(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년08월10일
(11) 등록번호 10-2141836
(24) 등록일자 2020년07월31일

(51) 국제특허분류(Int. Cl.)
G06Q 20/42 (2012.01) *G06F 21/00* (2006.01)
G06F 21/43 (2013.01) *H04L 29/06* (2006.01)
(52) CPC특허분류
G06Q 20/425 (2013.01)
G06F 21/00 (2018.05)
(21) 출원번호 10-2019-7002737(분할)
(22) 출원일자(국제) 2014년06월20일
심사청구일자 2019년01월28일
(85) 번역문제출일자 2019년01월28일
(65) 공개번호 10-2019-0014124
(43) 공개일자 2019년02월11일
(62) 원출원 특허 10-2015-7033482
원출원일자(국제) 2014년06월20일
심사청구일자 2015년11월24일
(86) 국제출원번호 PCT/US2014/043347
(87) 국제공개번호 WO 2014/209781
국제공개일자 2014년12월31일
(30) 우선권주장
14/309,538 2014년06월19일 미국(US)
201310252777.2 2013년06월24일 중국(CN)
(56) 선행기술조사문헌
KR1020100046128 A*
(뒷면에 계속)
전체 청구항 수 : 총 11 항

(73) 특허권자
알리바바 그룹 홀딩 리미티드
케이만군도, 그랜드 케이만, 피오박스 847, 원 캐피탈 플레이스 4층
(72) 발명자
차오 카이
중국 311121 항저우 위항 디스트릭 넘버 969 웨스트 웬 이 로드 빌딩 3 5층 알리바바 그룹 리갈 디파트먼트
(74) 대리인
장훈

심사관 : 박장환

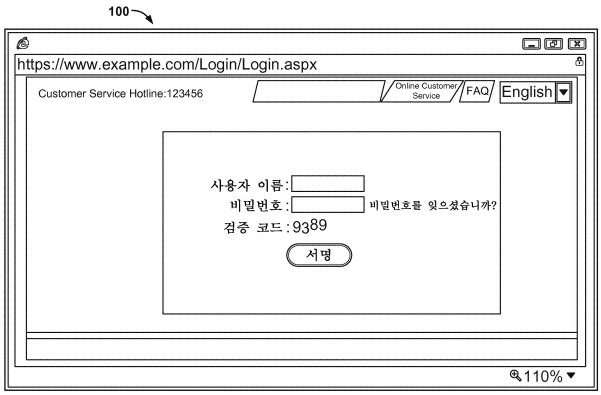
(54) 발명의 명칭 **이중 인증**

(57) 요 약

본 발명의 실시예들은 사용자 신원을 인증하기 위한 방법, 사용자 신원을 인증하기 위한 시스템, 및 사용자 신원을 인증하기 위한 컴퓨터 프로그램 제품에 관련한 것이다. 사용자 신원을 인증하기 위한 방법이 제공된다. 상기 방법은 서버에 의해 제 1 검증 코드를 생성하는 단계, 사용자 신원 인증을 요구하는 서비스의 애플리케이션 시나

(뒷면에 계속)

대 표 도



리오에서 상기 제 1 검증 코드를 사용자에게 디스플레이하는 단계, 사용자에 의해 전송된 제 2 검증 코드를 상기 애플리케이션 시나리오 외의 다른 애플리케이션을 통해 수신하는 단계, 사용자에 의해 전송된 제 2 검증 코드를 서버에 의해 생성된 제 1 검증 코드와 비교하는 단계, 및 상기 사용자가 사용자 신원을 통과했는지의 여부를 상기 비교의 결과를 기초로 하여, 결정하는 단계를 포함한다.

(52) CPC특허분류
G06F 21/43 (2013.01)
H04L 63/08 (2013.01)
H04L 63/18 (2013.01)

(56) 선행기술조사문헌
KR1020070078051 A*
KR1020120044329 A*
KR1020130045134 A
KR1020060015964 A
KR1020010087564 A
JP2007108973 A
KR100949055 B1*
KR1020110081977 A*
*는 심사관에 의하여 인용된 문헌

명 세 서

청구범위

청구항 1

사용자 신원을 인증하기 위한 방법에 있어서,

서버에 의해 제 1 검증 코드를 생성하는 단계로서, 상기 제 1 검증 코드는 사용자의 휴대폰 번호에 대응하고, 상기 사용자의 상기 휴대폰 번호는 등록 동안 상기 서버에 저장되고, 상기 제 1 검증 코드를 생성하는 단계는 상기 사용자의 상기 휴대폰 번호 및 상기 서버에 등록된 사용자 ID와 함께 상기 제 1 검증 코드를 저장하는 단계를 포함하는, 상기 제 1 검증 코드를 생성하는 단계;

상기 서버를 이용하여, 사용자 신원 인증을 요구하는 서비스의 애플리케이션 시나리오에서 상기 사용자에게 상기 제 1 검증 코드를 디스플레이하는 단계로서, 상기 사용자 신원 인증은 상기 사용자에 의해 입력된 사용자 이름 및 비밀번호를 수신하는 단계를 포함하는, 상기 제 1 검증 코드를 디스플레이하는 단계;

상기 서버를 이용하여, 프롬프트를 디스플레이하는 단계로서,

상기 애플리케이션 시나리오 외의 애플리케이션을 사용하여 상기 서버로 제 2 검증 코드를 전송하라고 상기 사용자에게 명령하는 상기 프롬프트를 상기 애플리케이션 시나리오에 디스플레이하는 단계를 포함하고, 상기 애플리케이션 시나리오 및 상기 애플리케이션 시나리오 외의 애플리케이션은 동일한 단말 장치 상에서 구현되고, 상기 애플리케이션 시나리오 외의 애플리케이션은 텍스트 메시징 애플리케이션에 대응하는, 상기 프롬프트를 디스플레이하는 단계;

상기 서버를 이용하여, 상기 사용자에 의해 전송된 상기 제 2 검증 코드를 상기 애플리케이션 시나리오 외의 상기 애플리케이션을 통해 수신하는 단계로서, 상기 제 2 검증 코드는 상기 사용자의 다른 전화번호에 대응하는, 상기 제 2 검증 코드를 수신하는 단계;

상기 사용자의 상기 휴대폰 번호를 상기 사용자의 상기 다른 전화번호와 비교하는 것을 포함하는, 상기 서버를 이용하여, 상기 사용자에 의해 전송된 상기 제 2 검증 코드와 상기 서버에 의해 생성된 상기 제 1 검증 코드를 비교하는 단계; 및

상기 서버를 이용하여, 상기 사용자가 신원 인증을 통과했는지의 여부를 상기 비교의 결과를 기초로 하여 결정하는 단계를 포함하고, 상기 사용자가 신원 인증을 통과했는지의 여부를 결정하는 단계는:

상기 제 2 검증 코드가 상기 제 1 검증코드와 일치한다는 결정에 응답하여,

상기 제 1 검증 코드를 이용하여 상기 서버에 등록된 상기 저장된 사용자 ID를 검색하는 단계;

상기 애플리케이션 시나리오 외의 상기 애플리케이션의 사용자 ID를 상기 서버에 등록된 상기 저장된 사용자 ID와 비교하는 단계; 및

상기 애플리케이션 시나리오 외의 상기 애플리케이션의 상기 사용자 ID가 상기 서버에 등록된 상기 저장된 사용자 ID와 일치한다는 결정에 응답하여, 상기 사용자가 신원 인증을 통과했다고 결정하는 단계를 포함하는, 사용자 신원을 인증하기 위한 방법.

청구항 2

삭제

청구항 3

제 1 항에 있어서,

사용자 신원 인증을 요구하는 상기 서비스의 상기 애플리케이션 시나리오는 웹 페이지 또는 클라이언트 애플리케이션에 대응하는, 사용자 신원을 인증하기 위한 방법.

청구항 4

제 1 항에 있어서,

상기 애플리케이션 시나리오 외의 상기 애플리케이션은 메시지를 상기 사용자에게 전송할 수 있는 애플리케이션에 대응하고;

상기 메시지는 상기 제 2 검증 코드를 포함하는, 사용자 신원을 인증하기 위한 방법.

청구항 5

삭제

청구항 6

제 4 항에 있어서,

상기 메시지는 텍스트 메시지에 대응하는, 사용자 신원을 인증하기 위한 방법.

청구항 7

제 1 항에 있어서, 상기 제 1 검증 코드는 무작위로 생성되는, 사용자 신원을 인증하기 위한 방법.

청구항 8

사용자 신원을 인증하기 위한 시스템에 있어서,

적어도 하나의 프로세서로서:

서버에 의해 제 1 검증 코드를 생성하고, 상기 제 1 검증 코드는 사용자의 휴대폰 번호에 대응하고, 상기 사용자의 상기 휴대폰 번호는 등록 동안 상기 서버에 저장되고, 상기 제 1 검증 코드의 생성은 상기 사용자의 상기 휴대폰 번호 및 상기 서버에 등록된 사용자 ID와 함께 상기 제 1 검증 코드를 저장하는 것을 포함하고;

사용자 신원 인증을 요구하는 서비스의 애플리케이션 시나리오에서, 상기 제 1 검증 코드를 상기 사용자에게 디스플레이하고, 상기 사용자 신원 인증은 상기 사용자에 의해 입력된 사용자 이름 및 비밀번호를 수신하는 것을 포함하고;

프롬프트를 디스플레이하고,

상기 애플리케이션 시나리오에 상기 프롬프트를 디스플레이하고, 상기 프롬프트는 상기 애플리케이션 시나리오 외의 애플리케이션을 사용하여 상기 서버로 제 2 검증 코드를 전송하라고 상기 사용자에게 명령하고, 상기 애플리케이션 시나리오 및 상기 애플리케이션 시나리오 외의 애플리케이션은 동일한 단말 장치 상에서 구현되고, 상기 애플리케이션 시나리오 외의 애플리케이션은 텍스트 메시징 애플리케이션에 대응하고;

상기 사용자에 의해 전송된 상기 제 2 검증 코드를 상기 애플리케이션 시나리오 외의 애플리케이션을 통해 수신하고, 상기 제 2 검증 코드는 상기 사용자의 다른 전화번호에 대응하고;

상기 사용자의 상기 휴대폰 번호를 상기 사용자의 상기 다른 전화번호와 비교하는 것을 포함하여, 상기 사용자에 의해 전송된 상기 제 2 검증 코드와 상기 서버에 의해 생성된 상기 제 1 검증 코드를 비교하고;

상기 제 2 검증 코드가 상기 제 1 검증 코드와 일치한다는 결정에 응답하여,

상기 제 1 검증 코드를 이용하여 상기 서버에 등록된 상기 저장된 사용자 ID를 검색하는 것;

상기 애플리케이션 시나리오 외의 상기 애플리케이션의 사용자 ID를 상기 서버에 등록된 상기 저장된 사용자 ID와 비교하는 것; 및

상기 애플리케이션 시나리오 외의 상기 애플리케이션의 상기 사용자 ID가 상기 서버에 등록된 상기 저장된 사용자 ID와 일치한다는 결정에 응답하여, 상기 사용자가 신원 인증을 통과했다고 결정하는 것을 포함하여, 상기 사용자가 신원 인증을 통과했는지의 여부를 상기 비교의 결과를 기초로 하여 결정하도록 구성된 적어도 하나의 프로세서; 및

상기 적어도 하나의 프로세서에 연결되고 상기 적어도 하나의 프로세서에 명령어들을 제공하도록 구성된 메모리를 포함하는, 사용자 신원을 인증하기 위한 시스템.

청구항 9

삭제

청구항 10

제 8 항에 있어서,

사용자 신원의 인증을 요구하는 상기 서비스의 상기 애플리케이션 시나리오는 웹 페이지 또는 클라이언트 애플리케이션인, 사용자 신원을 인증하기 위한 시스템.

청구항 11

제 8 항에 있어서,

상기 애플리케이션 시나리오 외의 상기 애플리케이션은 상기 서버에 메시지를 전송할 수 있는 애플리케이션에 대응하고;

상기 메시지는 상기 제 2 검증 코드를 포함하는, 사용자 신원을 인증하기 위한 시스템.

청구항 12

삭제

청구항 13

제 11 항에 있어서,

상기 메시지는 텍스트 메시지에 대응하는, 사용자 신원을 인증하기 위한 시스템.

청구항 14

컴퓨터 명령어들을 포함하고, 사용자 신원을 인증하기 위한 컴퓨터 프로그램을 저장한 유형의 비-일시적 컴퓨터 판독가능한 저장 매체에 있어서,

상기 컴퓨터 명령어들은

서버에 의해 제 1 검증 코드를 생성하고, 상기 제 1 검증 코드는 사용자의 휴대폰 번호에 대응하고, 상기 사용자의 상기 휴대폰 번호는 등록 동안 상기 서버에 저장되고, 상기 제 1 검증 코드의 생성은 상기 사용자의 상기 휴대폰 번호 및 상기 서버에 등록된 사용자 ID와 함께 상기 제 1 검증 코드를 저장하는 것을 포함하고;

사용자 신원 인증을 요구하는 서비스의 애플리케이션 시나리오에서 상기 제 1 검증 코드를 상기 사용자에게 디스플레이하고, 상기 사용자 신원 인증은 상기 사용자에 의해 입력된 사용자 이름 및 비밀번호를 수신하는 것을 포함하고;

프롬프트를 디스플레이하고,

상기 애플리케이션 시나리오에 상기 프롬프트를 디스플레이하고, 상기 프롬프트는 상기 애플리케이션 시나리오 외의 애플리케이션을 사용하여 상기 서버로 제 2 검증 코드를 전송하라고 상기 사용자에게 명령하고, 상기 애플리케이션 시나리오 및 상기 애플리케이션 시나리오 외의 애플리케이션은 동일한 단말 장치 상에서 구현되고, 상기 애플리케이션 시나리오 외의 애플리케이션은 텍스트 메시징 애플리케이션에 대응하고;

사용자에 의해 전송된 상기 제 2 검증 코드를 상기 애플리케이션 시나리오 외의 애플리케이션을 통해 수신하고, 상기 제 2 검증 코드는 상기 사용자의 다른 전화번호에 대응하고;

상기 사용자의 상기 휴대폰 번호를 상기 사용자의 상기 다른 전화번호와 비교하는 것을 포함하여, 상기 사용자에 의해 전송된 상기 제 2 검증 코드를 상기 서버에 의해 생성된 상기 제 1 검증 코드와 비교하고;

상기 제 2 검증 코드가 상기 제 1 검증코드와 일치한다는 결정에 응답하여,

상기 제 1 검증 코드를 이용하여 상기 서버에 등록된 상기 저장된 사용자 ID를 검색하는 것;

상기 애플리케이션 시나리오 외의 상기 애플리케이션의 사용자 ID를 상기 서버에 등록된 상기

저장된 사용자 ID와 비교하는 것; 및

상기 애플리케이션 시나리오 외의 상기 애플리케이션의 상기 사용자 ID가 상기 서버에 등록된 상기 저장된 사용자 ID와 일치한다는 결정에 응답하여, 상기 사용자가 신원 인증을 통과했다고 결정하는 것을 포함하여, 상기 사용자가 신원 인증을 통과했는지의 여부를 상기 비교의 결과를 기초로 하여 결정하기 위한 컴퓨터 명령어들인, 유형의 비-일시적 컴퓨터 판독가능한 저장 매체.

청구항 15

제 1 항에 있어서,

상기 애플리케이션 시나리오 외의 상기 애플리케이션에 디스플레이된 상기 프롬프트는 텍스트 메시지를 디플레이된 전화번호로 전송하라고 상기 사용자에게 명령하는, 사용자 신원을 인증하기 위한 방법.

청구항 16

삭제

발명의 설명

기 술 분 야

[0001] 본 출원은 본 명세서에 모든 목적들을 위해 참조로 포함되는, 2013년 6월 24일자 출원되고 발명의 명칭이 "사용자 신원을 인증하기 위해 사용된 방법 및 장치"(A METHOD AND DEVICE USED TO AUTHENTICATE USER IDENTITY)인 중화 인민 공화국 특허 출원 번호 201310252777.2 를 우선권으로 주장한다.

[0002] 본 출원은 사용자 신원을 인증하기 위한 방법 및 시스템에 관한 것이다.

배 경 기 술

[0003] 인터넷의 발전과 함께, 이전에 현실에서 대면하여 수행된 많은 활동들이 점차적으로 인터넷을 통한 통신들로 대체되고 있다.

[0004] 네트워크 애플리케이션들의 확산으로, 온라인 쇼핑 및 온라인 결재를 위한 네트워크 애플리케이션들을 사용하는 사람들의 수가 증가하고 있다. 보안을 보장하기 위해서, 동작을 수행하기 위해 온라인 뱅킹과 같은 높은 보안 요구사항들을 갖는 시스템들에 액세스하는 경우, 사용자들은 일반적으로 처음에 그들의 신원("신원 검증"(identity verification) 또는 "허가"(authorization)로 또한 알려진)을 인증하도록 요구받는다. 사용자의 신원이 요구 사항들의 세트에 부합하는 경우에만 사용자는 유효한 사용자로 확인된다.

[0005] 하나의 종래의 신원 인증 방법은 다음과 같다: 사용자가 시스템에 액세스할 경우, 시스템이 위치한 서버가 통신 서비스 또는 SMS 서비스 인터페이스를 사용하는 단문 메시지 시스템(SMS : short message system)를 통해 사용자의 휴대폰에 텍스트 메시지를 보내고, 텍스트 메시지는 서버에 의해 임의로 생성된 검증 코드(verification code)를 포함한다. 이러한 텍스트 메시지를 수신하자마자, 사용자는 시스템의 로그인 화면으로 텍스트 메시지에 포함된 검증 코드를 입력한다. 이어서, 입력된 검증 코드는 서버로 전송된다. 서버는 수신된 검증 코드를 이전에 전송된 검증 코드에 대해 비교한다. 두 코드가 일치하면, 사용자는 인증된 것으로 판정된다.

[0006] 특히, 무작위 숫자(a random number)가 서버에서 생성되고 텍스트 메시지를 통해 지정된 휴대폰으로 전송될 수 있다. 무작위 숫자를 수신하자마자, 사용자는 로그인 과정에서 이러한 무작위 숫자를 입력하고, 무작위 숫자를 서버로 제출한다. 서버는 그 무작위 숫자를 검증함으로써, 사용자가 지정된 휴대폰의 소유자인 것을 확인하고, 그것에 의해서 사용자는 신원 인증을 통과한다.

발명의 내용

해결하려는 과제

[0007] 그러나, 보안 위험들이 상기 종래의 신원 인증 방법에서 존재한다. 해커들 또는 사기꾼들은 부정하게 텍스트 메시지의 내용을 얻기 위해, 휴대폰 트로이 목마를 끼워 넣음으로써 또는 속임을 사용함으로써 텍스트 메시지를 아마도 가로챌 수 있고, 피해자들은 이러한 과정(핸드폰 트로이 목마들의 경우) 동안 모른 채로 있을 것이고, 또는 단순하게 사기꾼들에게 텍스트 메시지의 내용들을 말할 것이다(속임의 경우). 그 결과, 사기꾼들 및/또는

해커들은 텍스트 메시지의 내용을 얻을 것이며 성공적으로 피해자들의 신원이나 자금을 훔칠 것이다.

과제의 해결 수단

[0008] 본 발명은, 장치; 시스템; 물질의 조성; 컴퓨터 판독가능한 저장 매체에 포함된 컴퓨터 프로그램 제품; 및/또는 프로세서에 연결된 메모리에 저장되고 및/또는 프로세서에 연결된 메모리에 의해 제공된 명령어들(instructions)을 실행하도록 구성된 프로세서와 같은 프로세서를 프로세스로서 포함하여 다양한 방법들로 실행될 수 있다. 본 명세서에서, 이들 구현들 또는 본 본 발명이 취할 수 있는 임의의 다른 형태는 기술들로 지칭될 수 있다. 일반적으로, 개시된 프로세스들의 단계들의 순서는 본 발명의 범위 내에서 변경될 수 있다. 달리 언급되지 않는 한, 임무를 수행하도록 구성된 것으로 설명된 프로세서 또는 메모리와 같은 구성요소는 주어진 시간에서의 임무를 수행하도록 일시적으로 구성된 일반적인 구성요소로서 또는 그 임무를 수행하도록 제조된 특정 구성요소로서 구현될 수 있다. 본 명세서에서 사용된 바와 같이, 용어 프로세서('processor')는 하나 이상의 장치들, 회로들 및/또는 컴퓨터 프로그램 명령어들과 같은 데이터를 처리하도록 구성된 프로세싱 코어들로 지칭된다.

[0009] 본 발명의 하나 이상의 실시예들의 상세한 설명은 본 발명의 원리들을 도시하는 첨부된 도면들을 따라 이하에 제공된다. 본 발명은 이러한 실시예들과 관련하여 설명되지만, 본 발명은 임의의 실시예에 제한되지 않는다. 본 발명의 범위는 오직 청구항들에 의해 제한되고 본 발명은 다양한 대안들, 변형들 및 등가물들을 포함한다. 다양한 특정 세부사항들은 본 발명의 완전한 이해를 제공하기 위해 다음의 설명에서 설명된다. 이러한 세부사항들은 예시의 목적으로 제공되고 본 발명은 이러한 특정 세부사항들의 일부 또는 전부 없이 청구항들에 따라 실시될 수 있다. 본 발명과 관련된 기술 분야들에 알려진 기술적 물질이 본 발명이 불필요하게 불명료하지 않도록 명확성을 위하여 상세히 설명되지 않았다.

[0010] 본 출원은 인증 기술을 설명한다. 일부 실시예들에서, 서버는 더이상 지정된 휴대폰에 검증 코드를 전송하지 않고, 대신 애플리케이션 시나리오에 따라 검증 코드를 지정된 휴대폰에 직접 방출한다. 사용자는 애플리케이션 시나리오 동안 얻어진 검증 코드를 애플리케이션 시나리오 외의 애플리케이션을 사용하여 업링크 메시지를 통하여 서버로 전송한다. 일부 실시예들에서, 애플리케이션 시나리오는 애플리케이션과 관련될 수 있다. 전형적으로, 애플리케이션 시나리오는 애플리케이션이 사용되는 방법과 시기를 설명한다. 예를 들어, 애플리케이션 시나리오는 지불 애플리케이션과 관련된다. 지불 애플리케이션은 돈이 구매와 관련된 다른 당사자에게 지불되는 것을 허용하거나 돈을 다른 당사자로 이체할 수 있다. 일반적으로, 전자 상거래 웹 사이트에 대한 지불 애플리케이션은 체크 아웃 점원에 해당한다. 사용자가 검증 성공 프롬프트(a verification successful prompt)를 수신하기 전에, 서버는 신원 인증("신원 검증" 또는 "허가" 이라고도 불리는)이 성공적인지 확인하고, 애플리케이션 시나리오에서 제출된 서비스 요청을 발표하고, 그럼으로써 사용자 신원의 인증과 보안을 보호하는 것을 달성한다.

[0011] 본 발명의 다양한 실시예들은 다음의 상세한 설명과 첨부된 도면들에 개시된다.

[0012] 본 명세서에 설명된 도면들의 목적은 본 애플리케이션의 추가 이해를 제공하는 것이며 도면들은 본 출원의 일부를 구성한다. 본 출원의 예시적인 실시예들 및 이러한 실시예들의 설명들은 본 출원을 설명하기 위한 것이며, 본 출원에 부적절한 제한을 의미하지 않는다.

도면의 간단한 설명

[0013] 도 1은 인증 서비스의 애플리케이션 시나리오의 예시를 도시한 도면.

도 2는 사용자 신원을 인증하기 위한 과정에 대한 실시예의 플로우챠트.

도 3은 사용자 신원을 인증하기 위한 장치에 대한 실시예의 구조적 블록 다이어그램.

도 4는 결정 모듈에 대한 실시예의 구조적 블록 다이어그램.

도 5는 사용자 신원을 인증하기 위한 시스템에 대한 실시예의 구조적 다이어그램.

도 6은 사용자 신원을 인증하기 위한 컴퓨터 시스템에 대한 실시예의 구조적 다이어그램.

발명을 실시하기 위한 구체적인 내용

[0014] 도 1은 인증 서비스에 대한 애플리케이션 시나리오의 예시를 나타낸다. 이러한 애플리케이션

시나리오(100)에서, 사용자가 청구서를 지불하고 제품을 구매하는 등을 하는 웹 서비스와 같은 서비스는 사용자에 의해 현재 사용되고 있는 제품 또는 서비스를 지칭한다. 서비스의 애플리케이션 시나리오는 현재 사용되고 있는 제품 또는 서비스의 시나리오를 지칭한다.

[0015] 애플리케이션 시나리오(100)에서, 신원 인증은 사용자가 사용자 이름과 비밀번호를 입력해야만 하는 곳에서 수행된다.

[0016] 검증 코드는 애플리케이션 시나리오(100)에서 디스플레이된다.

[0017] 도 1에 도시된 바와 같이, 일부 실시예들에서, 애플리케이션 시나리오(100)는 웹 페이지이다. 다른 실시예들에서, 애플리케이션 시나리오(100)는 웹 페이지인 것에 제한되지 않고, 기업 애플리케이션, 서버 애플리케이션, 클라이언트 애플리케이션, 또는 애플리케이션의 또 다른 유형이 될 수 있다. 사실, 애플리케이션 시나리오는 신원 인증을 요구하는, 예를 들어 비밀번호의 입력을 요구하는 임의의 시나리오가 될 수 있다. 이러한 애플리케이션 시나리오들은 계좌 번호 요청, 비밀번호 변경, 새로운 계좌 허용 요청, 계좌 번호 변경, 온라인 쇼핑, 온라인 결제, 휴대폰 결재, 커뮤니티 액세스 제어(community access controls) 등을 포함하지만 이에 제한되는 것은 아니다.

[0018] 도 2는 사용자 신원을 인증하기 위한 프로세스에 대한 실시예의 플로우챠트이다. 일부 실시예들에서, 프로세스(200)는 도 1의 애플리케이션 시나리오(100)에 적용되고 도 5의 서버(520)에 의해 실시되고, 다음을 포함한다:

[0019] 단계(210)에서, 서버는 검증 코드를 생성한다.

[0020] 일부 실시예들에서, 서버는 검증 코드를 생성하기 위한 임의의 적절한 방법을 사용한다.

[0021] 일부 실시예들에서, 검증 코드는 무작위 숫자에 상응한다.

[0022] 일부 실시예들에서, 검증 코드는 숫자, 영어 알파벳 텍스트들, 숫자들 및 영어 알파벳 텍스트들, 한자들, 또는 이들의 조합과 같은 다른 텍스트들을 포함한다.

[0023] 단계(220)에서, 서버는 신원 인증을 필요로 하는 서비스의 애플리케이션 시나리오에서 검증 코드를 사용자에게 디스플레이한다.

[0024] 도 1에 도시된 바와 같이, 일부 실시예들에서, 서버는 검증 코드를 애플리케이션 시나리오(100)에서 직접적으로 디스플레이한다.

[0025] 일부 실시예들에서, 문구들 "검증 코드를 디스플레이"("display verification code")가 애플리케이션 시나리오(100)에서 디스플레이된다. 예를 들어, 문구들 "검증 코드를 디스플레이"를 기재한 버튼이 애플리케이션 시나리오(100)에서 표시된다. 사용자가 "검증 코드를 디스플레이" 버튼을 클릭할 경우, 검증 코드는 애플리케이션 시나리오(100)에서 사용자에게 디스플레이된다.

[0026] 도 2를 참조하여, 선택적으로 단계 225에서, 서버는 사용자에게 프롬트(a prompt)를 디스플레이한다. 프롬트는 사용자가 애플리케이션 시나리오 외에 애플리케이션을 통해 디스플레이된 검증 코드를 서버로 전송하도록 촉구하기 위해 사용된다.

[0027] 일부 실시예들에서, 서버는 애플리케이션 시나리오에서 이러한 프롬트를 디스플레이한다. 예를 들어, 이러한 프롬트는 사용자가 디스플레이된 검증 코드를 서버로 전송하는 방법을 촉구하기 위해 도 1에 도시된 애플리케이션 시나리오(100)에 디스플레이된다. 예로서, "검증을 완성하기 위해 텍스트 메시지를 통해 검증 코드를 번호 (408) 555-1234로 전송해 주세요"("please send the verification code via text message to the number (408) 555-1234 to complete verification")와 같은 내용이 도 1에 도시된 애플리케이션 시나리오에서 디스플레이된다.

[0028] 일부 실시예들에서, 서버는 현재의 애플리케이션 시나리오가 발생하는 애플리케이션 이외의 애플리케이션에서 프롬트 메시지들을 디스플레이한다. 예를 들어, 애플리케이션 시나리오가 온라인 결제에 관련된 경우, 서버는 이러한 프롬트를 지불 페이지에 표시하기보다, 지정된 휴대폰 번호에 단문 메시지 서비스(SMS)(또한 "텍스트메시지"로 알려진) 프롬프트를 전송한다. 일부 실시예들에서, 서버가 사용자에게 충분한 보안 교육 정보를 제공하는 반면, 서버는 또한 사용자가 애플리케이션에서 구동중인 애플리케이션 외에 애플리케이션을 사용하는 SMS 프롬트에 응답하는 것을 또한 요구한다. 응답의 내용은 애플리케이션 시나리오에 표시된 검증 코드를 포함한다. 이러한 예시에서, 지정된 휴대폰 번호는 사용자가 서버에 등록한 휴대폰 번호에 상응한다.

[0029] 사용자가 텍스트 메시지를 통해 검증 코드에 응답하는 경우, 통신 서비스 제공자는 SMS 서비스 채널을 통해 텍스트 메시지를 서버로 전송한다. 서버는 수신된 텍스트 메시지의 전송자의 휴대폰 번호를 사용자가 등록 과정 동안 저장하고, 다운스트림 SMS 텍스트 메시지가 전송된 휴대폰 번호와 확인한다. 일부 실시예들에서, 사용자는 이전에 그들의 인터넷 계정과 휴대폰 번호를 결합하고, 이는 사용자가 SMS 텍스트 메시지를 통해 통지 메시지들을 수신할 수 있게 허용한다. 휴대폰 번호들이 일치하는 경우, 수신된 텍스트 메시지 내의 검증 코드는 전송된 텍스트 메시지 내의 검증 코드와 비교된다. 검증 코드가 일치한 경우, 사용자의 검증은 성공적으로 완료될 것이다.

[0030] 단계(230)에서, 서버는 사용자에 의해 전송된 검증 코드를 애플리케이션 시나리오를 구동하는 애플리케이션 외에 또 다른 애플리케이션을 통해 수신한다.

[0031] 일부 실시예들에서, 애플리케이션 시나리오를 구동하는 애플리케이션 외에 애플리케이션은 서버에 메시지를 전송할 수 있는 애플리케이션과 상응하고, 표시된 검증 코드는 이러한 메시지들 내에 포함된다.

[0032] 일부 실시예들에서, 검증 코드를 전송하기 위해 사용자에 의해 사용된 애플리케이션은 텍스트 메시징 애플리케이션, 예로서, WeChat, QQ,등이다.

[0033] 일부 실시예들에서, 텍스트 메시징 애플리케이션에서, 사용자는 표시된 검증 코드를 명령 프롬트에 포함된 목적지 전화번호 또는 연락처에 대한 텍스트 메시지를 통해 서버로 전송한다. 전형적으로, 텍스트 메시지들을 전송할 수 있는 장치는 휴대폰을 포함하지만, 이러한 장치는 기술 분야에 이미 존재하거나 미래에 개발되어 지상 전화(landline telephone)과 같은 텍스트 메시지들을 전송할 수 있는 다른 장치를 또한 포함한다. 휴대폰을 통해 검증 코드를 수신하고, 온라인으로 검증 코드를 입력하는 종래의 방법들과는 대조적으로, 예를 들어 휴대폰을 사용하여, 검증 코드가 웹 페이지에 표시되어 휴대폰을 통해 전송된다.

[0034] 일부 실시예들에서, 사용자는 표시된 검증 코드의 전송을 촉구하는 SMS에 응답한다.

[0035] 일부 실시예들에서, 애플리케이션 시나리오 이외의 다른 애플리케이션은 상이한 단말 장치에서 구현된다. 예를 들어, 애플리케이션 시나리오는 태블릿 PC에서 구현된 온라인 결제 애플리케이션이고, 애플리케이션 시나리오 이외의 애플리케이션은 휴대폰에서 구현된 텍스트 메시징 애플리케이션이다. 이러한 상황에서, 검증 코드는 태블릿 PC 상의 웹 페이지를 통해 표시되고, 휴대폰은 검증 코드를 서버로 전송한다.

[0036] 일부 실시예들에서, 애플리케이션 시나리오 이외의 애플리케이션 및 애플리케이션 시나리오는 동일한 단말 장치에서 구현된다. 예를 들어, 애플리케이션 시나리오는 스마트폰을 사용하는 온라인 결재 애플리케이션이고, 애플리케이션 시나리오 이외의 애플리케이션은 동일한 스마트폰을 사용하는 텍스트 메시징 애플리케이션이다. 이러한 상황에서, 검증 코드는 스마트폰 상의 웹페이지를 통해 표시되고, 검증 코드는 동일한 스마트폰을 사용하는 텍스트 메시지에 의해 서버로 전송된다.

[0037] 단계(240)에서, 서버는 서버에 의해 생성된 검증 코드와 사용자로부터의 검증 코드를 비교한다. 일부 실시예들에서, 서버에 의해 생성된 검증 코드들, 검증되는 사용자의 신원 정보와 같은 관련 정보, 및 사용자에 의해 이전에 등록된 휴대폰 번호 등이 데이터 스토어(예로서, 테이블 또는 그와 유사한 것)에 저장되어 검사와 비교를 허용한다.

[0038] 서버는 동시에 여러 상이한 사용자들에게 많은 검증 코드들을 전송할 수 있기 때문에, 수신된 검증 코드를 확인하기 위한 적어도 두 가지 기술들이 존재한다. 제 1 기술에서, 서버는 애플리케이션 시나리오에 고유의 무작위 숫자를 생성하고, 서버는 그 무작위 숫자를 사용자의 휴대폰 번호에 함께 저장한다. 일부 실시예들에서, 사용자 ID는 사용자의 휴대폰 번호와 무작위 숫자와 함께 저장된다. 검증 코드(무작위 숫자)가 서버에 의해 수신되는 경우, 서버는 검증을 위해 휴대폰 번호와 사용자 ID를 인증 번호(무작위 숫자)를 통해 검색(retrieve)한다.

[0039] 제 2 기술에서, 서버는 데이터 스토어에 있는 사용자 ID와 휴대폰 번호의 관계를 검증함으로써 사용자 ID를 얻기 위해 휴대폰 번호를 사용한다.

[0040] 단계(250)에서, 서버는 사용자가 비교의 결과를 기초로 하여 신원인증을 통과하였는지의 여부를 결정한다.

[0041] 일부 실시예들에서, 사용자로부터의 검증 코드가 생성된 검증 코드와 동일한 경우, 서버는 사용자가 신원인증을 통과했다고 결정한다.

[0042] 일부 실시예들에서, 사용자부터의 검증 코드가 서버에 의해 생성된 검증 코드와 동일한 경우, 서버는 메시지를 전송하기 위해 사용된 다른 애플리케이션의 사용자 ID를 서버에 저장된 사용자 ID와 비교한다. 메시지를 전송하

기 위해 사용된 다른 애플리케이션의 사용자 ID가 서버에 저장된 사용자 ID와 동일한 경우, 서버는 사용자가 신원인증을 통과했다고 결정한다.

[0043] 일부 실시예들에서, 다른 애플리케이션은 텍스트 메시징 애플리케이션에 상응하고, 메시지는 텍스트 메시지에 상응한다. 이러한 예에서, 사용자 ID는 휴대폰 번호 또는 전화번호에 상응한다.

[0044] 일 실시예에서, 사용자로부터 업링크 메시지 응답을 수신시, 서버는 업링크 메시지 응답의 내용 및 업링크 메시지 응답을 전송한 휴대폰의 번호를 서버의 검증 코드 및 사용자가 서버에 등록한 휴대폰 번호와 비교한다. 일부 실시예들에서, 서버는 업링크 메시지 응답의 내용에 포함된 검증 코드를 검색하여 이러한 검증 코드와 연관된 사용자 정보, 예로서, 사용자에 의해 등록된 휴대폰 번호를 찾는다. 업링크 메시지 응답을 전송하는 휴대폰의 번호가 등록된 번호와 비교되어, 일치하는지 결정한다.

[0045] 일부 실시예들에서, 다른 애플리케이션은 WeChat 또는 QQ와 상응하고, 메시지는 WeChat 메시지 또는 QQ 메시지와 상응한다. 이러한 예시에서, 사용자 ID는 WeChat 번호 또는 QQ 번호와 상응한다. WeChat 및 QQ는 메시징 애플리케이션의 예시이다. 게다가, 예로서, Whatsapp 등과 같은 다른 메시징 애플리케이션이 사용될 수 있다.

[0046] 또 다른 예시에서, 사용자로부터 업링크 메시지 응답을 수신하자마자, 서버는 업링크 메시지 응답의 내용 및 업링크 메시지 응답을 전송하기 위해 사용되는 WeChat 번호 또는 QQ 번호를 서버의 검증 코드 및 사용자가 서버에 등록한 WeChat 번호 또는 QQ 번호와 비교한다.

[0047] 일부 실시예들에서, 사용자 신원이 검증(즉 신원 인증이 통과)될 때, 서버는 사용자 신원이 애플리케이션 시나리오 외에 애플리케이션을 통해 증명되었던 것을 나타내는 프롬트 메시지(예를 들어, 사용자 신원이 증명되었다는 SMS 프롬트를 사용자에게 전송함으로써)를 전송하고, 업링크 인증 통과 상태가 서버에서 설정된다.

[0048] 일부 실시예들에서, 서버는 서비스를 위한 애플리케이션 시나리오의 인터페이스 상에 사용자 신원이 인증되었다는 것과 업링크 인증 통과 상태 설정이 서버 상에 설정되었다는 것을 나타내는 프롬트 메시지를 나타낸다.

[0049] 일부 실시예들에서, 사용자가 인증을 통과한 프롬트 메시지를 발견한 이후에, 서비스 요청이 사용자에 의해 또는 장치를 통해 제출된다. 서버는 인증 통과 상태 설정을 기초로 하여 서비스 요청을 방출한다(releases).

[0050] 일부 실시예들에서, 애플리케이션 시나리오를 통한 검증 코드의 통지 이후에, 서버는 상기 업링크 메시지 방법을 기초로 하여 신원인증을 수행하고, 신원인증 동안, 서버는 동적 검증 코드들 및 그들의 미리 설정된 값을 갖는 업링크 모바일 핸드폰 번호의 일관성을 보장한다. 즉, 다운링크 메시지 내용의 누설 또는 트로이 목마 차단으로 인한 보안 위험들은 생성되지 않는다.

[0051] 도 3은 사용자 신원을 인증하기 위한 장치에 대한 실시예의 구조적 블록 다이어그램이다. 일부 실시예들에서, 장치(300)는 도 2의 과정(200)을 실시하고, 생성 모듈(310), 디스플레이 모듈(320), 수신 모듈(330), 비교 모듈(340) 및 결정 모듈(350)을 포함한다.

[0052] 일부 실시예들에서, 생성 모듈(310)은 서버에 검증 코드를 생성한다.

[0053] 일부 실시예들에서, 디스플레이 모듈(320)은 사용자 신원 인증을 요구하는 서비스의 애플리케이션 시나리오에서 사용자에게 검증 코드를 디스플레이한다.

[0054] 일부 실시예들에서, 수신 모듈(330)은 사용자에 의해 서버로 전송된 검증 코드를 애플리케이션 시나리오 외의 다른 애플리케이션을 통해 수신한다.

[0055] 일부 실시예들에서, 비교 모듈(340)은 사용자로부터의 검증 코드와 서버에 의해 생성된 검증 코드를 비교한다.

[0056] 일부 실시예들에서, 결정 모듈(350)은 사용자가 신원인증을 통과했는지의 여부를 비교의 결과들을 기초로 하여, 결정한다.

[0057] 도 4는 결정 모듈에 대한 실시예의 구조적 블록 다이어그램이다. 일부 실시예들에서, 결정 모듈(400)은 도 3의 결정 모듈(350)의 구현이고, 제 1 결정모듈(410), 사용자 ID 비교 모듈(420) 및 제 2 결정 모듈(430)을 포함한다.

[0058] 일부 실시예들에서, 사용자로부터의 검증 코드가 서버에 의해 생성된 검증 코드와 동일할 경우, 제 1 결정 모듈(410)은 사용자가 신원 인증을 통과했다고 결정한다.

[0059] 일부 실시예들에서, 애플리케이션 시나리오 외에 애플리케이션은 서버에 메시지를 전송할 수 있는 애플리케이션

에 상응하고, 디스플레이된 검증 코드는 메시지들에 포함된다.

[0060] 일부 실시예들에서, 사용자로부터의 검증 코드는 서버에 의해 생성된 검증 코드와 동일할 때, 사용자 ID 비교 모듈(420)은 메시지를 전송하기 위해 사용된 다른 애플리케이션의 사용자 ID를 서버 상에 등록된 사용자 ID와 비교한다.

[0061] 일부 실시예들에서, 메시지를 전송하기 위해 사용된 다른 애플리케이션의 사용자 ID는 서버에 등록된 사용자 ID와 동일할 때, 제 2 결정 모듈(430)은 사용자가 신원 인증을 통과했다고 결정한다.

[0062] 일부 실시예들에서, 애플리케이션 시나리오 외에 애플리케이션은 텍스트 메시징 애플리케이션에 상응하고, 메시지들은 텍스트 메시지들에 상응한다.

[0063] 일부 실시예들에서, 사용자 ID는 휴대폰 번호 또는 전화번호에 상응한다.

[0064] 도 3을 다시 참조하여, 일부 실시예들에서, 장치(300)는 또한 제 1 프롬팅 모듈(360)을 포함한다.

[0065] 일부 실시예들에서, 제 1 프롬팅 모듈(360)은 애플리케이션 시나리오에 프롬트 메시지들을 디스플레이한다. 프롬트 메시지들은 사용자가 검증 코드를 애플리케이션 시나리오 외에 애플리케이션을 통해 서버로 전송하도록 촉구한다.

[0066] 일부 실시예들에서, 장치(300)는 또한 제 2 프롬팅 모듈(370)을 포함한다.

[0067] 일부 실시예들에서, 제 2 프롬팅 모듈(370)은 프롬트 메시지들을 애플리케이션 시나리오 외에 애플리케이션에서 디스플레이한다. 프롬트 메시지들은 사용자가 검증 코드를 애플리케이션 시나리오 외에 애플리케이션을 통해 서버로 전송하도록 촉구한다.

[0068] 일부 실시예들에서, 검증 코드는 무작위 숫자에 상응한다.

[0069] 본 출원이 인터넷 애플리케이션 시나리오들의 예시들을 사용하여 상술되었지만, 본 출원은 인터넷 애플리케이션 시나리오들에 제한되지 않고, 오히려 신원 인증 또는 비밀번호 입력을 포함하는 임의의 애플리케이션 시나리오에 적용될 수 있다.

[0070] 예를 들어, 본 발명은 커뮤니티 액세스 제어에 적용될 수 있다. 사용자가 커뮤니티 액세스 제어 포인트에 비밀번호를 입력할 경우, 액세스 제어 스위치 포인트에서 사용자 인터페이스 상에 디스플레이된 검증 코드는 휴대폰 텍스트 메시지를 통해 서버로 전송될 수 있다(예를 들어, 서버는 부동산 회사(property company)에 의해 관리된다). 서버는 사용자에 의해 전송된 검증 코드를 휴대폰 텍스트 메시지를 통해 수신하고, 그 검증 코드를 서버의 검증 코드와 비교하고, 사용자가 신원인증을 통과했는지의 여부를 그 비교의 결과를 기초로 결정한다. 그럼으로써 서버는 사용자가 커뮤니티로 액세스하도록 허용되는지의 여부를 결정한다.

[0071] 도 5는 사용자 신원을 인증하기 위한 시스템에 대한 실시예의 구조적 다이어그램이다. 일부 실시예들에서, 시스템(500)은 네트워크(530)를 통해 서버(520)로 연결된 클라이언트(510)를 포함한다. 일부 실시예들에서, 클라이언트(510)를 사용하는 사용자의 신원은 서버(520)에 의해 인증된다.

[0072] 도 6은 사용자 신원을 인증하기 위한 프로그램화된 컴퓨터 시스템에 대한 실시예를 도시하는 기능적 다이어그램이다. 알 수 있는 바와 같이, 다른 컴퓨터 시스템 구조들 및 구성들은 사용자 신원을 인증하기 위해 사용될 수 있다. 이하에서 설명되는 다양한 서브시스템들을 포함하는 컴퓨터 시스템(600)은 적어도 하나의 마이크로프로세서 서브시스템(프로세서 또는 중앙 처리 장치(CPU)로도 언급됨)(602)를 포함한다. 예를 들어, 프로세서(602)는 단일-칩 프로세서에 의해 또는 다중 프로세서들에 의해 구현될 수 있다. 일부 실시예들에서, 프로세서(602)는 컴퓨터 시스템(600)의 동작을 제어하는 범용 디지털 프로세서이다. 메모리(610)로부터 검색된 명령어들을 사용하여, 프로세서(602)는 입력 데이터의 수신과 조작, 출력 장치들(예로서, 디스플레이(618)) 상의 데이터의 출력과 디스플레이를 제어한다.

[0073] 프로세서(602)는 제 1 주기억 장치, 전형적으로 랜덤 엑세스 메모리(RAM) 및 제 2 주기억 장치 구역, 전형적으로 읽기-전용 메모리(ROM)를 포함할 수 있는 메모리(610)와 양-방향으로 연결된다. 관련 기술분야에 잘 알려진 바와 같이, 주기억 장치는 일반적인 저장 구역으로서 및 스크래치 패드 메모리로서 사용될 수 있고, 또한 입력 데이터와 처리된 데이터를 저장하기 위해 사용될 수 있다. 주기억 장치는 또한 프로세서(602) 상에서 동작하는 프로세스들을 위한 다른 데이터 및 명령어들 외에도, 데이터 오브젝트들 및 텍스트 오브젝트들의 형태로 프로그래밍 명령어들 및 데이터를 또한 저장할 수 있다. 또한 관련 기술분야에 잘 알려진 바와 같이, 주기억 장치는 프로세서(602)에 의해 사용되는 기초 동작 명령어들, 프로그램 코드, 데이터 및 오브젝트들을 전형적으로 포함

하고, 이것의 기능들(예로서, 프로그램화된 명령어들)을 수행한다. 예를 들어, 메모리(610)는 예로서, 데이터 액세스이 양-방향 또는 단-방향성이 될 필요가 있는지에 따라서, 이하에 설명된 임의의 적합한 컴퓨터-판독가능한 저장 매체를 포함할 수 있다. 예를 들어, 처리기(602)는 또한 캐시 메모리(도시되지 않음)에서 필요한 데이터를 직접 및 매우 빠르게 검색할 수 있고 빈번하게 저장할 수 있다.

[0074] 탈착 가능한(removable) 대용량 저장 장치(612)는 컴퓨터 시스템(600)을 위한 추가 데이터 저장 용량을 제공하고, 양-방향적으로(읽기/쓰기) 또는 단-방향적으로(읽기 전용) 프로세서(602)에 연결된다. 예를 들어, 저장 장치(612)는 또한 자기 테이프, 플래시 메모리, PC-CARDS, 이동식 대용량 저장 장치들, 홀로그래픽 저장 장치들, 및 다른 저장 장치들을 포함할 수 있다. 고정된 대용량 저장 장치(620)는 또한 예를 들어 추가 데이터 저장 용량을 제공할 수 있다. 대용량 저장장치(620)의 가장 일반적인 예는 하드 디스크 드라이브이다. 대용량 저장장치들(612, 620)은 일반적으로 프로세서(620)에 의해 일반적으로 적극 사용중이 아닌 추가 프로그래밍 명령어들, 데이터, 등을 저장한다. 대용량 저장장치들(612 및 620) 내에 보유된 정보가 필요하다면, 가상 메모리로서 메모리(610)(예로서, RAM)의 표준 방식으로 통합될 수 있다.

[0075] 저장 장치 서브시스템들에 대한 액세스를 프로세서(602)에 제공하는 것 외에도, 버스(614)는 또한 다른 서브시스템들 및 장치들에 대한 액세스를 제공하기 위해 사용될 수 있다. 도시된 바와 같이, 이들은 보조 입력/출력 장치 인터페이스, 사운드 카드, 스피커들, 및 다른 서브시스템들뿐만 아니라 디스플레이 모니터(618), 네트워크 인터페이스(616), 키보드(604) 및 포인팅 장치(606)를 필요할 때 포함할 수 있다. 예를 들어, 포인팅 장치(606)는 마우스, 스타일러스, 트랙 볼, 또는 태블릿이 될 수 있고, 그래픽 사용자 인터페이스와 상호작용하기 위해 유용한다.

[0076] 네트워크 인터페이스(616)는 프로세서(602)로 하여금 또 다른 컴퓨터, 컴퓨터 네트워크, 또는 도시된 바와 같은 네트워크 연결을 사용하는 통신 네트워크에 연결되도록 허용한다. 예를 들어, 네트워크 인터페이스(616)를 통해, 프로세서(602)는 방법/프로세스 단계들을 수행하는 과정에서 또 다른 네트워크로부터 정보(예로서, 데이터 객체들 또는 프로그램 명령어들)를 수신할 수 있거나 또는 또 다른 네트워크로의 정보를 출력할 수 있다. 프로세서상에서 실행될 일련의 명령어들로서 종종 표현되는 정보는 또 다른 네트워크로부터 수신될 수 있고 또 다른 네트워크로 출력될 수 있다. 인터페이스 카드 또는 유사한 장치와 프로세서(602)에 의해 구현된(예로서, 실행된/수행된) 적합한 소프트웨어는 컴퓨터 시스템(600)을 외부 네트워크에 연결하기 위해 및 기준 프로토콜들에 따라 데이터를 전송하기 위해 사용될 수 있다. 예를 들어, 본 명세서에 개시된 다양한 프로세스 실시예들은 프로세서(602)에서 실행될 수 있거나, 또는 처리의 일부를 공유하는 원격 프로세서와 연계된 인터넷, 상호 네트워크들, 또는 로컬 어리어 네트워크들과 같은 네트워크를 거쳐서 수행될 수 있다. 추가 대용량 저장 장치들(도시되지 않음)은 또한 네트워크 인터페이스(616)를 통해 프로세서(602)에 연결될 수 있다.

[0077] 보조 I/O 장치 인터페이스(도시되지 않음)는 컴퓨터 시스템(600)과 연계하여 사용될 수 있다. 보조 I/O 장치 인터페이스는 프로세서(602)로 하여금 마이크로폰들, 터치감음 디스플레이들, 트랜스듀서 카드 판독기들, 테이프 판독기들, 음성 또는 필기 인식기들, 생체 판독기들, 카메라들, 이동식 대용량 저장 장치들 및 다른 컴퓨터들과 같은 다른 장치들에 데이터를 송신하고, 보다 일반적으로 다른 장치들로부터 데이터를 수신하는 것을 허용하는 일반적이고 맞춤형 인터페이스들을 포함할 수 있다.

[0078] 도 6에 도시된 컴퓨터 시스템은 본 명세서에 개시된 다양한 실시예들에 사용하기에 적합한 컴퓨터 시스템의 일례에 불과하다. 이러한 사용에 적합한 다른 컴퓨터 시스템들은 추가 이하의 서브시스템들을 포함할 수 있다. 게다가, 버스(614)는 서브 시스템을 연결하는 역할을 하는 임의의 상호 접속 방식의 예시이다. 서브 시스템의 다른 구성을 갖는 다른 컴퓨터 아키텍처들도 또한 사용될 수 있다.

[0079] 상술된 유닛들은 하나 이상의 일반적인 목적의 프로세서들을 실행하는 소프트웨어 구성요소들로서, 프로그램화된 로직 장치들 및/또는 특정 기능들을 수행하도록 설계된 주문형 집적 회로와 같은 하드웨어로서, 또는 이들의 조합들이 구현될 수 있다. 일부 실시예들에서, 유닛들은 컴퓨터 장치(개인 컴퓨터들, 서버들, 네트워크 장지, 등과 같은)가 본 발명의 실시예들에 설명된 방법들을 구현하게 하기 위한 다수의 명령어들을 포함하는 비 휘발성 저장 매체(광학 디스크, 플래시 저장 장치, 모바일 하드 디스크, 등과 같은)에 저장될 수 있는 소프트웨어 제품들의 형태로 구현될 수 있다. 유닛들은 싱글 디바이스로 구현될 수 있거나 여러 장치에 분산될 수 있다. 유닛들의 기능들은 병합될 수 있거나, 또는 복수의 서브 유닛들로 더 분할될 수 있다.

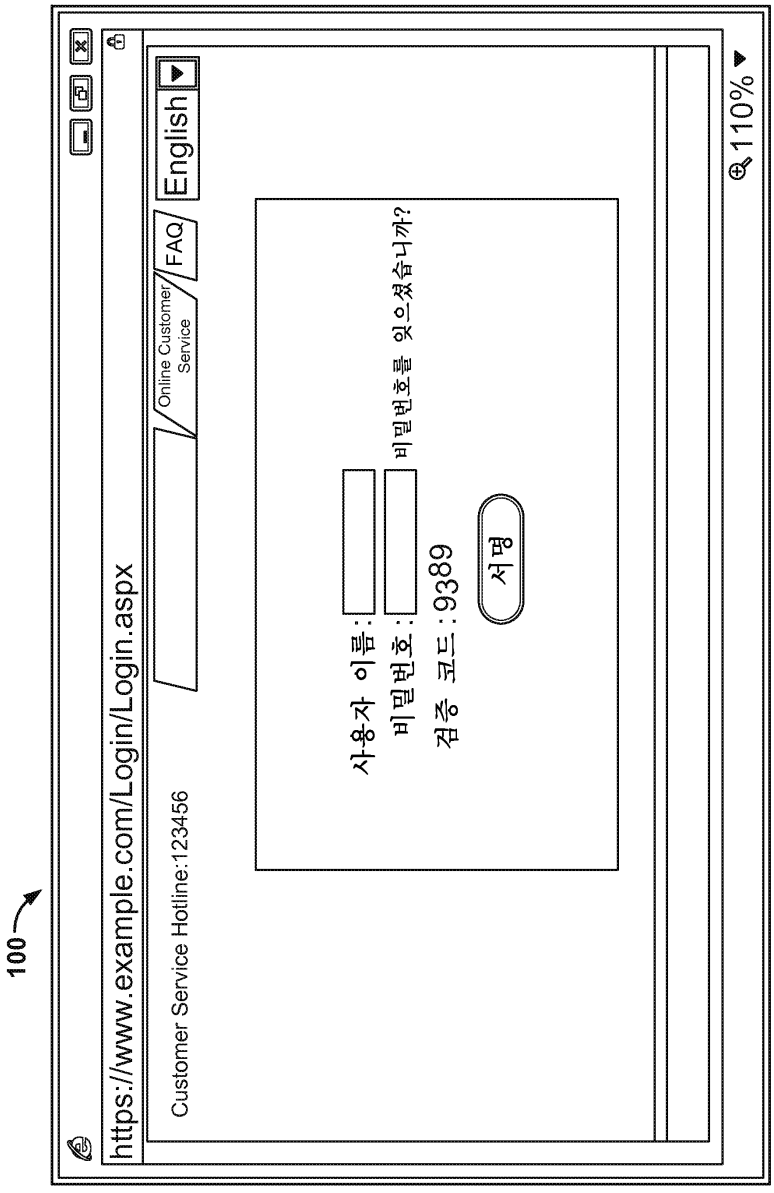
[0080] 본 명세서에 개시된 실시예들의 관점에서 설명된 방법들 또는 알고리즘 단계들은 하드웨어, 프로세서로 실행되는 소프트웨어 모듈들, 또는 이 둘의 조합을 사용하여 구현될 수 있다. 소프트웨어 모듈들은 랜덤 액세스 메모리(RAM), 메모리 판독-가능 메모리(ROM), 전기적으로 프로그램화된 ROM, 전기적으로 소거가능한 프로그램화된

ROM, 레지스터들, 하드 드라이브들, 리무버블 디스크들, CD-ROM, 또는 기술 분야에 알려진 저장 매체의 임의의 다른 형태들에 설치될 수 있다.

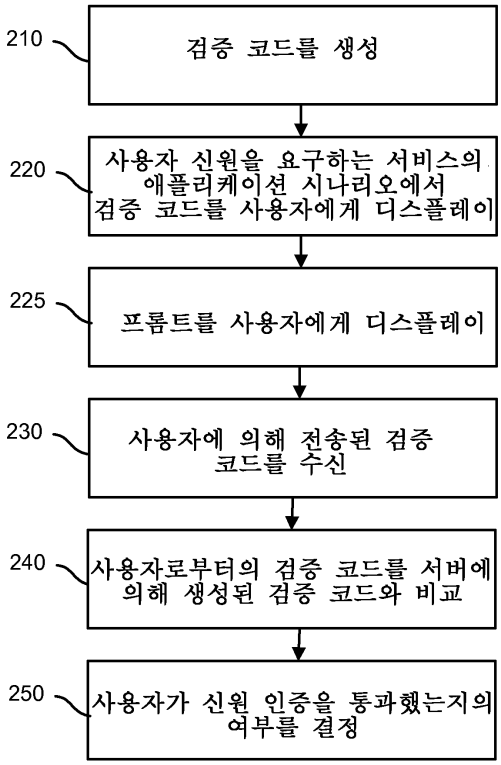
[0081] 전술한 실시예들은 명확한 이해를 목적으로 다소 상세하게 설명되었지만, 본 발명은 제공된 세부사항들에 제한되지 않는다. 본 발명을 실시하는 많은 대안의 방법들이 존재한다. 개시된 실시예들은 제한적인 것이 아니라 예시적이다.

도면

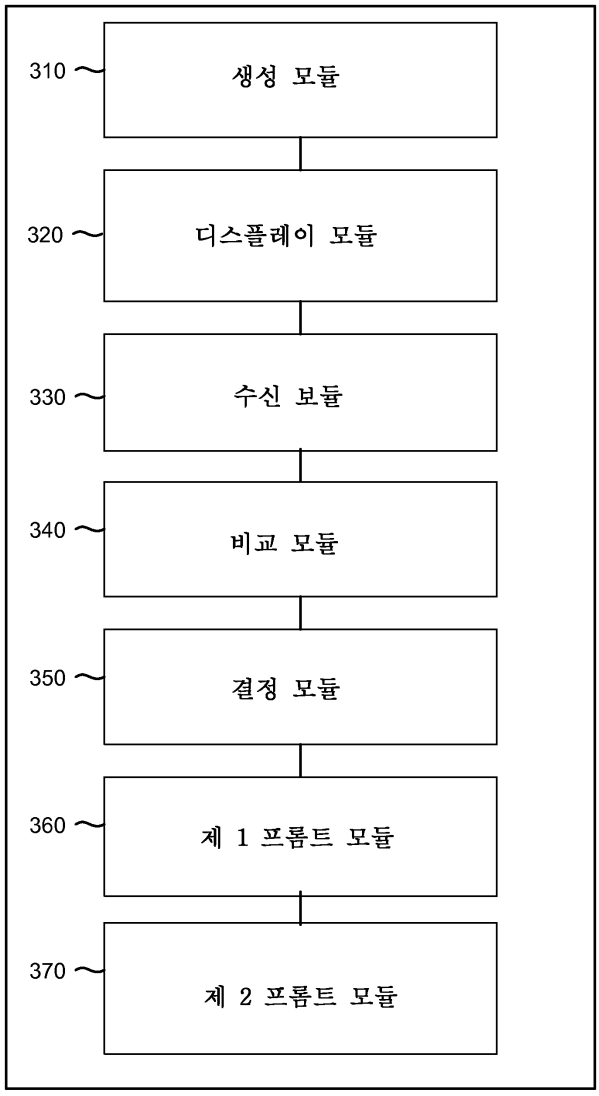
도면1



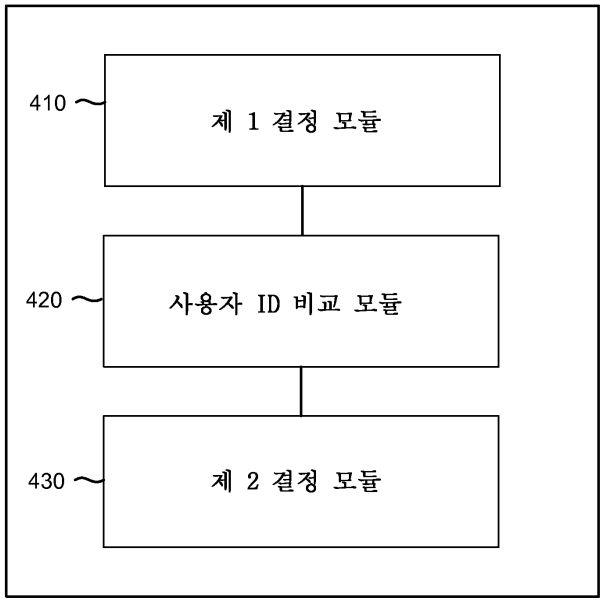
도면2


210
검증 코드를 생성
220
사용자 신원을 요구하는 서비스의 애플리케이션 시나리오에서 검증 코드를 사용자에게 디스플레이
225
프롬트를 사용자에게 디스플레이
230
사용자에 의해 전송된 검증 코드를 수신
240
사용자로부터의 검증 코드를 서버에 의해 생성된 검증 코드와 비교
250
사용자가 신원 인증을 통과했는지의 여부를 결정

도면3

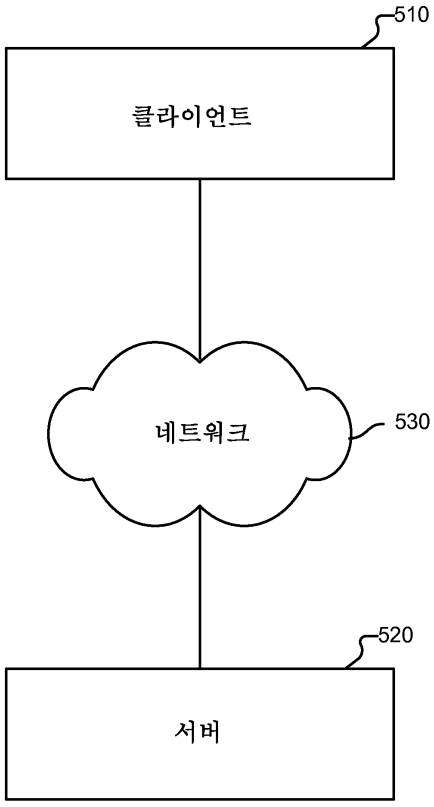

310
생성 모듈
320
디스플레이 모듈
330
수신 모듈
340
비교 모듈
350
결정 모듈
360
제 1 프롬트 모듈
370
제 2 프롬트 모듈
300

도면4

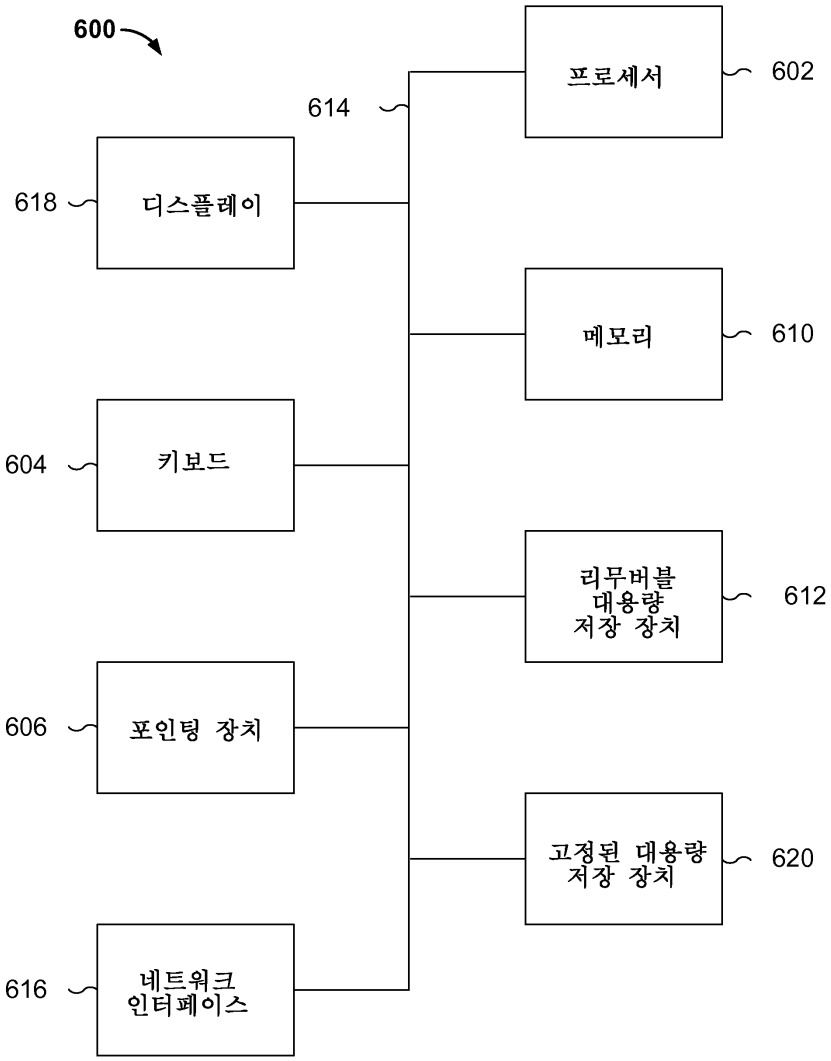


400

도면5



도면6


600
614
프로세서
602
618
디스플레이
메모리
610
604
키보드
리무버블
대용량
저장 장치
612
606
포인팅 장치
고정된 대용량
저장 장치
620
616
네트워크
인터페이스