(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년10월20일
(11) 등록번호 10-2457683
(24) 등록일자 2022년10월18일

(51) 국제특허분류(Int. Cl.)
G06Q 20/40 (2012.01) *G06Q 20/38* (2012.01)
(52) CPC특허분류
G06Q 20/4016 (2013.01)
G06Q 20/22 (2013.01)
(21) 출원번호 10-2017-7003450
(22) 출원일자(국제) 2015년07월30일
심사청구일자 2020년07월28일
(85) 번역문제출일자 2017년02월07일
(65) 공개번호 10-2017-0041731
(43) 공개일자 2017년04월17일
(86) 국제출원번호 PCT/US2015/042799
(87) 국제공개번호 WO 2016/019093
국제공개일자 2016년02월04일
(30) 우선권주장
14/448,868 2014년07월31일 미국(US)
(56) 선행기술조사문헌
JP2007514333 A*
JP2010097467 A*
JP4939121 B2*
US08380637 B2*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
노크 노크 랩스, 인코포레이티드
미국 캘리포니아 산호세 잔커 로드 2890 스위트 203 (우: 95134)
(72) 발명자
바크다사리안, 데이빗
미국 캘리포니아 팔로 알토 스위트 105 겡 로드 2100 (우: 94303)
(74) 대리인
특허법인 남앤남

전체 청구항 수 : 총 22 항 심사관 : 권현수

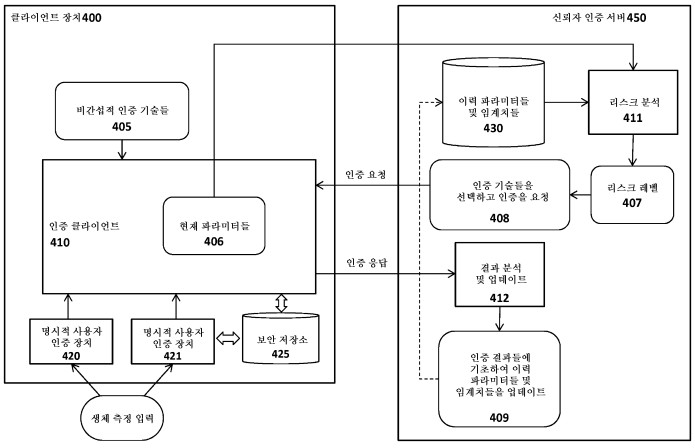
(54) 발명의 명칭 **데이터 분석을 사용하여 인증을 수행하기 위한 시스템 및 방법**

(57) 요 약

기계 학습과 같은 데이터 분석을 사용하여 인증을 수행하기 위한 시스템, 장치, 방법 및 기계 판독 가능 매체가 설명된다. 예를 들어, 방법의 일 실시예는: 클라이언트 장치 상의 사용자 활동에 관련된 파라미터들의 세트를 선택하는 단계; 현재 트랜잭션에 대해 사용자를 인증하기 위한 요청을 수신하는 단계; 그에 응답하여 현재 트랜

(뒷면에 계속)

대 표 도 - 도4a



잭션과 연관된 파라미터들과 기존 데이터세트로부터의 이력 파라미터들 사이의 거리를 계산하는 단계; 현재 트랜잭션과 연관된 파라미터들과 이력 파라미터들 사이의 계산된 거리들에 기초하여 현재 트랜잭션과 연관된 리스크 레벨을 결정하는 단계; 리스크 레벨에 기초하여 사용자를 인증하는 데 요구되는 하나 이상의 인증 기술을 선택하는 단계; 하나 이상의 인증 기술을 수행하여 사용자를 인증하려고 시도하고 인증 결과를 생성하는 단계; 및 현재 트랜잭션과 연관된 파라미터들 및 인증 결과를 사용하여 이력 파라미터들을 업데이트하는 단계를 포함한다.

(52) CPC특허분류
G06Q 20/38215 (2013.01)
G06Q 20/40145 (2013.01)

명 세 서

청구범위

청구항 1

인증 시스템 내에서 구현되는 방법으로서,

클라이언트 장치 상의 사용자 활동에 관련된 파라미터들의 세트를 선택하는 단계;

현재 트랜잭션에 대해 사용자를 인증하기 위한 요청을 수신하는 단계;

그에 응답하여 상기 현재 트랜잭션과 연관된 파라미터들과 기존 데이터세트로부터의 이력 파라미터들 사이의 거리를 계산하는 단계;

상기 현재 트랜잭션과 연관된 파라미터들과 상기 이력 파라미터들 사이의 상기 계산된 거리들에 기초하여 상기 현재 트랜잭션과 연관된 리스크 레벨을 결정하는 단계;

상기 리스크 레벨에 기초하여 상기 사용자를 인증하는 데 요구되는 하나 이상의 인증 기술들을 선택하는 단계;

상기 사용자를 인증하려고 시도하기 위해 상기 하나 이상의 인증 기술들을 수행하여 인증 결과를 생성하는 단계; 및

상기 인증 결과를 반영하기 위해 상기 이력 파라미터들을 업데이트하는 단계 – 상기 인증 결과에 따라, 상기 현재 트랜잭션과 연관된 파라미터들과 연관된 리스크성이 감소 또는 증가됨 –

을 포함하고,

상기 사용자 활동과 관련된 파라미터들의 세트는, 각각의 파라미터와 이전 인증 이벤트들의 결과들 사이의 상관관계(correlation)를 식별하는 머신 러닝 알고리즘을 이용하여 선택되는, 인증 시스템 내에서 구현되는 방법.

청구항 2

제1항에 있어서, 상기 파라미터들은, 인증을 수행하는 데 사용되는 인증기 식별자들 또는 키들과 연관된 파라미터들, 인증의 시간과 연관된 파라미터들, 인증의 위치와 연관된 파라미터들, 네트워크 접속성과 연관된 파라미터들 또는 클라이언트 장치 인증기에 의해 생성된 생체 측정 점수(biometric score)와 연관된 파라미터들 중 적어도 하나를 포함하는, 인증 시스템 내에서 구현되는 방법.

청구항 3

제1항에 있어서, 상기 리스크 레벨은, 상기 현재 트랜잭션과 연관된 파라미터들 중 하나 이상의 파라미터와 이에 대응하는 이력 파라미터들 사이의 거리가 특정 임계치 미만인 경우, 정상적 사용자 거동을 나타내는 제1 레벨로 설정되는, 인증 시스템 내에서 구현되는 방법.

청구항 4

제3항에 있어서, 상기 리스크 레벨은, 상기 현재 트랜잭션과 연관된 파라미터들 중 하나 이상의 파라미터와 이에 대응하는 이력 파라미터들 사이의 거리가 특정 임계치 초과인 경우, 의심스러운 사용자 거동을 나타내는 제2 레벨로 설정되는, 인증 시스템 내에서 구현되는 방법.

청구항 5

제1항에 있어서, 상기 인증 기술들을 선택하는 단계는,

상대적으로 더 높은 리스크 레벨들에 대해 더 엄격한 인증 기술들을 선택하고, 상대적으로 더 낮은 리스크 레벨들에 대해 상대적으로 덜 엄격한 인증 기술들을 선택하거나 인증 기술들을 선택하지 않는 단계를 포함하는, 인증 시스템 내에서 구현되는 방법.

청구항 6

제5항에 있어서, 상기 더 엄격한 인증 기술들은 명시적 생체 측정 사용자 인증을 포함하는, 인증 시스템 내에서 구현되는 방법.

청구항 7

제6항에 있어서, 상기 덜 엄격한 인증 기술들은 비간섭적(non-intrusive) 인증 기술들을 포함하는, 인증 시스템 내에서 구현되는 방법.

청구항 8

삭제

청구항 9

제1항에 있어서, 성공적 인증 이벤트들 또는 실패한 인증 이벤트들 중 적어도 하나와 상대적으로 높은 상관을 갖는 파라미터들이 상기 파라미터들의 세트에 포함되도록 선택되는, 인증 시스템 내에서 구현되는 방법.

청구항 10

제1항에 있어서, 상기 현재 트랜잭션과 연관된 파라미터들과 이력 파라미터들 사이의 거리를 계산하는 단계는 상기 파라미터들의 가우스 분포(Gaussian distribution)를 사용하여 이상 검출(anomaly detection)을 수행하는 단계를 포함하는, 인증 시스템 내에서 구현되는 방법.

청구항 11

프로그램 코드가 저장된 비일시적 기계 판독가능 매체로서,

상기 프로그램 코드는, 기계에 의해 실행될 때, 상기 기계로 하여금,

클라이언트 장치 상의 사용자 활동에 관련된 파라미터들의 세트를 선택하고;

현재 트랜잭션에 대해 사용자를 인증하기 위한 요청을 수신하고;

그에 응답하여 상기 현재 트랜잭션과 연관된 파라미터들과 기존 데이터세트로부터의 이력 파라미터들 사이의 거리를 계산하고;

상기 현재 트랜잭션과 연관된 파라미터들과 상기 이력 파라미터들 사이의 상기 계산된 거리들에 기초하여 상기 현재 트랜잭션과 연관된 리스크 레벨을 결정하고;

상기 리스크 레벨에 기초하여 상기 사용자를 인증하는 데 요구되는 하나 이상의 인증 기술들을 선택하고;

상기 사용자를 인증하려고 시도하기 위해 상기 하나 이상의 인증 기술들을 수행하여 인증 결과를 생성하고; 그리고

상기 인증 결과를 반영하기 위해 상기 이력 파라미터들을 업데이트하는 동작들을 수행하도록 하고,

상기 인증 결과에 따라, 상기 현재 트랜잭션과 연관된 파라미터들과 연관된 리스크성이 감소 또는 증가되며,

상기 사용자 활동에 관련된 파라미터들의 세트는, 각각의 파라미터와 이전의 인증 이벤트들의 결과들 사이의 상관관계를 식별하는 머신 러닝 알고리즘을 이용하여 선택되는,

비일시적 기계 판독가능 매체.

청구항 12

제11항에 있어서, 상기 파라미터들은, 인증을 수행하는 데 사용되는 인증기 식별자들 또는 키들과 연관된 파라미터들, 인증의 시간과 연관된 파라미터들, 인증의 위치와 연관된 파라미터들, 네트워크 접속성과 연관된 파라미터들 또는 클라이언트 장치 인증기에 의해 생성된 생체 측정 점수와 연관된 파라미터들 중 적어도 하나를 포함하는, 비일시적 기계 판독가능 매체.

청구항 13

제11항에 있어서, 상기 리스크 레벨은, 상기 현재 트랜잭션과 연관된 파라미터들 중 하나 이상의 파라미터와 이에 대응하는 이력 파라미터들 사이의 거리가 특정 임계치 미만인 경우, 정상적 사용자 거동을 나타내는 제1 레벨로 설정되는, 비일시적 기계 판독가능 매체.

청구항 14

제13항에 있어서, 상기 리스크 레벨은, 상기 현재 트랜잭션과 연관된 파라미터들 중 하나 이상의 파라미터와 이에 대응하는 이력 파라미터들 사이의 거리가 특정 임계치 초과인 경우, 의심스러운 사용자 거동을 나타내는 제2 레벨로 설정되는, 비일시적 기계 판독가능 매체.

청구항 15

제11항에 있어서, 상기 인증 기술들을 선택하는 것은,

상대적으로 더 높은 리스크 레벨들에 대해 더 엄격한 인증 기술들을 선택하고, 상대적으로 더 낮은 리스크 레벨들에 대해 상대적으로 덜 엄격한 인증 기술들을 선택하거나 인증 기술들을 선택하지 않는 것을 포함하는, 비일시적 기계 판독가능 매체.

청구항 16

제15항에 있어서, 상기 더 엄격한 인증 기술들은 명시적 생체 측정 사용자 인증을 포함하는, 비일시적 기계 판독가능 매체.

청구항 17

제16항에 있어서, 상기 덜 엄격한 인증 기술들은 비간섭적 인증 기술들을 포함하는, 비일시적 기계 판독가능 매체.

청구항 18

삭제

청구항 19

제11항에 있어서, 성공적 인증 이벤트들 또는 실패한 인증 이벤트들 중 적어도 하나와 상대적으로 높은 상관을 갖는 파라미터들이 상기 파라미터들의 세트에 포함되도록 선택되는, 비일시적 기계 판독가능 매체.

청구항 20

제11항에 있어서, 상기 현재 트랜잭션과 연관된 파라미터들과 이력 파라미터들 사이의 거리를 계산하는 것은 상기 파라미터들의 가우스 분포를 사용하여 이상 검출을 수행하는 것을 포함하는, 비일시적 기계 판독가능 매체.

청구항 21

시스템으로서,

현재 사용자의 활동에 관련된 파라미터들의 세트를 제공하는 클라이언트 장치;

현재 트랜잭션에 대해 사용자를 인증하기 위한 요청을 수신하는 인증 서버; 및

결과 분석 및 업데이트 회로

를 포함하며,

상기 인증 서버는, 요청을 수신하는 것에 응답하여 상기 현재 트랜잭션과 연관된 파라미터들과 기존 데이터세트로부터의 이력 파라미터들 사이의 거리를 계산하는 리스크 분석 회로(circuitry)를 포함하고,

상기 리스크 분석 회로는 상기 현재 트랜잭션과 연관된 파라미터들과 상기 이력 파라미터들 사이의 상기 계산된 거리들에 기초하여 상기 현재 트랜잭션과 연관된 리스크 레벨을 결정하고, 상기 리스크 레벨에 기초하여 상기 사용자를 인증하는 데 요구되는 하나 이상의 인증 기술들을 선택하며,

상기 클라이언트 장치는, 상기 사용자를 인증하려고 시도하기 위해 상기 하나 이상의 인증 기술을 수행하는 인

증 엔진을 포함하며, 인증 결과를 생성하고,

상기 결과 분석 및 업데이트 회로는 상기 인증 결과를 반영하기 위해 상기 이력 파라미터들을 업데이트하며, 상기 인증 결과에 따라, 상기 현재 트랜잭션과 연관된 파라미터들과 연관된 리스크성은 감소 또는 증가되고,

상기 현재 사용자의 활동과 관련된 파라미터들의 세트는, 각각의 파라미터와 이전의 인증 이벤트들의 결과들 사이의 상관관계를 식별하는 머신 러닝 알고리즘을 이용하여 선택되는,

시스템.

청구항 22

제21항에 있어서, 상기 파라미터들은, 인증을 수행하는 데 사용되는 인증기 식별자들 또는 키들과 연관된 파라미터들, 인증의 시간과 연관된 파라미터들, 인증의 위치와 연관된 파라미터들, 네트워크 접속성과 연관된 파라미터들 또는 클라이언트 장치 인증기에 의해 생성된 생체 측정 점수와 연관된 파라미터들 중 적어도 하나를 포함하는, 시스템.

청구항 23

제21항에 있어서, 상기 리스크 레벨은, 상기 현재 트랜잭션과 연관된 파라미터들 중 하나 이상의 파라미터와 이에 대응하는 이력 파라미터들 사이의 거리가 특정 임계치 미만인 경우, 정상적 사용자 거동을 나타내는 제1 레벨로 설정되는, 시스템.

청구항 24

제23항에 있어서, 상기 리스크 레벨은, 상기 현재 트랜잭션과 연관된 파라미터들 중 하나 이상의 파라미터와 이에 대응하는 이력 파라미터들 사이의 거리가 특정 임계치 초과인 경우, 의심스러운 사용자 거동을 나타내는 제2 레벨로 설정되는, 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 일반적으로 데이터 처리 시스템들의 분야에 관한 것이다. 보다 상세하게는, 본 발명은 기계 학습과 같은 데이터 분석을 사용하여 인증을 수행하기 위한 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 생체 측정 센서(biometric sensor)들을 이용하여 네트워크를 통해 보안 사용자 인증을 제공하기 위한 시스템들이 또한 설계되어 왔다. 그러한 시스템들에서는, 원격 서버에 대해 사용자를 인증하기 위해, 인증기에 의해 생성된 점수, 및/또는 다른 인증 데이터가 네트워크를 통해 전송될 수 있다. 예를 들어, 미국 특허 출원 제2011/0082801호("'801 출원")는 강한 인증(예를 들어, 신분 도용 및 피싱에 대한 보호), 보안 트랜잭션(예를 들어, 트랜잭션에 대한 "브라우저 내 멀웨어(malware in the browser)" 및 "중간자(man in the middle)" 공격에 대한 보호), 및 클라이언트 인증 토큰의 등재/관리(예를 들어, 지문 판독기, 얼굴 인식 장치, 스마트카드, 신뢰 플랫폼 모듈 등)를 제공하는 네트워크 상에서의 사용자 등록 및 인증을 위한 프레임워크를 설명한다.

[0003] 본 출원의 양수인은 '801 출원에서 설명된 인증 프레임워크에 대한 다양한 개량을 개발하였다. 이러한 개량들 중 일부는 본 양수인에게 양도된 다음과 같은 미국 특허 출원들의 세트에서 설명된다: 제13/730,761호, 인증 능력들을 결정하기 위한 조회 시스템 및 방법(Query System and Method to Determine Authentication Capabilities); 제13/730,776호, 다수의 인증 장치들로 효율적으로 등록, 기록, 및 인증하기 위한 시스템 및 방법(System and Method for Efficiently Enrolling, Registering, and Authenticating With Multiple Authentication Devices); 제13/730,780호, 인증 프레임워크 내에서 랜덤 챌린지들을 처리하기 위한 시스템 및 방법(System and Method for Processing Random Challenges Within an Authentication Framework); 제13/730,791호, 인증 프레임워크 내에서 프라이버시 클래스들을 구현하기 위한 시스템 및 방법(System and Method for Implementing Privacy Classes Within an Authentication Framework); 제13/730,795호, 인증 프레임워크 내에서 트랜잭션 시그널링을 구현하기 위한 시스템 및 방법(System and Method for Implementing Transaction Signaling Within an Authentication Framework); 및 제14/218,504호, 진보된 인증 기술들 및 응용들(Advanced Authentication Techniques and Applications)(이하, "'504 출원"). 이러한 출원들은 때때로

본 명세서에서 ("공계류 중인 출원들")로 지칭된다.

[0004] 간단히, 공계류 중인 출원들은 사용자가 클라이언트 장치 상의 생체 측정 장치들(예를 들어, 지문 센서들)과 같은 인증 장치들(또는 인증기들)에 등록하는 인증 기술들을 설명한다. 사용자가 생체 측정 장치에 등록할 때, (예를 들어, 손가락 스와이핑, 사진 스냅핑, 음성 기록 등에 의해) 생체 측정 참조 데이터가 캡처된다. 이어서, 사용자는 네트워크를 통해 하나 이상의 서버(예를 들어, 공계류 중인 출원들에서 설명된 바와 같은 보안 트랜잭션 서비스들을 갖춘 웹사이트 또는 다른 신뢰자(relying party))에 인증 장치들을 등록/프로비저닝한 후에; 등록 프로세스 동안 교환된 데이터(예를 들어, 인증 장치들 내에 프로비저닝된 암호 키들)를 이용하여 그러한 서버들에서 인증받을 수 있다. 인증되면, 사용자는 웹사이트 또는 다른 신뢰자와의 하나 이상의 온라인 트랜잭션을 수행하도록 허용된다. 공계류 중인 출원들에서 설명된 프레임워크에서는, 사용자를 고유하게 식별하는 데 사용될 수 있는 지문 데이터 및 다른 데이터와 같은 민감한 정보를 사용자의 인증 장치 상에 국지적으로 유지하여 사용자의 프라이버시를 보호할 수 있다.

[0005] '504 출원은, 단지 몇 가지 예로, 복합 인증기들을 설계하고, 인증 보증 레벨들을 지능적으로 생성하고, 비간섭적(non-intrusive) 사용자 검증을 이용하고, 인증 데이터를 새로운 인증 장치들로 전송하고, 인증 데이터를 클라이언트 리스크 데이터로 증대시키고, 인증 정책들을 적응적으로 적용하고, 신뢰 고리들을 생성하기 위한 기술들을 비롯한 다양한 추가 기술들을 설명한다.

도면의 간단한 설명

[0006] 아래의 도면들과 관련된 아래의 상세한 설명으로부터 본 발명의 더 양호한 이해가 얻어질 수 있으며, 도면들에서:

도 1a 및 도 1b는 보안 인증 시스템 아키텍처의 2개의 상이한 실시예를 나타낸다.

도 2는 키들이 어떻게 인증 장치들 내에 등록될 수 있는지를 보여주는 트랜잭션 도면이다.

도 3은 원격 인증을 보여주는 트랜잭션 도면을 나타낸다.

도 4a 및 도 4b는 기계 학습 기술들을 사용하여 인증을 수행하기 위한 시스템의 상이한 실시예들을 나타낸다.

도 5는 기계 학습 기술들을 사용하여 인증을 수행하기 위한 방법의 일 실시예를 나타낸다.

도 6은 기계 학습 기술들을 사용하여 인증을 수행하기 위한 방법의 다른 실시예를 나타낸다.

도 7은 서버들 및/또는 클라이언트들을 위해 사용되는 컴퓨터 아키텍처의 일 실시예를 나타낸다.

도 8은 서버들 및/또는 클라이언트들을 위해 사용되는 컴퓨터 아키텍처의 일 실시예를 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0007] 아래에서는 진보된 인증 기술들 및 관련 응용들을 구현하기 위한 기기, 방법 및 기계 판독 가능 매체의 실시예들이 설명된다. 설명 전반에서, 설명의 목적으로, 본 발명의 완전한 이해를 제공하기 위해, 다수의 구체적인 상세들이 설명된다. 그러나, 본 발명은 이러한 구체적인 상세들 중 일부 없이도 실시될 수 있다는 것이 당업자에게 명백할 것이다. 다른 경우들에서, 본 발명의 기본 원리들을 불명확하게 하지 않기 위해 주지 구조들 및 장치들은 도시되지 않거나 블록도 형태로 도시된다.

[0008] 하기에 논의되는 본 발명의 실시예들은 생체 측정 양상 또는 PIN 엔트리와 같은 사용자 검증 능력을 갖는 인증 장치들을 포함한다. 이러한 장치들은 때때로 본 명세서에서 "토큰", "인증 장치" 또는 "인증기"로 지칭된다. 소정 실시예들이 얼굴 인식 하드웨어/소프트웨어(예를 들어, 사용자의 얼굴을 인식하고 사용자의 눈 움직임을 추적하기 위한 카메라 및 관련 소프트웨어)에 집중되지만, 일부 실시예들은 예를 들어 지문 센서, 음성 인식 하드웨어/소프트웨어(예를 들어, 사용자의 음성을 인식하기 위한 마이크 및 관련 소프트웨어) 및 광학 인식 능력(예를 들어, 사용자의 망막을 스캐닝하기 위한 광학 스캐너 및 관련 소프트웨어)을 비롯한 추가 생체 측정 장치들을 이용할 수 있다. 사용자 검증 능력은 PIN 엔트리와 같은 비생체 측정 양상도 포함할 수 있다. 인증기들은 암호 동작 및 키 저장을 위해 신뢰 플랫폼 모듈(TPM), 스마트카드 및 보안 요소와 같은 장치들을 이용할 수 있다.

[0009] 이동 생체 측정 구현에서, 생체 측정 장치는 신뢰자로부터 원격적일 수 있다. 본 명세서에서 사용되는 바와 같이, 용어 "원격"은 생체 측정 센서가 그것이 통신적으로 결합되는 컴퓨터의 보안 경계의 일부가 아니라는 것을

의미한다(예를 들어, 그것이 신뢰자 컴퓨터와 동일한 물리적 울타리 안에 넣어지지 않는다). 예로서, 생체 측정 장치는 네트워크(예를 들어, 인터넷, 무선 네트워크 링크 등)를 통해 또는 USB 포트와 같은 주변장치 입력을 통해 신뢰자에 결합될 수 있다. 이러한 조건들하에서는, 신뢰자가 장치가 신뢰자에 의해 허가된 장치(예를 들어, 허용 가능한 레벨의 인증 강도 및 무결성 보호를 제공하는 장치)인지 그리고/또는 해커가 생체 측정 장치를 손상시켰거나 심지어는 교체했는지를 알기 위한 방법이 존재하지 않을 수 있다. 생체 측정 장치의 신뢰성은 장치의 특정 구현에 의존한다.

[0010] 용어 "국지적"은 본 명세서에서 사용자가 ATM(automatic teller machine) 또는 POS(point of sale) 소매 체크아웃 위치와 같은 특정 위치에서 트랜잭션을 몸소 완료하고 있다는 사실을 지칭하는 데 사용된다. 그러나, 하기에 논의되는 바와 같이, 사용자를 인증하는 데 채용되는 인증 기술들은 원격 서버들 및/또는 다른 데이터 처리 장치들과의 네트워크를 통한 통신과 같은 비위치 컴포넌트들을 포함할 수 있다. 더욱이, 본 명세서에서는 (ATM 및 소매 위치와 같은) 특정 실시예들이 설명되지만, 본 발명의 기본 원리들은 트랜잭션이 최종 사용자에 의해 국지적으로 개시되는 임의의 시스템의 상황 안에서 구현될 수 있다는 점에 유의해야 한다.

[0011] 용어 "신뢰자"는 때때로 본 명세서에서 사용자 트랜잭션이 시도되는 엔티티(예를 들어, 사용자 트랜잭션을 수행하는 웹사이트 또는 온라인 서비스)뿐만 아니라, 본 명세서에서 설명되는 기본 인증 기술들을 수행할 수 있는 그러한 엔티티를 대신하여 구현되는 것으로 때때로 지칭되는 보안 트랜잭션 서버들도 지칭하는 데 사용된다. 보안 트랜잭션 서버들은 신뢰자에 의해 소유되고/되거나 그의 제어하에 있을 수 있거나, 사업 협정의 일부로서 신뢰자에게 보안 트랜잭션 서비스들을 제공하는 제삼자의 제어하에 있을 수 있다.

[0012] 용어 "서버"는 본 명세서에서 클라이언트로부터 네트워크를 통해 요청들을 수신하고, 그에 응답하여 하나 이상의 동작을 수행하고, 전형적으로 동작들의 결과들을 포함하는 응답을 클라이언트로 전송하는 하드웨어 플랫폼 상에서(또는 다수의 하드웨어 플랫폼에 걸쳐) 실행되는 소프트웨어를 지칭하는 데 사용된다. 서버는 클라이언트 요청들에 응답하여 네트워크 "서비스"를 클라이언트들로 제공하거나, 제공하는 것을 돕는다. 중요하게, 서버는 단일 컴퓨터(예를 들어, 서버 소프트웨어를 실행하기 위한 단일 하드웨어 장치)로 한정되지 않으며, 사실상 다수의 하드웨어 플랫폼에 걸쳐, 잠재적으로는 다수의 지리학적 위치에 분산될 수 있다.

[0013] 예시적인 시스템 아키텍처 및 트랜잭션

[0014] 도 1a 및 도 1b는 인증 장치들을 등록하고(또한 때때로 "프로비저닝"으로 지칭됨) 사용자를 인증하기 위한 클라이언트측 및 서버측 컴포넌트들을 포함하는 시스템 아키텍처의 2개의 실시예를 나타낸다. 도 1a에 도시된 실시예는 웹사이트와 통신하기 위해 웹 브라우저 플러그인 기반 아키텍처를 이용하는 반면, 도 1b에 도시된 실시예는 웹 브라우저를 필요로 하지 않는다. 사용자를 인증 장치들에 등록하고, 인증 장치들을 보안 서버에 등록하고, 사용자를 검증하는 것과 같은, 본 명세서에서 설명되는 다양한 기술들은 이러한 시스템 아키텍처들 중 어느 것에서도 구현될 수 있다. 따라서, 도 1a에 도시된 아키텍처는 후술하는 실시예들 중 여러 실시예의 동작을 설명하는 데 사용되지만, 동일한 기본 원리들은 (예를 들어, 서버(130)와 클라이언트 상의 보안 트랜잭션 서비스(101) 간의 통신을 위한 매개물로서의 브라우저 플러그인(105)을 제거함으로써) 도 1b에 도시된 시스템 상에서 쉽게 구현될 수 있다.

[0015] 먼저, 도 1a를 참조하면, 도시된 실시예는 최종 사용자를 등록 및 검증하기 위한 (때때로 당업계에서 인증 "토큰" 또는 "인증기"로 지칭되는) 하나 이상의 인증 장치들(110 내지 112)을 구비한 클라이언트(100)를 포함한다. 전술한 바와 같이, 인증 장치들(110 내지 112)은 지문 센서, 음성 인식 하드웨어/소프트웨어(예를 들어, 사용자의 음성을 인식하기 위한 마이크 및 관련 소프트웨어), 얼굴 인식 하드웨어/소프트웨어(예를 들어, 사용자의 얼굴을 인식하기 위한 카메라 및 관련 소프트웨어) 및 광학 인식 능력(예를 들어, 사용자의 망막을 스캐닝하기 위한 광학 스캐너 및 관련 소프트웨어)과 같은 생체 측정 장치, 및 PIN 검증과 같은 비생체 측정 양상들에 대한 지원을 포함할 수 있다. 인증 장치들은 암호 동작들 및 키 저장을 위해 신뢰 플랫폼 모듈(TPM), 스마트카드 또는 보안 요소를 이용할 수 있다.

[0016] 인증 장치들(110 내지 112)은 보안 트랜잭션 서비스(101)에 의해 노출되는 인터페이스(102)(예를 들어, 애플리케이션 프로그래밍 인터페이스 또는 API)를 통해 클라이언트에 통신적으로 결합된다. 보안 트랜잭션 서비스(101)는 네트워크를 통해 하나 이상의 보안 트랜잭션 서버(132, 133)와 통신하기 위한 그리고 웹 브라우저(104)의 상황 내에서 실행되는 보안 트랜잭션 플러그인(105)과 인터페이스하기 위한 보안 애플리케이션이다. 도시된 바와 같이, 인터페이스(102)는 장치 식별 코드, 사용자 식별 코드, 인증 장치에 의해 보호되는 사용자 등록 데이터(예를 들어, 스캐닝된 지문 또는 다른 생체 측정 데이터), 및 본 명세서에서 설명되는 보안 인증 기술들을 수행하는 데 사용되는 인증 장치에 의해 봉인된 키들과 같은, 인증 장치들(110 내지 112) 각각과 관련된 정

보를 저장하는 클라이언트(100) 상의 보안 저장 장치(120)에 대한 보안 액세스도 제공할 수 있다. 예를 들어, 하기에 상세히 논의되는 바와 같이, 고유 키가 인증 장치들 각각 내에 저장되고, 인터넷과 같은 네트워크를 통해 서버들(130)에 통신할 때 사용될 수 있다.

[0017] 하기에 논의되는 바와 같이, 웹사이트들(131) 또는 다른 서버들과의 HTTP 또는 HTTPS 트랜잭션들과 같은 소정 타입의 네트워크 트랜잭션들이 보안 트랜잭션 플러그인(105)에 의해 지원된다. 일 실시예에서, 보안 트랜잭션 플러그인은 보안 기업 또는 웹 목적지(130)(아래에서 때때로 간단히 "서버(130)"로 지칭됨) 내의 웹 서버(131)에 의해 웹페이지의 HTML 코드 내에 삽입된 특정 HTML 태그들에 응답하여 개시된다. 그러한 태그의 검출에 응답하여, 보안 트랜잭션 플러그인(105)은 처리를 위해 트랜잭션들을 보안 트랜잭션 서비스(101)로 전송할 수 있다. 게다가, (예를 들어, 보안 키 교환과 같은) 소정 타입의 트랜잭션들을 위해, 보안 트랜잭션 서비스(101)는 구내(즉, 웹사이트와 같은 곳에 배치된) 트랜잭션 서버(132)와의 또는 구외 트랜잭션 서버(133)와의 직접 통신 채널을 개설할 수 있다.

[0018] 보안 트랜잭션 서버들(132, 133)은 후술하는 보안 인증 트랜잭션들을 지원하는 데 필요한 사용자 데이터, 인증 장치 데이터, 키들 및 다른 보안 정보를 저장하기 위한 보안 트랜잭션 데이터베이스(120)에 결합된다. 그러나, 본 발명의 기본 원리들은 도 1a에 도시된 보안 기업 또는 웹 목적지(130) 내의 논리 컴포넌트들의 분리를 필요로 하지 않는다는 점에 유의해야 한다. 예를 들어, 웹사이트(131) 및 보안 트랜잭션 서버들(132, 133)은 단일 물리 서버 또는 개별 물리 서버들 내에 구현될 수 있다. 더욱이, 웹사이트(131) 및 트랜잭션 서버들(132, 133)은 후술하는 기능들을 수행하기 위해 하나 이상의 서버 상에서 실행되는 통합 소프트웨어 모듈 내에 구현될 수 있다.

[0019] 전술한 바와 같이, 본 발명의 기본 원리들은 도 1a에 도시된 브라우저 기반 아키텍처로 한정되지 않는다. 도 1b는 독립 애플리케이션(154)이 보안 트랜잭션 서비스(101)에 의해 제공되는 기능을 이용하여 네트워크를 통해 사용자를 인증하는 대안 구현을 나타낸다. 일 실시예에서, 애플리케이션(154)은 아래에서 상세히 설명되는 사용자/클라이언트 인증 기술들을 수행하기 위해 보안 트랜잭션 서버들(132, 133)에 의존하는 하나 이상의 네트워크 서비스(151)와의 통신 세션들을 설정하도록 설계된다.

[0020] 도 1a 및 도 1b에 도시된 실시예들 중 어느 하나에서, 보안 트랜잭션 서버들(132, 133)은 키들을 생성할 수 있고, 이어서 이 키들은 보안 트랜잭션 서비스(101)로 안전하게 전송되고, 보안 저장소(120) 내에 인증 장치들 내로 저장된다. 게다가, 보안 트랜잭션 서버들(132, 133)은 서버측의 보안 트랜잭션 데이터베이스(120)를 관리한다.

[0021] 인증 장치들을 원격으로 등록하고 신뢰자로 인증하는 것과 연관된 소정 기본 원리들이 도 2 및 도 3과 관련하여 설명될 것이며, 이어서 기계 학습 기술들을 사용하여 인증을 수행하기 위한 본 발명의 실시예들의 상세한 설명이 이어질 것이다.

[0022] 도 2는 클라이언트 상의 인증 장치들(예컨대 도 1a 및 도 1b의 클라이언트(100) 상의 장치들(110 내지 112))을 등록하기(때때로 인증 장치들을 "프로비저닝"하는 것으로 지칭됨) 위한 일련의 트랜잭션들을 나타낸다. 단순화를 위해, 보안 트랜잭션 서비스(101) 및 인터페이스(102)는 인증 클라이언트(201)로서 함께 조합되고, 보안 트랜잭션 서버들(132, 133)을 포함하는 보안 기업 또는 웹 목적지(130)는 신뢰자(202)로서 표현된다.

[0023] 인증기(예를 들어, 지문 인증기, 음성 인증기 등)의 등록 동안, 인증기와 연관된 키는 인증 클라이언트(201)와 신뢰자(202) 사이에서 공유된다. 도 1a 및 도 1b를 다시 참조하면, 키는 클라이언트(100)의 보안 저장소(120) 및 보안 트랜잭션 서버들(132, 133)에 의해 사용되는 보안 트랜잭션 데이터베이스(120) 내에 저장될 수 있다. 일 실시예에서, 키는 보안 트랜잭션 서버들(132, 133) 중 하나에 의해 생성되는 대칭 키이다. 그러나, 하기에 논의되는 다른 실시예에서는, 비대칭 키들이 사용된다. 이 실시예에서, 공개/비공개 키 쌍은 보안 트랜잭션 서버들(132, 133)에 의해 생성될 수 있다. 이어서, 공개 키는 보안 트랜잭션 서버들(132, 133)에 의해 저장될 수 있으며, 관련 비공개 키는 클라이언트 상의 보안 저장소(120) 내에 저장될 수 있다. 대안 실시예에서, 키(들)는 클라이언트(100) 상에서 (예를 들어, 보안 트랜잭션 서버들(132, 133)보다는 인증 장치 또는 인증 장치 인터페이스에 의해) 생성될 수 있다. 본 발명의 기본 원리들은 임의의 특정 타입의 키들 또는 키들을 생성하는 방식으로 한정되지 않는다.

[0024] 보안 키 프로비저닝 프로토콜은 일 실시예에서 보안 통신 채널을 통해 클라이언트와 키를 공유하는 데 채용된다. 키 프로비저닝 프로토콜의 일례는 동적 대칭 키 프로비저닝 프로토콜(DSKPP)(예를 들어, RFC(Request for Comments) 6063 참조)이다. 그러나, 본 발명의 기본 원리들은 임의의 특정 키 프로비저닝 프

로토콜로 한정되지 않는다. 하나의 특정 실시예에서, 클라이언트는 공개/비공개 키 쌍을 생성하여 공개 키를 서버로 전송하며, 이는 증명 키로 증명될 수 있다.

[0025] 도 2에 도시된 구체적인 상세들로 돌아가서, 등록 프로세스를 개시하기 위하여, 신뢰자(202)는 장치 등록 동안 인증 클라이언트(201)에 의해 제시되어야 하는 랜덤 생성 챌린지(예를 들어, 암호 논스)를 생성한다. 랜덤 챌린지는 제한된 기간 동안 유효할 수 있다. 이에 응답하여, 인증 클라이언트(201)는 신뢰자(202)와의 대역외 보안 접속(예를 들어, 대역외 트랜잭션)을 개시하고, 키 프로비저닝 프로토콜(예를 들어, 전술한 DSKPP 프로토콜)을 이용하여 신뢰자(202)와 통신한다. 보안 접속을 개시하기 위하여, 인증 클라이언트(201)는 랜덤 챌린지를 (잠재적으로는 랜덤 챌린지에 대해 생성된 서명과 함께) 다시 신뢰자(202)에게 제공할 수 있다. 게다가, 인증 클라이언트(201)는 (예를 들어, 프로비저닝되는 인증 장치(들)의 타입을 고유하게 식별하는 인증 증명 ID(AAID)를 이용하여) 프로비저닝될 등록될 사용자의 아이덴티티(예를 들어, 사용자 ID 또는 다른 코드) 및 인증 장치(들)의 아이덴티티를 전송할 수 있다.

[0026] 신뢰자는 사용자 이름 또는 ID 코드(예를 들어, 사용자 계정 데이터베이스)를 이용하여 사용자를 찾고, (예를 들어, 서명을 사용하거나, 단순히 랜덤 챌린지를 전송된 것과 비교함으로써) 랜덤 챌린지를 확인하고, 하나가 전송되었으면(예를 들어, AAID) 인증 장치의 인증 코드를 확인하고, 사용자 및 인증 장치(들)에 대해 보안 트랜잭션 데이터베이스(예를 들어, 도 1a 및 도 1b의 데이터베이스(120)) 내의 새로운 엔트리를 생성한다. 일 실시예에서, 신뢰자는 그것이 인증을 허용하는 인증 장치들의 데이터베이스를 유지한다. 그것은 프로비저닝되는 인증 장치(들)가 인증에 허용 가능한지 여부를 결정하기 위해 AAID(또는 다른 인증 장치(들) 코드)로 이 데이터베이스에 문의할 수 있다. 만약 그러한 경우, 그것은 등록 프로세스를 계속할 것이다.

[0027] 일 실시예에서, 신뢰자(202)는 프로비저닝되는 각각의 인증 장치에 대한 인증 키를 생성한다. 그것은 키를 보안 데이터베이스에 기록하고, 키 프로비저닝 프로토콜을 사용하여 키를 인증 클라이언트(201)로 다시 전송한다. 일단 완료되면, 인증 장치와 신뢰자(202)는 대칭 키가 사용된 경우에는 동일 키를, 또는 비대칭 키들이 사용된 경우에는 상이한 키들을 공유한다. 예를 들어, 비대칭 키들이 사용된 경우, 신뢰자(202)는 공개 키를 저장하고 비공개 키를 인증 클라이언트(201)에 제공할 수 있다. 신뢰자(202)로부터 비공개 키를 수신하면, 인증 클라이언트(201)는 인증 장치 내로 키를 프로비저닝한다(그것을 인증 장치와 연관된 보안 저장소 내에 저장함). 이어서 그것은 (후술하는 바와 같이) 사용자의 인증 동안 키를 사용할 수 있다. 대안 실시예에서, 키(들)는 인증 클라이언트(201)에 의해 생성되고, 키 프로비저닝 프로토콜은 키(들)를 신뢰자(202)에 제공하는 데 사용된다. 어느 경우이든, 프로비저닝이 완료되면, 인증 클라이언트(201) 및 신뢰자(202)는 각각 키를 갖고, 인증 클라이언트(201)는 신뢰자에게 완료를 통지한다.

[0028] 도 3은 프로비저닝된 인증 장치들을 이용한 사용자 인증을 위한 일련의 트랜잭션들을 나타낸다. 장치 등록이 완료되면(도 2에 설명된 바와 같이), 신뢰자(202)는 유효한 인증 응답으로서 클라이언트 상의 국지적 인증 장치에 의해 생성된 인증 응답(때때로 "토큰"으로 지칭됨)을 허용할 것이다.

[0029] 도 3에 도시된 구체적인 상세들로 돌아가서, 사용자가 인증을 필요로 하는 신뢰자(202)와의 트랜잭션을 개시하는 것(예를 들어, 신뢰자의 웹사이트로부터 지불을 개시하는 것, 개인 사용자 계정 데이터에 액세스하는 것 등)에 응답하여, 신뢰자(202)는 랜덤 챌린지(예를 들어, 암호 논스)를 포함하는 인증 요청을 생성한다. 일 실시예에서, 랜덤 챌린지는 그와 연관된 시간 제한을 갖는다(예를 들어, 그것은 특정된 기간 동안 유효하다). 신뢰자는 또한 인증을 위해 인증 클라이언트(201)에 의해 사용될 인증기를 식별할 수 있다. 전술한 바와 같이, 신뢰자는 클라이언트 상에서 이용가능한 각각의 인증 장치를 프로비저닝할 수 있고 각각의 프로비저닝된 인증기에 대한 공개 키를 저장한다. 따라서, 그것은 인증기의 공개 키를 사용할 수 있거나, 또는 인증기 ID(예를 들어, AAID)를 사용하여 사용될 인증기를 식별할 수 있다. 대안적으로, 그것은 사용자가 선택할 수 있는 인증 옵션들의 목록을 클라이언트에 제공할 수 있다.

[0030] 인증 요청의 수신에 응답하여, 사용자는 (예를 들어, 웹 페이지 또는 인증 애플리케이션/앱의 GUI 의 형태로) 인증을 요청하는 그래픽 사용자 인터페이스(GUI)를 제시받을 수 있다. 이어서 사용자는 인증을 수행한다(예를 들어, 지문 판독기 상에서 손가락을 스와이핑하는 등). 이에 응답하여, 인증 클라이언트(201)는 인증기와 연관된 비공개 키를 이용해 랜덤 챌린지에 대한 서명을 포함하는 인증 응답을 생성한다. 그것은 또한 인증 응답 내에 사용자 ID 코드와 같은 다른 관련 데이터를 포함할 수 있다.

[0031] 인증 응답을 수신하면, 신뢰자는 (예를 들어, 인증기와 연관된 공개 키를 사용하여) 랜덤 챌린지에 대한 서명을 확인하고 사용자의 아이덴티티를 확인할 수 있다. 일단 인증이 완료되면, 도시된 바와 같이, 신뢰자와의 보안 트랜잭션에 들어가도록 허용된다.

[0032] 전송 계층 보안(Transport Layer Security; TLS) 또는 보안 소켓 계층(Secure Sockets Layer; SSL)과 같은 보안 통신 프로토콜이, 도 2 및 도 3에 도시된 트랜잭션들 중 임의의 것 또는 전부에 대해 신뢰자(201)와 인증 클라이언트(202) 사이의 보안 접속을 설정하는 데 사용될 수 있다.

[0033] 데이터 분석을 사용하여 인증을 수행하기 위한 시스템 및 방법

[0034] 본 발명의 실시예들은 더 큰 규모의 인증-관련 데이터를 봄으로써 사용자들 및 장치들의 상이한 거동 패턴들을 검출하고 이들 패턴을 사용하여 트랜잭션들에 대한 인증 리스크를 조정하기 위한 기술들을 포함한다. 전통적인 인증 시스템들은 패스워드 또는 암호 응답과 같은, 사용자 또는 장치로부터 오는 단일 데이터 신호를 분석하고, 이 신호에 기초하여 최종 인증 결정을 한다. 대조적으로, 후술하는 본 발명의 실시예들은 사용자 인증과 연관된 다양한 상이한 신호들 및 데이터에 기초하여 더 큰 규모의 분석을 수행하여, 전통적 시스템들로 검출될 수 없는 현재 트랜잭션에 관련된 관심있는 패턴들을 식별한다.

[0035] 전술한 바와 같이, 전통적 인증 시스템들은 사용자 패스워드 및 인증 키들과 같은 인증 데이터의 단일 소스를 기초로 한다. 서버들은 일반적으로 사용자 인증 데이터를 사용자 레코드들에 저장하고, 각각의 인증 이벤트 동안 적절한 인증 데이터를 수신할 것으로 예상한다. 그것들은 이진 체크를 수행한다 - 즉, 인증 데이터의 검증이 성공하면 사용자는 인증되고, 검증이 실패하면 사용자는 인증되지 않는다. 이 기법은 오늘날 수천 개의 웹 사이트들에서 성공적으로 작동한다.

[0036] 사용자가 클라이언트 장치의 생체 측정 인증들을 사용하여 서버에 인증할 수 있게 하는 차세대 인증 프로토콜들에서도, 필수적 인증 접근법은 이진 검증들 - 즉, 인증기들에 의해 제공된 암호 서명들의 검증들 - 을 기초로 한다. 클라이언트 장치는 다수의 암호 서명들을 제공할 수 있지만, 서버는 단순히 이들 암호 서명을 검증하고 성공 또는 실패의 이진 결정을 한다.

[0037] 이러한 시스템들의 단점은 그것들이 진보된 공격들에 취약하다는 점이다. 제공된 인증 데이터가 서버측 검증을 통과하는 한, 인증은 성공적인 것으로 간주된다. 그러나, 클라이언트측 인증기들이 손상되고 공격자가 유효한 인증 데이터를 생성할 수 있는 경우, 이들 시스템은 손상될 수 있다. 더 큰 규모의 데이터를 봄으로써 더 진보된 분석을 수행하지 않으면, 이러한 공격들을 검출하고 적절하게 응답하는 것이 매우 어렵다.

[0038] 클라이언트측 인증기들이 사용자를 인증 서버에 인증하는 데 사용되는 시스템들은(도 1a, 도 1b, 도 2 및 도 3에 관하여 전술한 바와 같은), 관심있는 패턴들을 결정하기 위해 추가로 분석될 수 있는 관심있는 데이터 포인트들에 대한 액세스를 갖는다. 그러한 시스템들이 수집하는 데이터가 많을수록, 분석은 더욱 풍부해질 것이다. 분석은 인증-전, 인증 중, 및/또는 인증-후에 수행될 수 있다. 예를 들어, 일 실시예에서, 인증 서버는 특정 사용자의 이전의 모든 인증 시도들을 보고, 이 사용자에게 전형적인 더 큰 패턴 내에 현재 인증 동작이 맞는지 여부를 알 수 있다. 그것이 전형적인 패턴으로부터 벗어나는 경우, 현재 동작은 덜 전형적이고 따라서 덜 신뢰되고/더 위험하다. 대조적으로, 현재 인증 동작이 이전 패턴들 내에 맞는 경우, 시스템은 사용자를 압도하지 않고 추가의 인증을 요구하지 않기로 결정하거나, 또는 덜 간섭적인 인증 기술들을 이용하기로 결정할 수 있다.

[0039] 도 4a는, 데이터 분석을 수행하여 현재 파라미터들에 기초하여 리스크 레벨을 결정하고 인증 기술들을 선택하기 위한 로직이 인증 서버(450) 상에서 수행되는, 본 발명의 일 실시예를 나타낸다. 도 4b는 로직이 클라이언트 장치(400) 상에 구현되는 다른 실시예를 나타낸다. 본 발명의 기본 원리들은 분석이 서버측에서 수행되는지 또는 클라이언트측에서 수행되는지에 상관없이 동일하게 유지된다.

[0040] 도 4a의 실시예를 먼저 참조하면, 예시적인 클라이언트 장치(400)는 하나 이상의 명시적 사용자 인증 장치들(420, 421) 및/또는 비간섭적 인증 기술들(405)을 사용하여 사용자를 인증하기 위한 인증 클라이언트(410)를 포함한다. 명시적 사용자 인증 장치들(420, 421)은, 지문 인증기, 음성 또는 얼굴 인식, 망막 스캐닝, 또는 사용자가 PIN과 같은 비밀 패스워드를 입력할 수 있는 키보드(가상 또는 물리적)와 같은 명시적 사용자 입력을 필요로 하는 임의의 형태의 인증을 나타낸다.

[0041] 비간섭적 인증 기술들(405)은 적법한 사용자가 클라이언트 장치(400)를 소유하고 있을 가능성을 결정하기 위해 관련 데이터를 수집하는 데 사용될 수 있다. 제한이 아닌 예로서, 비간섭적 인증 기술들(405)은 (예를 들어, GPS 또는 다른 위치 메커니즘들을 통해) 사용자의 현재 위치를 결정하는 것, 및 최종 사용자에 의해 방문되는 것으로 알려진 위치들(예를 들어, 사용자의 "집" 및 "직장" 위치들)과 현재 위치를 비교하는 것을 포함할 수 있다. 예를 들어, 클라이언트 장치(400)의 현재 위치가 사용자의 직장인 경우, 이것은 명시적 사용자 인증이 요구되는지(예를 들어, 인증 장치들(420, 421) 중 하나를 통해) 여부 및/또는 명시적 사용자 인증의 레벨을 결정할 때 인증 클라이언트(410)에 의해 사용될 수 있다.

[0042] 하나의 특정 실시예에서, "위치"의 정의는 (GPS에서와 같이) 물리 좌표들의 세트와 관련되지 않을 수 있는 대신, 피어 장치들 또는 다른 타입의 네트워크 장치들의 세트의 존재에 의해 규정될 수 있다. 예를 들어, 직장에 있을 때, 클라이언트의 무선 네트워크 어댑터들(예를 들어, 와이파이 어댑터, 블루투스 어댑터, LTE 어댑터 등)은 피어 네트워크 장치들(예를 들어, 다른 컴퓨터, 이동 전화, 태블릿 등) 및 네트워크 기반구조 장치들(예를 들어, 와이파이 액세스 포인트, 셀 타워 등)의 세트를 일관성 있게 "볼" 수 있다. 따라서, 이러한 장치들의 존재는 사용자가 직장에 있을 때 인증에 사용될 수 있다. 예를 들어 사용자가 집에 있을 때 유사한 방식으로 장치들의 존재에 의해 다른 위치들이 정의될 수 있다.

[0043] 다른 비간섭적 인증 기술들(405)은 가속도계와 같은 클라이언트 장치(400) 상의 센서들로부터 데이터를 수집하는 것을 포함할 수 있다. 예를 들어, 사용자의 생체 측정 보속(gait)은 사용자의 통상적인 걸음 패턴의 보속 "지문"을 생성하도록 설계된 소프트웨어 및/또는 하드웨어와 조합하여 가속도계 또는 다른 유형의 센서를 이용하여 측정될 수 있다. 또한, 현재 온도, 습도, 압력 및 다른 환경 데이터가 수집되고 클라이언트 장치(400)의 주장된(alleged) 현재 위치에 대한 알려진 환경 데이터와 비교될 수 있다(예를 들어, 현재 환경 판독치들이 현재 표명된(asserted) 위치와 일치하는지 확인하기 위해). 게다가, 비간섭적 인증 기술들은 장치들(420, 421)을 사용하여 마지막 성공적인 명시적 인증 이후의 시간을 측정하는 것을 포함할 수 있다. 시간이 짧을수록, 현재 사용자가 클라이언트 장치의 적법한 사용자일 가능성이 더 높다. 이들 및 다른 타입의 데이터가 수집되고, 현재 사용자가 클라이언트 장치(400)의 적법한 사용자일 가능성(및 따라서 명시적 사용자 인증이 요구되는 정도)을 결정하기 위해 분석될 수 있다.

[0044] 전술한 바와 같이, 보안 저장 장치(425)는 인증 장치들(220, 221) 각각과 연관된 인증 키들을 저장하는 데 사용될 수 있다. 인증 키들은 보안 통신 채널을 통해 신뢰자(250)와의 통신을 서명하고 암호화하는데 사용될 수 있다.

[0045] 일 실시예에서, 현재 파라미터들(406)은 신뢰자 인증 서버(450) 상에서 실행되는 리스크 분석 모듈(411)에 의해 클라이언트 장치(400)로부터 수집된다. 다수의 예시적인 파라미터들이 이하에 설명된다. 이어서 리스크 분석 모듈(411)은 현재 트랜잭션에 대한 리스크 레벨(407)을 결정하기 위해, 인증 서버(450) 상의 저장소 내에 유지되는 이력 파라미터들 및 임계치들(430)과 현재 파라미터들(406)을 비교할 수 있다. 일 실시예에서, 리스크 레벨(407)은 현재 파라미터들(406)이 이전의 성공적 인증들 동안 수집된 이력 파라미터들(430)로부터 벗어나는 정도(예를 들어, 현재 파라미터들과 이력 파라미터들 사이의 "거리") 및/또는 현재 파라미터들(406)이 이전의 실패한 인증 시도들 또는 사기성 인증 시도들(이는 더 큰 리스크를 나타내는 경향이 있을 것이다) 동안 수집된 이력 파라미터들(430)과 상관되는 정도를 나타낸다. 하기에 상세히 논의되는 바와 같이, 일 실시예에서, 리스크 레벨(407)은, 현재 파라미터들(406)과 이력 파라미터들(430) 사이의 거리를 특정하기 위해 거리 함수를 사용하는 이상 검출(anomaly detection) 알고리즘을 사용하여 결정된다(하기에 상세히 논의되는 바와 같음).

[0046] 일 실시예에서, 검출된 리스크 레벨(407)에 기초하여, 인증 서버(450)는 사용자를 인증하는 데 요구되는 인증 기술들(408)을 선택한다. 일반적으로, 리스크 레벨(407)이 클수록(예를 들어, "정상적" 거동을 나타내는 파라미터들로부터의 거리가 클수록), 인증은 더 엄격하다. 예를 들어, 일 실시예에서, 리스크 레벨이 특정된 임계치를 초과하는 경우, 인증 서버(450)는 하나 이상의 명시적 사용자 인증 장치들(420, 421)을 사용하여 인증을 요구할 수 있다. 대조적으로, 특정된 임계치 미만의 리스크 레벨인 경우, 비간섭적 인증 기술들(405)은 충분할 수 있다. 전술한 바와 같이, 신뢰자로부터 전송된 인증 요청은 암호 논스와 같은 다른 형태의 보안-관련된 데이터를 포함할 수 있다.

[0047] 신뢰자로부터 전송된 인증 요청에 응답하여, 인증 클라이언트(410)는 (명시적 인증이 요구되는 경우) 하나 이상의 특정된 인증 장치들(420, 421)을 사용하여 인증을 수행하도록 사용자에게 프롬프트한다. 사용자가 성공적으로 인증하는 경우(예를 들어, 등록된 손가락을 지문 인증기 상에 스와이핑함), 인증 클라이언트(410)는 성공적 인증을 나타내는 인증 응답을 다시 전송한다. 인증 클라이언트(410)는 암호 논스 및/또는 인증기의 암호화 키를 사용하여 생성된 서명과 같은 다른 보안-관련된 데이터를 인증 응답과 함께 전송할 수 있다. 이어서 인증 서버(450)는 인증 응답을 검증할 수 있다(예를 들어, 암호 논스를 검증하고 대응하는 인증기 키를 사용하여 서명을 검증함). 검증이 성공적이면, 사용자는 원하는 트랜잭션을 수행하도록 허용될 것이다. 예를 들어, 일 실시예에서, 인증 서버(450)는 사용자가 트랜잭션을 완료할 수 있도록 성공적 인증의 표시를 신뢰자 웹 서버로 전송할 수 있다.

[0048] 일 실시예에서, 결과 분석 및 업데이트 모듈(412)은 성공적 인증 또는 실패한 인증 시도와 연관된 파라미터들을 분석하여, 이력 파라미터들 및 임계치들에 대한 업데이트들(409)을 생성한다. 예를 들어, 인증이 성공적이면,

현재 파라미터들(406)은 성공적 인증들과 연관된 이력 파라미터들(430)로서 추가될 수 있다(따라서 이들 파라미터와 연관된 "리스크성"을 감소시킴). 대조적으로, 인증이 실패하는 경우 그리고/또는 사기가 검출되는 경우, 결과 분석 및 업데이트 모듈(412)에 의해 생성된 업데이트는 현재 파라미터들(406) 중 하나 이상을 실패한 인증 시도들과 연관시킬 수 있다(예를 들어, 향후 인증 시도들에서의 그 파라미터들의 존재는 더 높은 리스크를 나타내게 됨). 예를 들어, 현재 파라미터들(406)이 사용자가 이전에 관찰되지 않은 위치에 있음을 나타내고 인증이 실패한 것으로 나타내는 경우, 결과 분석 및 업데이트 모듈(412)은 이 위치와 연관된 임계치들 및/또는 가중치들을 업데이트하여 이 위치와 연관된 리스크를 증가시킬 수 있다. 이어서, 생성된 데이터는 이력 인증 파라미터들 및 임계치 데이터베이스(430)와 통합된다. 기계 학습 알고리즘들(후술하는 바와 같음)을 포함하는 다양한 상이한 타입의 알고리즘들이, 결과 분석 및 업데이트 모듈(412)에 의해 이력 데이터에 대한 업데이트들을 제공하는 데 사용될 수 있다.

[0049] 이러한 방식으로, 결과 분석 및 업데이트 모듈(412)은 계속해서 새로운 인증 이벤트들(성공 및 실패)에 대한 상관(correlation)들을 분석 및 생성하고 그에 응답하여 기존 이력 데이터(430)를 업데이트한다. 이어서 리스크 분석 모듈(411)은 후속적인 인증 시도들에 대해 업데이트된 이력 데이터(430)를 사용할 수 있다. 도 4a 및 도 4b에서 개별 모듈들로 도시되었지만, 리스크 분석 모듈(411) 및 결과 분석 및 업데이트 모듈(412)은 계속해서 사용자 활동에 관련된 파라미터들을 평가하고 이력 데이터베이스(430)를 업데이트하기 위한 단일의 통합된 기계 학습 모듈로서 구현될 수 있다.

[0050] 일 실시예에서, 이력 파라미터들 및 임계치들(430)은 사용자의 "정상적" 패턴들에만 기초하여 설정된다. 즉, 실패한 인증 이벤트들 또는 사기성 활동들에 관련된 데이터를 통합하기보다는, 이력 파라미터들(430)은 성공적 인증 이벤트들에만 관련된 데이터를 포함하도록 업데이트될 수 있다. 따라서, 이 실시예에서, 리스크 분석 모듈(411)은 이 정상적 사용자 프로파일로부터의 편차를 측정하고 정상적 사용자 거동으로부터의 편차의 양에 기초하여(예를 들어, 후술하는 바와 같이 하나 이상의 임계치들을 넘었는지의 여부에 기초하여) 리스크 레벨(407)을 생성하려고 시도할 것이다.

[0051] 도 4b는, 리스크 분석 모듈(411) 및 결과 분석 및 업데이트 모듈(412)이 인증 서버(450) 상에서보다는(또는 인증 서버 상의 구현에 추가하여) 인증 클라이언트(410) 내에서 구현되는 실시예를 나타낸다. 도 4a에 도시된 서버측 실시예에서와 같이, 본 실시예에서 리스크 분석 모듈(411)은 현재 트랜잭션과 연관된 리스크 레벨(407)을 결정하기 위해 현재 파라미터들(406)과 이력 파라미터들(430) 사이의 상관들을 평가한다. 리스크 레벨(407)에 기초하여, 인증 클라이언트는 하나 이상의 인증 기술(408)을 선택하고 인증 결과들을 결과 분석 및 업데이트 모듈(412)에 제공하며, 이것은 이어서 현재 파라미터들(406) 및 인증 결과들에 기초하여 이력 파라미터들 및 임계치를 업데이트한다. 평가될 수 있는 다양한 특정 파라미터들 및 인증 결과들이 아래에 제공된다.

[0052] 일 실시예에서, 리스크 레벨(407)을 결정하기 위해 수집되고 평가되는 파라미터들은 각각의 사용자의 아이덴티티 및 인증 서버에 등록된 인증기들(420, 421)에 관련된 다양한 데이터를 포함할 수 있으며, 이는 예를 들어, 등록된 인증 장치(들)의 타입들을 고유하게 식별하는 인증 증명 ID들(AAID들); 인증기 등록 동안 교환된(그리고 클라이언트 및 인증 서버 상의 보안 저장소(425)에 저장된) 키들와 연관된 키 ID들; 키들로 생성된 암호 서명들을 확인하는 데 사용되는 암호 키 데이터; 서명들이 키들로 생성된 횟수를 나타내는 서명 카운터; 인증기들 각각의 버전을 나타내는 인증기 버전을 포함한다. 게다가, 리스크 레벨을 결정하기 위해 사용되는 파라미터들은 인증기들 각각과 연관된 메타데이터, 예컨대 AAID(위에서 언급함), 인증기 벤더, 인증기 타입(예를 들어, 인증기가 클라이언트의 내부에 있는지 외부에 있는지를 나타내는), 인증 인자(예를 들어, 지문, 성문, 존재 등), 및 키 보호 방법(예를 들어, 신뢰된 실행 환경, 보안 요소들 등)을 포함할 수 있다.

[0053] 보다 상세한 분석을 수행하기 위해, 본 발명의 일 실시예는 다음의 상이한 파라미터들 중 하나 이상을 수집하고 분석한다:

[0054] 1. 암호 키 사용 데이터에 관련된 파라미터들

[0055] ° 동작의 타임스탬프

[0056] ° 사용된 키의 KeyID

[0057] ° 수행된 인증 동작

[0058] ° 서명 검증의 성공 또는 실패의 표시

[0059] ° 동작과 연관된 트랜잭션 ID

[0060] ° 이 동작과 연관된 트랜잭션 리스크 점수

[0061] ° 최종 트랜잭션 인증 상태(성공 또는 실패)

[0062] 2. 키들의 상태 전환들에 관련된 파라미터들

[0063] ° 전환의 타임스탬프

[0064] ° 전환하는 키의 KeyID

[0065] ° 전환하는 인증기의 인증기 버전

[0066] ° 전환된 상태(예를 들어, 양호, 공격받는 중, 등록취소됨(deregistered), 복제됨, 손상됨)

[0067] 3. 인증-후 사기 보고들에 관련된 파라미터들

[0068] ° 사기의 타임스탬프

[0069] ° 사기성으로 보고된 트랜잭션의 트랜잭션 ID

[0070] 4. 키들의 이력 보안 강도에 관련된 파라미터들

[0071] ° 샘플링의 타임스탬프

[0072] ° 암호 키의 KeyID

[0073] ° 샘플링의 시간까지의 보안 강도

[0074] 5. 인증기들의 이력 보안 강도에 관련된 파라미터들

[0075] ° 샘플링의 타임스탬프

[0076] ° 인증기의 AAID

[0077] ° 샘플링의 시간까지의 보안 강도

[0078] 6. 대안 데이터 소스들로부터 수집된 추가 파라미터들

[0079] ° 사용자 장치 GPS 위치

[0080] ° WiFi를 둘러싸는 사용자 장치 정보

[0081] ° 사용자 장치의 디지털 지문

[0082] ° 사용자의 생체 측정 장치로부터 수집된 생체 측정 점수

[0083] 7. 사용자 활동 파라미터들

[0084] ° 사용자 등록의 타임스탬프

[0085] ° 마지막 성공적 로그인의 타임스탬프

[0086] ° 마지막 국지적 인증 방법 및 그것의 타임스탬프

[0087] 일 실시예에서, 리스크 분석 모듈(411)은 하기에 특정된 방식으로 파라미터들을 평가함으로써 현재 리스크 레벨(407)을 결정한다. 평가들은 (1) 클라이언트 장치 상의 AAID들 및 키들에 관련된 파라미터들; (2) 사용자 인증의 시간에 관련된 파라미터들; (3) 클라이언트 장치의 위치에 관련된 파라미터들; (4) 클라이언트 장치의 네트

워크 접속성에 관련된 파라미터들; 및 (5) (예를 들어, 사용자 인증 시도에 응답하여) 인증 클라이언트에 의해 생성된 생체 측정 점수에 관련된 파라미터들에 기초할 수 있다.

[0088] 1. AAID들 및 키들

[0089] 일 실시예에서, 암호 키 또는 AAID가 과거에 성공적으로 사용된 횟수는 그 암호 키 또는 AAID의 사용과 연관된 리스크를 감소시킬 것이다. 대조적으로, 암호 키 또는 AAID가 실패한 인증 시도 또는 시도된 사기와 연관된 횟수는 그 암호 키 또는 AAID와 연관된 리스크를 증가시킬 것이다. 일 실시예에서, 성공적 인증 시도들의 수는 다른 암호 키들 또는 AAID들을 사용하는 인증 시도들과 비교될 수 있다. 이 키/AAID가 다른 키들/AAID들보다 훨씬 덜 자주 사용되는 경우, 이것은 그것의 사용과 연관된 리스크 레벨을 증가시킬 수 있다.

[0090] 평가될 수 있는 다른 변수들은 암호 키가 사용된 마지막 시간 및 이 사용자가 임의의 인증기를 사용한 마지막 시간을 포함한다. 예를 들어, 사용자가 인증기(또는 임의의 인증기)를 장기간(예를 들어, 임계치 초과) 사용하지 않은 경우, 이것은 인증기와 연관된 리스크를 증가시킬 수 있다. 게다가, 암호 키가 복제된 적이 있는지 그리고/또는 이 AAID의 키들이 복제되는 빈도가 리스크를 결정하는 데 고려될 수 있다 (예를 들어, 더 많은 복제가 더 많은 리스크를 나타내는 것으로).

[0091] 평가될 수 있는 추가 변수들은 이 암호 키의 상태가 "공격받는 중(under_attack)"으로 변경된 빈도(따라서 더 큰 리스크를 나타냄), 이 사용자가 자신의 계정으로부터 인증기들을 삭제한 횟수, 사용자가 특정 AAID를 등록/등록취소한 횟수, 사용자들이 이 AAID를 등록취소한 빈도, 사용자가 등록취소할 것을 선택하기 전에 사용자가 이 AAID를 사용한 시간의 길이; 이 벤더가 임의의 인증기를 손상한 횟수; 이 인증기 버전이 손상된 횟수; 이 사용자가 상이한 특정된 기간들(예를 들어, 마지막 20초, 5분, 60분, 1일, 7일) 내에 인증기들을 등록하려고 시도한 횟수; 및 이 사용자가 마지막 특정된 기간(예를 들어, 20초, 5분, 60분, 1일, 7일) 내에 인증기를 사용해 인증하려고 시도한 횟수를 포함한다.

[0092] 2. 인증의 시간

[0093] 일 실시예에서, 사용자가 전형적으로 인증을 요청하는 하루 중 기간, 사용자가 전형적으로 인증을 요청하는 일/주/월별 횟수는 리스크를 결정하기 위해 평가될 수 있다. 예를 들어, 현재 인증 요청이 전형적인 시간 및/또는 일(day)에 있지 않은 경우 그리고/또는 인증이 일/주/월별로 요청된 횟수가 기준을 벗어나는 경우, 이것은 사기성 활동을 나타낼 수 있다. 평가될 수 있는 다른 변수는 이것이 이 특정 인증기에 대한 인증을 위한 적절한 시간인지 여부에 대한 표시이다.

[0094] 3. 위치

[0095] 일 실시예에서, 리스크를 결정하기 위해 평가된 위치 변수들은 이 인증기가 현재 위치 근처에서 발견된 횟수, 이 인증기가 주어진 위치 근처에서 발견된 마지막 시간, 이 위치 근처에서 과거에 발견된 사기의 양, 이 AAID를 사용해 이 위치에서 발견된 사기의 양, 이 사용자에 대한 보통의 위치들로부터 이 위치의 거리, 이 위치가 사용자가 마지막으로 인증한 위치로부터 떨어진 거리, 및 이 위치/국가와 연관된 일반적인 리스크를 포함한다.

[0096] 4. 네트워크 접속성

[0097] 일 실시예에서, 리스크를 결정하기 위해 평가된 네트워크 변수들은 이 사용자/키가 주어진 WiFi (또는 다른 네트워크) 범위 근처에서 발견된 횟수; 주어진 WiFi (또는 다른 네트워크) 범위 내의 장치가 사기성 활동들에 관여된 횟수; 및 주어진 WiFi가 현재 주장된 위치에서 실제로 이용가능할 가능성을 포함한다.

[0098] 5. 생체 측정 점수

[0099] 일 실시예에서, 클라이언트의 인증기(420, 421)에 의해 생성된 생체 측정 점수는 리스크를 결정하는 데 사용될 수 있다. 예를 들어, 생체 측정 점수의 통계적 평균이 이 AAID에 대해 결정될 수 있다. 현재 점수가 평균으로부터 특정된 거리이면, 이것은 더 큰 리스크를 나타낼 수 있다. 게다가, 이 특정 사용자에 대한 평균 생체 측정 점수는 현재 점수와 비교될 수 있다. 다시 한번 말하면, 현재 점수가 평균으로부터 특정된 거리이면, 이것은 더 큰 리스크를 나타낼 수 있다.

[0100] 본 발명의 일 실시예에서, 기계 학습 기술들이 사기성 활동 및/또는 적법한 활동(전술한 것들과 같은)을 나타내는 특정 파라미터들을 식별하는 데 채용된다. 도 5는 리스크를 평가하기 위한 파라미터들을 결정하고 평가하기 위한 방법의 일 실시예를 나타낸다. 이 방법은 도 4a 및 도 4b에 도시된 시스템 아키텍처들의 상황 내에서 구현될 수 있지만, 임의의 특정 시스템 아키텍처로 한정되지 않는다.

[0101] 501에서, 사기성 활동에 상관될 수 있는 많은 파라미터들이 선택된다. 일 실시예에서, 파라미터들의 초기 세트는, 파라미터들 및 인증 결과들이 파라미터들 및 사기성 및/또는 적법한 활동들 사이의 상관들을 식별하는 기계 학습 알고리즘에 대한 입력으로서 제공되는 트레이닝 프로세스를 사용해 선택된다. 최종 결과는, 적법한 그리고/또는 사기성 활동들에 높게 상관되는 소정 파라미터들이 식별된다는 것이다.

[0102] 502에서, 하나 이상의 임계치(T)가 파라미터들의 평가에 기초하여 선택된다. 일 실시예에서, 선택된 임계치들은 "사기성", "의심스러운" 및/또는 "정상적" 활동들 사이의 경계들을 정의한다. 예를 들어, 임계치들이, 인증 시도들이 "정상적"인 것으로 고려되는 시간 범위들에 대해 설정될 수 있다. 이 범위들 밖의 시간들은 의심스럽거나 사기성인 것으로 간주될 수 있으며 그에 따라 리스크 레벨을 증가시킬 수 있다. 다양한 다른 임계치들이 전술한 파라미터들 중 임의의 것 또는 전부를 사용하여 결정될 수 있다. 일 실시예에서, 임계치들은, 언급한 바와 같이, 사기성/적법한 활동과 다양한 파라미터들 사이의 상관을 식별하는 기계 학습 알고리즘에 의해 자동으로 설정될 수 있다.

[0103] 초기 파라미터들 및 임계치들이 결정되면, 503에서 현재 트랜잭션에 대한 파라미터들의 거리가 기존 이력 파라미터들과 비교된다. 이는 일 실시예에서 기계 학습 또는 데이터 세트들 사이의 상관들을 결정할 수 있는 다른 알고리즘을 사용하여 수학적 접근법으로 달성된다. 일반적으로, "정상적" 파라미터들까지의 거리가 클수록, 현재 트랜잭션과 연관된 리스크는 더 크다.

[0104] 평가에 뒤이어, 504에서, 파라미터들에 대한 최종 값이 이력 데이터 세트와 비교될 때 선택된 임계치(들) 내에 있는지 여부에 대한 결정이 이루어진다. 그렇지 않은 경우, 505에서 이것은 비정상적 활동(예를 들어, 의심스러운 또는 사기성)으로 결정되고, 사용자는 더 엄격한 인증 기술들(예를 들어, 명시적 생체 측정 인증)을 사용하여 인증하도록 요구될 수 있다. 도 4에 도시된 실시예에서, 리스크 레벨(407)은 증가될 수 있고, 이에 따라 더 엄격한 인증을 요구할 수 있다. 파라미터들이 선택된 임계치들 내에 있는 경우, 506에서 상호작용은 정상적 활동으로 간주되고 덜 엄격한(또는 엄격하지 않은) 인증이 사용될 수 있다(예를 들어, 전술한 바와 같은 비간섭적 인증).

[0105] 어느 경우이든, 506에서, 이력 데이터는 최근 인증 결과들을 반영하도록 업데이트된다. 이러한 방식으로, 의심스러운 또는 사기성 활동을 검출하는 데 사용된 이력 데이터는 새로운 데이터 포인트들 및 임계치들을 반영하도록 계속해서 업데이트될 수 있다. 예를 들어, 사용자가 비특징적 위치로부터 또는 비정상적 시간에 트랜잭션에 들어가는 경우, 이것은 505에서 비정상적 활동으로서 식별될 수 있다. 그러나, 사용자가 성공적으로 인증하는 경우, 506에서 이력 데이터는 적법한 사용자가 이 특정 위치 및 시간에 인증했다는 사실을 반영하도록 업데이트될 수 있다. 결과적으로, 이 특정 위치 및/또는 시간은 더 이상 "비정상적인" 것으로 간주되지 않을 수 있으며, 또는 보다 정확하게는, 이 위치 및/또는 시간과 연관된 "리스크성"은 감소될 수 있다.

[0106] 상이한 수학적 접근법들이 현재 트랜잭션의 파라미터들 및 이력 파라미터들 사이의 "거리"를 결정하는 데 사용될 수 있다(예를 들어, 도 5의 동작(503)). 하나의 특정 접근법은 가우스 분포(Gaussian distribution)에 기초할 수 있는 이상 검출(Anomaly Detection)로 알려져 있다. 아래의 논의는 이상 검출에 초점을 맞출 것이지만, 다양한 다른 기계 학습 알고리즘들이 또한 적용될 수 있다.

[0107] 본 발명의 일 실시예에 채용된 이상 검출 알고리즘이 도 6에 도시된다. 601에서, 사기성 활동을 나타내기 위해 사용될 수 있는 초기 파라미터들의 세트가 선택된다(P_1.. P_m). 이상적으로, 파라미터들은 사기성 및/또는 적법한 활동들과의 가장 강한 상관을 갖도록 선택된다. 전술한 바와 같이, 초기 파라미터들은 일정 기간 동안 수집된 기존 인증 데이터를 사용하는 트레이닝 프로세스를 사용하여 선택될 수 있다.

[0108] 602에서, 각각의 파라미터(P_i)에 대해, 기존 데이터 이력(h_1.. h_m)으로, 데이터세트는 그것이 충분히 가우스가 아닌 경우 정규화된다. 일단 정규화되면, 가우스 분포의 평균(μ) 및 분산(σ) 파라미터들은 데이터세트 이력(h_1.. h_m)에 기초하여 결정된다. 일 실시예에서, 이는 다음 식들을 사용하여 달성된다:

[0109] i. $$\mu_i = \frac{1}{m} \times \sum_{j=1}^{m} h_j$$

ii. $$\sigma_i^2 = \frac{1}{m} \times \sum_{j=1}^{m} (h_j - \mu_i)^2$$

[0110] 603에서, 파라미터들을 이용한 각각의 새로운 트랜잭션(X_1..X_m)에 대해, 각각의 새로운 파라미터에 대한 가우스

분포가 이력에 기초하여 계산된다. 일 실시예에서, 이것은 다음 식으로 달성된다:

[0111] i. $$p(x_i) = \frac{1}{\sigma_i\sqrt{2\pi}} \times e^{\frac{-(x_i-\mu_i)^2}{2\times\sigma_i^2}}$$

[0112] 604에서, $p(x)$가 조합된 모든 파라미터들에 대해 계산된다. 일 실시예에서, 이것은 다음 식에 따라 달성된다:

[0113] i. $$p(x) = \prod_{j=1}^{m} p(x_j)$$

[0114] 605에서 결정된, $p(x) < T$ (선택된 임계치)이면, 이것은 606에서 비정상적 거동으로 결정된다. 결과적으로, 하나 이상의 엄격한 인증 기술(예를 들어, 명시적 생체 측정 인증)이 요청될 수 있다. 그러나, $p(x) \geq T$이면, 607에서, 상호작용은 정상적 활동으로서 식별되고, 덜 엄격한 인증(예를 들어, 전술한 바와 같은 비간섭적 인증)이 요구되거나 인증이 요구되지 않을 수 있다.

[0115] 어느 경우이든, 608에서, 데이터세트 이력은 새로운 파라미터들(P_1.. P_m) 및 연관된 인증 결과들로 업데이트된다. 예를 들어, 인증이 606에서 성공적이었으면, 데이터세트 이력은 이들 파라미터와 연관된 성공적 인증을 반영하도록 업데이트될 수 있다.

[0116] 예시적인 데이터 처리 장치

[0117] 도 7은 본 발명의 일부 실시예들에서 사용될 수 있는 예시적인 클라이언트들 및 서버들을 나타내는 블록도이다. 도 7은 컴퓨터 시스템의 다양한 컴포넌트들을 도시하지만, 이것은 컴포넌트들을 상호접속하는 임의의 특정 아키텍처 또는 방식을 나타내는 것을 의도하지 않는다는 것을 이해해야 하는데, 이는 그러한 상세들이 본 발명과 밀접한 관련이 없기 때문이다. 더 적은 컴포넌트들 또는 더 많은 컴포넌트들을 갖는 다른 컴퓨터 시스템들도 본 발명과 관련하여 사용될 수 있다는 것을 알 것이다.

[0118] 도 7에 도시된 바와 같이, 데이터 처리 시스템의 형태인 컴퓨터 시스템(700)은 처리 시스템(720), 전원(725), 메모리(730) 및 비휘발성 메모리(740)(예를 들어, 하드 드라이브, 플래시 메모리, 상변화 메모리(PCM) 등)와 결합되는 버스(들)(750)를 포함한다. 버스(들)(750)는 당업계에 주지된 바와 같은 다양한 브리지, 제어기 및/또는 어댑터를 통해 서로 접속될 수 있다. 처리 시스템(720)은 메모리(730) 및/또는 비휘발성 메모리(740)로부터 명령어(들)를 회수하고, 명령어들을 실행하여 전술한 바와 같은 동작들을 수행할 수 있다. 버스(750)는 위의 컴포넌트들을 함께 상호접속하고, 또한 그러한 컴포넌트들을 옵션인 독(dock)(760), 디스플레이 제어기 및 디스플레이 장치(770), 입출력 장치들(780)(예를 들어, 네트워크 인터페이스 카드(NIC), 커서 제어(예를 들어, 마우스, 터치스크린, 터치패드 등), 키보드 등) 및 옵션인 무선 송수신기(들)(790)(예를 들어, 블루투스, 와이파이, 적외선 등)에 상호접속한다.

[0119] 도 8은 본 발명의 일부 실시예들에서 사용될 수 있는 예시적인 데이터 처리 시스템을 나타내는 블록도이다. 예를 들어, 데이터 처리 시스템(800)은 핸드헬드 컴퓨터, 개인 휴대 단말기(PDA), 이동 전화, 휴대용 게이밍 시스템, 휴대용 미디어 플레이어, 이동 전화, 미디어 플레이어 및/또는 게이밍 시스템을 포함할 수 있는 태블릿 또는 핸드헬드 컴퓨팅 장치일 수 있다. 다른 예로서, 데이터 처리 시스템(800)은 네트워크 컴퓨터, 또는 다른 장치 내의 내장된 처리 장치일 수 있다.

[0120] 본 발명의 일 실시예에 따르면, 데이터 처리 시스템(800)의 예시적인 아키텍처는 전술한 이동 장치들을 위해 사용될 수 있다. 데이터 처리 시스템(800)은 하나 이상의 마이크로프로세서 및/또는 집적 회로 상의 시스템을 포함할 수 있는 처리 시스템(820)을 포함한다. 처리 시스템(820)은 메모리(810), (하나 이상의 배터리를 포함하는) 전원(825), 오디오 입출력(840), 디스플레이 제어기 및 디스플레이 장치(860), 옵션인 입출력(850), 입력 장치(들)(870) 및 무선 송수신기(들)(830)와 결합된다. 도 8에 도시되지 않은 추가 컴포넌트들도 본 발명의 소정 실시예들에서 데이터 처리 시스템(800)의 일부일 수 있으며, 본 발명의 소정 실시예들에서는 도 8에 도시된 것보다 적은 컴포넌트들이 사용될 수 있다는 것을 알 것이다. 게다가, 도 8에 도시되지 않은 하나 이상의 버스가 당업계에 주지된 바와 같은 다양한 컴포넌트들을 상호접속하는 데 사용될 수 있는 것을 알 것이다.

[0121] 메모리(810)는 데이터 처리 시스템(800)에 의한 실행을 위해 데이터 및/또는 프로그램들을 저장할 수 있다. 오디오 입출력(840)은 마이크 및/또는 스피커를 포함하여, 예를 들어 스피커 및 마이크를 통해 음악을 재생하고/하거나 전화 기능을 제공할 수 있다. 디스플레이 제어기 및 디스플레이 장치(860)는 그래픽 사용자 인터페이스(GUI)를 포함할 수 있다. 무선(예를 들어, RF) 송수신기들(830)(예를 들어, 와이파이 송수신기, 적외선 송수신

기, 블루투스 송수신기, 무선 셀룰러 전화 송수신기 등)은 다른 데이터 처리 시스템들과 통신하는 데 사용될 수 있다. 하나 이상의 입력 장치(870)는 사용자가 시스템에 입력을 제공하는 것을 가능하게 한다. 이러한 입력 장치들은 키패드, 키보드, 터치 패널, 멀티 터치 패널 등일 수 있다. 옵션인 다른 입출력(850)은 독에 대한 커넥터일 수 있다.

[0122] 본 발명의 실시예들은 전술한 바와 같은 다양한 단계들을 포함할 수 있다. 단계들은 범용 또는 특수 목적 프로세서가 소정 단계들을 수행하게 하는 기계 실행 가능 명령어들로 구현될 수 있다. 대안적으로, 이러한 단계들은 단계들을 수행하기 위한 하드와이어드 로직을 포함하는 특정 하드웨어 컴포넌트들에 의해, 또는 프로그래밍된 컴퓨터 컴포넌트들과 맞춤형 하드웨어 컴포넌트들의 임의의 조합에 의해 수행될 수 있다.

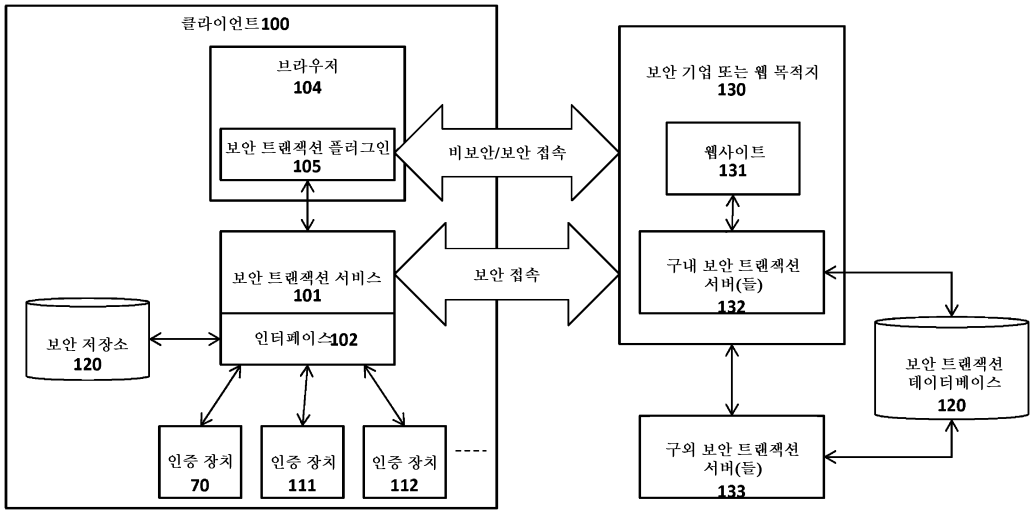
[0123] 본 발명의 요소들은 또한 기계 실행 가능 프로그램 코드를 저장하기 위한 기계 판독 가능 매체로서 제공될 수 있다. 기계 판독 가능 매체는 플로피 디스켓, 광 디스크, CD-ROM 및 광자기 디스크, ROM, RAM, EPROM, EEPROM, 자기 또는 광학 카드, 또는 전자 프로그램 코드를 저장하기에 적합한 다른 타입의 매체/기계 판독 가능 매체를 포함할 수 있지만 이에 한정되지 않는다.

[0124] 위의 설명 전반에서는, 설명의 목적으로, 본 발명의 완전한 이해를 제공하기 위해, 다수의 구체적인 상세들이 설명되었다. 그러나, 본 발명은 이러한 구체적인 상세들 중 일부 없이도 실시될 수 있다는 것이 당업자에게 명백할 것이다. 예를 들어, 본 명세서에서 설명되는 기능 모듈들 및 방법들은 소프트웨어, 하드웨어 또는 이들의 임의의 조합으로서 구현될 수 있다는 것을 당업자가 손쉽게 알 수 있을 것이다. 더욱이, 본 명세서에서는 본 발명의 일부 실시예들이 이동 컴퓨팅 환경의 상황 내에서 설명되지만, 본 발명의 기본 원리들은 이동 컴퓨팅 구현으로 한정되지 않는다. 예를 들어 데스크탑 또는 워크스테이션 컴퓨터들을 비롯한 사실상 임의의 타입의 클라이언트 또는 피어 데이터 처리 장치들이 일부 실시예들에서 사용될 수 있다. 따라서, 본 발명의 범주 및 사상은 아래의 청구범위의 관점에서 판단되어야 한다.

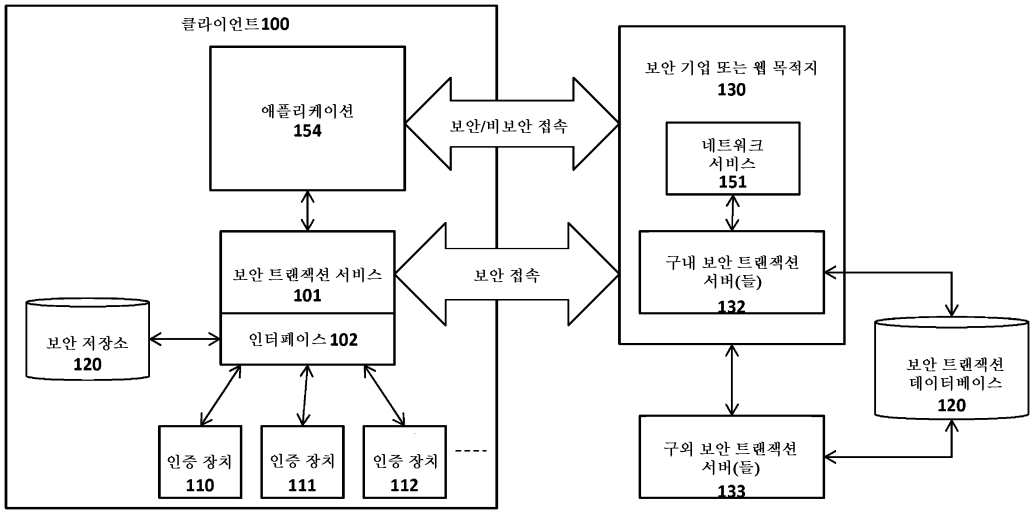
[0125] 본 발명의 실시예들은 전술한 바와 같은 다양한 단계들을 포함할 수 있다. 단계들은 범용 또는 특수 목적 프로세서가 소정 단계들을 수행하게 하는 기계 실행 가능 명령어들로 구현될 수 있다. 대안적으로, 이러한 단계들은 단계들을 수행하기 위한 하드와이어드 로직을 포함하는 특정 하드웨어 컴포넌트들에 의해, 또는 프로그래밍된 컴퓨터 컴포넌트들과 맞춤형 하드웨어 컴포넌트들의 임의의 조합에 의해 수행될 수 있다.

도면

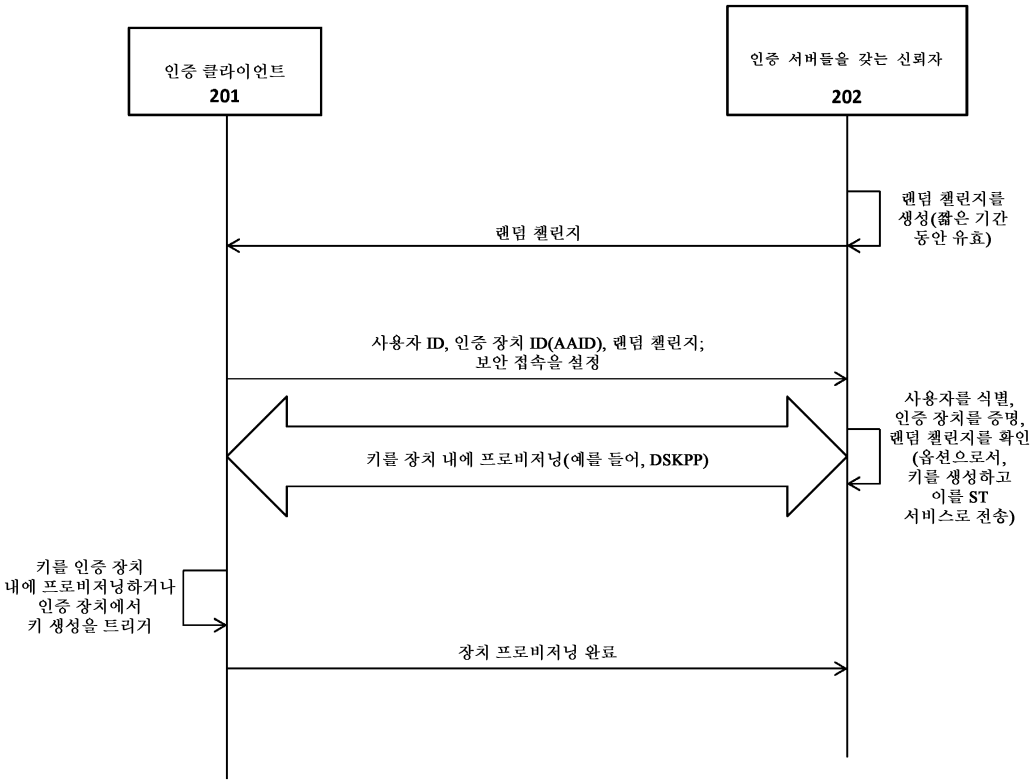
도면1a



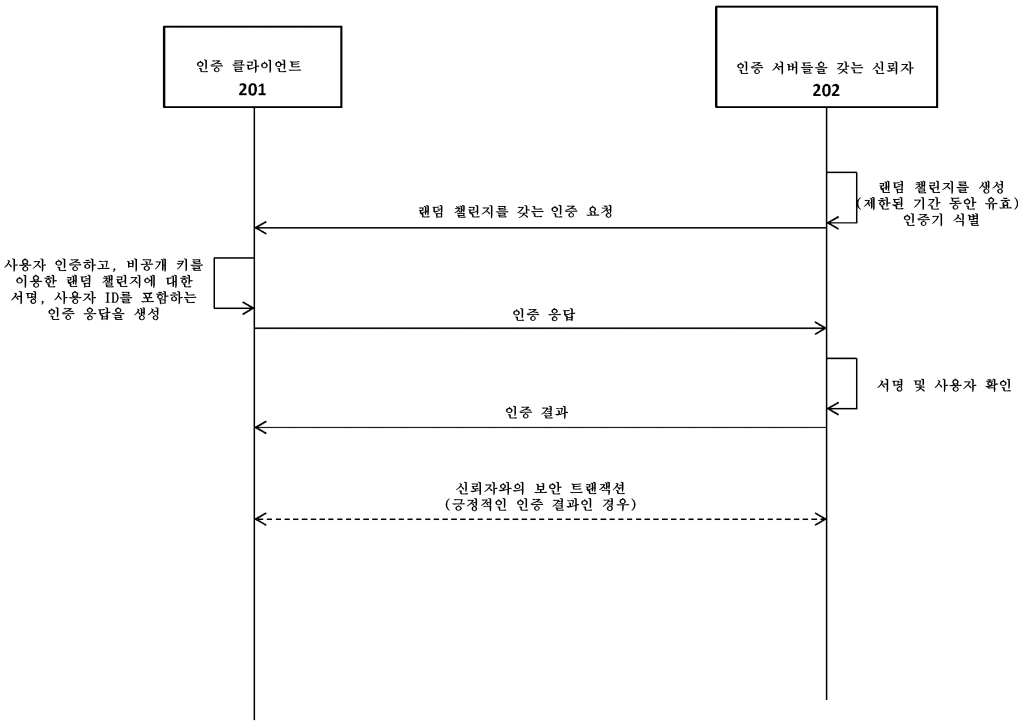
도면1b


클라이언트100
애플리케이션
154
보안/비보안 접속
보안 기업 또는 웹 목적지
130
네트워크
서비스
151
보안 트랜잭션 서비스
101
보안 접속
구내 보안 트랜잭션
서버(들)
132
보안 저장소
120
인터페이스 102
보안 트랜잭션
데이터베이스
120
인증 장치
110
인증 장치
111
인증 장치
112
구외 보안 트랜잭션
서버(들)
133

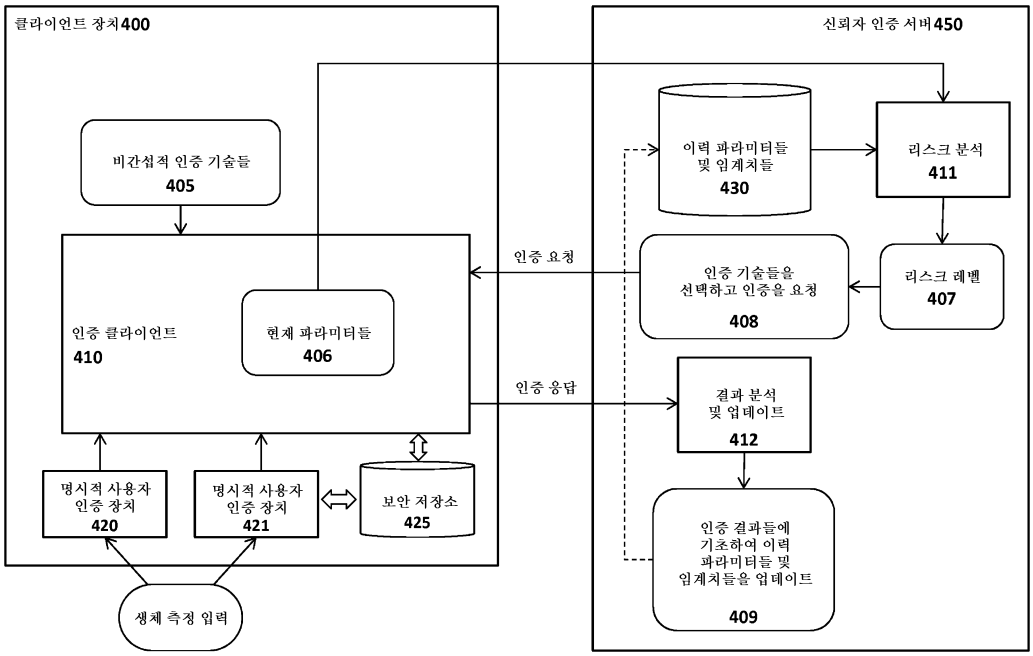
도면2


인증 클라이언트
201
인증 서버들을 갖는 신뢰자
202
랜덤 챌린지를
생성(짧은 기간
동안 유효)
랜덤 챌린지
사용자 ID, 인증 장치 ID(AAID), 랜덤 챌린지;
보안 접속을 설정
사용자를 식별,
인증 장치를 증명,
랜덤 챌린지를 확인
(옵션으로서,
키를 생성하고
이를 ST
서비스로 전송)
키를 장치 내에 프로비저닝(예를 들어, DSKPP)
키를 인증 장치
내에 프로비저닝하거나
인증 장치에서
키 생성을 트리거
장치 프로비저닝 완료

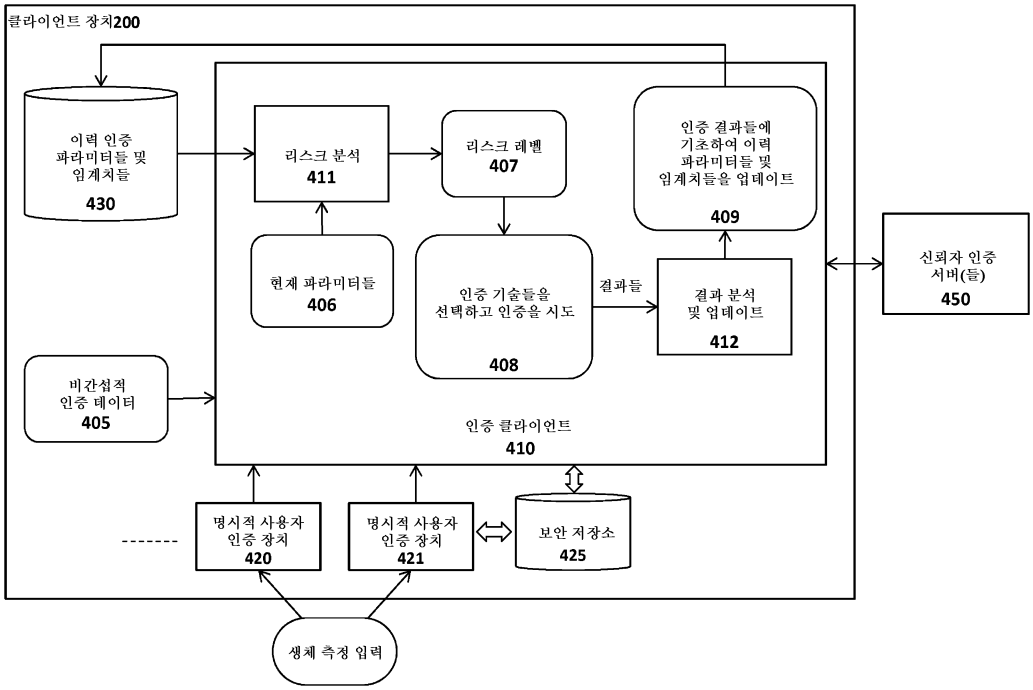
도면3


인증 클라이언트
201
인증 서버들을 갖는 신뢰자
202
랜덤 챌린지를 생성
(제한된 기간 동안 유효)
인증기 식별
랜덤 챌린지를 갖는 인증 요청
사용자 인증하고, 비공개 키를
이용한 랜덤 챌린지에 대한
서명, 사용자 ID를 포함하는
인증 응답을 생성
인증 응답
서명 및 사용자 확인
인증 결과
신뢰자와의 보안 트랜잭션
(긍정적인 인증 결과인 경우)

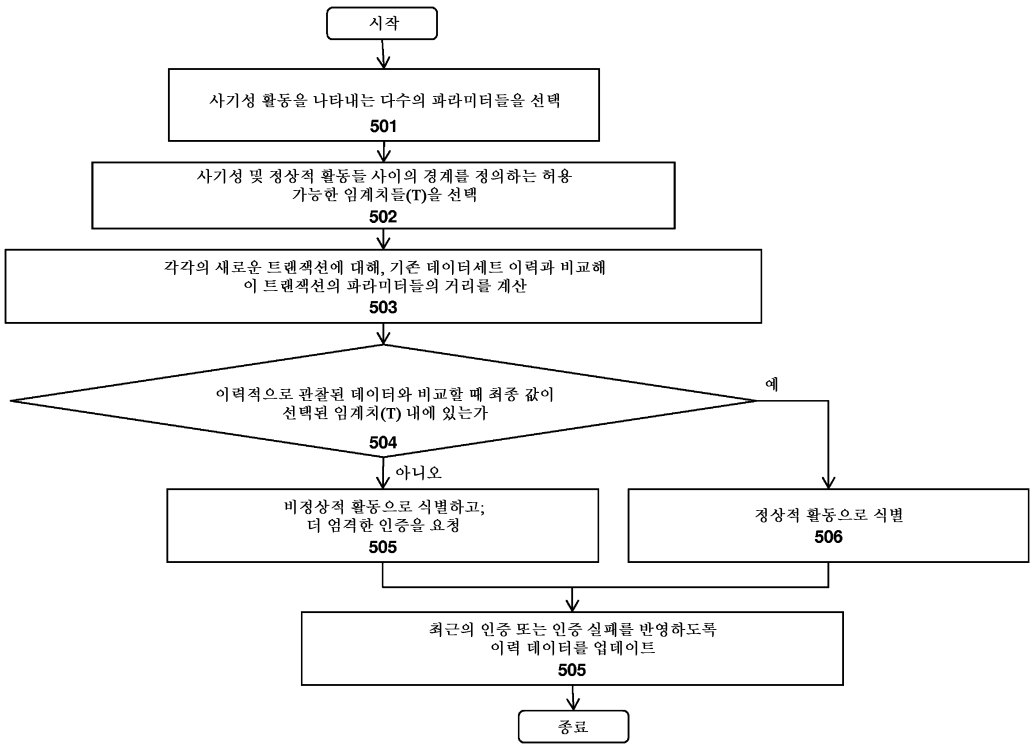
도면4a


클라이언트 장치400
신뢰자 인증 서버450
비간섭적 인증 기술들
405
이력 파라미터들
및 임계치들
430
리스크 분석
411
인증 요청
인증 기술들을
선택하고 인증을 요청
408
리스크 레벨
407
인증 클라이언트
410
현재 파라미터들
406
인증 응답
결과 분석
및 업데이트
412
명시적 사용자
인증 장치
420
명시적 사용자
인증 장치
421
보안 저장소
425
인증 결과들에
기초하여 이력
파라미터들 및
임계치들을 업데이트
409
생체 측정 입력

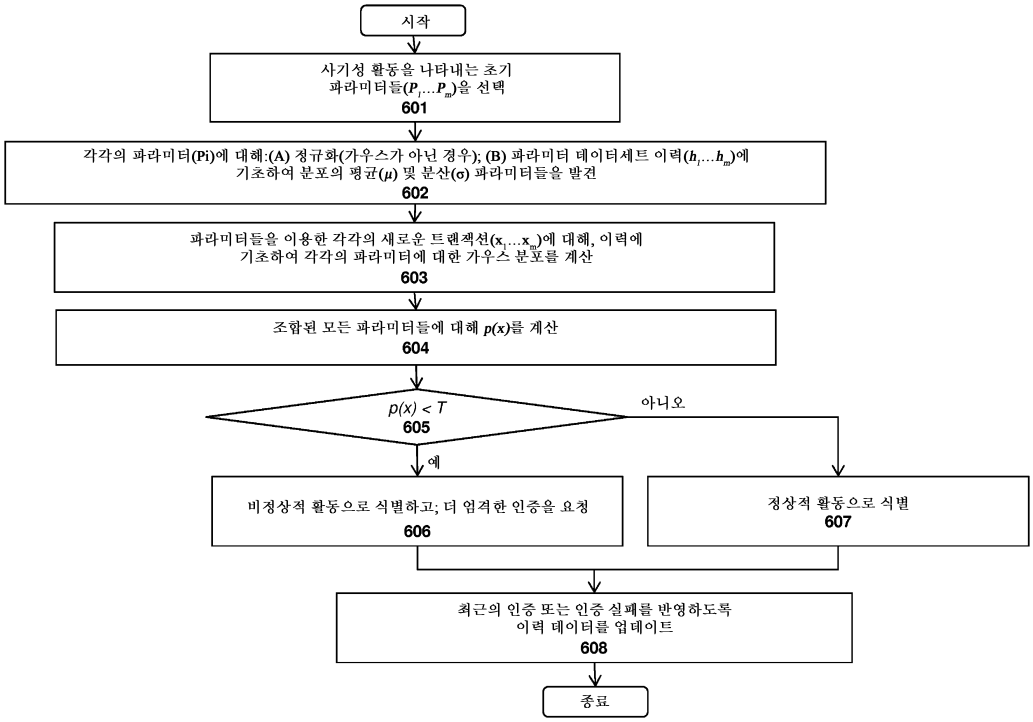
도면4b


클라이언트 장치200
이력 인증 파라미터들 및 임계치들
430
리스크 분석
411
리스크 레벨
407
인증 결과들에 기초하여 이력 파라미터들 및 임계치들을 업데이트
409
현재 파라미터들
406
인증 기술들을 선택하고 인증을 시도
408
결과들
결과 분석 및 업데이트
412
신뢰자 인증 서버(들)
450
비간섭적 인증 데이터
405
인증 클라이언트
410
명시적 사용자 인증 장치
420
명시적 사용자 인증 장치
421
보안 저장소
425
생체 측정 입력

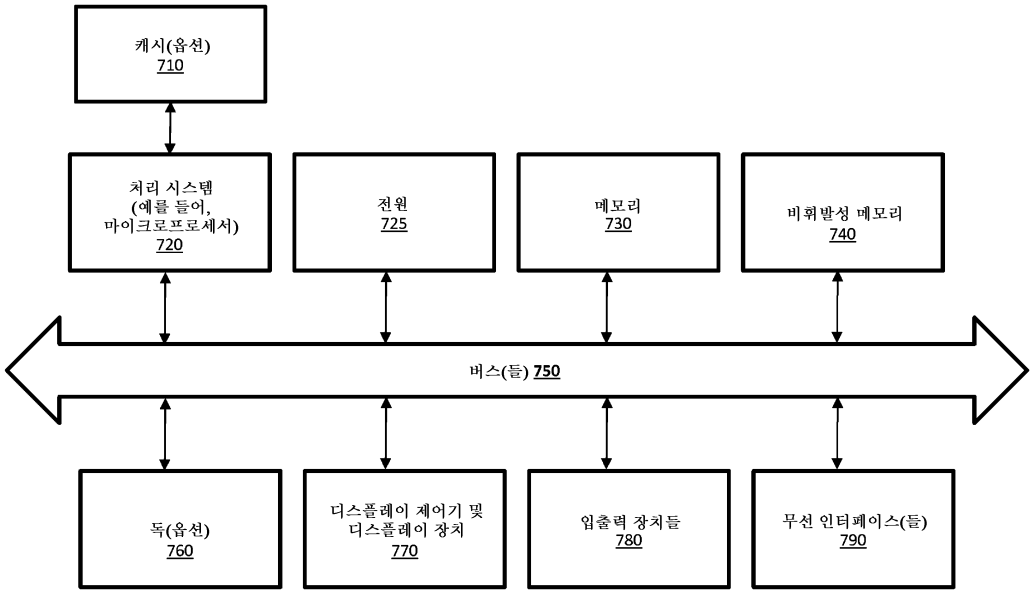
도면5


시작
사기성 활동을 나타내는 다수의 파라미터들을 선택
501
사기성 및 정상적 활동들 사이의 경계를 정의하는 허용 가능한 임계치들(T)을 선택
502
각각의 새로운 트랜잭션에 대해, 기존 데이터세트 이력과 비교해 이 트랜잭션의 파라미터들의 거리를 계산
503
이력적으로 관찰된 데이터와 비교할 때 최종 값이 선택된 임계치(T) 내에 있는가
504
예
아니오
비정상적 활동으로 식별하고; 더 엄격한 인증을 요청
505
정상적 활동으로 식별
506
최근의 인증 또는 인증 실패를 반영하도록 이력 데이터를 업데이트
505
종료

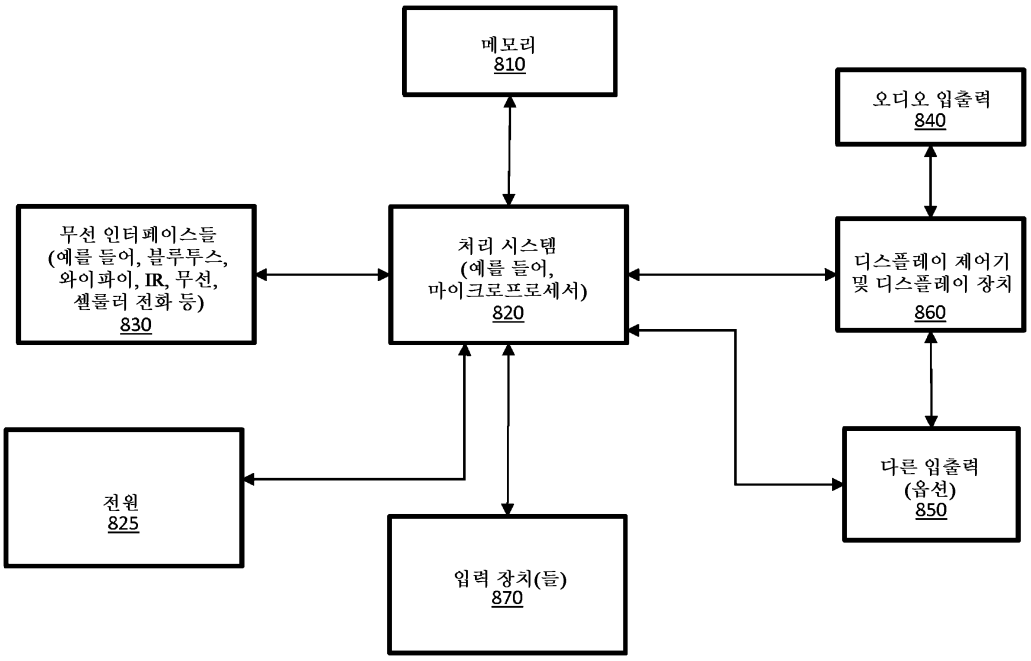
도면6


시작
사기성 활동을 나타내는 초기 파라미터들($P_1,...P_m$)을 선택
601
각각의 파라미터(Pi)에 대해:(A) 정규화(가우스가 아닌 경우); (B) 파라미터 데이터세트 이력($h_1,...h_m$)에 기초하여 분포의 평균(μ) 및 분산(σ) 파라미터들을 발견
602
파라미터들을 이용한 각각의 새로운 트랜잭션($x_1,...x_m$)에 대해, 이력에 기초하여 각각의 파라미터에 대한 가우스 분포를 계산
603
조합된 모든 파라미터들에 대해 $p(x)$를 계산
604
$p(x) < T$
605
아니오
예
비정상적 활동으로 식별하고; 더 엄격한 인증을 요청
606
정상적 활동으로 식별
607
최근의 인증 또는 인증 실패를 반영하도록 이력 데이터를 업데이트
608
종료

도면7


캐시(옵션)
710
처리 시스템 (예를 들어, 마이크로프로세서)
720
전원
725
메모리
730
비휘발성 메모리
740
버스(들) 750
독(옵션)
760
디스플레이 제어기 및 디스플레이 장치
770
입출력 장치들
780
무선 인터페이스(들)
790

도면8


메모리
810
오디오 입출력
840
무선 인터페이스들
(예를 들어, 블루투스,
와이파이, IR, 무선,
셀룰러 전화 등)
830
처리 시스템
(예를 들어,
마이크로프로세서)
820
디스플레이 제어기
및 디스플레이 장치
860
전원
825
다른 입출력
(옵션)
850
입력 장치(들)
870