이 요구된다. 이러한 검증은 디바이스가 링 내에서 승인되기 전에 대역 외에서 수행될 수 있다. 제2 링(300)은 다른 3개의 디바이스들이 iOS 디바이스들이 아니기 때문에, 3개의 멤버들, 즉, 2개의 스마트폰들(105, 110) 및 태블릿(115)을 갖는다.
- [0035] 도 4는 멤버십을 위해 (i) 디바이스가 (패스코드/패스워드 강도에 대한 프록시로서의 역할을 하는) 적어도 12개의 문자들을 갖는 패스코드/패스워드를 가질 것 및 (ii) 사용자가 디바이스를 링 내에서 승인할 것을 필요로 하는 제3 링(400)을 도시한다. 이전의 링(300)과 마찬가지로, 사용자 승인 요건은 임의의 랜덤한 사용자 디바이스가 충분한 길이의 패스코드를 갖자마자 링에 조인하는 것을 방지한다. 또한, 링(300)에 대해 기술된 바와 같

이, 일부 실시예들에서, 사용자가 보안 패스코드/패스워드를 갖는 것으로서 디바이스를 승인하는 것을 요청하는 프롬프트가 사용자의 확립된 디바이스 상에 나타난다. 이러한 링(400)은 3개의 멤버들, 즉, 제1 스마트폰(105), 랩톱(120), 및 홈 데스크톱(130)을 갖는다.

[0036] 도 5는 멤버십을 위해 디바이스가 (i) 기업 프로파일 구성물이 설치되어 있을 것 및 (ii) 클라우드 서비스 패스워드를 알고 있을 것을 필요로 하는 제4 링(500)을 도시한다. 일부 실시예들에서, 디바이스들은 기업 프로파일의 일부로서 제공되는 개인 키로 링에 조인하기 위한 멤버십 요청에 서명하는 것에 의해 기업 프로파일 구성물의 소유를 증명할 수 있고, 프로세스는 도 13을 참조하여 하기에 보다 상세히 기술된다. 새로운 디바이스가 서명된 멤버십 요청을 전송하는 것에 의해 링 내에서의 멤버십을 요청할 때, 확립된 디바이스들 중 하나가 기업 프로파일 공개 키를 사용하여 이러한 요청을 검증한다. 클라우드 서비스 패스워드는, 기업의 임의의 멤버보다는, 특정 사용자에게 의해 소유된 디바이스들로부터 멤버십을 제한한다. 이는 (클라우드 서비스 패스워드를 입력했던 것에 의해) 사용자가 링에 조인하는 디바이스를 승인하는 것을 보장하기 위한 검증 메커니즘으로서의 역할을 한다. 사용자 디바이스들 중 단지 2개만이 이러한 기업 프로파일이 설치되어 있기 때문에, 링(500)은 스마트폰(105) 및 랩톱(120)만을 포함한다.

[0037] 마지막으로, 도 6은 멤버십을 위해 (i) 디바이스가 패스워드를 가질 것 및 (ii) 대역 외 프로세스를 이용하여 디바이스가 진품 애플 디바이스로서 검증될 것을 필요로 하는 제5 링(600)을 도시한다. 일부 실시예들은 상이한 링 멤버십들에 대해 다양한 대역 외 증명서들을 필요로 하여, 제3자가 확립된 디바이스가 요청 디바이스들 링 내에서 허용하기 위해 요청 디바이스가 어서트하는 일부 태양을 인증할 것을 필요로 한다. 예를 들어, 그러한 제3자 검증은 디바이스의 유효성, 디바이스 상의 보안 프로세서의 존재 등을 증명하는 데 사용될 수 있는데, 이들 중 임의의 것이 링 멤버십 요건들일 수 있다. 멤버십 기준의 대역 외 검증은 특정 시간에 멤버십 기준이 참인지를 단지 검증하지만, 링의 존재는 정기적인 제3자 검증을 필요로 하는 일 없이 어서트된 기준의 지속적인 증명을 가능하게 한다. 이러한 링의 경우, 모든 디바이스들(105 내지 130)이 애플 디바이스들이기 때문에, 패스워드를 갖는 이들(스마트폰들(105, 110), 태블릿(115), 랩톱(120), 및 데스크톱(130)) 모두는 링(600)에 조인하는 것이 가능하다.

[0038] 상기의 예들에서, 요청 디바이스에 대한 링들 중 임의의 링 내에서의 멤버십은 링에 이미 확립된 디바이스에 의한 멤버십 기준의 검증에 어떻게든 좌우된다. 일부 실시예들은 링들의 3개의 상이한 티어(tier)들을 가능하게 한다: (1) 단순히 멤버십을 어서트하는 것에 의해 임의의 디바이스가 조인할 수 있는 자가 어서션 링(self-assertion ring)들, (2) 디바이스가 멤버십을 어서트할뿐만 아니라 암호화 시크릿의 지식을 증명할 것을 필요로 하는 애플리케이션 링들, 및 (3) 자가 어서션(그리고 일부 경우들에서, 암호화 시크릿의 지식)뿐만 아니라 링에 이미 확립된 디바이스의 승인을 필요로 하는 콘코던스 링(concordance ring)들.

[0039] 일부 실시예들에서, 자가 어서션 링들은 일반적으로 많은 보안을 제공하지 않고 그에 따라 일반적으로 뷰 요건들을 전개시키는 데 사용되지 않는다(즉, 자신에 관한 사실을 단순히 어서트하는 디바이스는 그 디바이스가 임의의 추가적인 동기화 데이터에 액세스하지 못한다). 그 대신에, 검증이 없는 이러한 사실들의 어서션은 애플리케이션 링들 및 콘코던스 링들에 대한 멤버십 요청들 내에서 사용되는 디바이스 아이덴티티의 일부일 수 있다. 자가 어서션 링의 예는 디바이스가 존재한다는 것 또는 디바이스가 패스코드를 갖는다는 것을 디바이스가 어서트하는 것이 유일한 멤버십 기준이 되는 링일 것이고, 이때 디바이스는 이러한 어서션을 하자마자 링에 자동으로 추가된다.

[0040] 일부 실시예들에서, 애플리케이션 링의 예는 기업 키를 필요로 하지만 추가적인 검증을 필요로 하지 않는 링이다. 따라서, 링에 조인하기 위해, 디바이스는 (예컨대, 개인 키로 신청서에 서명하는 것에 의해) 그것이 기업 키를 갖는다는 것을 증명해야 한다. 그러나, 그러한 링에는 어떠한 추가적인 레벨의 검증도 필요하지 않다. 예를 들어, 사용자는 그러한 디바이스를 승인할 필요가 없고, 그에 따라 암호화 시크릿을 소유한(그에 따라 필요한 키를 생성할 수 있는) 임의의 디바이스가 링에 조인할 수 있다.

[0041] 마지막으로, 콘코던스 링은 뷰들(즉, 특정 타입들의 데이터를 동기화시키는 디바이스들의 그룹들)을 정의하는데 가장 보편적으로 사용되는 링의 타입이다. 언급된 바와 같이, 콘코던스 링은 디바이스가 링 내에서의 멤버십을 요청하는 것 및 링에 이미 확립된 디바이스 상에서 (예컨대, 사용자에게 승인을 프롬프트하는 것에 의해) 신청서가 명시적으로 검증될 것을 필요로 한다. 콘코던스 링은 또한 특정 암호화 시크릿(예컨대, 사용자의 클라우드 서비스 패스워드, 기업 키 등에 기초하여 생성된 키)의 증명서를 필요로 할 수 있지만, 일단 그 키로부터 생성된 서명이 확립된 디바이스에 의해 검증된다면, 확립된 디바이스는 디바이스의 사용자에게 요청 디바이스가 링에 조인해야 하는지를 검증하도록 프롬프트한다.

- [0042] 또한, 일부 실시예들은 디바이스가 링에 있어야 하는지를 검증하기 위한 다양한 대역 외 사용자 상호작용 기법들(예컨대, 암호화 시크릿의 대역 외 증명서)을 사용할 수 있다. 예를 들어, 일부 실시예들은 확립된 디바이스가 암호화 시크릿을 생성하게 하고, 확립된 디바이스가 요청 디바이스를 신뢰하도록 하기 위해 사용자가 이러한 시크릿을 요청 디바이스에 반송하는 것에 의존한다. 예를로서, 확립된 디바이스는 공개/개인 키 쌍이 생성되게 할 수 있는 난수를 생성할 수 있다. 사용자가 요청 디바이스 상에 이것을 입력할 때, 요청 디바이스는 개인 키를 생성할 수 있고 생성된 개인 키로 링 멤버십 요청에 서명할 수 있다. 유사하게, 확립된 디바이스는 오디오 또는 이미지 데이터(예컨대, QR(Quick Response) 코드)를 생성할 수 있고, 요청 디바이스가 이러한 데이터를 캡처할 것을 필요로 할 수 있고, 데이터로부터 결정적 방식으로 공개/개인 키 쌍을 생성할 수 있다. 당업자는, 관련된 2가지 타입들의 디바이스들(예컨대, 폰 상에서 생성된 QR 코드의 사진을 촬영하고, 하나의 디바이스를 특정 방식으로 다른 디바이스에 근접하게 이동시키고, 등등을 하는 스마트워치)에 따라, 다수의 그러한 기법들이 가능할 수 있다는 것을 인식할 것이다.
- [0043] 링들은 디바이스들로 하여금 다른 디바이스들이 특정 속성들을 갖는지를 검증하게 하고, 이러한 속성들의 증명서를 지속하여 디바이스들이 속성들을 정기적으로 검증할 필요가 없도록 한다. 링들을 사용하면, 일부 실시예들은, 디바이스들이 특정 속성들을 검증한 디바이스들과 특정 데이터 아이템들을 공유하게 하는 하나 이상의 동기화 서브그룹들 또는 뷰들을 디바이스들이 형성할 수 있게 한다. 따라서, 일부 실시예들에서 각각의 뷰의 참여는 하나 이상의 링들 내에서의 멤버십에 기초하여 정의되는데; 즉, (하나 이상의 특정된 링들 내의 멤버들로서 허용된 것에 의해) 뷰 조건들을 충족시키는 디바이스들만이 뷰와 연관된 동기화된 데이터를 공유할 수 있다.
- [0044] 뷰들은 사용자 디바이스들 사이에서 동기화되는 상이한 타입들의 데이터의 계층화를 가능하게 한다. 예를로서, 사용자는 특정 데이터(예컨대, 대부분의 사진들, 민감하지 않은 문서들, 금융 정보 또는 신용 카드 번호들)의 액세스가 가능하지 않게 하는 패스워드들(들)을 모든 사용자의 디바이스들 사이에서 공유되기를 원할 수 있다. 다른 한편으로, 사용자는 다른 데이터(예컨대, 민감한 사진들, 기밀 문서들, 사용자의 신용 카드 정보를 저장하는 금융 웹사이트들 또는 전자 상거래 사이트들)의 패스워드들(들)이 덜 안전한 디바이스들(예컨대, 패스워드에 의해 보호되지 않는 스트리밍 비디오 셋톱 박스)로부터 멀리 있기를 원할 수 있다. 또한, 일부 데이터는 특정 타입들의 디바이스들 상에서 어떠한 사용도 하지 않을 수도 있다(모바일 애플리케이션들에 대한 패스워드들은 그러한 애플리케이션들을 지원하지 않는 랩톱 또는 데스크톱 디바이스들 상에서 유용하지 않을 수도 있다).
- [0045] 도 7 내지 도 9는 도 1의 디바이스들의 세트에 대한 상이한 뷰들의 예들을 도시한다. 이러한 도면들에서, 각각의 뷰는 링들(200 내지 600) 중 하나 이상의 링 내에서의 멤버십에 기초하여 정의된다. 일부 실시예들은 단지 뷰 조건들이 링 멤버십에 기초하게 하는 한편, 다른 실시예들은 또한 디바이스가 뷰에 참여하기 위한 다른 타입들의 조건들(예컨대, 링 멤버십 조건들로서 전술된 것들과 같은 디바이스 속성들)을 허용한다. (링 멤버십에 기초하여 뷰 조건들을 정의한다는) 이러한 의미에서, 링들은 이들이 디바이스들의 특정 속성들을 인증하는 데 사용된다는 점에서 인증 기관과 유사하게 작용하고, 그 특정 속성들은 디바이스들이 이어서 동기화 목적들을 위해 다른 디바이스들을 신뢰하는 데 사용할 수 있다.
- [0046] 도 7에 도시된 바와 같이, 제1 뷰(700)에의 참여는 제1 링(200) 내에서의 멤버십에 의해 정의된다. 이와 같이, 6개의 디바이스들(105 내지 130) 모두가 제1 뷰에 참여한다. 이 도면은 6개의 디바이스들(105 내지 130)이 풀 메시(full mesh) 프레임워크에서 접속된다는 것을 도시하는데, 이때 디바이스들 각각은 다른 디바이스들 모두와 동기화하는 것이 가능하다. 미국 특허 공개 제2014/0281540호에 기술된 바와 같이, 일부 실시예들은 사용자 디바이스들 사이의 동기화를 위해 풀 메시 접속을 사용하는 반면, 다른 실시예들은 다른 네트워크 구성물들(예컨대, 디바이스들 중 하나를 중심 허브로 하는 스타 네트워크)을 이용한다.
- [0047] 이 도면은 3개의 데이터 아이템들(705 내지 715)이 제1 뷰(700)에 속한다는 것을 나타낸다. 일부 실시예들에서, 도 7에 도시된 바와 같이, 디바이스 상에 저장된 각각의 데이터 아이템은 데이터 아이템이 어느 뷰(들)에 속하는지를 특정하는 뷰 정보로 태그된다(디바이스들이 동기화하는 타입의 것인 각각의 데이터 아이템의 경우; 동기화에 대해 적격하지 않은 데이터 아이템들은 그와 같이 태그되지 않을 것이다). 디바이스들 중 하나가 (예컨대, 새로운 패스워드의 사용자 입력, 카메라로부터의 새로운 사진의 임포트, 새로운 문서의 생성 등으로부터) 동기화 데이터 아이템들의 세트에 추가할 새로운 데이터 아이템을 수신할 때, 디바이스는 데이터를 하나 이상의 뷰들에 속하는 것으로서 동적으로 태그한다. 예를 들어, 디바이스들의 세트에 대한 뷰들이 정의되는 방법에 따라, 데이터가 생성된 애플리케이션(예컨대, Wi-Fi 네트워크들/패스워드들 대 온라인 계정 사용자명들/패스워드들), 사용자명/계정이 액세스를 얻는 웹사이트의 타입(예컨대, 금융 웹사이트 대 비금융 웹사이트),

데이터가 기업과 관련되는지 아닌지의 여부 등에 기초하여 데이터가 태깅될 수 있다.

[0048] 일부 실시예들에서, 3개의 데이터 아이템들(705 내지 715)은 3개의 디바이스들 각각에 저장된다. 일단 디바이스들 중 하나가 이러한 데이터 아이템들 중 하나를 수신한다면, 그 디바이스는 별개의 암호화된 채널들(즉, 각각의 쌍의 디바이스들 사이의 별개의 채널)을 통해 데이터 아이템을 다른 디바이스들과 공유한다. 따라서, 사용자가 우선 데스크톱 컴퓨터(130) 상에 패스워드 아이템(715)을 입력하는 경우, 데스크톱은 별개의 채널들을 통해 이러한 아이템을 다른 디바이스들(105 내지 125) 각각과 공유한다. 일부 실시예들에서, 이러한 채널들은, 미국 특허 공개 제2014/0281540호에 그리고 하기에 보다 상세히 기술되는 바와 같이, 오프-더-레코드(OTR) 메시징과 같은 패스워드 인증 키 교환(password-authenticated key exchange, PAKE)을 이용하여 암호화된다.

[0049] 또한 미국 특허 공개 제2014/0281540호에 기술된 바와 같이, 일부 실시예들에서, 포인트-투-포인트 접속들은 클라우드 서비스 중재자를 사용한다. 즉, 디바이스들 중 하나(예컨대, 스마트폰(105))가 데이터 아이템(705)을 제2 디바이스(예컨대, 태블릿(115))와 공유하기 위해, 전송 디바이스는 (2개의 디바이스들 사이의 접속의 공개 키로 암호화되는) 데이터 아이템을 클라우드 서비스들 내의 중간 저장소로 전송한다. 이어서, 제2 디바이스는 중간 저장소로부터 데이터 아이템을 검색하고 데이터 아이템을 암호화해제한다. PAKE를 이용하는 것은 디바이스들이 클라우드 서비스의 소유자로부터의 중간자 공격에 영향을 받는 일 없이 이러한 방식으로 동기화 데이터 아이템들을 공유할 수 있게 한다.

[0050] 제1 뷰(700)가 모든 디바이스들을 포함하는 반면, 도 8은 참여를 위해 제3 링(400) 및 제4 링(500) 양측 모두에서 멤버십을 필요로 하는 제2 뷰를 도시한다. 이러한 뷰는, 본질적으로, 디바이스가 기업 디바이스이고(즉, 기업 프로파일이 설치되어 있고) 고도로 안전한 패스워드(보안을 위한 프록시로서 사용되는 길이를 갖는, 적어도 12개의 문자들)를 갖는 것으로서 검증될 것을 필요로 한다. 단지 2개의 디바이스들, 즉, 스마트폰(105) 및 랩톱(120)만이 이러한 뷰에 참여한다. 도시된 바와 같이, 뷰는 3개의 데이터 아이템들(805 내지 815)을 포함하고, 그 각각은 이러한 제2 뷰(V2)에 속하는 것으로서 태깅된다. 예를 들어, 데이터 아이템들은 이들이 특정 기업 애플리케이션들과 관련되거나, 또는 사용자가 작업 관련된 것으로서 명시한 파일들인 경우, 제2 뷰(800)에 속하는 것으로서 태깅될 수 있다. 이러한 경우, 제3 링(400)에의 멤버십의 추가는 사용자가 이들의 패스워드들 중 하나를 보다 짧고 덜 안전한 패스워드로 변경하지 않는 것을 보장하고, 이는 그렇게 하면 제3 링(400), 그리고 그에 따라 뷰(800)에서 퇴출되게 될 것이기 때문이다. 또한, 데이터 아이템들 중 하나(815)는 제2 뷰(V2) 및 제3 뷰(V3) 양측 모두에 속하는 것으로서 태깅된다. 일부 실시예들에서, 데이터 아이템들은 다수의 뷰들에 속할 수 있고, 이러한 뷰들 중 임의의 뷰에 속하는 디바이스들에 공유된다.

[0051] 마지막으로, 도 9는 제2 링(300) 및 제5 링(600) 양측 모두에서 멤버십을 필요로 하는(즉, 디바이스가 진품 애플 디바이스로서 검증된 패스워드를 갖는 iOS 디바이스일 것을 필요로 하는) 제3뷰(900)를 도시한다. 이러한 제3뷰(900)의 경우, 3개의 디바이스들(105 내지 115)이 참여하고, 2개의 데이터 아이템들(815, 905)이 이러한 2개의 디바이스들 사이에서 공유된다. 데이터 아이템(815)은 이러한 디바이스들이 제2 뷰(800)에 참여하지 않더라도 디바이스들(110, 115)과 동기화된다. 디바이스가 데이터 아이템이 속하는 각각의 뷰의 멤버일 것을 필요로 하는 다른 실시예들에서, 스마트폰(105)은 그 데이터 아이템(815)을 다른 디바이스들 중 임의의 것과 공유하는 것이 허용되지 않을 것이다.

[0052] 일부 실시예들은 제3자 개발자들 또는 디바이스들 자체의 사용자에 의한 동기화 데이터 아이템들의 이러한 계층화의 커스터마이제이션(customization)을 허용한다. 예를 들어, 일부 실시예들은 개발자들이 특정 애플리케이션들과 연관된 데이터에 대한 링들 및/또는 뷰들을 설계하기 위한 툴킷(toolkit)을 제공한다. 예를 들어, 기업 애플리케이션의 개발자는 기업 애플리케이션과 연관된 데이터 아이템들을 공유하는 디바이스들에 대한 조건들을 설계할 수 있다(즉, 특정 패스워드 강도 또는 다른 디바이스 조건들을 지정할 수 있다). 일부 실시예들에서, 디바이스들은 사용자들이 그들의 디바이스들이 데이터를 동기화시키는 방법을 커스터마이징할 수 있게 하기 위한 사용자 인터페이스를 포함한다. 즉, 사용자들은 가능한 조건들의 세트에 기초하여 이들의 데이터 아이템들에 대해 상이한 뷰들을 설계할 수 있고, 디바이스들은 링들을 뷰들로 그룹화하는 것을 통한 사용자 선택들을 구현할 것이다. 그러나, 다른 실시예들에서, 링들 및 뷰들의 설계는 사용자 디바이스들의 세트를 설계하는 디바이스 제조자에 의해 이루어진다.

[0053] II. 디바이스 아키텍처

[0054] 도 10은 디바이스들을 검증 서브그룹들(링들) 및 동기화 서브그룹들(뷰들)로 그룹화하는 것을 가능하게 하기 위한 일부 실시예들의 디바이스(1000)의 소프트웨어 아키텍처를 개념적으로 도시한다. 이러한 경우, 디바이스(1000)는 클라우드 서비스 계정과 연관된 여러 개(N개)의 디바이스들 중 하나이다. 이러한 그리고 후속 섹션들

에서의 논의를 위해, 링들에 조인하고 뷰들을 통해 데이터 아이템들을 공유하는 다양한 디바이스들이 모두 (예컨대, 클라우드 서비스 계정 또는 다른 사용자 검증 메커니즘을 통해) 단일 사용자와 연관된다고 가정될 것이다. 따라서, 디바이스(1000)에 더하여, 도 10은 한 세트의 추가적인 디바이스들(D_2 내지 D_N)(1005)을 도시한다. 디바이스(1000), 및 다른 디바이스들(1005)은 데이터를 저장하는 것 그리고 네트워크와 통신하는 것이 가능한 임의의 상이한 타입의 전자 디바이스일 수 있다. 예를 들어, 이러한 디바이스들은 스마트폰들, 태블릿들, 랩톱 및/또는 데스크톱 컴퓨터들, 스마트워치들, 셋톱 박스들(텔레비전으로부터 분리되거나 그에 통합된 것), 다른 디바이스 상에서 동작하는 가상 디바이스들(예컨대, 가상 기계들) 등을 포함할 수 있다.

[0055] 도시된 바와 같이, 디바이스(1000)는 동기화 엔진(1010), 링 평가자(ring assessor)(1015), 뷰 평가자(1020), 데이터 태거(data tagger)(1025), 및 애플리케이션들의 세트(1030)를 포함한다. 또한, 디바이스는 키체인 데이터 아이템들을 위한 저장소들(1035), 디바이스 및 링 서명 키들(1040), 및 뷰 및 링 요건들 및 기술(view and ring requirements and description)(1045)을 포함한다. 이러한 저장소들 모두는 별개의 물리적 저장소들(예를 들어, 키들이 뷰 및 링 요건들/기술보다 더 안전한 저장소에 저장될 수 있음) 또는 동일한 물리적 저장소(예컨대, 하드 디스크, 솔리드 스테이트 메모리, 랜덤 액세스 메모리 등)의 일부일 수 있다. 또한, 데이터의 일부는 모듈들의 코드 내에 내장될 수 있다. 예를 들어, 뷰 기술 및 요건들이 고정되는 경우, 이러한 정보는 이러한 모듈들에 의해 저장소로부터 인출되는 별개의 데이터보다는, 뷰 평가자 및 데이터 태거의 일부일 수 있다.

[0056] 일부 실시예들에서, 키체인 데이터 저장소(1035)는 디바이스(1000)와 다른 디바이스들(1005) 사이에서 동기화되는 데이터 아이템들인 키체인 데이터 아이템들을 저장한다. 일부 실시예들에서, 이러한 데이터 아이템들은 디바이스(1000) 상에 저장되어 디바이스와 연관된 공개 키로 암호화된다(그리고 다른 디바이스들 상에 저장되어 그러한 다른 디바이스들의 공개 키들로 암호화된다). 일부 실시예들에서, 이러한 공개 키는 디바이스가 초기에 포맷화될 때 디바이스에 의해 안전한 방식으로 생성된 디바이스 특정 키이다. 또한, 일부 실시예들에서, 디바이스 상에 저장된 각각의 데이터 아이템은 하나 이상의 뷰들에 속하는 것으로서 태깅된다.

[0057] 일부 실시예들에서, 디바이스 및 링 서명 키 저장소(1040)는 디바이스가 데이터 저장, 데이터 동기화, 및 링 멤버십 조인/검증을 위해 사용하는 다양한 키들을 저장한다. 예를 들어, 디바이스 키는 디바이스(1000) 상의 저장을 위한 데이터 아이템들을 암호화하기 위해 일부 실시예들에 의해 사용되고, 발명의 명칭이 "Backup System with Multiple Recovery Keys"인 미국 특허 출원 제14/871,498호뿐만 아니라, 미국 가특허 출원들 제62/168,894호 및 제62/172,128호에 보다 상세히 기술된 바와 같이, 디바이스들(1000 또는 1005) 중 하나에 의해 백업된 데이터를 복구하는 데 또한 사용된다. 하기에 더 상세히 기술되는 바와 같이, 키 저장소(1040)는 또한 링 서명 키들(예컨대, 클라우드 서비스 계정 패스워드와 같은 공유된 사용자 크리덴셜(credential)로부터 생성된 키, 여러 상이한 링들에 조인하는 데 사용되는 기업 또는 다른 키들)뿐만 아니라 디바이스들 사이에서의 전송 동안 동기화 데이터 아이템들을 보호하기 위한 키들(즉, 디바이스(1000)와 디바이스들(1005) 각각 사이의 PAKE 보호 채널들을 위한 키들)을 저장할 수 있다. 일부 실시예들에서, 이러한 키들은 단일 저장소에보다는, 디바이스(1000) 상의 여러 상이한 위치들에 저장될 수 있다. 예를 들어, 키들 중 일부는, 디바이스(1000)의 표준 동작과는 별개로, 보안 프로세서에 저장될 수 있다.

[0058] 뷰 및 링 요건들 및 기술 저장소(1045)는, 제3자 개발자들, 디바이스 제조자, 또는 사용자에 의해 정의된 바와 같은, 상이한 링들에 대한 요건들을 개념적으로 저장한다. 이러한 요건들은, 이전 섹션에서 나타낸 바와 같이, 다양한 크리덴셜 및/또는 암호화 키들(예컨대, 공유된 사용자 패스워드 또는 다른 크리덴셜, 기업 키 등)의 소유, 다양한 디바이스 및/또는 애플리케이션 속성들(예컨대, 패스코드 길이, 운영 체제, 애플리케이션 구성물 등)의 어서션, 다양한 속성들(예컨대, 운영 체제, 디바이스 유효성 등)의 대역 외 검증, 또는 다양한 사용자 액션들(예컨대, 하나의 디바이스 상에서 보여지는 코드를 다른 디바이스 상에 입력하는 것, 하나의 디바이스를 다른 디바이스의 근접도 내에서 이동시키는 것, 하나의 디바이스의 사진을 다른 디바이스로 촬영하는 것 등)을 포함할 수 있다. 또한, 저장소(1045)는 일부 실시예들에서 특정 디바이스(즉, 디바이스(1000) 또는 다른 디바이스들(1005) 중 하나)가 각각의 상이한 뷰에 참여하기 위해 어느 링들의 멤버여야 하는지를 식별하는 뷰 요건들을 저장한다. 또한, 저장소(1045)는, 각각의 뷰에 대해, 어느 타입들의 데이터 아이템들이 뷰에 속하는지를 식별하는 뷰 기술을 포함한다. 이러한 뷰 기술은 데이터 아이템이 어느 애플리케이션으로부터 수신되는지(예컨대, 제1 뷰에 대한 Wi-Fi 애플리케이션으로부터의 패스워드들, 제2 뷰에 대한 웹 브라우저 애플리케이션으로부터의 패스워드들), 패스워드가 어느 월드 와이드 웹 도메인과 관련되는지(예컨대, 특정 뷰에 할당되는 금융 웹 도메인들의 포괄적인 리스트로부터의 패스워드들)를 포함하는 다양한 특성들에 기초하여 뷰에 대한 데이터 아이템들을 식별할 수 있다. 일부 실시예들에서, 뷰 기술은 특정 뷰에 속하는 것으로서 태깅된 데이터 아이템들을 단순히 특정하고, 사용자는 데이터 아이템을 처음 입력할 때 뷰들의 리스트로부터 선택한다.

- [0059] 애플리케이션들(1030)을 통해, 디바이스(1000)의 사용자는 일부 실시예들에서 키체인 데이터를 입력할 수 있다. 애플리케이션들(1030)은, 디바이스 운영 체제와 통합되고 디바이스 제조자로부터 유래하는 애플리케이션들(예컨대, 빌트인 브라우저 또는 이메일 애플리케이션, Wi-Fi 애플리케이션 등)뿐만 아니라 제3자 애플리케이션들(예컨대, बैंकिंग 애플리케이션들, 게임 애플리케이션들, 스트리밍 비디오 애플리케이션들 등)을 포함할 수 있다. 사용자는 이러한 애플리케이션들(1030)을 통해 사용자명들 및 패스워드들, 또는 다른 키체인 데이터를 입력한다. 또한, 애플리케이션들은 다른 방식으로(예컨대, 암호화 키를 생성하는 것, 사진을 캡처하는 것 등에 의해) 키체인 데이터를 수신할 수 있다. 일부 실시예들에서 애플리케이션들(1030)에 의해 캡처된 키체인 데이터(1050)는 데이터 태거(1025)로 전송된다.
- [0060] 데이터 태거(1025)는 애플리케이션들(1030)로부터 수신된 키체인 데이터(1050)(및 데이터 아이템들이 아직 부정보로 태깅되지 않을 때 임의의 다른 소스들로부터의 키체인 데이터 아이템들)를 태깅하는 것을 처리한다. 일부 실시예들에서, 도식된 바와 같이, 데이터 태거(1025)는 부 기술 및 요건 저장소(1045)로부터 부 기술 정보(1055)를 인출하고 이러한 정보를 이용하여 키체인 데이터 아이템들(1050) 각각이 어느 부들에 속하는지를 판정한다. 다른 실시예들에서, 언급된 바와 같이, 부 기술은 데이터 태거 코드의 일부이고, 저장소로부터 검색될 필요가 없다.
- [0061] 데이터 태거(1025)는 이러한 부 정보를 키체인 데이터에 첨부한다. 일부 실시예들에서, 데이터 태거는 부 태깅된 키체인 데이터(1060)를 (도식된 바와 같은) 동기화 엔진(1010)으로 전송하고, 그 동기화 엔진은 암호화 키 및 함수를 사용하여 데이터 아이템들을 암호화하고 이들을 키체인 데이터 저장소(1035)에 저장한다. 다른 실시예들에서, 데이터 태거는 암호화 함수를 사용하여 부 태깅된 키체인 데이터(1060)를 암호화하고, 동기화 엔진(1010)을 수반하지 않고서 이러한 데이터를 저장소(1035)에 직접 저장한다. 어느 경우든, 일부 실시예들은 데이터 아이템을 암호화하지만 부 태그들을 암호화되지 않은 상태로 두어, 데이터 아이템이 속하는 부들이 데이터를 암호화해제하는 일 없이 (예컨대, 동기화 엔진(1010)에 의해) 식별될 수 있다.
- [0062] 링 평가자(1015)는 (i) 디바이스(1000)가 링들에 조인하기 위한 요청들을 생성하고 (ii) 디바이스(1000)가 이미 멤버인 링들에 조인하기 위한, 다른 디바이스들(1005)로부터의 요청들을 평가한다. 요청들을 생성하기 위해, 일부 실시예들의 링 평가자(1015)는 자체 평가자 모듈(1016)을 포함한다. 이 모듈은 링 요건들(1065)을 사용하여 디바이스(1000)가 링에 대한 멤버십 기준을 충족시킬 때를 판정한다. 링 요건들(1065)은 (예컨대, 디바이스의 사용자에게 의해 또는 제3자 개발자들에 의해 정의되는 경우) 저장소(1045)로부터 검색되거나 또는 (예컨대, 디바이스 제조자에 의해 하드 코딩된 경우) 링 평가자 코드의 일부일 수 있다. 일부 실시예들에서, 자체 평가자(1016)는 디바이스(1000)가 아직 멤버가 아닌 링에 대한 요건들을 충족시키거나, 또는 이미 멤버인 링에 대한 요건들을 더 이상 충족시키지 않도록 하는 방식으로, 그 디바이스가 변경되었는지 여부를 판정하기 위해 주기적으로 체크한다. 다른 실시예들에서, 자체 평가자(1016)는 이벤트 구동 방식으로 동작한다. 즉, 디바이스 속성(또는 링 멤버십에 영향을 미치는 다른 기준)이 변경될 때, 디바이스의 링 상태가 변경되어야 하는지 여부를 판정하기 위해 자체 평가자(1016)에 통지된다.
- [0063] 자체 평가자(1016)가 (사용자가 링 멤버십을 승인하거나 또는 코드를 디바이스들(1005) 중 하나로부터 디바이스(1000)로 반송하는 것(또는 그 역도 성립함)과 같은 임의의 요청 구동 액션들 이외에) 디바이스가 새로운 링에 조인하기 위한 기준을 충족시키는 것을 식별할 때, 링 평가자(1015)는 링 요청에 필요한 임의의 키들(1067)(예컨대, 디바이스 아이덴티티의 일부로서 사용되는 디바이스 공개 키, 요청에 서명하는 데 사용되는 디바이스 개인 키 및/또는 임의의 링 특정 키들)을 사용하여 링 조인 요청(1070)을 생성하고 그에 서명한다. 그러한 요청의 상세 사항들은 링 조인 요청의 생성 및 전송을 도식하는 도 13을 참조하여 하기에 기술된다. 이 도면에 도시되지 않았지만, 링 평가자(1015)는 자체 평가자(1016)가 그 디바이스가 더 이상 특정 링의 멤버가 아니어야 하는 것으로 판정할 때 다른 디바이스들에도 통지들을 또한 전송할 수 있다.
- [0064] 링 평가자(1015)는 또한 다른 디바이스들(1005)로부터 수신된 링 조인 요청들(1075)을 검증하기 위한 크리덴셜 체커 모듈(1017)을 포함한다. 디바이스(1000)와 마찬가지로, 다른 디바이스들 중 하나가 그것이 링에 조인하기 위한 기준을 충족시키는 것으로 판정할 때, 그 디바이스는 링 조인 요청을 생성하고 링에 있는 다른 디바이스들에게 전송한다(일부 실시예들에서, 각각의 디바이스는 멤버가 아닌 것들을 포함하는 디바이스들의 리스트를 각각의 링에 저장한다). 디바이스(1000)가 그러한 요청을 수신할 때, 크리덴셜 체커(1017)는 요청 디바이스가 그것이 조인을 요청하고 있는 링 내에서 허용되어야 하는지 여부를 검증한다. 이는 요청이 적절한 키(들)로 서명되어 있는지를 검증하는 것, 임의의 대역 외 기준이 충족되었거나 또는 대역 외 체크들(예컨대, 요청 디바이스가 유효한 디바이스인지, 디바이스(1000) 상에서 생성된 코드가 요청 디바이스 상에 적절히 입력되었는지 등)을 수행하는 것, 디바이스가 링에 조인하기 위한 그의 기준을 적절히 어서트하였는지, 디바이스(1000)의 사용자가

요청 디바이스를 승인하였는지 등을 검증하는 것을 수반할 수 있다. 링 조인 요청이 검증될 때, 링 평가자(1015)는 링 상태 메시지(도시되지 않음)를 링에 있는 다른 디바이스들(1005)로 전송한다. 일부 실시예들에서, 링 상태 메시지는, 최근 추가된 디바이스를 포함하는, 링 내의 디바이스들의 리스트이다. 이는 요청 디바이스에게 링에 성공적으로 조인하였음을 통지할 뿐만 아니라, 다른 디바이스들에게 디바이스(1000)가 요청 디바이스의 멤버십을 승인하였음(그리고 그에 따라 이들이 멤버십 요청을 별개로 프로세싱할 필요가 없음)을 통지하도록 하는 역할을 한다. 일부 실시예들에서, 이러한 통지 메시지는 링 특정 키 쌍의 개인 키(예컨대, 멤버십 요청에 서명하는 데 사용된 키)로 서명된다.

[0065] 링 평가자(1015)는 또한 뷰 평가자(1020)가 디바이스(1000)뿐만 아니라 다른 디바이스들(1005)의 현재 링 상태(1080)를 정기적으로 알도록 유지한다. 일부 실시예들에서, 뷰 평가자(1020)는 링 평가자(1015)로부터(또는 링 평가자가 이러한 정보를 저장하는 저장소로부터) 필요에 따라 이러한 정보를 요청한다. 뷰 평가자(1020)는 디바이스들(디바이스(1000) 및 다른 디바이스들(1005)을 포함함) 중 어느 것이 디바이스들의 그룹에 대해 정의된 상이한 뷰들 각각에 참여하는지를 판정하는 것을 담당한다. 구체적으로, 일부 실시예들에서, 뷰 평가자는 (모든 디바이스들의 현재 링 멤버십 상태에 기초하여, 임의의 주어진 시점에서) 뷰들과 디바이스들 사이의 맵핑(즉, 각각의 디바이스에 대해, 디바이스가 어느 뷰들에 참여하는지; 또는 각각의 뷰에 대해, 어느 디바이스가 참여하는지)을 판정한다. 뷰 평가자(1020)는, 다시, 여러 상이한 실시예들에서 디바이스 제조자에 의해 뷰 평가자 내에 코딩될 수 있는 또는 제3자 개발자들 및/또는 사용자들에 의해 생성된 가변 정보일 수 있는 뷰 요건들(1085)에 기초하여 이러한 판정을 행한다.

[0066] 뷰에 참여하기 위해 디바이스가 어느 링들의 멤버여야 하는지를 정의하는 것에 더하여, 일부 실시예들의 뷰 요건들은 디바이스들 사이에서 뷰에 대한 데이터를 동기화하는 데 사용되는 채널에 대한 임의의 요건들을 (뷰들의 일부 또는 전부에 대해) 특정할 수 있다. 상기에 언급된 바와 같이, 일부 실시예들에서, 디바이스들은, 예컨대, (동기화 동안 데이터 아이템들이 암호화되는 공유 키에 의존하는) PAKE를 사용하여, 피어-투-피어 암호화된 채널들을 형성한다. 또한, 일부 뷰들은 디바이스에게 자체에서 공개/개인 키 쌍의 소유를 필요로 하는 링의 멤버일 것을 필요로 한다. 일부의 그러한 뷰들은 2개의 디바이스들 사이의 채널이 PAKE에 대한 공유 키에 더하여(또는 그에 대한 대안으로서) 이러한 키를 사용할 것을 필요로 한다. 예를 들어, 기업 개인 키의 소유를 필요로 하는 기업 링 내에서의 멤버십을 필요로 하는 기업 뷰의 경우, 일부 실시예들은 기업 개인 키를 사용하여 그 뷰에 대해 동기화된 데이터 아이템들을 암호화한다. 따라서, 뷰 평가자(1020)는 (i) 뷰들과 디바이스들 사이의 맵핑(1090) 및 (ii) 각각의 뷰에 대한 동기화 채널들에 대한 요건들(1095)을 동기화 엔진(1010)에게 제공한다.

[0067] 일부 실시예들에서, 동기화 엔진(1010)은 뷰 태깅된 키체인 데이터 아이템들을 다른 디바이스들(1005)과 동기화시키는 것을 담당한다. 일부 실시예들에서, 동기화 엔진(1010)은 그것이 데이터 아이템들을 다른 디바이스와 동기화시켜야 하는 것으로 판정하고, 뷰 평가자(1020)로부터 특정 다른 디바이스가 참여하는 뷰들의 리스트(1090) 및 뷰들 각각에 대한 임의의 특수 채널 요건들을 수신한다. 일부 실시예들에서, 동기화 엔진(1010)은 한 번에 오직 하나의 채널을 동기화시키고, 그래서 그것은 단지 디바이스(1000)와 다른 디바이스 사이의 특정 채널을 사용하는 뷰들의 리스트(특수 채널 요건들이 없는 경우, 이는 다른 디바이스 및 디바이스(1000) 양측 모두가 참여하는 모든 뷰들일 것이다)를 뷰 평가자(1020)로부터 요청한다. 동기화 엔진(1010)은 키체인 데이터 저장소(1035)로부터 정확한 뷰들에 속하는 뷰 태깅된 키체인 데이터 아이템들(1097)을 검색하고 보안 채널을 통해 이러한 데이터 아이템들을 다른 디바이스와 동기화시킨다. 일부 실시예들에서, 이는 디바이스 상에서의 저장 동안 사용된 키체인 데이터 아이템들에 대한 암호화를 제거하는 것 및 보안 채널에 대해 사용된 공유 키로 키체인 데이터 아이템들을 재암호화하는 것을 수반한다.

[0068] 당업자는 이 도면에 도시된 모듈들의 세트가 임의의 수의 목적들을 위한 광범위한 모듈들을 포함하는 디바이스의 소프트웨어 아키텍처의 서브세트라는 것을 인식할 것이다. 또한, 도시된 모듈들 중 많은 것이 그 자체가 여러 개의 모듈들을 포함할 것이고, 도시된 모듈들 중 여러 개의 모듈들에 의해 재사용될 수 있는 다양한 모듈들이 도시되지 않는다. 예를 들어, (도 16 및 도 17을 참조하여 하기에 도시되는 바와 같이) 데이터를 다른 디바이스들과 동기화시킬 때의 동기화 엔진 및 (도 13에 하기에 도시되는 바와 같이, 다른 디바이스들의 링 신청서들에 서명하기 위한 그리고/또는 링 신청서들을 검증하기 위한) 링 평가자에 의해 암호화 및/또는 암호화해제 함수들이 사용될 수 있다.

[0069] **III. 링들의 조인**

[0070] 디바이스가 링에 조인하기 위해, 일부 실시예들은 디바이스가 링에 조인하기 위한 요청에 서명할 것 및 링에 이

미 있는 디바이스들 중 하나에 의해 승인된 요청을 가질 것을 필요로 한다. 예를 들어, 일부 실시예들에서, 디바이스가 암호화 시크릿의 소유를 필요로 하는 링에 대한 요건들을 충족시킬 때, 디바이스는 (i) (다른 디바이스들과 이미 공유된) 그의 공개 키 및 링으로의 신청 날짜/시간에 암호화 시크릿으로부터 생성된 개인 키로 서명하고, (ii) 이러한 서명을 링에 조인하는 데 사용되는 그의 아이덴티티로 패키징하고, (iii) 아이덴티티에 그 자신의 개인 키로 서명한다. 이어서, 이러한 서명은 링에 조인하기 위한 요청으로서 링 내의 다른 디바이스들로 전송된다. 다른 디바이스들 중 하나가 요청 디바이스가 링에 조인하기 위한 모든 요건들을 충족시키는지를 검증할 때, 확립된 디바이스는, 추가되는 새로운 디바이스를 포함하는, 링 내의 다른 디바이스들에게 통지한다. 일부 실시예들에서, 이러한 통지는, 새로운 디바이스를 현재 포함하는, 링의 멤버들의 리스트를 포함한다.

[0071] 도 11은 링 내에서의 멤버십을 요청하기 위한 일부 실시예들의 프로세스(1100)를 개념적으로 도시한다. 일부 실시예들에서, 디바이스(예컨대, 디바이스의 링 평가자)는 디바이스가 링에 조인하기 위한 모든 요건들을 충족시키는 것으로 판정할 때 프로세스(1100)를 수행한다. 디바이스 속성이 변경되어(예컨대, 사용자가 디바이스로의 액세스를 보호하기 위해 패스코드를 추가하는 것, 암호화 키를 포함하는 구성물이 디바이스 상에 설치되는 것, 사용자가 디바이스 상에 클라우드 서비스 계정 패스워드를 입력하는 것 등), 디바이스가 멤버가 아닌 링에 현재 조인할 수 있을 때, 디바이스는 일부 실시예들에서 프로세스(1100)(또는 유사한 프로세스)를 수행한다.

[0072] 도시된 바와 같이, 프로세스(1100)는 (1105에서) 디바이스 서명 키 쌍을 검색하는 것으로 시작한다. 일부 실시예들에서, 이는 디바이스 운영 체제가 초기에 디바이스의 사용자에게 의해 시작 및 구성될 때 디바이스에 의해 랜덤하게 생성되는(그리고 디바이스 상에 저장되는) 공개/개인 키 쌍이다. 즉, 사용자가 우선 디바이스를 구입하고 사용자의 사용을 위해 디바이스를 구성할 때(또는 디바이스의 운영 체제를 리셋 및 재구성할 때), 디바이스는 랜덤화된 시드 데이터(seed data)에 기초하여 공개/개인 키 쌍을 생성한다. 일부 실시예들에서 키 쌍에 대한 시드 데이터는 어떠한 디바이스 하드웨어와도 관련되지 않아서, 새로운 키 쌍이 디바이스에 대해 생성되는 경우(사용자가 디바이스를 재포맷화(reformat)하는 경우), 새로운 키 쌍은 이전 키 쌍과의 어떠한 암호화 관계도 갖지 않을 것이다. 일부 실시예들에서, 디바이스는 사용자에게 속하는 다른 디바이스들(즉, 디바이스가 링들에 조인하게 하는 디바이스들)과 공유되는 디바이스 공개 키를 그의 아이덴티티의 일부로서 사용한다. 디바이스는 (발명의 명칭이 "Backup System with Multiple Recovery Keys"인 미국 특허 출원 제14/871,498호뿐만 아니라, 미국 가특허 출원들 제62/168,894호 및 제62/172,128호에 기재된 바와 같은) 백업 복구를 위해서뿐만 아니라, 그것이 저장한 데이터 아이템들을 암호화하기 위해 그의 개인 키를 사용한다. 또한, 일부 실시예들에서, 디바이스는 그의 개인 키를 사용하여 링 멤버십 요청들에 서명한다.

[0073] 다음으로, 프로세스(1100)는 (1110에서) 디바이스가 멤버십을 요청하고 있는 링이 검증을 위해 시크릿 키의 증명서를 사용하는지 여부를 판정한다. 즉, 일부 링들은, 멤버십을 요청하는 디바이스가 (예컨대, 멤버십 요청에 서명하는 것에 의해) 그것이 특정 개인 키를 소유함을 나타낼 것을 필요로 하는데, 그에 대해 확립된 디바이스들은 공개 키를 갖는다.

[0074] 그러한 키가 필요할 때, 프로세스는 (1115에서) 링 요건 데이터에 기초하여 링 서명 키 쌍을 생성한다(또는 키가 이미 생성된 경우에는, 링 서명 키 쌍을 검색한다). 예를 들어, 일부 실시예들은 사용자가 링에 조인하기 위해 특정 패스코드/패스워드를 입력할 것을 필요로 한다. 이어서, 디바이스는 이러한 패스워드로부터 결정적 방식으로 키 쌍을 생성하고, 이는 링 멤버십 요청에 사용된다. 일부 실시예들에서, 키 쌍이 생성되는 시드 데이터는 특정 목적을 위해 디바이스를 구성하는 일부로서 디바이스에 제공된다. 예를 들어, 디바이스가 기업에 소유되고 기업의 고용인에 의해 사용되는 경우, 기업은 공개/개인 키 쌍을 생성하는 데 사용되는 시드 데이터를 포함하는 이들의 기업 특정 구성물을 디바이스 상에 설치할 수 있고, 그 디바이스는 기업 특정 링에 조인하는 데 사용할 수 있다. 유사하게, 애플리케이션 다운로드에서 이용가능한 암호화 데이터를 사용하여 애플리케이션 특정 링에 조인될 수 있다.

[0075] 또한, 프로세스는 (1120에서) 임의의 추가적인 링 크리덴셜 검증을 수행한다. 이는 링 멤버십에 필요하지만 외부 확인을 필요로 하지 않는 디바이스의 자체 확인 특정 속성들을 수반할 수 있다. 예를 들어, 일부 실시예들은 디바이스가 어서트할 것을 필요로 하지만, 그것이 특정 운영 체제를 실행하는 것, 특정 타입의 디바이스인 것(디바이스 타입은 스마트폰, 스마트폰의 특정 브랜드(예컨대, 애플, 노키아, HTC 등), 디바이스의 특정 버전(예컨대, 아이폰 5, 아이폰 6 등) 등과 같은 넓은 카테고리일 수 있다), 적어도 특정 길이의 패스코드를 갖는 것 등을 임의의 암호화 또는 대역 외 방식으로 증명하지 않는다.

[0076] 추가적인 링 크리덴셜 검증은 또한 (일부 실시예들에서, 링 멤버십 요청이 전송되기 전보다는, 전송된 후에 수행되는) 대역 외 검증을 수반할 수 있다. 대역 외 검증은 디바이스가 링 내에서의 멤버십에 필요한 속성을 단

순히 어서트하기보다는 증명할 것을 필요로 한다. 예를 들어, 디바이스는, 제3자를 통해, 그것이 특정 제조자로부터의 유효한 디바이스를 갖고 있는지, 그것이 특정 운영 체제를 실행하는지, 그의 패스코드가 적어도 특정 길이인지, 또는 다른 속성들을 증명하는 것을 필요로 할 수 있다.

[0077] 다음으로, 프로세스는 (1125에서) 디바이스 개인 키뿐만 아니라 임의의 개인 링 서명 키(즉, 동작(1115)에서 생성된 임의의 키)를 사용하여 링 멤버십 신청서에 서명한다. 이는 디바이스가, 그의 링 멤버십 신청서를 통해, (i) 그것은 그 디바이스만이 그의 공유 공개 키와 쌍을 이루는 개인 키를 갖고 있기 때문에 자신이라고 주장하는 디바이스라는 것, 및 (ii) 그것이 링에 조인하는 데 필요한 암호화 시크릿을 소유한다는 것을 증명하는 것을 가능하게 한다. 일부 실시예들에서, 서명된 링 멤버십 신청서는 또한 신청 시간뿐만 아니라 그의 공개 키를 포함하는 다른 디바이스 식별 정보를 포함한다. 일부 실시예들의 서명된 링 요청은 도 13을 참조하여 하기에 보다 상세히 기술된다.

[0078] 마지막으로, 프로세스는 (1130에서) 서명된 링 멤버십 신청서를 이미 링에 있는 다른 디바이스들로 전송한다. 일부 실시예들에서, (예컨대, 사용자 계정에 로그인하는 것에 의해, 사용자 패스워드를 필요로 하는 링에 조인하는 것에 의해, 등등에 의해) 사용자와 연관된 각각의 디바이스는 각각의 가능한 링의 멤버들인 디바이스들의 리스트를 저장하고, 이러한 리스트를 사용하여 링 멤버십 요청을 링 내의 다른 디바이스들로 전송한다. 이러한 디바이스들 중 하나가 (예컨대, 하기에 기술되는 도 12에 도시된 것과 같은 프로세스를 이용하여) 멤버십 요청을 승인하는 한, 디바이스는 링에 추가된다.

[0079] 도 12는 디바이스를 링 내에서 허용할지 여부를 판정하기 위한 일부 실시예들의 프로세스(1200)를 개념적으로 도시한다. 일부 실시예들에서, 제1 디바이스는 프로세스(1100)(또는 유사한 프로세스)를 수행하여 링 멤버십을 위한 서명된 요청을 생성하고, 요청을 링의 멤버들로서 확립된 디바이스들로 전송한다. 이어서, 이러한 확립된 디바이스들 중 하나(또는 그 이상)가 프로세스(1200)(또는 유사한 프로세스)를 수행하여 (멤버십 요청이 적절하다고 가정하면) 디바이스를 링 내에서 허용하거나, 또는 링에 조인하기 위한 요청을 거부한다.

[0080] 도시된 바와 같이, 프로세스(1200)는 (1205에서) (프로세스(1200)가 실행하고 있는) 로컬 디바이스가 이미 속한 링에 조인하기 위한, 다른 디바이스로부터의 요청을 수신하는 것으로 시작한다. 일부 실시예들에서, 이러한 요청은 링에 조인하기를 원하는 다른 디바이스로부터의 포인트-투-포인트 접속(point-to-point connection)을 통해 수신된다. 이러한 포인트-투-포인트 접속은 직접 접속(예컨대, 디바이스들 사이의 블루투스 접속 등)을 통해 또는 중앙 리포지토리(central repository)를 통해 전송될 수 있다. 예를 들어, 일부 실시예들에서, 요청 디바이스는 중앙 리포지토리에 저장되는 메시지들을 여러 개의 확립된 디바이스들로 전송하고, 확립된 디바이스들 각각은 이들이 활성일 때 이러한 요청들을 검색한다. 즉, 잠기거나 전원이 꺼진 디바이스는 그것이 잠금해제되고 전원이 켜지고 등이 될 때까지 요청을 수신하지 못할 수도 있다.

[0081] 요청의 수신 시에, 프로세스는 (1210에서) 요청이 다른 디바이스에 의해 이미 승인되었는지 여부를 판정한다. 일부 실시예들에서, 요청 디바이스가 멤버십 요청을 링 내의 확립된 디바이스들 각각으로 전송하기 때문에, 일부 경우들에서, 확립된 디바이스들 중 하나는 다른 확립된 디바이스들 중 하나가 이미 요청 디바이스를 링에 추가한 것으로 판정하기 위해서만 요청을 프로세싱하기 시작할 것이다. 일부 실시예들에서, 확립된 디바이스는 요청 디바이스가 링에 추가될 때 통지를 다른 확립된 디바이스들 및 새로운 디바이스로 전송한다. 이러한 경우, 프로세스(1200)는 종료된다.

[0082] 요청 디바이스가 아직 링에 추가되지 않았다고 가정하면, 프로세스(1200)는 (1215에서) 요청이 링을 적절히 식별하는지 여부를 판정한다. 링에 조인하기 위해, 일부 실시예들은 요청 디바이스가 링의 멤버들 및/또는 링의 다른 태양들을 식별하는 요청을 생성할 것을 필요로 한다. 요청이 링을 적절히 식별하지 않는 경우, 프로세스가 종료된다.

[0083] 다음으로, 프로세스는 (1220에서) 요청 디바이스가 링 내에서의 멤버십을 위한 모든 기준을 충족시키는지 여부를 판정한다. 기술된 바와 같이, 이는 요청에 서명하기 위해 키를 사용하는 것, 요청 디바이스의 속성들(그의 운영 체제, 디바이스의 타입 등)을 어서트하는 것, 또는 대역 외에서 링 멤버십의 요건을 검증하는 것에 의해 특정 암호화 키의 소유를 증명하는 것을 포함할 수 있다. 따라서, 요청 디바이스가 모든 기준을 충족시키는지 여부를 판정하는 동작은 대역 외 프로세스를 개시하는 것 또는 대역 외 프로세스가 요청 디바이스의 특정 기준을 확인하기 위해 이미 수행되었는지 여부를 판정하는 것을 수반할 수 있다. 요청 디바이스가 기준을 충족시키지 않는 경우, 프로세스가 종료된다(그리고 요청 디바이스가 링에 추가되지 않는다).

[0084] 마지막으로, 요청 디바이스가 이와 달리 링 멤버십에 대해 승인되는 경우, 프로세스는 (1225에서) 링이 사용자

승인을 필요로 하는지 여부를 판정한다. 이는, 그것이 요청 디바이스가 링 내에서 허용되기 위해 승인 디바이스 상의 사용자 액션을 필요로 한다는 점에서, 특정 타입의 링 기준이다. 어떠한 사용자 승인도 필요하지 않을 때, 프로세스는 하기에 기술되는 1240으로 진행하여, 요청 디바이스를 링에 추가한다.

[0085] 요청 디바이스의 사용자 승인이 링 멤버십에 필요할 때, 프로세스는 (1230에서) 로컬 디바이스(프로세스(1200)를 수행하는 디바이스) 상에 승인 프롬프트를 디스플레이한다. 이러한 프롬프트는 디바이스가 링에 조인하기 위한 멤버십을 요청하고 있다는 것을 단순히 나타낼 수 있거나, 또는 추가적인 컨텍스트를 제공할 수 있다. 예를 들어, 프롬프트는 디바이스의 이름(예컨대, 존의 아이폰), 디바이스의 타입, 링의 이름, 또는 요청이 유효한지 여부를 평가함에 있어서 사용자에게 도움이 되는 다른 정보를 나타낼 수 있다. 이어서, 프로세스는 사용자가 요청 디바이스를 링 내에서 허용할지 여부를 나타내기를 기다린다(도시되지 않음).

[0086] 일단 사용자가 프롬프트에 응답한다면, 프로세스(1200)는 (1235에서) 사용자가 요청 디바이스를 승인하였는지 여부를 판정한다. 사용자가 요청 디바이스를 승인하지 않을 때, 프로세스가 종료된다. 그러나, 사용자가 요청 디바이스를 승인할 때, 프로세스는 (1240에서) 요청 디바이스를 링에 추가한다. 일부 실시예들에서, (프로세스(1200)를 수행하는) 확립된 디바이스는 링의 모든 멤버들의 리스트를 이용하여 링의 모든 멤버들(요청 디바이스를 포함함)에게 메시지를 전송하는 것에 의해 요청 디바이스를 링에 추가한다. 일부 실시예들은 전송 디바이스의 개인 키로 이러한 메시지에 서명한다.

[0087] 도 13은 4개의 스테이지들(1305 내지 1320)을 통해 링에 조인하도록 요청하고 제2 디바이스(1325)에 의해 승인되는 제1 디바이스(1300)를 개념적으로 도시한다. 제1 디바이스(1300)는, 스마트폰, 스마트워치, 태블릿, 랩톱 또는 데스크톱 컴퓨터 등과 같은, 링에 조인할 수 있는 임의의 타입의 전자 디바이스일 수 있다. 제1 디바이스(1300)에 대해, 이 도면은 제1 디바이스(1300)가 (제1 디바이스(D1)(1300)를 포함하는) 디바이스들의 그룹이 참여하는 다양한 링들에 관한 정보를 저장하는 제1 저장소(1330)를 포함하는 것을 도시한다. 제1 스테이지(1305)에 도시된 바와 같이, 이들은 멤버들로서 D2 및 D3을 갖는 제1 링, 멤버들로서 3개의 디바이스들 모두를 갖는 제2 링, 및 유일한 멤버로서 D2를 갖는 제3 링을 포함한다. 제1 디바이스(1300)는 또한 다른 디바이스들 및/또는 링들과 관련된 다양한 키들을 저장하는 제2 저장소(1335)를 포함한다. 이들은 디바이스(1300) 자체의 공개/개인 키 쌍뿐만 아니라, D2 및 D3에 대한 공개 키들을 포함한다.

[0088] 이러한 제1 스테이지(1305)에서, 기업 프로파일(1340)이 제1 디바이스(1300) 상에 설치된다. 제2 스테이지(1310)에 도시된 바와 같이, 기업 프로파일(1340)은 키 저장소(1335)에 저장되는 기업 키 쌍(또는 기업 키 쌍이 생성되는 시드 데이터)을 포함한다. 기업 프로파일(1340)은 또한 디바이스(1300) 상에 애플리케이션들, 다양한 보안 수단들 등의 설치를 포함할 수 있다.

[0089] 제3 스테이지(1315)에서, 디바이스(1300)의 링 평가자(1345)는 디바이스가 제1 링에 조인하기 위한 크리덴셜들(즉, 기업 개인 키)을 현재 소유하고 있는 것으로 판정한다. 이와 같이, 링 평가자는 요청 서명자(1350)를 사용하여 요청을 생성한다. 일부 실시예들에서, 요청 서명자는 메시지 또는 다른 데이터 조각에 서명하기 위해 개인 키를 사용하는 암호화 디지털 서명 생성 함수이다. 이어서, 제1 디바이스(D1)(1300)는 요청(1355)을 제2 디바이스(D2)(1325)로 전송한다. 도시되지 않았지만, 일부 실시예들에서, 제1 디바이스(1300)는 또한 요청을 D3으로 전송한다.

[0090] 일부 실시예들에서, 요청(1355)은 도 11에 도시된 것과 같은 프로세스를 이용하여 제1 디바이스(1300)에 의해 생성된다. 구체적으로, 일부 실시예들에서, 디바이스(1300)는 (i) (다른 디바이스들과 이미 공유된) 그의 공개 키 및 링으로의 신청 날짜/시간에 암호화 시크릿으로부터 생성된 개인 키로 서명하고, (ii) 이러한 서명을 링에 조인하는 데 사용되는 그의 아이덴티티로 패키징하고, (iii) 아이덴티티에 그 자신의 개인 키로 서명한다. 도시된 바와 같이, 요청(1355)의 가장 중심부는 디바이스의 공개 키뿐만 아니라 제1 디바이스가 링에 신청하고 있는 시간을 포함한다. 이어서, 이러한 세트의 데이터(공개 키 + 신청 시간)는 링 특정 개인 키(즉, 기업 프로파일의 일부로서 디바이스(1300)에 의해 수신된 기업 키)로 서명된다. 디바이스 아이덴티티(또한 피어 정보로도 지칭됨)는 이러한 서명뿐만 아니라, 디바이스에 관한 다른 데이터(예컨대, 그의 이름, 하드웨어 특정 식별자, 및/또는 다른 데이터)를 포함한다. 이어서, 이러한 디바이스 아이덴티티는 디바이스(1300)의 개인 키로 서명되어, 그에 의해 요청이 사실상 제1 디바이스로부터 유래하고 있음을 인증한다.

[0091] 제4 스테이지(1320)에서, 제2 디바이스(1325)는 요청(1355)을 수신하고 요청을 검증한다. 제2 디바이스(1325)는 (이전에 공유된) 제1 디바이스의 공개 키뿐만 아니라 기업 공개 키(이 디바이스는 이미 기업 링에 있고, 그에 따라 기업 키 쌍을 저장한다)를 사용하는 서명 검증기(1360)를 사용한다. 서명 검증기(1360)가 요청이 제1 디바이스에 의해 적절히 서명되어 있는지를 검증하는 경우, 제2 디바이스(1325) 상의 링 평가자(1365)는 제1 디

바이스(1300)를 제1 링에 추가한다. 이 도면에 도시되지 않았지만, 제2 디바이스(1325)는 3개의 디바이스들 모두가 제1 링의 멤버됨을 나타내는 메시지를 D1 및 D3 양측 모두로 전송한다. 일부 실시예들에서, 이러한 메시지는 제2 디바이스(1325)에 의해 서명된다.

[0092] 도 13의 제1 디바이스에 의해 조인된 링은 기업 링 키의 소유를 증명하는 요청에 대한 서명만을 필요로 한다. 그러나, 언급된 바와 같이, 일부 경우들에서 링들은 추가적인 요건들을 또한 필요로 할 수 있다. 도 14는 동일한 디바이스(1300)가 시크릿 암호화 키의 소유뿐만 아니라 중앙 기관을 통한 디바이스 속성의 검증을 필요로 하는, 5개의 스테이지들(1405 내지 1425)을 통해 제3 링에 조인하는 것을 개념적으로 도시한다. 제1 스테이지(1405)에서, 디바이스(1300)는 제3 링에 대한 암호화 시크릿(1430)을 (예컨대, 사용자 입력, 다운로드 등을 통해) 수신한다. 그 결과, 제2 스테이지(1410)는 제1 디바이스(1300) 상의 키 저장소가 암호화 시크릿(1430)으로부터 생성된 공개/개인 키 쌍을 포함하는 것을 도시한다.

[0093] 제3 스테이지에서, 제1 디바이스(1300)는 제1 링을 제2 디바이스(1325)에 조인하기 위해 서명된 요청(1435)을 전송한다. 이러한 경우, 제2 디바이스가 현재 링의 멤버인 유일한 디바이스이기 때문에, 제1 디바이스는 단지 요청을 제2 디바이스로만 전송한다. 일부 실시예들에서, 요청(1435)은 이전 도면에 도시된 요청(1355)과 동일한 방식으로 서명된다. 즉, 요청은 제1 디바이스의 공개 키와 함께 제1 링으로의 신청 시간을 포함하고, 암호화 시크릿(1430)으로부터 생성된 개인 키로 서명된다. 이어서, 이러한 정보는 디바이스 아이덴티티로 패키징되고, 그 디바이스 아이덴티티는 이어서 디바이스(1300)의 개인 키로 서명된다.

[0094] 제4 스테이지에서, 제1 디바이스를 제1 링 내에 수용하기 전에, 제2 디바이스(1325)는 제1 디바이스(1300)의 속성의 검증(1440)을 수신한다. 이러한 경우, 디바이스들은 중앙 기관(1445)을 이용하여 디바이스들 중 어느 하나에 의해 개시될 수 있는 프로세스를 통해 디바이스 속성을 검증한다. 중앙 기관(1445)은 디바이스가 진품인 것 또는 디바이스가 특정 운영 체제를 갖고 있는 것을 검증하는 디바이스의 제조자일 수 있다. 상기에 논의된 바와 같이, 대역 외 프로세스는, 다양한 실시예들에서, 중앙 기관보다는 사용자 액션들을 수반하거나, 또는 2개의 디바이스들 사이의 직접적인 정보 교환을 수반할 수 있다. 마지막으로, 제5 스테이지(1425)에서, 제2 디바이스(1325)는 이전 도면에서와 같이 요청을 검증하고 제1 링에 제1 디바이스(1300)를 추가한다.

[0095] IV. 동기화 프로세스

[0096] 디바이스들이 링들(검증 목적들을 위한 서브그룹들) 내에 확립되면, 이들은 뷰들(동기화 목적들을 위한 서브그룹들) 내에 배열될 수 있다. 언급된 바와 같이, 일부 실시예들에서 링들은 디바이스들을 뷰들로 조직화하는 데 사용되고, 그 뷰들은 디바이스 상에 저장된 어느 데이터 아이템들이 다른 디바이스들과 동기화되어야 하는지를 판정하는 데 사용된다. 일부 실시예들에서, 뷰들은 (i) 디바이스가 뷰에 참여하기 위한 요건들의 세트 및 (ii) 뷰에 참여하는 디바이스들 사이에서 동기화되는 데이터 아이템의 타입에 의해 정의된다. 일부 실시예들에서, 뷰들에 대한 요건들의 세트는 (도 7 내지 도 9를 참조하여 상기에 나타난 바와 같은) 하나 이상의 링들 내에서의 멤버십이다.

[0097] 뷰들은 관련 디바이스들의 세트가 데이터 아이템들을 서로 동기화시키는 것을 가능하게 하는 데 사용된다. 다양한 실시예들에서, 이러한 동기화된 데이터 아이템들은 온라인 계정들(예컨대, 금융 서비스 웹사이트들, 온라인 포럼 사이트들, 미디어 콘텐츠 제공자들, 온라인 소매 사이트들 등)에 대한 사용자명들 및 패스워드들, 암호화 키들 및/또는 시크릿들(즉, 키들이 생성될 수 있는 데이터), 중앙 서버 상에 저장된 애플리케이션 관련 데이터로의 액세스를 허용하는 애플리케이션 특정 서비스 키들, 네트워크(예컨대, Wi-Fi 네트워크) 패스워드들, 노트들, 사진들, 문서들 및 다른 파일들 등 중의 일부 또는 전부를 포함한다.

[0098] 도 15는 제1 디바이스로부터의 키체인 데이터를 제2 디바이스와 동기화시키기 위한 일부 실시예들의 프로세스(1500)를 개념적으로 도시한다. 이러한 경우, 프로세스는 제1 및 제2 디바이스들 사이의 특정 보안 채널에 대한 동기화 프로세스를 수행하고, 그 특정 보안 채널은 디바이스들 사이의 유일한 보안 채널이거나 또는 디바이스들 사이의 여러 개의 보안 채널들 중 하나일 수 있다. 이러한 프로세스가 특정 보안 채널을 통해 모든 뷰들에 대한 동기화를 수행하지만, 다른 실시예들은 특정 뷰에 대한 모든 디바이스들, 또는 특정 디바이스에 대한 (채널과 관계없는) 모든 뷰들에 대한 동기화를 (한 번에) 수행하는 프로세스들을 사용할 수 있다.

[0099] 도시된 바와 같이, 프로세스(1500)는 (1505에서) 특정 채널을 통해 특정 원격 디바이스에 대한 데이터를 동기화하라는 커맨드를 수신하는 것으로 시작한다. 일부 실시예들에서, 프로세스는 제2 원격 디바이스와 함께 적어도 하나의 뷰에 참여하는 제1 디바이스 상에서 수행된다. 제1 디바이스는 데이터 아이템들을 주기적으로 제2 디바이스와 동기화시킬 수 있거나, 사용자 커맨드들에 기초하여 데이터 아이템들을 동기화시킬 수 있거나, 또는 제1

디바이스가 새로운 데이터 아이템을 수신하고 (데이터 아이템들이 속하는 뷰들의 세트에 기초하여) 데이터 아이템이 제2 디바이스와 동기화되어야 하는 것으로 판정할 때마다 데이터 아이템들을 동기화시킬 수 있다.

[0100] 일부 실시예들에서, 디바이스들의 전체 그룹 내의 디바이스들의 각각의 쌍은 데이터 아이템들을 동기화시키는 데 사용하기 위해 이들 자신들 사이에 (예컨대, 오프-더-레코드(OTR) 메시징 프로토콜을 이용하여) 보안 채널을 생성한다. 일부 실시예들에서, 뷰들이 보안 채널에 대한 임의의 추가적인 요건들을 부과하지 않는 한, 제1 디바이스는 양측 모두의 디바이스들이 참여하는 모든 뷰들에 대한 식별된 동기화 데이터 아이템들을 보안 채널을 통해 제2 디바이스로 전송한다. 뷰가 보안 채널에 추가적인 요건들을 부과할 때(예컨대, 검증 서브그룹 내에서의 멤버십에 필요한 암호화 키로 데이터 아이템들을 암호화하는 것), 제1 디바이스는 다수의 상이한 보안 채널들을 사용하여 데이터 아이템들의 세트를 제2 디바이스와 동기화시킬 수 있다. 이러한 경우, 일부 실시예들에서 프로세스(1500)는 각각의 채널에 대해 별개로 수행된다.

[0101] 다음으로, 프로세스는 (1510에서) 양측 모두의 디바이스들(동기화를 수행하는 로컬 디바이스 및 데이터가 동기화될 디바이스)이 참여하는 뷰들의 세트를 식별한다. 일부 실시예들에서, 디바이스 내의 뷰 평가자 모듈은 원격 디바이스가 맴버인 링들에 기초하여, 원격 디바이스가 참여하는 뷰들의 세트를 생성한다. 상기에 논의된 바와 같이, 각각의 디바이스는 그룹 내의 각각의 다른 디바이스가 맴버인 링들을 추적하여, 데이터가 뷰들을 판정하는 데 사용될 수 있게 한다. 유사하게, 디바이스는, 그 자신의 링 맴버십들에 기초하여, 그것이 어느 뷰들에 참여하는지를 알고 있다.

[0102] 프로세스(1500)는 (1515에서) 식별된 세트에서의 임의의 뷰(양측 모두의 디바이스들이 참여하는 뷰들)에 대해 태깅되고 이전에 원격 디바이스와 동기화되지 않았던 새로운 동기화 데이터 아이템들을 식별한다. 디바이스는 그의 키체인에 일부이고 원격 디바이스가 또한 참여하는 적어도 하나의 뷰에 속하는 데이터(즉, 그것이 맴버인 뷰들에 속하는 데이터)를 단지 동기화시킨다. 제1 디바이스가 (예컨대, 새로운 패스워드의 사용자 입력, 새로운 사진의 임포트 또는 다운로드 등으로부터) 동기화 데이터 아이템들의 세트에 추가할 새로운 데이터 아이템을 수신할 때, 일부 실시예들의 디바이스는 데이터를 하나 이상의 뷰들에 속하는 것으로서 동적으로 태깅한다. 예를 들어, 데이터가 내부에 생성된 애플리케이션(예컨대, Wi-Fi 네트워크들/패스워드들 대 온라인 계정 사용자명들/패스워드들), 사용자명/계정이 액세스를 얻는 웹사이트의 타입(예컨대, 금융 웹사이트 대 비금융 웹사이트), 데이터가 기업과 관련되는지 아닌지의 여부 등에 기초하여 데이터가 태깅될 수 있다. 데이터 아이템들을 원격 디바이스와 동기화시킬 때, 제1 디바이스는 그것이 저장하고 제2 디바이스로 아직 전송되지 않은(그리고 제2 디바이스가 참여하는 뷰들에 속하는) 모든 동기화 데이터 아이템들을 식별한다.

[0103] 식별된 데이터 아이템들로, 프로세스(1500)는 (1520에서) 이러한 새로운 데이터 아이템들이 로컬 디바이스 상에 저장될 때 이들을 암호화해제한다. 일부 실시예들에서, 암호화해제 프로세스는 로컬 디바이스의 개인 키, 즉, 그 디바이스에게만 알려져 있는 키를 사용한다. 일부 실시예들에서, 데이터 아이템들은 디바이스 공개 키를 사용하여 암호화된 암호화 형태로 디바이스 상에 저장된다. 일부 실시예들은 또한 링에 조인하는 데 사용되는 키 쌍(예컨대, 사용자 패스워드 기반 키 쌍, 기업 키 쌍 등)의 공개 키와 같이 디바이스 상의 저장을 위한 하나 이상의 추가적인 키들로 데이터 아이템들을 암호화한다. 디바이스 상의 저장을 위해 데이터 아이템을 암호화하는 데 사용되는 각각의 공개 키에 대해, 프로세스는 대응하는 개인 키를 사용하여 데이터 아이템을 암호화해제한다.

[0104] 다음으로, 프로세스는 (1525에서) 아이템들이 전송될 보안 채널의 요건들에 따라 원격 디바이스로의 전송을 위해 데이터 아이템들을 암호화한다. 언급된 바와 같이, 일부 실시예들은 디바이스들 사이의 메시지들을 암호화하는 데 사용되는 공유 키에 의존하는 패스워드 인증 키 교환(PAKE)을 사용한다. 일부 경우들에서, 특정 뷰에 대한 뷰 요건들은, 추가적인 키(예컨대, 링에 조인하기 위해 소유가 요구되는 키, 특정 뷰에 대한 요건인 맴버십)를 사용하는 것과 같은, 특정 뷰에 속하는 데이터 아이템들을 동기화시키기 위한 보안 채널에 대한 추가적인 제한들을 부과할 수 있다. 따라서, 일부 실시예들은 적어도 공유 키로, 그리고 가능하다면 추가적인 키들로 데이터 아이템들을 암호화한다.

[0105] 마지막으로, 프로세스는 (1530에서) 디바이스들 사이의 보안 채널에 걸쳐 뷰에 대한 암호화된 아이템들을 원격 디바이스로 전송한다. 상이한 실시예들에서, 이러한 보안 채널은 수신 디바이스가 잠금해제될 때에도 일시적인 저장을 허용하는 중앙집중형 서비스(예컨대, 양측 모두의 디바이스들이 로그인되는 클라우드 서비스 계정을 위한 저장소)를 통과시킬 수 있다. 그러나, 일부 실시예들에서, 보안 채널의 사용은 중간자 공격들에 대해 이러한 통신들을 보호한다. 다른 실시예들은 (예컨대, 블루투스 접속을 통해) 직접 피어-투-피어 접속들을 사용한다. 암호화된 아이템들의 수신 시에, 일부 실시예들에서 원격 디바이스는 (채널 상에서 암호화된 바와 같은)

아이템들을 암호화해제하고, 그 자신의 공개 키를 사용하여 로컬 저장을 위해 이들을 재암호화한다. 일부 실시예들에서, 원격 디바이스는 또한 프로세스(1500)와 유사한 프로세스를 수행하여 그의 새로운 데이터 아이템들 중 임의의 것을 로컬 디바이스와 동기화시킨다.

[0106] 도 16 및 도 17은 데이터를 서로 동기화시키는 한 쌍의 디바이스들(1600, 1650)을 개념적으로 도시한다. 구체적으로, 도 16은, 2개의 스테이지들(1605, 1610)을 통한, 제1 디바이스(1600)에 의한 동기화를 위한 새로운 데이터 아이템의 수신을 도시한다. 제1 스테이지(1605)는 2개의 디바이스들(1600, 1650) 각각에 의해 저장된 아이템들을 도시한다. 이러한 예에서, 제1 디바이스(1600)는 뷰들(V1, V2)에 참여하는 한편, 제2 디바이스(1650)는 뷰들(V1, V3)에 참여한다. 도시된 바와 같이, 제1 디바이스는 아이템 1(1615), 아이템 2(1620), 및 아이템 3(1625)을 저장한다. 2개의 제1 아이템들(1615, 1620)은 제1 뷰(V1)에 속하는 한편, 제3 아이템(1625)은 제2 뷰(V3)에 속하고, 데이터 아이템들이 그에 따라 태깅된다. 제2 디바이스는 아이템 1(1615), 아이템 2(1620), 및 아이템 4(1630)를 저장한다. 제4 아이템(1630)은 V3에 속하는데, 이는 이러한 아이템이 제2 디바이스(1650) 상에만 저장되는 이유이다. 마지막으로, 이러한 스테이지는 상이한 키들에 의한 데이터 아이템들의 암호화를 표현하기 위해 이러한 그리고 후속 도면들에서 사용되는 표현들을 나타내는 범례를 도시한다. 제1 디바이스(1600) 상에 저장된 아이템들은 제1 디바이스의 키로 암호화되는 한편, 제2 디바이스(1650) 상에 저장된 아이템들은 제2 디바이스의 키로 암호화된다.

[0107] 제2 스테이지에서, 제1 디바이스(1600)의 사용자(이 사용자는 또한 제2 디바이스(1650)의 사용자이고, 그에 따라 디바이스들은 데이터를 서로 동기화시킨다)는 애플리케이션(1640)을 통해 데이터 아이템 5(1635)를 디바이스에 제공한다. 이는 사용자가 패스워드를 입력하게 하는 웹 브라우저 애플리케이션, 패스워드를 사용하는 제3자 애플리케이션, 사용자가 새로운 파일을 생성하게 하는 애플리케이션(예컨대, 워드 프로세싱 애플리케이션을 통한 문서, 카메라 애플리케이션을 통해 캡처된 이미지 등), 또는 디바이스(1600)가 데이터를 수신하게 하는 다른 애플리케이션일 수 있다.

[0108] 이러한 제5 데이터 아이템(1635)은 제1 디바이스(1600) 상의 데이터 태거(1645)로 전송되고, 그 데이터 태거는 데이터 아이템을 제1 뷰(V1)에 속하는 것으로서 식별하고, 아이템을 그에 따라 태깅한다. 이는 아이템이 수신되게 한 애플리케이션(1640), 또는 데이터 아이템을 식별하는 다른 데이터(그의 파일 타입, 그것이 연관된 웹 도메인 등)에 기인할 수 있다. 아이템은 또한 (예컨대, RSA, DSS, 타원 곡선 암호화 등과 같은 비대칭 암호화를 수행하는) 암호화 함수(1655)로 전송된다. 암호화 함수(1655)는 제1 디바이스(도시되지 않음)의 공개 키를 사용하여 저장을 위해 데이터 아이템(1635)을 암호화한다. 일부 실시예들에서, 이 도면에 도시된 바와 같이, 이러한 정보가 민감하지 않고 디바이스가 뷰 데이터에 액세스하기 위해 암호화해제가 요구되어서는 안 되기 때문에, 뷰 정보는 암호화되지 않는다.

[0109] 도 17은 3개의 스테이지들(1705 내지 1715)을 통한 제1 디바이스(1600)로부터의 새로운 데이터 아이템(1635)의 제2 디바이스(1650)와의 동기화를 도시한다. 제1 스테이지(1705)에 도시된 바와 같이, 제1 디바이스(1600) 상의 뷰 평가자 모듈(1720)은 동기화 엔진(1725)에게 데이터를 제2 디바이스와 동기화시키도록 통지한다. 디바이스들의 뷰들의 맵핑은, V1이 디바이스들 양측 모두가 참여하는 유일한 뷰인 것을, 그리고 그에 따라 V1에 속하는 것으로서 태깅된 데이터 아이템들만이 디바이스들 사이에서 동기화되어야 함을 나타낸다.

[0110] 따라서, 제2 스테이지(1710)에서, 제1 디바이스(1600)는 새로운 데이터 아이템(1635)을 제2 디바이스(1650)로 전송한다. 이 도면에서 새로운 데이터 아이템(1635)의 표현에 대해 여러 파선 및 점선으로 도시된 바와 같이, 제1 디바이스는 그 자신의 개인 키(및 잠재적으로 필요한 임의의 다른 키)를 사용하여 저장된 데이터 아이템을 암호화해제하고, 이어서 디바이스들 사이의 보안 채널에 대해 공유 키를 사용하여 데이터 아이템의 평문 버전을 암호화한다. 이어서, 제1 디바이스(1600) 상의 동기화 엔진(1725)은 보안 채널에 걸쳐 암호화된 데이터 아이템(1635)을 전송하는데, 여기서 그것은 제2 디바이스(1650) 상의 동기화 엔진(1730)에 의해 수신된다. 일부 실시예들에서, 보안 채널의 요건으로서, 데이터 아이템(1635) 상의 뷰 태그는 또한 공유 키를 사용하여 암호화된다. 언급된 바와 같이, 2개의 디바이스들(1600, 1650) 사이의 직접 접속으로서 도시되었지만, 일부 실시예들에서, 데이터 아이템(1635)은 제1 디바이스(1600)에 의해 중앙 리포지토리(예컨대, 클라우드 저장소)로 전송되고, 그에 후속하여 제2 디바이스(1650)에 의해 리포지토리로부터 인출된다.

[0111] 제3 스테이지(1715)는 데이터 아이템(1635)을 저장하는 제2 디바이스(1650)를 도시한다. 데이터 아이템을 수신한 후에, 디바이스(1650)는 보안 채널의 공유 키(및 V1에 대한 채널 요건들에 따라, 필요한 임의의 다른 키들)를 사용하여 아이템을 암호화해제하고, 이어서 그 자신의 공개 키(그리고 가능하다면 추가적인 암호화 키들)를 사용하여 저장을 위해 키를 암호화한다.

- [0112] 언급된 바와 같이, 상이한 실시예들에서 동기화 데이터 아이템들은 패스워드/사용자명 조합들, Wi-Fi 네트워크들 및 대응하는 패스워드들, 암호화 키들, 파일들 등을 포함하는 여러 상이한 타입들의 아이템들을 포함할 수 있다. 일부 실시예들에서, 데이터 아이템들은 내포된 키들의 계층 구조를 통해 클라우드 서비스에 저장된 애플리케이션 관련 데이터로의 액세스를 가능하게 하는 애플리케이션 특정 키들을 포함한다. 즉, 디바이스 상의 각각의 애플리케이션(또는 디바이스 상의 애플리케이션들의 서브세트 각각)에 대해, 동기화 데이터는 애플리케이션 특정 개인 키(예컨대, 사진 애플리케이션 키)를 포함한다.
- [0113] 애플리케이션 특정 개인 키가 키들 및 데이터 필드들의 트리에 저장된 데이터에 액세스하는 데 사용되고, 이는 궁극적으로 애플리케이션 데이터 자체로의 액세스를 허용한다. 이러한 보호 구조체는 도 18 및 도 19에 도시된다. 도 18은 일부 실시예들에서 중앙집중형 리포지토리(예컨대, 클라우드 저장소)에 저장되고 디바이스가 다운로드하는 것이 가능한 컨테이너 구조체(1800)를 도시한다. 컨테이너 구조체(1800)는 그 자신의 개인 키(1805)(또는 개인 키를 생성하는 데 사용되는 시드 데이터)를 포함하여 애플리케이션 특정 공개 키로 암호화된다. 따라서, 이러한 컨테이너 개인 키로의 액세스는 키체인 데이터 아이템으로서 동기화되는 애플리케이션 특정 개인 키의 소유를 필요로 한다. 애플리케이션의 하이 레벨 오버뷰를 표현하는 컨테이너 구조체(1800)는, 액세스하기 위해 어떠한 키들도 필요로 하지 않는 암호화되지 않은 필드들(1810)(Field_1 내지 Field_M)의 세트뿐만 아니라, 컨테이너 공개 키(1805)로 각각 암호화되는(그리고 그에 따라 액세스를 위해 컨테이너 개인 키의 소유를 필요로 하는) 필드들(1815)(Field_M+1 내지 Field_N)의 세트 양측 모두를 포함한다.
- [0114] 또한, 컨테이너 공개 키는 구역 구조체(zone structure)(1900)의 일부인 구역 개인 키(1905)를 암호화하는 데 사용된다. 따라서, 구역 구조체로의 액세스는 컨테이너 개인 키(1805)로의 액세스를 필요로 하고, 이는 차례로 애플리케이션 특정 서비스 키로의 액세스를 필요로 한다. 컨테이너 구조체(1800)와 마찬가지로, 구역 구조체(1900)는 여러 개의 암호화되지 않은 필드들(1910)(Field_1 내지 Field_Q), 및 구역 키로 암호화된 여러 개의 필드들(1915)(Field_Q+1 내지 Field_R)을 포함한다. 컨테이너가 애플리케이션의 하이 레벨 오버뷰를 표현하지만, 일부 실시예들에서 구역은 컨테이너 내의 특정 데이터베이스 또는 테이블을 표현한다. 예를 들어, 구역은 애플리케이션과 연관된 사진들의 세트를 표현할 수 있는데, 이때 각각의 사진은 레코드에 의해 표현된다(그리고 레코드들은 구역에 의해 표시된다).
- [0115] 일부 실시예들에서, 구역에 의해 참조되는 레코드들 각각은 애플리케이션 데이터의 특정 조각(예컨대, 특정 사진)에 대한 키를 포함할 수 있다. 일부 실시예들에서, 각각의 레코드는 그의 구역 공개 키로 암호화된 키를 가지며, 그에 따라 액세스하기 위해 구역 개인 키를 필요로 한다. 레코드는 암호화되지 않은 필드들 및 암호화된 필드들을 갖는 구역 및 컨테이너처럼 구조화된다. 예를 들어, 사진 레코드에 대한 필드들은 사진에 대한 제목, 위치, 타임스탬프 등뿐만 아니라, 실제로 사진을 잠금해제하는 키를 저장할 수 있다. 일부 실시예들에서, 구역 키에 의해 잠금해제된 레코드 키는 공개/개인 키 쌍의 개인 키보다는 대칭 키이다.
- [0116] 동기화 프로세스를 통해 공유되는 것에 더하여, 미국 가특허 출원들 제62/168,894호 및 제62/172,128호뿐만 아니라, 미국 특허 출원 제14/871,498호 및 미국 특허 공개 제2014/0093084호에 기술된 바와 같이, 일부 실시예들에서는 보안 에스크로 시스템(secure escrow system)을 통해 애플리케이션 특정 키체인 데이터 아이템들이 복구 가능하다.
- [0117] **V. 그룹 멤버십에 대한 동적 변경들**
- [0118] 도 2 내지 도 6에 도시된 바와 같이, 일부 실시예들에서, 디바이스들은 다수의 링들의 멤버들일 수 있다. 또한, 디바이스들은 디바이스들이 새롭게 요건들을 충족시키게 되도록 또는 더 이상 다양한 링들의 요건들을 충족시키지 않도록 디바이스들의 속성들이 변경될 때 이러한 링들 안팎으로 동적으로 이동할 수 있다. 디바이스의 속성들이 변경되어(예컨대, 특정 암호화 시크릿을 포함하는 프로파일이 디바이스 상에 설치되는 것, 사용자가 디바이스 패스코드 길이를 변경하는 것 또는 패스코드를 디바이스에 추가하는 것 등) 디바이스가 링에 대해 적격하게 될 때, 디바이스는, 전송된 바와 같이, 링 내에서의 멤버십을 위한 요청을 생성 및 전송한다. 다른 한편으로, 디바이스의 속성들이 변경되어 디바이스가 현재 멤버인 링 내에서의 멤버십을 위한 요건들을 디바이스가 더 이상 충족시키지 못할 때, 디바이스는 그것이 더 이상 링의 멤버이어서는 안 된다는 것을 검출하고, 이러한 통지를 링의 멤버들인 다른 디바이스들로 송신한다.
- [0119] 링에 조인하거나 그를 이탈하는 디바이스는 하나 이상의 뷰들에의 디바이스의 참여에도 또한 영향을 미칠 수 있다. 예를 들어, 디바이스가 링에 조인할 때, 그 디바이스는 새로운 뷰에 현재 참여하는 것이 가능할 수 있고, 그에 따라 그 새로운 뷰에 속하는 데이터를 (동기화 프로세스를 통해) 수신해야 한다. 다른 한편으로, 디바이스가 링을 이탈할 때, 디바이스가 더 이상 멤버가 아닌 특정 링 내에서의 멤버십을 필요로 하는 하나 이상의 뷰

들에 디바이스가 참여하는 것이 더 이상 허용되지 않을 수도 있다. 이는 특정 디바이스와 연관된 다른 디바이스들에 의해 인식될 것이고, 그 다른 디바이스들은 이러한 영향받는 뷰들에 속하는 데이터를 특정 디바이스와 더 이상 공유하지 않을 것이다. 또한, 일부 실시예들에서, 특정 디바이스는 그것이 더 이상 자격이 부여되지 않은 모든 데이터 아이템들을 삭제할 것이다. 다른 실시예에서, 디바이스가 더 이상 뷰에 대한 새로운 데이터를 수신하지 않더라도, 사용자가 디바이스 상에서 데이터를 유지하기를 원할 경우에, 디바이스는 임의의 데이터를 삭제하기 전에 사용자에게 문의한다.

[0120] 도 20은 디바이스의 링 멤버십, 및 후속하여, 그의 뷰 참여를 동적으로 수정하기 위한 일부 실시예들의 프로세스(2000)를 개념적으로 도시한다. 프로세스(2000)가 디바이스에 의해 수행되어, 일부 실시예들에서, 그 자신의 링 멤버십을 평가하고 이어서 그의 뷰 참여를 평가한다. 상기에 나타난 바와 같이, 디바이스는 스마트폰, 스마트워치, 태블릿, 랩톱 컴퓨터, 데스크톱 컴퓨터, 또는 관련 디바이스들 사이에서 동기화 시스템에 참여하는 임의의 다른 디바이스일 수 있다.

[0121] 도시된 바와 같이, 프로세스(2000)는 (2005에서) (프로세스를 실행하는 디바이스의) 디바이스 구성물의 변경을 식별하는 것으로 시작한다. 이러한 디바이스 구성물의 변경은 사용자가 디바이스의 패스코드 변경한 것(예컨대, 4자리 패스코드로부터 긴 패스코드로 또는 그 반대로 변경하는 것, 디바이스 상에서 패스코드의 사용을 제거하는 것, 패스코드를 디바이스에 추가하는 것 등), 디바이스 상에 애플리케이션을 설치하는 것, 디바이스의 운영 체제를 업그레이드하는 것, 애플리케이션 또는 디바이스 설정들을 수정하는 것, 새로운 암호화 시크릿을 습득하는 것 등의 결과일 수 있다. 일부 실시예들은 열거된 세트의 링 요건들과 관련된 변경들을 정기적으로 체크하지만, 일부 실시예들에서 프로세스(2000)는 디바이스에 대한 특정 변경들이 프로세스(2000)의 특정 동작들이 수행되게 하는 이벤트 구동식이다.

[0122] 프로세스는 (2010에서) 변경으로 인해 링 멤버십에 임의의 추가들이 발생하는지 여부를 판정한다. 상기의 도 2 내지 도 6의 링들(200, 300, 400, 500, 600)을 참조하면, 그러한 변경들의 예들은, 사용자가 스마트폰(110) 또는 테이블(115) 상의 패스코드를 4개의 문자들보다는 적어도 12개의 문자들을 갖는 것으로 변경한 경우, 기업 구성물이 홈 데스크톱(130) 또는 이러한 디바이스들 중 어느 하나에 설치된 경우, 디바이스 패스코드가 스트리밍 비디오 셋톱 박스(125)에 추가된 경우 동일 수 있다. 상기에 논의된 바와 같이, 많은 다른 타입들의 변경들로 인해 또한 디바이스가 링 내에서의 멤버십에 대해 적격하게 될 수 있다.

[0123] 디바이스 구성물에 대한 변경으로 인해 적어도 하나의 링 내에서의 멤버십에 대한 적격성이 발생할 때, 프로세스는 (2015에서) 링에 조인하기 위한 요청을 생성하고 이러한 서명된 요청을 링 내의 다른 디바이스들로 전송한다. 일부 실시예들에서, 디바이스는 도 11의 프로세스(1100)를 수행하여 2015에서 서명된 링을 생성 및 전송한다. (멤버십 요청이 유효한 것으로 가정하여) 일단 디바이스가 링에 성공적으로 조인하였다면, 링 멤버십으로 인해 디바이스가 하나 이상의 추가적인 뷰들에 참여하게 되는 경우, 프로세스(1500) 또는 유사한 프로세스는 다른 디바이스들 중 하나에 의해 수행되어 이러한 추가적인 뷰들에 속하는 데이터 아이템들을 이러한 디바이스와 동기화시킬 수 있다.

[0124] 프로세스는 또한 (2020에서) 변경으로 인해 디바이스에 대한 임의의 링들로부터의 제거가 발생하는지 여부를 판정한다. 다시 도 2 내지 도 7의 링들을 참조하면, 그러한 변경들의 예들은 스마트폰(105) 또는 랩톱(120) 중 어느 하나로부터의 기업 구성물의 제거, 디바이스들(105 내지 120 또는 130) 중 임의의 디바이스로부터의 패스코드의 제거, 스마트폰(105), 랩톱(120), 또는 데스크톱(130) 상의 패스워드의 단축 동일 수 있다. 많은 다른 타입들의 변경들(예컨대, 디바이스로부터 패스워드 또는 암호화 키를 철회하는 것)은 또한 디바이스가 링 내에서의 멤버십 적격성도 또한 상실하게 할 수 있다.

[0125] 디바이스 구성물 변경들 중 어느 것으로도 임의의 링들로부터의 디바이스의 제거가 발생하지 않은 경우, 프로세스(2000)가 종료된다. 그러나, 그렇지 않으면, 프로세스는 (2025에서) 링 내의 다른 디바이스들에게 링으로부터의 디바이스의 제거에 관해 통지한다. 일부 실시예들은 이러한 변경을 나타내기 위해 디바이스의 개인 키로 서명된 메시지를 전송한다. 링 내의 다른 디바이스들에게 통지하는 것에 더하여, 일부 실시예들은 또한 그 특정 링에 있지 않은 임의의 다른 관련 디바이스들(예컨대, 동일한 사용자의 다른 디바이스들)에게 통지한다. 예를 들어, (기업 구성물이 디바이스로부터 제거되었기 때문에) 스마트폰(105)이 링(500)으로부터 제거된 경우, 그것은 일부 실시예들에서 디바이스들(110 내지 130) 모두에게 통지할 것이다.

[0126] 디바이스 변경이 디바이스의 링 상태에 영향을 미치는지 아닌지의 여부를 판정하는 것에 더하여, 디바이스가 링을 이탈하는 경우, 프로세스(2000)는 또한 디바이스에 대한 잠재적인 뷰 참여 변경들을 처리한다. 따라서, 프로세스는 (2030에서) 링 멤버십 제거로 인해 뷰들 중 임의의 뷰로부터의 제거가 발생하는지 여부를 판정한다.

임의의 특정 뷰에 대한 참여가 하나 이상의 링들 내에서의 멤버십에 기초하여 판정되므로, 뷰 참여를 판정하는데 사용되는 링들 중 하나로부터의 제거로 인해 디바이스가 더 이상 뷰에 참여하기에 적격하지 않게 될 것이다. 예를 들어, 이전 단락의 예를 사용하면, 링(500)으로부터의 스마트폰(105)의 제거로 인해 그에 후속하여 스마트폰이 더 이상 제2 뷰(800)에 참여하기에 적격하지 않게 될 것이다.

[0127] 디바이스가 뷰로부터 제거될 때 뷰에 참여하는 다른 디바이스들에게 통지할 필요가 없는데, 이는 다른 디바이스들이 필요한 링들 중 하나로부터의 디바이스의 제거에 기초하여 동일한 결론을 이끌어낼 것이기 때문이다. 그러나, 일부 실시예들에서, 프로세스(2000)는 (2035에서) 디바이스가 참여하는 임의의 뷰들에 더 이상 속하지 않는 임의의 동기화 데이터 아이템들을 삭제한다. 상기에 언급된 바와 같이, 일부 실시예들은 이러한 데이터들을 자동으로 삭제하지 않지만, 그 대신에 (사용자가 읽고 싶지 않은 어떠한 데이터도 읽지 않도록) 데이터가 삭제되어야 하는지 여부를 사용자에게 문의하도록 프롬프트한다. 일부 실시예들에서, 사용자에게 프롬프트할지 여부는 뷰에 좌우된다. 예를 들어, 기업 뷰가 특정 레벨의 보안을 필요로 하는 경우, 기업은 디바이스가 더 이상 보안 제약들을 충족시키지 못하는 경우 데이터를 유지하는 옵션을 사용자에게 제공하는 것을 원하지 않을 수도 있다. 그러나, 그러한 뷰는 뷰로부터의 제거를 발생시킨 변경을 되돌리는 옵션(예컨대, 보다 짧은 패스워드로 변경을 되돌리는 것)을 사용자에게 제공할 수 있다.

[0128] 도 21a 및 도 21b는 4개의 스테이지들(2105 내지 2120)을 통해 디바이스들 중 하나가 링으로부터 제거되도록 그의 패스워드가 변경될 때의 도 16 및 도 17로부터의 디바이스들(1600, 1650)을 도시한다. 제1 스테이지(2105)에 도시된 바와 같이, 제2 디바이스(1650)는 뷰(V3)에 속하는 데이터 아이템(1630)뿐만 아니라, 뷰(V1)에 속하는 동기화 데이터 아이템들(1615, 1620, 1635)을 저장한다. 이러한 스테이지에서, 디바이스(1650)의 사용자는 그의 패스코드를 12자리 패스코드("012345678910")로부터 4자리 패스코드 "1234"로 수정한다.

[0129] 그 결과, 제2 스테이지(2110)에서, 제2 디바이스(1650)의 링 평가자(2125)는 디바이스의 패스코드가 더 이상 충분히 길지 않기 때문에 디바이스가 더 이상 링(링 3)의 멤버여서는 안 된다는 것을 식별한다. 따라서, 제2 디바이스(1650)는 제2 디바이스가 더 이상 링(3)의 멤버가 아닌 것을 제1 디바이스에게 통지하는 메시지(2130)를 제1 디바이스(1600)로 전송한다. 일부 실시예들에서, 도시된 바와 같이, 메시지는 링 상태의 변경에 대한 이유를 나타내지만, 다른 실시예들은 추가적인 데이터 없이 통지를 단순히 전송한다.

[0130] 제3 스테이지에서, 제1 디바이스(1600) 및 제2 디바이스(1650) 양측 모두는 링 3으로부터의 제2 디바이스의 제거를 프로세싱한다. 제1 디바이스 상의 링 평가자(2135)는 이러한 링으로부터의 제2 디바이스의 제거를 나타내고, 또한 링 상태의 변경을 뷰 평가자(1720)에게 통지하여, 뷰 평가자가 장래의 동기화 동작들을 위해 제2 디바이스의 뷰 상태가 조금이라도 변경되었는지 여부를 판정할 수 있다. 제2 디바이스 상에서, 링 평가자(2125)는 뷰 평가자(2140)에게 이러한 동일 변경을 통지하고, 뷰 평가자는 그 결과(즉, 링 3 멤버십이 뷰(V1)에 대한 요건이기 때문에) 제2 디바이스(1650)가 더 이상 뷰(V1)에 참여하지 않아야 한다는 것을 식별한다.

[0131] 따라서, 뷰 평가자(2140)는 제2 디바이스로부터 데이터 아이템들(1615, 1620, 1635)을 제거하는데, 이는 이들이 디바이스가 더 이상 참여하지 않는 뷰(V1)에 속하기 때문이다. 제4 스테이지(2140)는 이러한 결과를 도시하고, 이때 제2 디바이스(1650)가 데이터(1630)(뷰(V3)에 속함)만을 저장한다.

[0132] VI. 전자 시스템

[0133] 수많은 전술된 특징들 및 적용예들은 컴퓨터 판독가능 저장 매체(또한 컴퓨터 판독가능 매체로도 지칭됨) 상에 기록된 한 세트의 명령어들로서 명시되는 소프트웨어 프로세스들로서 구현된다. 이러한 명령어들이 하나 이상의 계산 또는 프로세싱 유닛(들)(예컨대, 하나 이상의 프로세서들, 프로세서들의 코어들, 또는 다른 프로세싱 유닛들)에 의해 실행될 시, 그들은 프로세싱 유닛(들)이 명령어들에서 지시된 동작들을 수행하도록 한다. 컴퓨터 판독가능 매체들의 예들은, CD-ROM들, 플래시 드라이브들, 랜덤 액세스 메모리(RAM) 칩들, 하드 드라이브들, 소거가능한 프로그래밍가능 판독 전용 메모리(erasable programmable read-only memory, EPROM)들, 전기적으로 소거가능한 프로그래밍가능 판독 전용 메모리(electrically erasable programmable read-only memory, EEPROM)들 등을 포함하지만 이로 제한되지는 않는다. 컴퓨터 판독가능 매체들은 무선으로 또는 유선 접속들을 통해 전달하는 반송파(carrier wave)들 및 전자 신호들을 포함하지 않는다.

[0134] 본 명세서에서, 용어 "소프트웨어"는 판독 전용 메모리에 위치한 펌웨어, 또는 프로세서에 의해 프로세싱되는 메모리로 판독될 수 있는, 자기 저장소에 저장된 애플리케이션들을 포함하는 것으로 의미된다. 또한, 일부 실시예들에서, 다수의 소프트웨어 발명들은 보다 큰 프로그램의 하위-부분들로서 구현되면서, 별개의 소프트웨어 발명들로 남아 있을 수 있다. 일부 실시예들에서, 다수의 소프트웨어 발명들은 또한 별개의 프로그램들로서 구

현될 수 있다. 마지막으로, 본 명세서에 기술된 소프트웨어 발명을 함께 구현하는 별개의 프로그램들의 임의의 조합은 본 발명의 범주 내에 있다. 일부 실시예들에서, 소프트웨어 프로그램들은, 하나 이상의 전자 시스템들 상에서 동작하도록 설치될 시에, 소프트웨어 프로그램들의 동작들을 실행 및 수행하는 하나 이상의 특정 기계 구현예들을 정의한다.

[0135] **A. 모바일 디바이스**

[0136] 일부 실시예들의 사용자 데이터 공유는 스마트폰들(예컨대, 아이폰들®) 및 태블릿들(예컨대, 아이패드들®)과 같은 모바일 디바이스들 상에서 발생한다. 도 22는 그러한 모바일 컴퓨팅 디바이스의 아키텍처(2200)의 일례이다. 도시된 바와 같이, 모바일 컴퓨팅 디바이스(2200)는 하나 이상의 프로세싱 유닛들(2205), 메모리 인터페이스(2210), 및 주변기기 인터페이스(2215)를 포함한다.

[0137] 주변기기 인터페이스(2215)는 다양한 센서들, 및 카메라 서브시스템(2220), 유선 통신 서브시스템(들)(2223), 무선 통신 서브시스템(들)(2225), 오디오 서브시스템(2230), I/O 서브시스템(2235) 등을 포함하는 서브시스템들에 커플링된다. 주변기기 인터페이스(2215)는 프로세싱 유닛들(2205)과 다양한 주변기기들 사이의 통신을 가능하게 한다. 예를 들어, 배향 센서(2245)(예컨대, 자이로스코프) 및 가속도 센서(2250)(예컨대, 가속도계)가 배향 및 가속도 기능들을 가능하게 하도록 주변기기 인터페이스(2215)에 커플링된다.

[0138] 카메라 서브시스템(2220)은 하나 이상의 광 센서들(2240)(예컨대, 전하 결합 디바이스(charged coupled device, CCD) 광 센서, 상보성 금속-산화물-반도체(CMOS) 광 센서 등)에 커플링된다. 광 센서들(2240)과 커플링된 카메라 서브시스템(2220)은 이미지 및/또는 비디오 데이터 캡처링과 같은 카메라 기능들을 가능하게 한다. 유선 통신 서브시스템(2223) 및 무선 통신 서브시스템(2225)은 통신 기능들을 가능하게 하는 역할을 한다.

[0139] 일부 실시예들에서, 무선 통신 서브시스템(2225)은 무선 주파수 수신기들 및 송신기들, 및 광 수신기들 및 송신기들(도 22에는 도시되지 않음)을 포함한다. 일부 실시예들의 이러한 수신기들 및 송신기들은 GSM 네트워크, Wi-Fi 네트워크, 블루투스 네트워크 등과 같은 하나 이상의 통신 네트워크들을 통해 동작하도록 구현된다. 오디오 서브시스템(2230)은 스피커에 커플링되어 오디오를 출력한다(예컨대, 음성 내비게이션 명령어들을 출력한다). 또한, 오디오 서브시스템(2230)은 일부 실시예들에서 음성 인에이블형 기능들을 가능하게 하도록 마이크 로폰에 커플링된다.

[0140] I/O 서브시스템(2235)은 디스플레이, 터치 스크린 등과 같은 입력/출력 주변기기 디바이스들과 프로세싱 유닛들(2205)의 데이터 버스 사이에서의 주변기기 인터페이스(2215)를 통한 전달을 수반한다. I/O 서브시스템(2235)은 터치 스크린 제어기(2255) 및 다른 입력 제어기들(2260)을 포함하여, 입력/출력 주변기기 디바이스들과 프로세싱 유닛들(2205)의 데이터 버스 사이에서의 전달을 가능하게 한다. 도시된 바와 같이, 터치 스크린 제어기(2255)는 터치 스크린(2265)에 커플링된다. 터치 스크린 제어기(2255)는 다수의 터치 감응 기술들 중 임의의 것을 이용하여 터치 스크린(2265) 상에서의 접촉 및 이동을 검출한다. 다른 입력 제어기들(2260)은 하나 이상의 버튼들과 같은 다른 입력/제어 디바이스들에 커플링된다. 일부 실시예들은 터치 상호작용들 대신 또는 이에 더해 근-터치 상호작용(near-touch interaction)들을 검출할 수 있는, 근-터치 감응 스크린 및 대응하는 제어기를 포함한다.

[0141] 메모리 인터페이스(2210)는 메모리(2270)에 커플링된다. 일부 실시예들에서, 메모리(2270)는 휘발성 메모리(예컨대, 고속 랜덤 액세스 메모리), 비휘발성 메모리(예컨대, 플래시 메모리), 휘발성 메모리와 비휘발성 메모리의 조합, 및/또는 임의의 다른 타입의 메모리를 포함한다. 도 22에 도시된 바와 같이, 메모리(2270)는 운영 체제(OS)(2271)를 저장한다. OS(2271)는, 기본 시스템 서비스들을 처리하고 하드웨어 의존형 태스크들을 수행하기 위한 명령어들을 포함한다.

[0142] 메모리(2270)는 또한 (예컨대, 피어-투-피어 데이터 공유를 위해, 또는 클라우드 기반 데이터 공유를 위해 인터넷을 통해 서버에 접속하기 위해) 하나 이상의 추가적인 디바이스들과 통신하는 것을 가능하게 하는 통신 명령어들(2274); 그래픽 사용자 인터페이스 프로세싱을 가능하게 하는 그래픽 사용자 인터페이스 명령어들(2276); 이미지 관련 프로세싱 및 기능들을 가능하게 하는 이미지 프로세싱 명령어들(2278); 입력 관련(예컨대, 터치 입력) 프로세스들 및 기능들을 가능하게 하는 입력 프로세싱 명령어들(2280); 오디오 관련 프로세스들 및 기능들을 가능하게 하는 오디오 프로세싱 명령어들(2282); 및 카메라 관련 프로세스들 및 기능들을 가능하게 하는 카메라 명령어들(2284)을 포함한다. 전송된 명령어들은 단지 예시적이며, 메모리(2270)는 일부 실시예들에서 추가적인 그리고/또는 다른 명령어들을 포함한다. 예를 들어, 스마트폰용 메모리는 전화 관련 프로세스들 및 기능들을 가능하게 하는 전화 명령어들을 포함할 수 있다. 전송된 명령어들은 별도의 소프트웨어 프로그램들 또

는 모듈들로서 구현될 필요는 없다. 모바일 컴퓨팅 디바이스의 다양한 기능들은, 하나 이상의 신호 프로세싱 및/또는 주문형 반도체들을 비롯하여 하드웨어 및/또는 소프트웨어로 구현될 수 있다.

[0143] 도 22에 도시된 컴포넌트들이 별개의 컴포넌트들로 도시되어 있지만, 당업자는 2개 이상의 컴포넌트들이 하나 이상의 집적 회로들 내에 통합될 수 있음을 인식할 것이다. 또한, 2개 이상의 컴포넌트들이 하나 이상의 통신 버스들 또는 신호 라인들에 의해 함께 커플링될 수 있다. 또한, 많은 기능들이 하나의 컴포넌트에 의해 수행되는 것으로 기술되었지만, 당업자는 도 22와 관련하여 기술된 기능들이 2개 이상의 집적 회로들에 분할될 수 있다는 것을 인식할 것이다.

[0144] B.컴퓨터 시스템

[0145] 도 23은 본 발명의 일부 실시예들을 구현하는 전자 시스템(2300)의 다른 예를 개념적으로 도시한다. 전자 시스템(2300)은 컴퓨터(예컨대, 데스크톱 컴퓨터, 개인용 컴퓨터, 태블릿 컴퓨터 등), 전화, PDA, 또는 임의의 다른 종류의 전자 또는 컴퓨팅 디바이스일 수 있다. 그러한 전자 시스템은 다양한 타입들의 컴퓨터 판독가능 매체들 및 다양한 다른 타입들의 컴퓨터 판독가능 매체들을 위한 인터페이스들을 포함한다. 전자 시스템(2300)은 버스(2305), 프로세싱 유닛(들)(2310), 그래픽 프로세싱 유닛(GPU)(2315), 시스템 메모리(2320), 네트워크(2325), 판독 전용 메모리(2330), 영구 저장 디바이스(2335), 입력 디바이스들(2340), 및 출력 디바이스들(2345)을 포함한다.

[0146] 버스(2305)는 전자 시스템(2300)의 다수의 내부 디바이스들을 통신가능하게 접속시키는 모든 시스템, 주변기기, 및 칩셋 버스들을 총괄하여 표현한다. 예를 들어보면, 버스(2305)는 판독 전용 메모리(2330), GPU(2315), 시스템 메모리(2320), 및 영구 저장 디바이스(2335)와 프로세싱 유닛(들)(2310)을 통신가능하게 접속시킨다.

[0147] 이러한 다양한 메모리 유닛들로부터, 프로세싱 유닛(들)(2310)은 본 발명의 프로세스들을 실행하기 위해 실행할 명령어들 및 프로세싱할 데이터를 검색한다. 프로세싱 유닛(들)은 서로 다른 실시예들에서 단일 프로세서 또는 멀티-코어 프로세서일 수 있다. 일부 명령어들은 GPU(2315)에 전달되어 그 GPU에 의해 실행된다. GPU(2315)는 다양한 계산들을 없애거나 프로세싱 유닛(들)(2310)에 의해 제공된 이미지 프로세싱을 보완할 수 있다. 일부 실시예들에서, 그러한 기능은 코어이미지(CoreImage)의 커널 셰이딩 언어(kernel shading language)를 사용하여 제공될 수 있다.

[0148] 판독 전용 메모리(ROM)(2330)는 프로세싱 유닛(들)(2310) 및 전자 시스템의 다른 모듈들에 의해 필요한 정적 데이터 및 명령어들을 저장한다. 다른 한편으로, 영구 저장 디바이스(2335)는 판독 및 기입 메모리 디바이스이다. 이러한 디바이스는 전자 시스템(2300)이 오프될 시에도 명령어들 및 데이터를 저장하는 비휘발성 메모리 유닛이다. 본 발명의 일부 실시예들은 영구 저장 디바이스(2335)로서 (자기 또는 광 디스크 및 그의 대응하는 디스크 드라이브, 통합형 플래시 메모리와 같은) 대용량 저장 디바이스를 사용한다.

[0149] 다른 실시예들은 영구 저장 디바이스로서 (플로피 디스크, 플래시 메모리 디바이스 등 및 그의 대응하는 드라이브와 같은) 제거가능한 저장 디바이스를 사용한다. 영구 저장 디바이스(2335)와 같이, 시스템 메모리(2320)는 판독 및 기입 메모리 디바이스이다. 그러나, 저장 디바이스(2335)와 달리, 시스템 메모리(2320)는 휘발성 판독 및 기입 메모리, 예컨대 랜덤 액세스 메모리이다. 시스템 메모리(2320)는 프로세서가 런타임 시 필요한 명령어들 및 데이터의 일부를 저장한다. 일부 실시예들에서, 본 발명의 프로세스들은 시스템 메모리(2320), 영구 저장 디바이스(2335), 및/또는 판독 전용 메모리(2330)에 저장된다. 예를 들어, 다양한 메모리 유닛들은 일부 실시예들에 따라 멀티미디어 클립들을 프로세싱하기 위한 명령어들을 포함한다. 이러한 다양한 메모리 유닛들로부터, 프로세싱 유닛(들)(2310)은 일부 실시예들의 프로세스들을 실행하기 위해 실행할 명령어들 및 프로세싱할 데이터를 검색한다.

[0150] 버스(2305)는 또한 입력 및 출력 디바이스들(2340, 2345)에 접속한다. 입력 디바이스들(2340)은 사용자가 전자 시스템으로 정보를 전송하게 하고 상기 전자 시스템에 대한 커맨드들을 선택하게 할 수 있다. 입력 디바이스들(2340)은 문자 및 숫자로 이루어진 키보드들 및 포인팅 디바이스들(또한 "커서 제어 디바이스들"이라고도 칭함), 카메라들(예컨대, 웹캠들), 마이크로폰들 또는 음성 커맨드들을 수신하는 유사한 디바이스들 등을 포함한다. 출력 디바이스들(2345)은 전자 시스템에 의해 발생된 이미지들 또는 그렇지 않다면 출력 데이터를 디스플레이한다. 출력 디바이스들(2345)은 프린터들 및 디스플레이 디바이스들, 예컨대 음극선관(CRT) 또는 액정 디스플레이(LCD), 나아가 스피커들 또는 유사한 오디오 출력 디바이스들을 포함한다. 일부 실시예들은 입력 디바이스와 출력 디바이스 양측 모두로서 기능하는 디바이스들 예컨대 터치스크린을 포함한다.

[0151] 마지막으로, 도 23에 도시된 바와 같이, 버스(2305)는 또한 네트워크 어댑터(도시되지 않음)를 통해 전자 시스

템(2300)을 네트워크(2325)에 커플링한다. 이러한 방식으로, 컴퓨터는 컴퓨터들의 네트워크(예컨대 근거리 네트워크("LAN")), 광역 네트워크("WAN"), 또는 인트라넷), 또는 네트워크들의 네트워크, 예컨대 인터넷의 일부일 수 있다. 전자 시스템(2300)의 임의의 또는 모든 컴포넌트들은 본 발명과 함께 사용될 수 있다.

[0152] 일부 실시예들은 전자 컴포넌트들, 예컨대 마이크로프로세서들, 기계 판독가능 또는 컴퓨터 판독가능 매체(대안으로, 컴퓨터 판독가능 저장 매체들, 기계 판독가능 매체들, 또는 기계 판독가능 저장 매체들로 지칭됨)에 컴퓨터 프로그램 명령어들을 저장한 저장소 및 메모리를 포함한다. 그러한 컴퓨터 판독가능 매체들 중 일부 예들은 RAM, ROM, CD-ROM(read-only compact disc)들, CD-R(recordable compact disc)들, CD-RW(rewritable compact disc)들, 판독 전용 DVD(digital versatile disc)들(예컨대, DVD-ROM, 듀얼-레이어 DVD-ROM), 다양한 기록가능/재기입가능 DVD들(예컨대, DVD-RAM, DVD-RW, DVD+RW 등), 플래시 메모리(예컨대, SD 카드들, 미니-SD 카드들, 마이크로-SD 카드들 등), 자기 및/또는 솔리드 스테이트 하드 드라이브, 판독 전용 및 기록가능 블루-레이(Blu-Ray)® 디스크들, 초고밀도 광 디스크들, 임의의 다른 광 또는 자기 매체들, 및 플로피 디스크들을 포함한다. 컴퓨터 판독가능 매체들은 적어도 하나의 프로세싱 유닛에 의해 실행 가능하고 다양한 동작들을 수행하기 위한 명령어들의 세트들을 포함하는 컴퓨터 프로그램을 저장할 수 있다. 컴퓨터 프로그램들 또는 컴퓨터 코드의 예시들은 기계 코드를 포함하고, 예컨대 컴파일러, 및 인터프리터를 사용하여 컴퓨터, 전자 컴포넌트 또는 마이크로프로세서에 의해 실행되는 보다 높은-레벨 코드를 포함한 파일들에 의해 만들어진다.

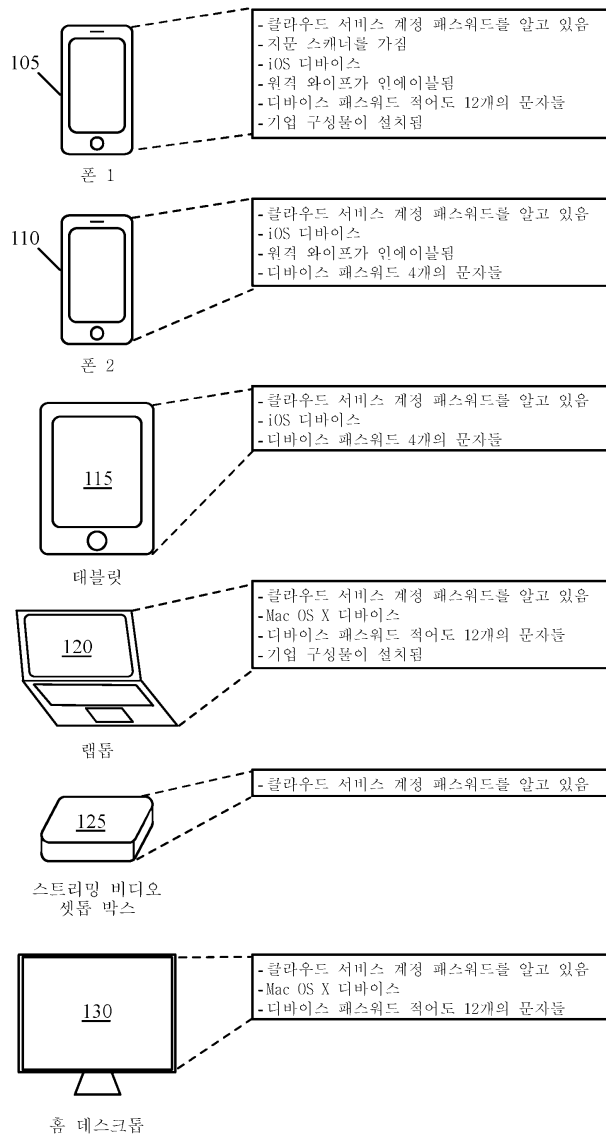
[0153] 상기 논의가 소프트웨어를 실행시키는 마이크로프로세서 또는 멀티-코어 프로세서들을 주로 언급하지만, 일부 실시예들은 하나 이상의 집적 회로들, 예컨대 ASIC(application specific integrated circuit)들 또는 FPGA(field programmable gate array)들에 의해 수행된다. 일부 실시예들에서, 그러한 집적 회로들은 회로 자체 상에 저장된 명령어들을 실행시킨다. 또한, 일부 실시예들은 프로그래밍가능 논리 디바이스(programmable logic device, PLD)들, ROM, 또는 RAM 디바이스들에 저장된 소프트웨어를 실행시킨다.

[0154] 본 명세서 및 본 출원의 임의의 청구항들에서 사용된 바와 같이, 용어들 "컴퓨터", "서버", "프로세서", 및 "메모리" 모두는 전자 또는 다른 기술적인 디바이스들을 지칭한다. 이러한 용어들은 사람 또는 사람들의 그룹들을 배제한다. 본 명세서의 목적들을 위해, 용어들 "디스플레이" 또는 "디스플레이하는"은 전자 디바이스 상에서 디스플레이하는 것을 의미한다. 본 명세서 및 본 출원의 임의의 청구항들에서 사용된 바와 같이, 용어들 "컴퓨터 판독가능 매체", "컴퓨터 판독가능 매체들", 및 "기계 판독가능 매체"는 컴퓨터에 의해 판독가능한 형태로 정보를 저장하는 유형적인(tangible) 물리적 객체들에 전적으로 한정된다. 이러한 용어들은 임의의 무선 신호들, 유선 다운로드 신호들, 및 임의의 다른 임시 신호들을 배제한다.

[0155] 본 발명이 다수의 특정 상세 사항들을 참조하여 기술되었지만, 당업자는 본 발명이 본 발명의 사상으로부터 벗어남이 없이 다른 특정 형태들로 구체화될 수 있다는 것을 인식할 것이다. 예를 들어, 다수의 도면들(도 11, 도 12, 도 15, 및 도 20을 포함함)은 프로세스들을 개념적으로 도시한다. 이러한 프로세스들의 특정 동작들은 도시되고 기술된 정확한 순서로 수행되지 않을 수도 있다. 특정 동작들은 하나의 연속적인 시리즈의 동작들로 수행되지 않을 수도 있으며, 상이한 특정 동작들이 상이한 실시예들에서 수행될 수 있다. 더욱이, 프로세스는 여러 개의 하위-프로세스들을 사용하여, 또는 보다 큰 매크로 프로세스의 일부로서 구현될 수 있다. 따라서, 당업자는 본 발명이 상기의 예시적인 상세 사항들에 의해 제한되는 것이 아니라 오히려 첨부된 청구범위에 의해 정의된다는 것을 이해할 것이다.

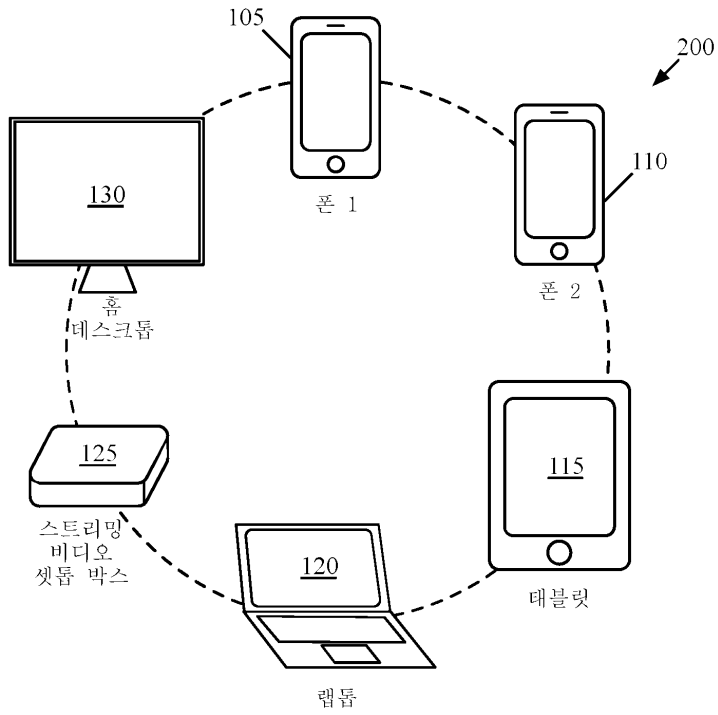
도면

도면1



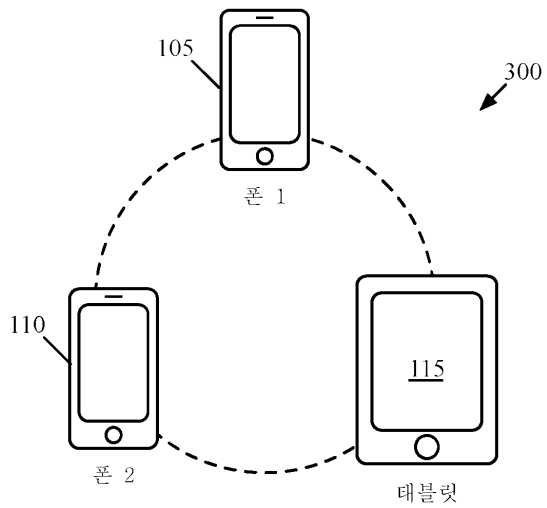
도면2

링 1: 클라우드 서비스 계정 패스워드를 알고 있음



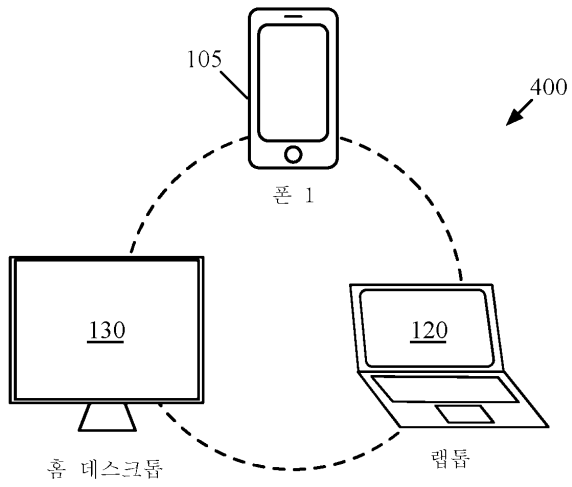
도면3

링 2: iOS 디바이스, 사용자 승인



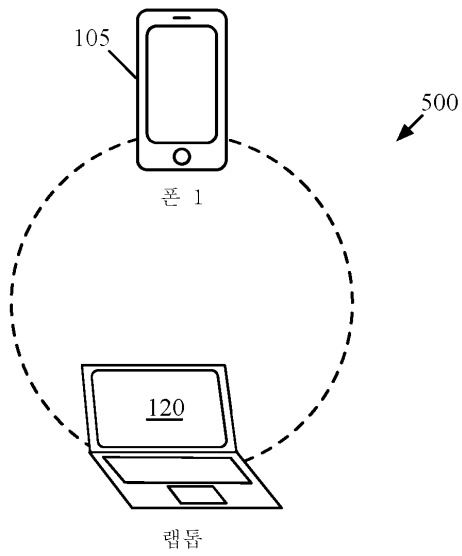
도면4

링 3: 패스워드 적어도 12개의 문자들, 사용자 승인



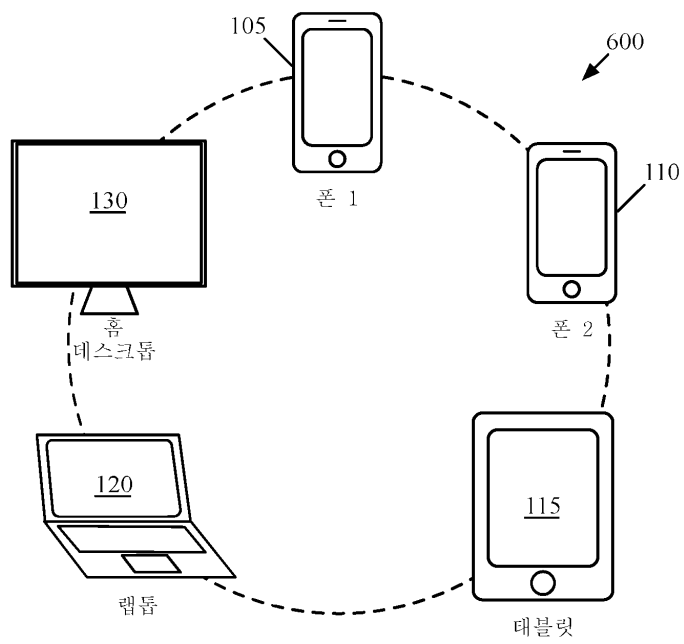
도면5

링 4: 기업 프로파일 구성물이 설치됨, 클라우드 서비스 계정 패스워드를 알고 있음

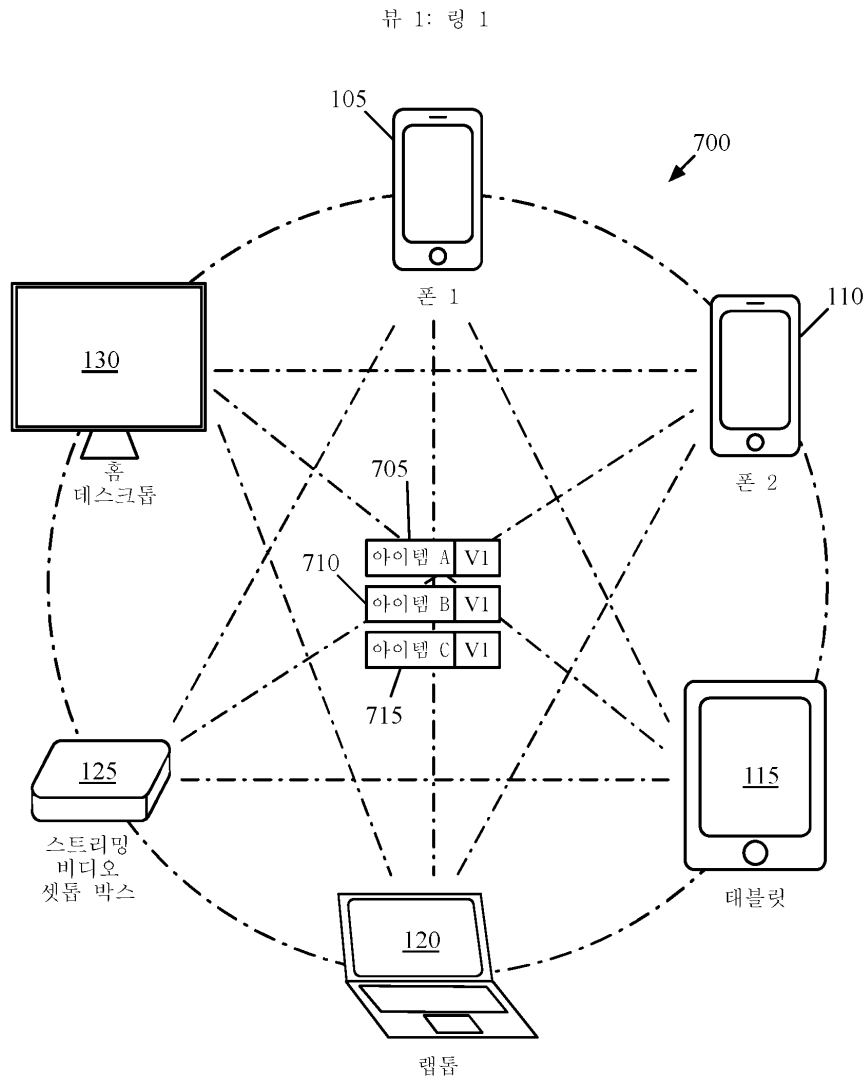


도면6

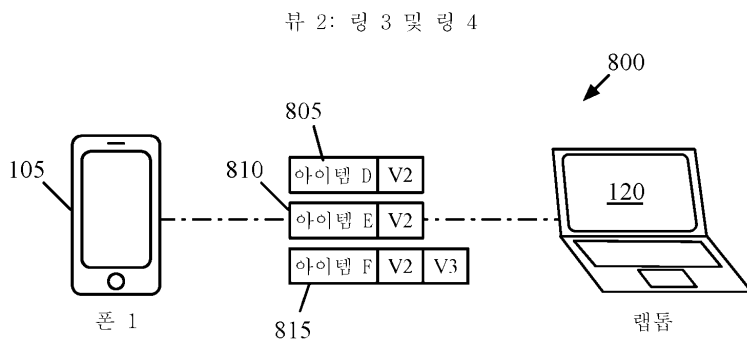
링 5: 애플 디바이스로서 대역 외에서 검증된 패스워드를 가짐



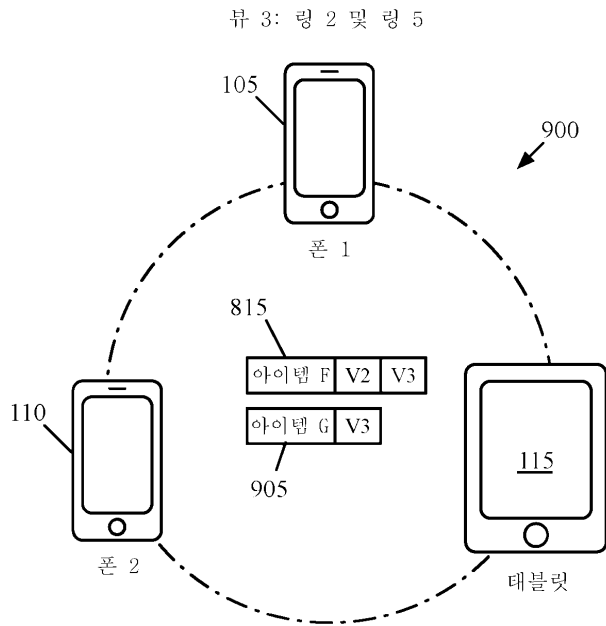
도면7



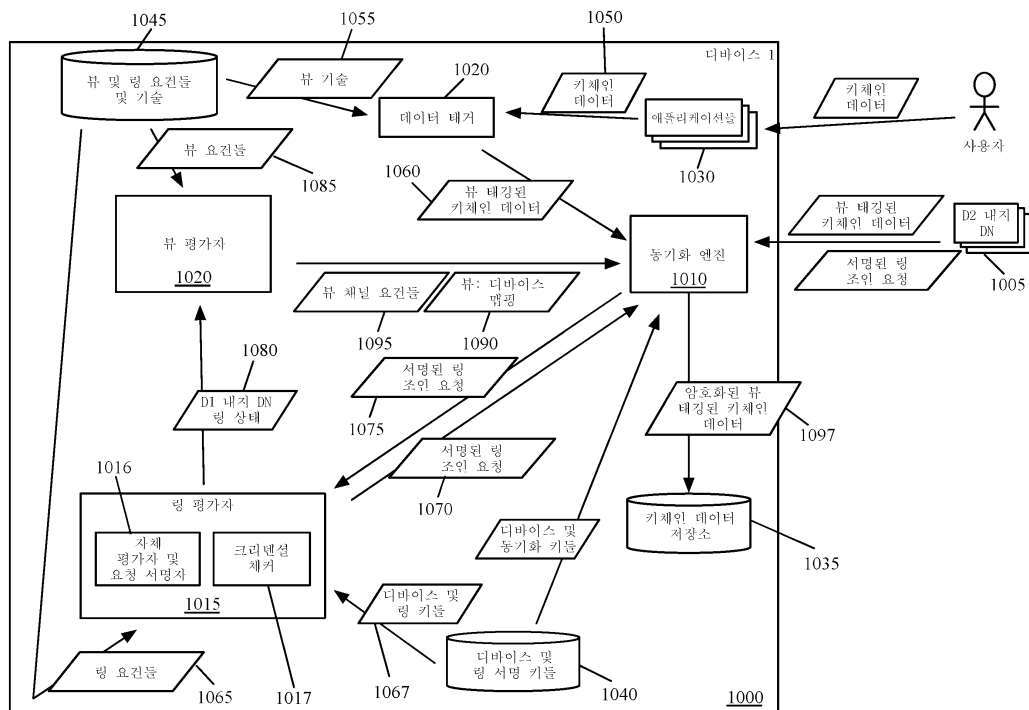
도면8



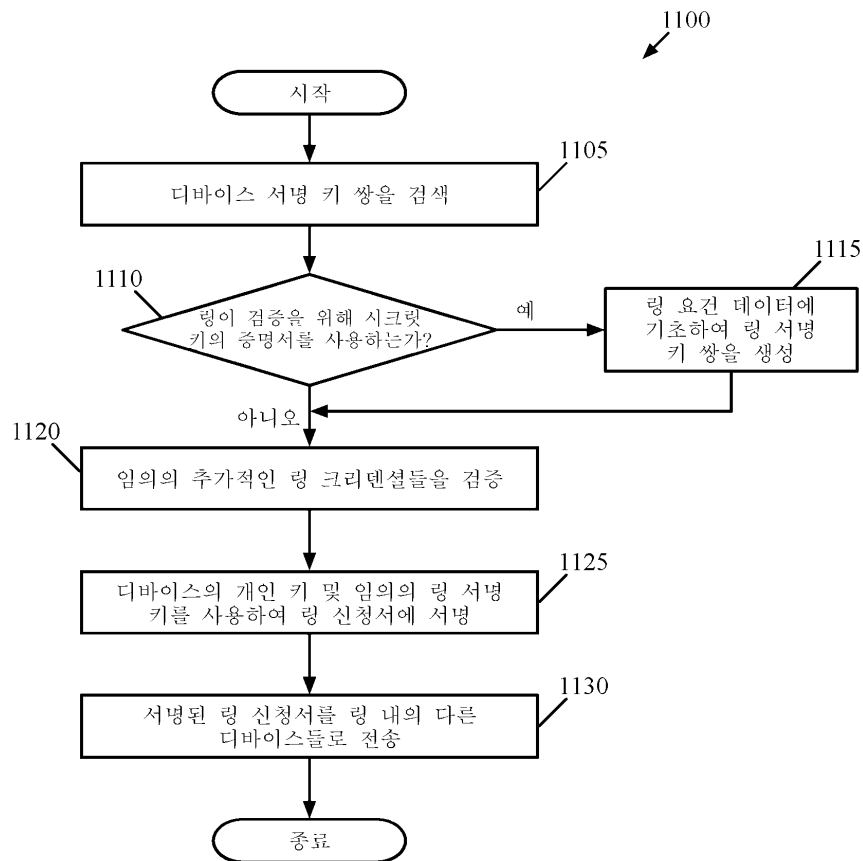
도면9



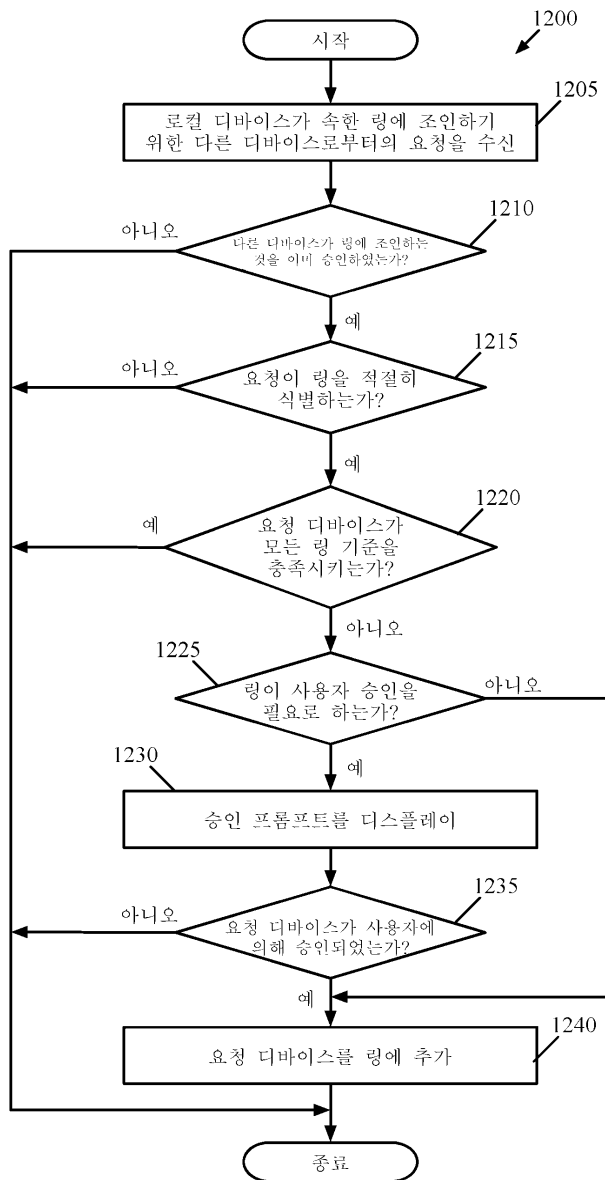
도면10



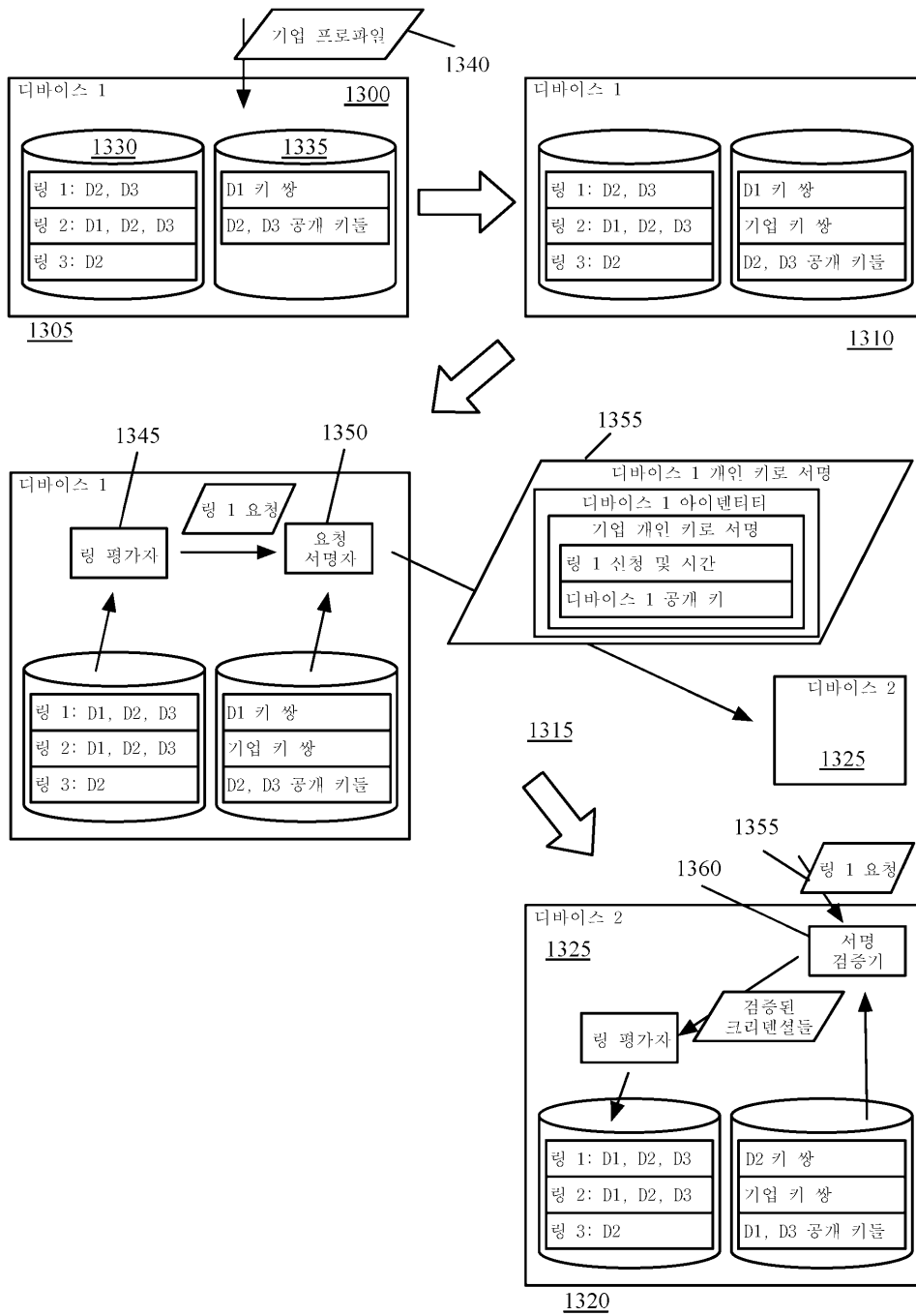
도면11



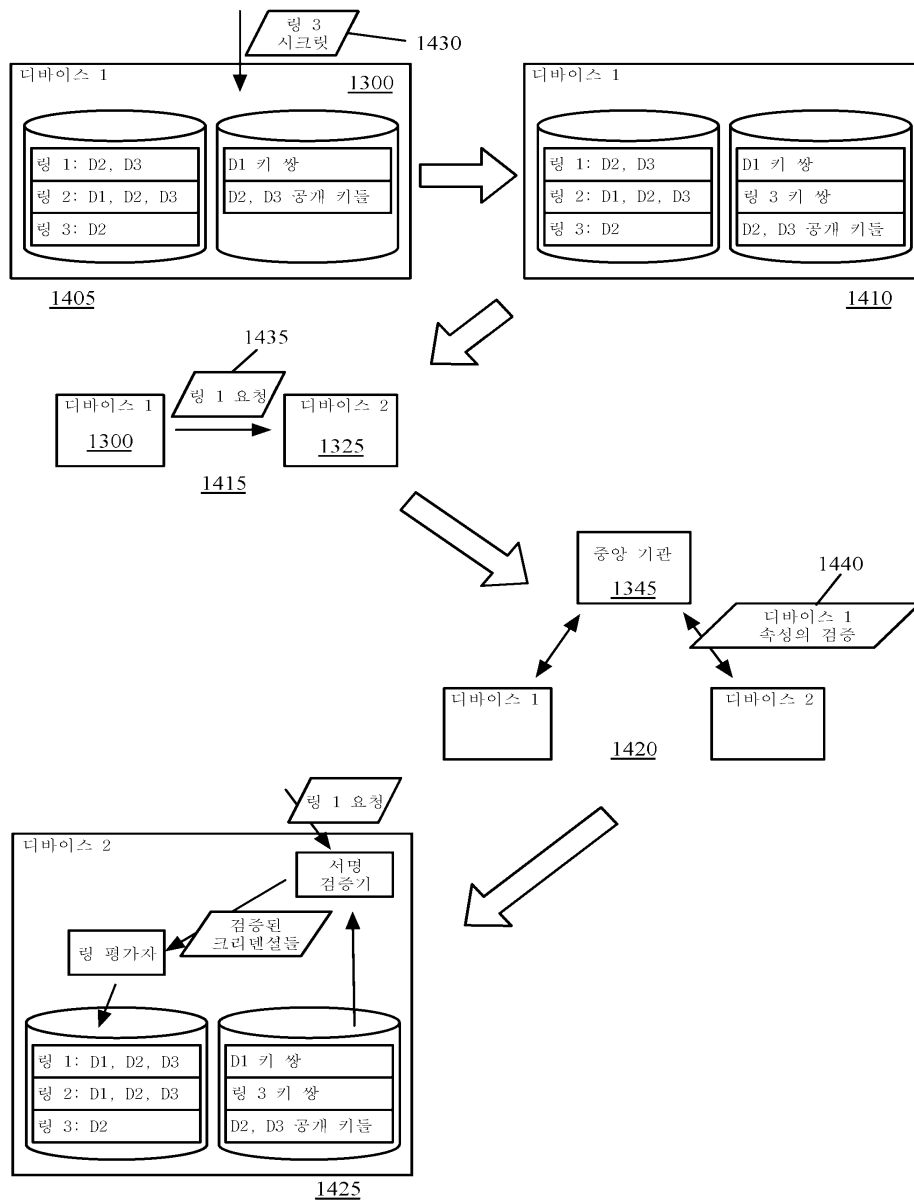
도면12



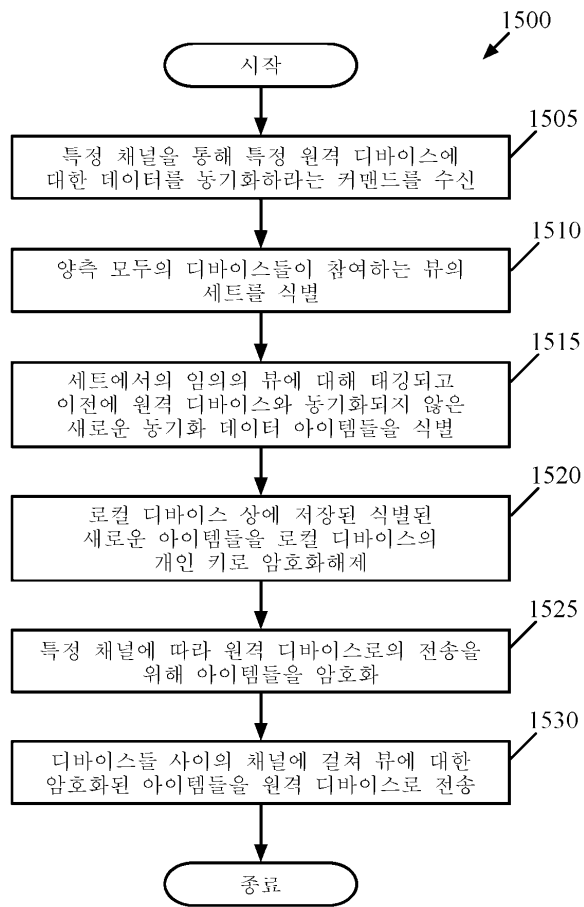
도면13



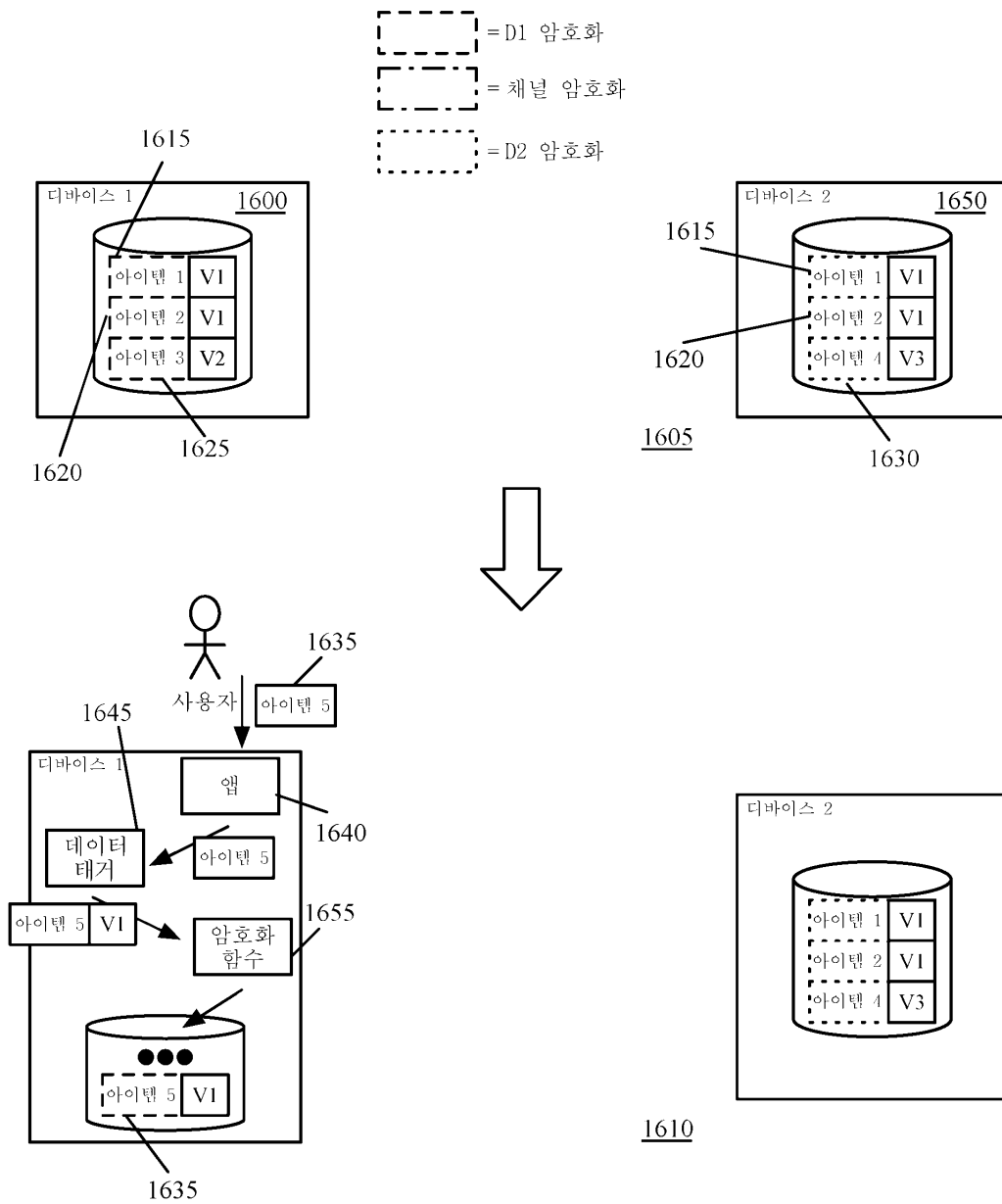
도면14



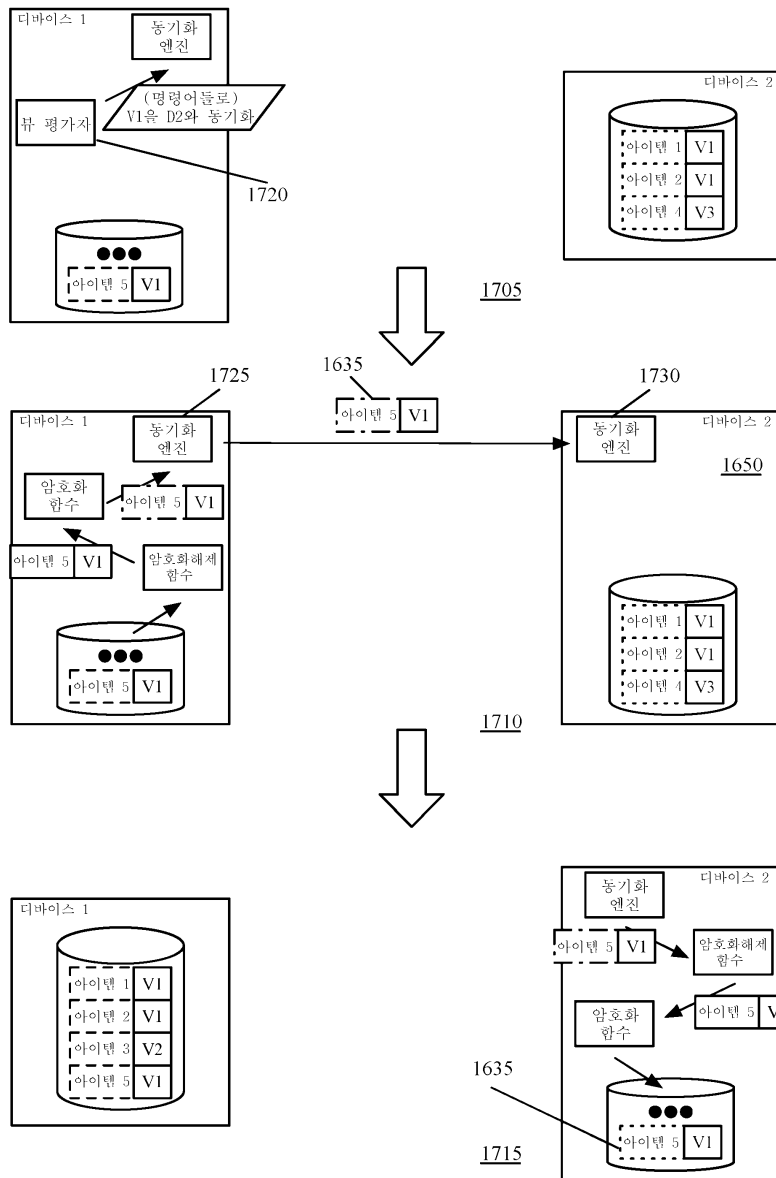
도면15



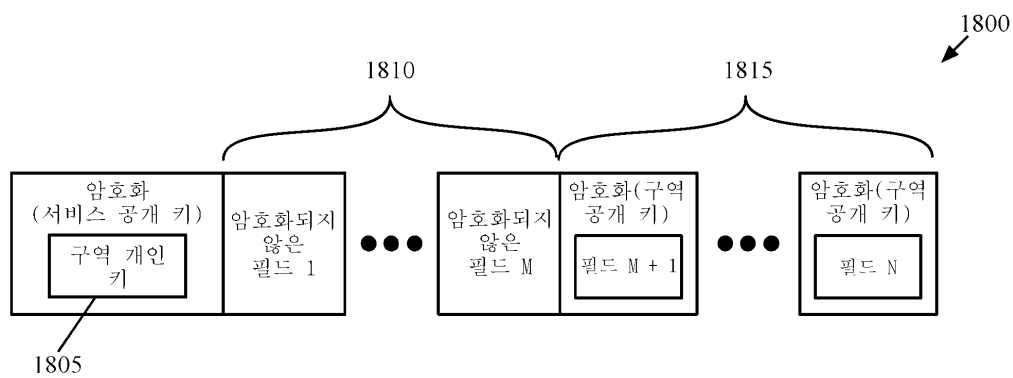
도면16



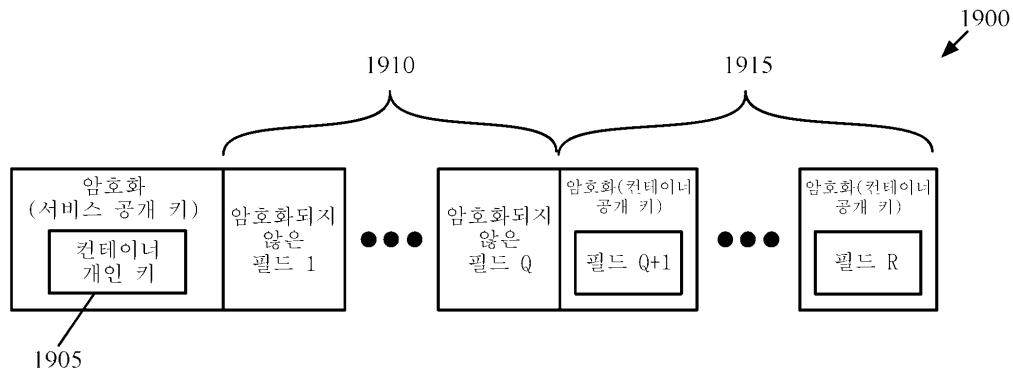
도면17



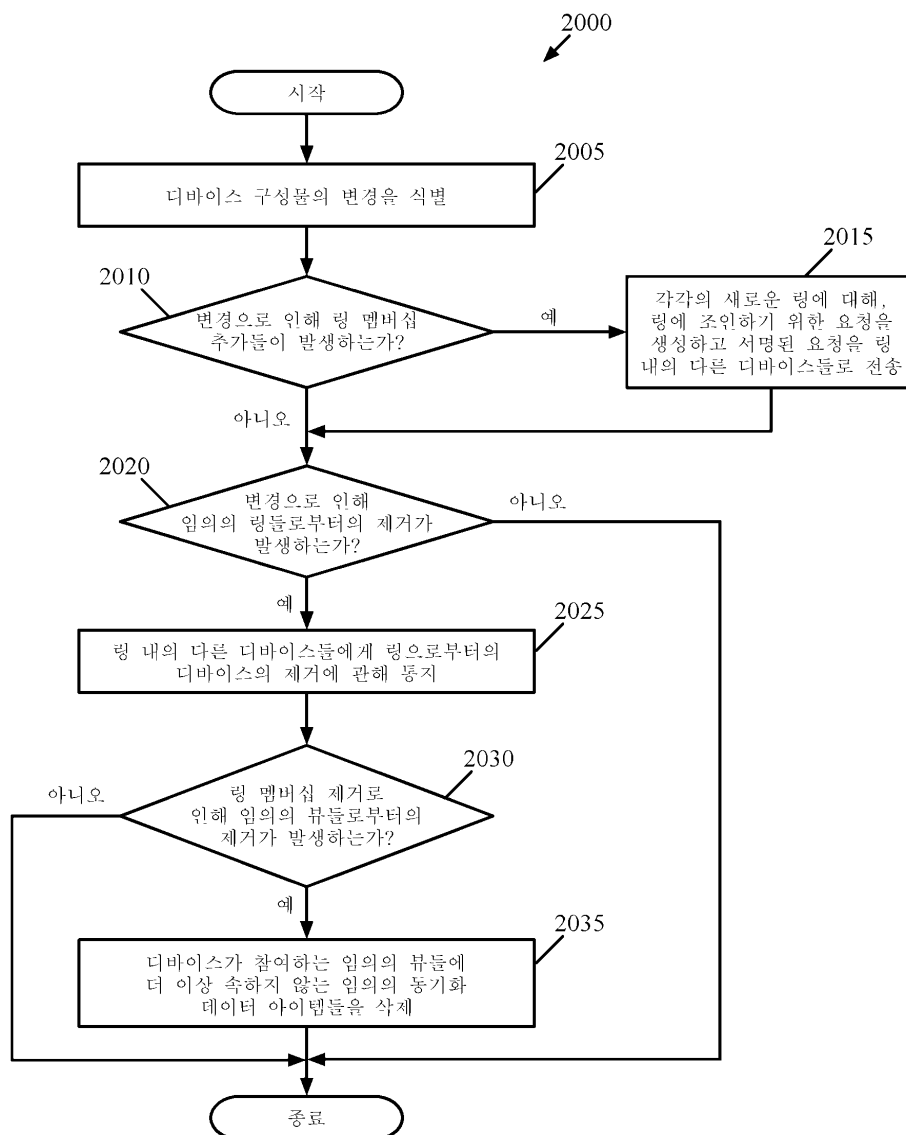
도면18



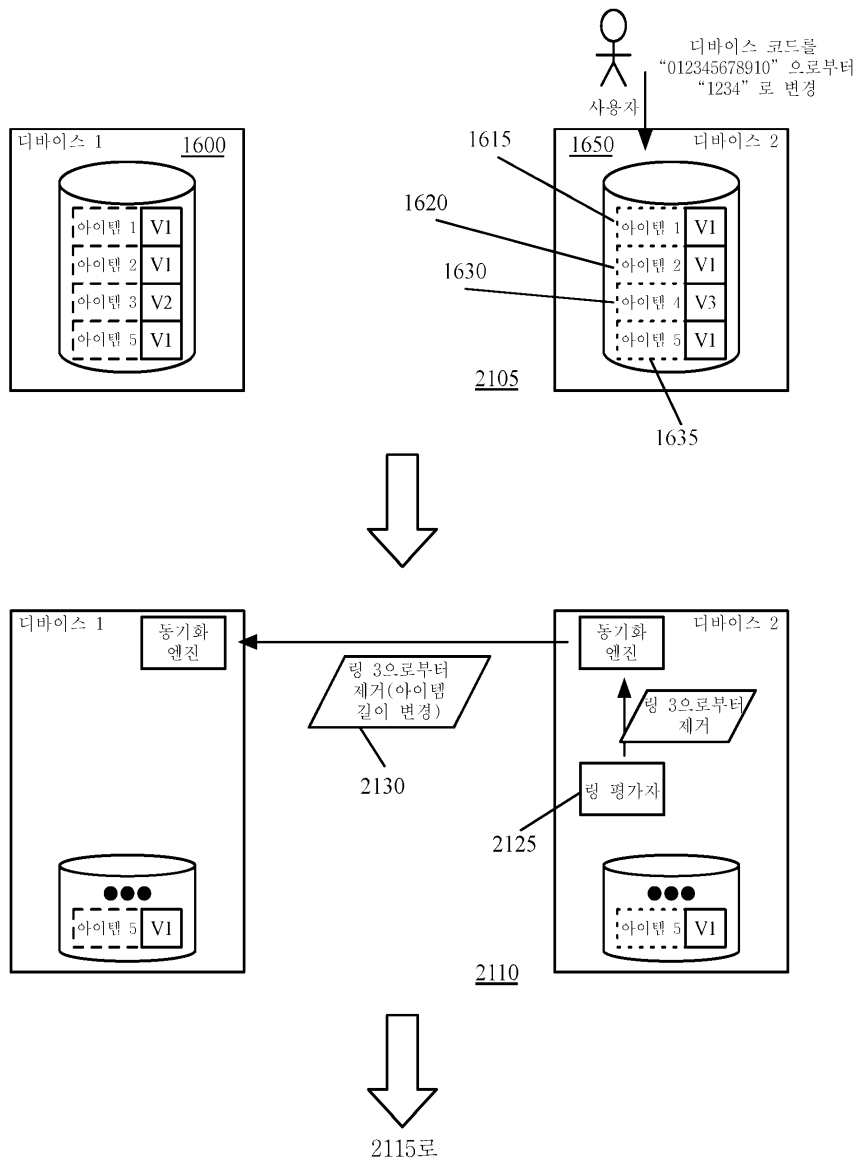
도면19



도면20

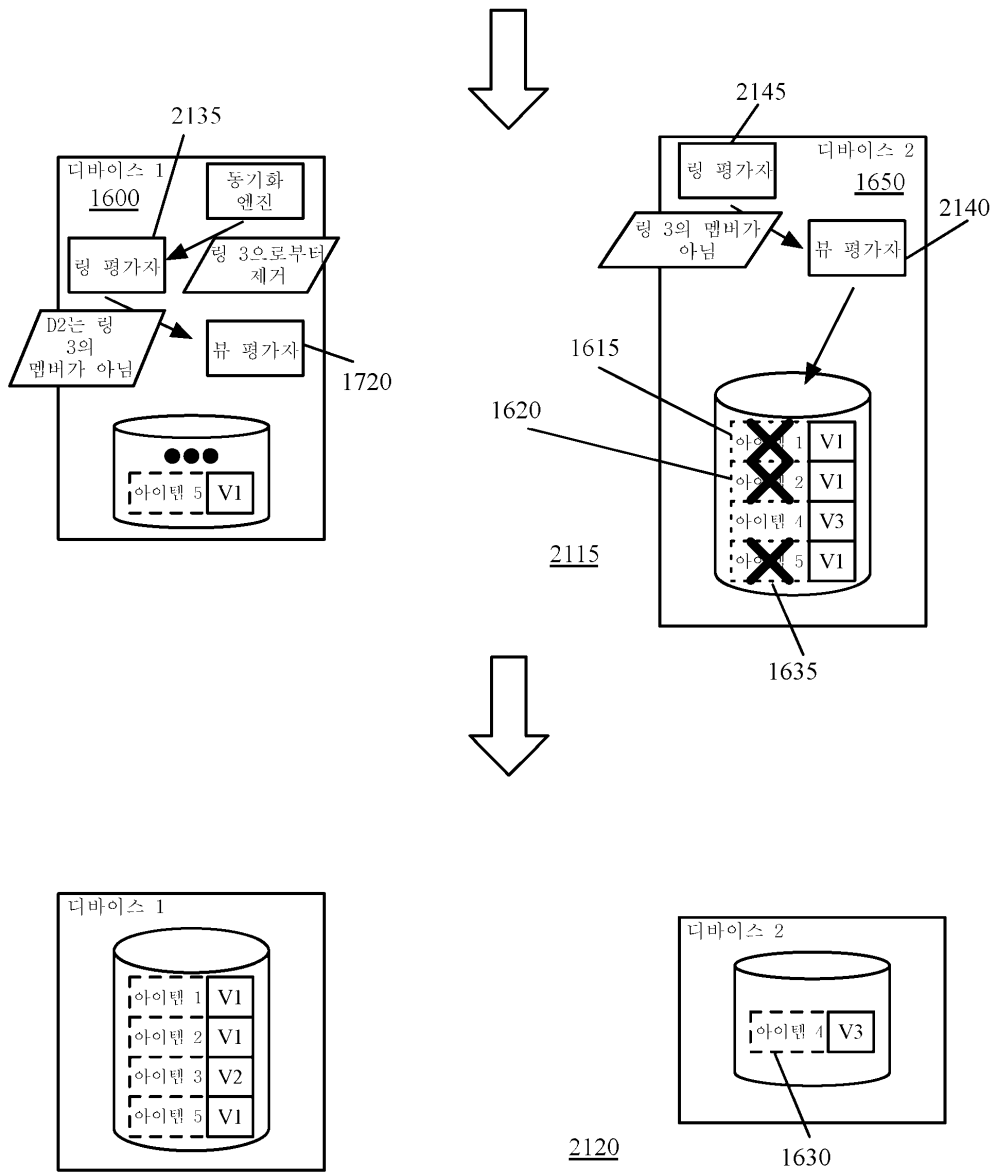


도면21a

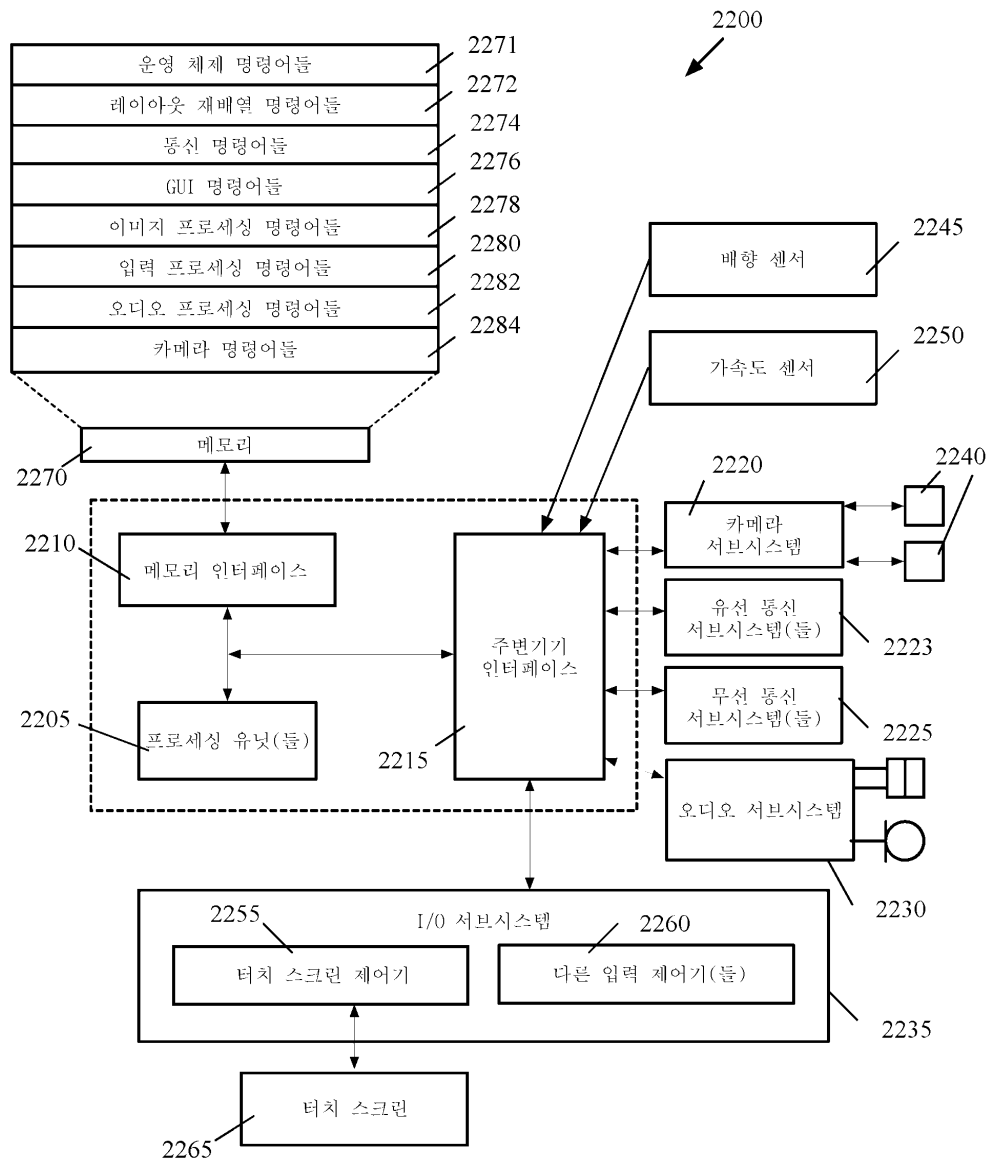


도 21 — 도 21a
— 도 21b

도면21b



도면22



도면23

