(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0003796
(43) 공개일자 2016년01월11일

(51) 국제특허분류(Int. Cl.)
G06F 21/36 (2013.01) *G06F 21/00* (2006.01)
G06Q 20/40 (2012.01)
(52) CPC특허분류
G06F 21/36 (2013.01)
G06F 21/00 (2013.01)
(21) 출원번호 10-2015-7033769
(22) 출원일자(국제) 2014년04월30일
심사청구일자 없음
(85) 번역문제출일자 2015년11월26일
(86) 국제출원번호 PCT/AU2014/050024
(87) 국제공개번호 WO 2014/176645
국제공개일자 2014년11월06일
(30) 우선권주장
2013901504 2013년04월30일 오스트레일리아(AU)

(71) 출원인
토큰 원 피티와이 리미티드
오스트레일리아 뉴 싸우스 웨일즈 2000, 밀러스 포인트, 켄트 스트리트 168-170, 옵저버터리 타워, 스위트 306
(72) 발명자
커프, 필립 앤쏘니 프레데릭
오스트레일리아 뉴 싸우스 웨일즈 2000 밀러스 포인트, 켄트 스트리트 306/168
에커슬리-마슬린, 세바스티안 존
오스트레일리아 뉴 싸우스 웨일즈 2067 채스우드 데이 스트리트 40/1
(뒷면에 계속)
(74) 대리인
박병창

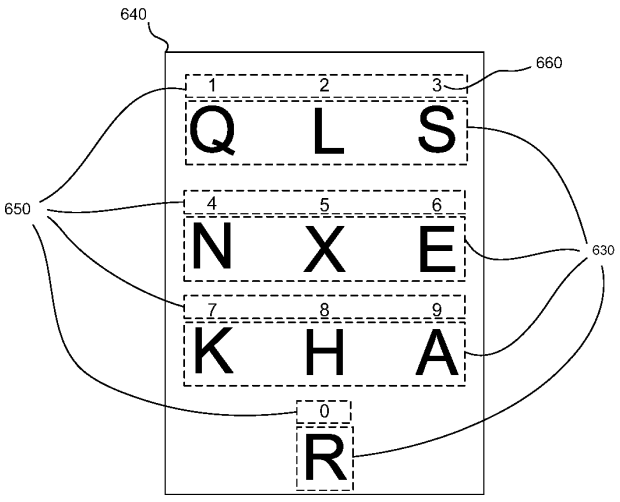
전체 청구항 수 : 총 25 항

(54) 발명의 명칭 **사용자 인증**

(57) 요 약

안전한 환경을 액세스하려고 시도하는 사용자를 인증하는 방법, 시스템, 서버 프로세싱 시스템 및 컴퓨터 판독가능 매체가 개시된다. 일 형태에서, 서버 프로세싱 시스템은, 인증 요청을 수신하여 안전한 환경을 액세스하려고 시도하는 사용자를 인증하고, 키맵으로부터의 선택 키에 대응하는 인덱스를 사용자 또는 사용자와 연관된 사용자 장치로 전송하고, 사용자 장치에 의해 제시된 선택 키 및 개인 식별자에 기초한 코드를 나타내는 데이터를 수신하고, 코드를 이용하여 사용자가 인증되었는지를 결정하도록 구성된다. 유리하게, 서버 프로세싱 시스템은 개인 식별자를 직접 나타내는 데이터를 저장하거나 수신하지 않아, 어느 누구도, 심지어 사용자가 액세스를 시도하려는 안전한 환경의 고용인조차도, 개인 식별자를 결정할 수 없다.

대 표 도 - 도6b



(52) CPC특허분류
G06Q 20/40 (2013.01)
G06F 2221/2149 (2013.01)
(72) 발명자
크레이저, 카밀
오스트레일리아 뉴 싸우스 웨일즈 2033 켄싱턴 데이 애비뉴 20
패디슨, 제레미 웨인
오스트레일리아 뉴 싸우스 웨일즈 2125 웨스트 페넌트 힐즈, 페넌트 힐즈 로드 526
그리브, 데이비드 로버트
오스트레일리아 뉴 싸우스 웨일즈 2152 노스메드, 롤란드 애비뉴 33

명 세 서

청구범위

청구항 1

원격 서버 프로세싱 시스템에 의해 제어되는 안전한 환경을 액세스하려고 시도하는 사용자를 인증하는 서버 프로세싱 시스템으로서, 상기 서버 프로세싱 시스템은,

상기 원격 서버 프로세싱 시스템으로부터 인증 요청을 수신하여 상기 안전한 환경을 액세스하려고 시도하는 사용자를 인증하고;

상기 사용자 장치의 메모리 또는 서버 액세스가능 메모리에 저장된 키맵으로부터의 선택 키에 대응하는 인덱스를 상기 사용자 또는 상기 사용자와 연관된 사용자 장치로 전송하고;

코드를 나타내는 데이터를 수신하고 - 상기 사용자는 상기 사용자 장치에 의해 제시된 선택 키 및 개인 식별자에 기초하여 상기 코드를 결정함 -;

상기 코드 및 상기 서버 액세스가능 메모리에 저장된 선택 키를 이용하여 상기 개인 식별자의 해시(hash) 값을 결정하고;

상기 결정된 해시 값을 상기 서버 액세스가능 메모리에 저장된 사용자 계정과 연관된 저장 해시 값과 비교하고;

상기 비교에 기초하여 상기 안전한 환경을 액세스하기 위하여 사용자가 인증되었는지를 나타내는 인증 응답을 상기 원격 서버 프로세싱 시스템으로 전송하도록

구성되는 서버 프로세싱 시스템.

청구항 2

제1항에 있어서, 상기 사용자는,

상기 사용자 장치와 독립적인 사용자 프로세싱 시스템, 또는

상기 사용자 장치

중의 하나로부터 상기 안전한 환경을 액세스하도록 시도하는 서버 프로세싱 시스템.

청구항 3

제1항 또는 제2항에 있어서, 상기 사용자 장치는 휴대용 프로세싱 시스템인 서버 프로세싱 시스템.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서, 상기 서버 프로세싱 시스템은,

상기 사용자의 아이덴티티를 증명하려고 시도하는 아이덴티티 데이터, 및

상기 사용자 장치를 식별하는 고유 장치 프로파일

을 나타내는 등록 요청을 수신하고;

상기 아이덴티티 데이터에 기초하여 상기 사용자의 아이덴티티를 확인하고;

상기 사용자의 아이덴티티의 긍정적인 확인에 기초하여 상기 사용자 계정을 생성하도록

구성되고,

상기 사용자 장치는 상기 고유 장치 프로파일에 기초하여 상기 사용자 계정과 연관된 서버 프로세싱 시스템.

청구항 5

제4항에 있어서, 사용자 등록시, 상기 서버 프로세싱 시스템은,

복수의 인덱스 키를 포함하는 상기 키맵을 상기 사용자 계정과 연관시키고;

상기 사용자 장치의 메모리에 저장하기 위하여 상기 키맵을 나타내는 데이터를 상기 사용자 장치로 전송하도록

구성되는 서버 프로세싱 시스템.

청구항 6

제5항에 있어서, 상기 서버 프로세싱 시스템은,

상기 사용자로부터 개인 식별자 등록 요청을 수신하고;

상기 키맵으로부터의 선택 키를 나타내는 인덱스를 상기 사용자 장치 또는 사용자로 전송하고;

등록 코드를 수신하고 - 상기 사용자는 상기 사용자 장치에 의해 제시된 선택 키 및 원하는 개인 식별자에 기초하여 상기 등록 코드를 결정함 -;

상기 등록 코드 및 상기 선택 키에 기초하여 상기 원하는 개인 식별자의 해시 값을 결정하고;

상기 해시 값을 상기 사용자 계정에 저장하도록

구성되는 서버 프로세싱 시스템.

청구항 7

제5항에 있어서, 상기 서버 프로세싱 시스템은,

상기 사용자로부터 개인 식별자 등록 요청을 수신하고;

상기 키맵으로부터의 제1 선택 키를 나타내는 제1 인덱스를 상기 사용자 장치 또는 사용자로 전송하고;

등록 코드를 수신하고 - 상기 사용자는 상기 사용자 장치에 의해 제시된 상기 제1 선택키 및 원하는 개인 식별자에 기초하여 상기 등록 코드를 결정함 -;

상기 등록 코드 및 상기 제1 선택 키에 기초하여 상기 원하는 개인 식별자의 제1 해시 값을 결정하고;

상기 키맵으로부터의 제2 선택 키를 나타내는 제2 인덱스를 상기 사용자 장치 또는 사용자로 전송하고;

제2 등록 코드를 수신하고 - 상기 사용자는 상기 제2 선택 키 및 상기 원하는 개인 식별자에 기초하여 상기 제2 등록 코드를 결정함 - ;

상기 제2 등록 코드 및 상기 키맵으로부터의 제2 인덱스에 대응하는 상기 제2 선택 키를 이용하여 제2 해시 값을 결정하고;

상기 제2 해시 값에 대응하는 제1 해시 값에 응답하여 상기 사용자 계정에 상기 제1 또는 제2 해시 값을 저장하도록

구성되는 서버 프로세싱 시스템.

청구항 8

제6항 또는 제7항에 있어서, 상기 서버 프로세싱 시스템은,

상기 사용자로부터 리셋 개인 식별자 요청을 수신하고;

상기 사용자의 아이덴티티의 확인을 가능하게 하고;

성공적인 확인에 응답하여, 상기 키맵으로부터의 선택 키의 인덱스를 상기 사용자 장치 또는 사용자로 전송하고;

리셋 코드를 수신하고 - 상기 사용자는 상기 사용자 장치에 의해 제시된 상기 선택 키 및 새로운 개인 식별자에 기초하여 상기 리셋 코드를 결정함 -;

상기 리셋 코드 및 상기 선택 키에 기초하여 상기 새로운 개인 식별자의 해시 값을 결정하고;

상기 새로운 개인 식별자의 해시 값을 상기 사용자 계정에 저장하도록

구성되는 서버 프로세싱 시스템.

청구항 9

제4항 내지 제8항 중 어느 한 항에 있어서, 상기 서버 프로세싱 시스템은 상기 사용자의 디지털 증명서에 의해 지시된 사용자의 아이덴티티를 나타내는 데이터를 상기 사용자 계정에 저장하도록 구성되는 서버 프로세싱 시스템.

청구항 10

제1항 내지 제9항 중 어느 한 항에 있어서, 상기 서버 프로세싱 시스템은 상기 사용자 장치로부터 인덱스 요청을 수신하도록 구성되고, 상기 인덱스 요청의 수신에 응답하여, 상기 서버 프로세싱 시스템은 상기 키맵으로부터의 선택 키의 인덱스를 상기 사용자 장치로 전송하는 서버 프로세싱 시스템.

청구항 11

원격 서버 프로세싱 시스템에 의해 제어되는 안전한 환경을 액세스하려고 시도하는 사용자를 인증하는 방법으로서, 상기 방법은, 상기 서버 프로세싱 시스템이,

상기 원격 서버 프로세싱 시스템으로부터 인증 요청을 수신하여 상기 안전한 환경을 액세스하려고 시도하는 사용자를 인증하는 단계;

상기 사용자 장치의 메모리 또는 서버 액세스가능 메모리에 저장된 키맵으로부터의 선택 키에 대응하는 인덱스를 상기 사용자 또는 상기 사용자와 연관된 사용자 장치로 전송하는 단계;

코드를 나타내는 데이터를 수신하는 단계 - 상기 사용자는 상기 사용자 장치에 의해 제시된 선택 키 및 개인 식별자에 기초하여 상기 코드를 결정함 -;

상기 코드 및 상기 서버 액세스가능 메모리에 저장된 선택 키를 이용하여 상기 개인 식별자의 해시 값을 결정하는 단계;

상기 결정된 해시 값을 상기 서버 액세스가능 메모리에 저장된 사용자 계정과 연관된 저장 해시 값과 비교하는 단계; 및

상기 비교에 기초하여 상기 안전한 환경에 액세스하기 위하여 사용자가 인증되었는지를 나타내는 인증 응답을 상기 원격 서버 프로세싱 시스템으로 전송하는 단계

를 포함하는 방법.

청구항 12

제11항에 있어서, 상기 사용자는,

상기 사용자 장치와 독립적인 사용자 프로세싱 시스템, 또는

상기 사용자 장치

중의 하나로부터 상기 안전한 환경을 액세스하도록 시도하는 방법.

청구항 13

제11항 또는 제12항에 있어서, 상기 사용자 장치는 휴대용 프로세싱 시스템인 방법.

청구항 14

제11항 내지 제13항 중 어느 한 항에 있어서, 상기 방법은, 상기 서버 프로세싱 시스템이,

상기 사용자의 아이덴티티를 증명하려고 시도하는 아이덴티티 데이터, 및

상기 사용자 장치를 식별하는 고유 장치 프로파일

을 나타내는 등록 요청을 수신하는 단계;

상기 아이덴티티 데이터에 기초하여 상기 사용자의 아이덴티티를 확인하는 단계; 및

상기 사용자의 아이덴티티의 긍정적인 확인에 기초하여 상기 사용자 계정을 생성하는 단계

를 포함하고,

상기 사용자 장치는 상기 고유 장치 프로파일에 기초하여 상기 사용자 계정과 연관된 방법.

청구항 15

제14항에 있어서, 상기 방법은, 사용자 등록시, 상기 서버 프로세싱 시스템이,

복수의 인덱스 키를 포함하는 상기 키맵을 상기 사용자 계정과 연관시키는 단계; 및

상기 사용자 장치의 메모리에 저장하기 위하여 상기 키맵을 나타내는 데이터를 상기 사용자 장치로 전송하는 단계

를 포함하는 방법.

청구항 16

제15항에 있어서, 상기 방법은, 상기 서버 프로세싱 시스템이,

상기 사용자로부터 개인 식별자 등록 요청을 수신하는 단계;

상기 키맵으로부터의 선택 키를 나타내는 인덱스를 상기 사용자 장치 또는 사용자로 전송하는 단계;

등록 코드를 수신하는 단계 - 상기 사용자는 상기 사용자 장치에 의해 제시된 선택 키 및 원하는 개인 식별자에 기초하여 상기 등록 코드를 결정함 -;

상기 등록 코드 및 상기 선택 키에 기초하여 상기 원하는 개인 식별자의 해시 값을 결정하는 단계; 및

상기 해시 값을 상기 사용자 계정에 저장하는 단계

를 포함하는 방법.

청구항 17

제15항에 있어서, 상기 방법은, 상기 서버 프로세싱 시스템이,

상기 사용자로부터 개인 식별자 등록 요청을 수신하는 단계;

상기 키맵으로부터의 제1 선택 키를 나타내는 제1 인덱스를 상기 사용자 장치 또는 사용자로 전송하는 단계;

제1 등록 코드를 수신하는 단계 - 상기 사용자는 상기 사용자 장치에 의해 제시된 상기 제1 선택키 및 원하는 개인 식별자에 기초하여 상기 제1 등록 코드를 결정함 -;

상기 제1 등록 코드 및 상기 제1 선택 키에 기초하여 상기 원하는 개인 식별자의 제1 해시 값을 결정하는 단계;

상기 키맵으로부터의 제2 선택 키를 나타내는 제2 인덱스를 상기 사용자 또는 사용자 장치로 전송하는 단계;

제2 등록 코드를 수신하는 단계 - 상기 사용자는 상기 사용자 장치에 의해 제시된 상기 제2 선택 키 및 상기 원하는 개인 식별자에 기초하여 상기 제2 등록 코드를 결정함 -;

상기 제2 등록 코드 및 상기 키맵으로부터의 제2 인덱스에 대응하는 상기 제2 선택 키를 이용하여 제2 해시 값을 결정하는 단계; 및

상기 제2 해시 값에 대응하는 제1 해시 값에 응답하여 상기 사용자 계정에 상기 제1 또는 제2 해시 값을 저장하는 단계

를 포함하는 방법.

청구항 18

제16항 또는 제17항에 있어서, 상기 방법은, 상기 서버 프로세싱 시스템이,

상기 사용자로부터 리셋 개인 식별자 요청을 수신하는 단계;

상기 사용자의 아이덴티티의 확인을 가능하게 하는 단계;

성공적인 확인에 응답하여, 상기 키맵으로부터의 선택 키의 인덱스를 상기 사용자 장치 또는 사용자로 전송하는 단계;

리셋 코드를 수신하는 단계 - 상기 사용자는 상기 선택 키 및 새로운 개인 식별자에 기초하여 상기 리셋 코드를 결정함 -;

상기 리셋 코드 및 상기 선택 키에 기초하여 상기 새로운 개인 식별자의 해시 값을 결정하는 단계; 및

상기 새로운 개인 식별자의 해시 값을 상기 사용자 계정에 저장하는 단계

를 포함하는 방법.

청구항 19

제14항 내지 제18항 중 어느 한 항에 있어서, 상기 방법은 서버 프로세싱 시스템이 상기 사용자의 디지털 증명서에 의해 지시된 사용자의 아이덴티티를 나타내는 데이터를 상기 사용자 계정에 저장하는 단계를 포함하는 방법.

청구항 20

제19항에 있어서, 상기 방법은 상기 서버 프로세싱 시스템이 상기 사용자 장치로부터 인덱스 요청을 수신하는 단계를 포함하고, 상기 인덱스 요청의 수신에 응답하여, 상기 서버 프로세싱 시스템은 상기 키맵으로부터의 선택 키의 인덱스를 상기 사용자 장치로 전송하는 방법.

청구항 21

원격 서버 프로세싱 시스템에 의해 제어되는 안전한 환경을 액세스하려고 시도하는 사용자를 인증하도록 서버 프로세싱 시스템을 구성하는 컴퓨터 판독가능 매체로서, 상기 컴퓨터 판독가능 매체는, 실행시, 제11항 내지 제20항 중 어느 한 항에 기재된 방법을 수행하도록 상기 서버 프로세싱 시스템을 구성하는 실행가능 명령을 포함하는 컴퓨터 판독가능 매체.

청구항 22

원격 서버 프로세싱 시스템에 의해 제어되는 안전한 환경을 액세스하려고 시도하는 사용자를 인증하는 시스템으로서, 상기 시스템은 서버 프로세싱 시스템 및 소프트웨어 애플리케이션을 포함하고, 상기 서버 프로세싱 시스템은,

상기 원격 서버 프로세싱 시스템으로부터 인증 요청을 수신하여 상기 안전한 환경을 액세스하려고 시도하는 사용자를 인증하고;

상기 사용자 장치의 메모리 또는 서버 액세스가능 메모리에 저장된 키맵으로부터의 선택 키에 대응하는 인덱스를 상기 사용자 또는 상기 사용자와 연관된 사용자 장치로 전송하고;

코드를 나타내는 데이터를 수신하고 - 상기 사용자는 상기 사용자 장치에 의해 제시된 선택 키 및 개인 식별자에 기초하여 상기 코드를 결정함 -;

상기 코드 및 상기 서버 액세스가능 메모리에 저장된 선택 키를 이용하여 상기 개인 식별자의 해시 값을 결정하고;

상기 결정된 해시 값을 상기 서버 액세스가능 메모리에 저장된 사용자 계정과 연관된 저장 해시 값과 비교하고;

상기 비교에 기초하여 상기 안전한 환경을 액세스하기 위하여 사용자가 인증되었는지를 나타내는 인증 응답을 상기 원격 서버 프로세싱 시스템으로 전송하도록

구성되고,

상기 소프트웨어 애플리케이션은 상기 사용자 장치에 의해 실행 가능하여,

상기 키맵을 수신하고,

상기 사용자 장치의 메모리에 상기 키맵을 저장하고,

상기 인덱스에 기초하여 상기 키맵으로부터의 상기 선택 키를 상기 사용자에게 제시하도록

상기 사용자 장치를 구성하는 시스템.

청구항 23

원격 서버 프로세싱 시스템에 의해 제어되는 안전한 환경을 액세스하려고 시도하는 사용자를 인증하는데 사용되는 개인 식별자를 사용자가 리셋하도록 하는 서버 프로세싱 시스템으로서, 상기 서버 프로세싱 시스템은,

상기 사용자로부터 리셋 개인 식별자 요청을 수신하고;

상기 사용자의 아이덴티티의 확인을 가능하게 하고;

성공적인 확인에 응답하여, 사용자 계정과 연관된 키맵으로부터의 선택 키에 대응하는 인덱스를 상기 사용자 장치 또는 사용자에게 전송하고 - 상기 키맵은 상기 사용자 장치의 메모리 및 서버 액세스가능 메모리에 저장됨 -;

리셋 코드를 수신하고 - 상기 사용자는 상기 선택 키맵 및 새로운 개인 식별자에 기초하여 상기 리셋 코드를 결정함 -;

상기 리셋 코드 및 상기 선택 키에 기초하여 상기 새로운 개인 식별자의 해시 값을 결정하고;

상기 새로운 개인 식별자의 해시 값을 상기 사용자 계정에 저장하도록

구성되는 서버 프로세싱 시스템.

청구항 24

원격 서버 프로세싱 시스템에 의해 제어되는 안전한 환경을 액세스하려고 시도하는 사용자를 인증하기 위하여 개인 식별자를 리셋하는 방법으로서, 상기 방법은, 상기 서버 프로세싱 시스템이,

상기 사용자로부터 리셋 개인 식별자 요청을 수신하는 단계;

상기 사용자의 아이덴티티의 확인을 가능하게 하는 단계;

성공적인 확인에 응답하여, 사용자 계정과 연관된 키맵으로부터의 선택 키에 대응하는 인덱스를 상기 사용자 장치 또는 사용자에게 전송하는 단계 - 상기 키맵은 상기 사용자 장치의 메모리 및 서버 액세스가능 메모리에 저장됨 -;

리셋 코드를 수신하는 단계 - 상기 사용자는 상기 선택 키맵 및 새로운 개인 식별자에 기초하여 상기 리셋 코드를 결정함 -;

상기 리셋 코드 및 상기 선택 키에 기초하여 상기 새로운 개인 식별자의 해시 값을 결정하는 단계; 및

상기 새로운 개인 식별자의 해시 값을 상기 사용자 계정에 저장하는 단계

를 포함하는 방법.

청구항 25

원격 서버 프로세싱 시스템에 의해 제어되는 안전한 환경을 액세스하려고 시도하는 사용자를 인증하는데 사용되는 개인 식별자를 사용자가 리셋하도록 하는 서버 프로세싱 시스템을 구성하는 컴퓨터 판독가능 매체로서, 상기 컴퓨터 판독가능 매체는, 실행시, 제24항에 기재된 방법을 수행하도록 상기 서버 프로세싱 시스템을 구성하는 실행가능 명령을 포함하는 컴퓨터 판독가능 매체.

발명의 설명

기 술 분 야

[0001] 관련 출원의 상호 참조

[0002] 본 출원은 2013년 4월 30일에 제출된 오스트레일리아 가출원 번호 2013901504의 우선권을 주장하며, 참고로 여기에 포함된다.

[0003] 본 발명은 사용자 인증을 위한 서버 프로세싱 시스템, 방법, 컴퓨터 판독가능 매체 및 시스템에 관한 것이다.

배 경 기 술

[0004] 일반적으로, 사용자가 안전한 웹 페이지 등의 안전한 환경으로의 액세스를 필요로 할 때, 안전한 환경으로의 액세스를 허가하기 전에 사용자의 인증이 필요하다. 현재 많은 방법이 존재한다.

[0005] 매우 공통적인 기술은 사용자가 사용자 아이덴티티 및 패스워드를 제공하도록 요청하는 것이다. 대부분의 경우, 사용자 아이덴티티 및 패스워드는 암호화되어 사용자 인증을 위한 서버 프로세싱 시스템으로 전송된다. 이러한 타입의 인증 기술에는 문제점이 존재한다. 예를 들어, 단말기 상에서 동작하는 악성 소프트웨어(즉, 키로깅(keylogging) 소프트웨어)가 사용자 입력을 로깅(logging)할 수 있고, 캡쳐된 사용자 아이덴티티와 패스워드는 나중의 사기적 활동에 악의적으로 사용될 수 있다.

[0006] 안전한 환경으로의 액세스를 요청하는 사용자를 인증하는데 생물학적 인증 기술이 또한 이용되어 왔다. 그러나, 사용자의 생물학적 특징이 변경될 수 없기 때문에, 사용자의 생물학적 특징(들)이 위태로운(compromise) 경우에 상당한 결점이 있다.

[0007] 스마트 카드 등의 물리적 토큰(token)이 또한 안전한 환경으로의 액세스를 요청하는 사용자를 인증하는 수단으로서 사용되어 왔다. 그러나, 이러한 장치는 언제나 장치를 휴대할 수 없는 사용자에게 불편하고 장치가 인증시 존재한다는 것만을 확인할 뿐 물리적 토큰을 제시한 사용자가 실제로 인증을 요청하는 정확한 사용자라는 것을 실제로 확인하지 못한다.

발명의 내용

과제의 해결 수단

[0008] 일 형태에 있어서, 원격 서버 프로세싱 시스템에 의해 제어되는 안전한 환경을 액세스하려고 시도하는 사용자를 인증하는 서버 프로세싱 시스템으로서, 상기 서버 프로세싱 시스템은, 상기 원격 서버 프로세싱 시스템으로부터 인증 요청을 수신하여 상기 안전한 환경을 액세스하려고 시도하는 사용자를 인증하고; 상기 사용자 장치의 메모리 또는 서버 액세스가능 메모리에 저장된 키맵으로부터의 선택 키에 대응하는 인덱스를 상기 사용자 또는 상기 사용자와 연관된 사용자 장치로 전송하고; 코드를 나타내는 데이터를 수신하고 - 상기 사용자는 상기 사용자 장치에 의해 제시된 선택 키 및 개인 식별자에 기초하여 상기 코드를 결정함 -; 상기 코드 및 상기 서버 액세스가능 메모리에 저장된 선택 키를 이용하여 상기 개인 식별자의 해시(hash) 값을 결정하고; 상기 결정된 해시 값을 상기 서버 액세스가능 메모리에 저장된 사용자 계정과 연관된 저장 해시 값과 비교하고; 상기 비교에 기초하여 상기 안전한 환경을 액세스하기 위하여 사용자가 인증되었는지를 나타내는 인증 응답을 상기 원격 서버 프로세싱 시스템으로 전송하도록 구성되는 서버 프로세싱 시스템이 제공된다.

[0009] 소정의 실시예에서, 상기 사용자는, 상기 사용자 장치와 독립적인 사용자 프로세싱 시스템, 또는 상기 사용자 장치 중의 하나로부터 상기 안전한 환경을 액세스하도록 시도한다..

[0010] 소정의 실시예에서, 상기 사용자 장치는 휴대용 프로세싱 시스템이다.

[0011] 상기 서버 프로세싱 시스템은, 상기 사용자의 아이덴티티를 증명하려고 시도하는 아이덴티티 데이터, 및 상기 사용자 장치를 식별하는 고유 장치 프로파일을 나타내는 등록 요청을 수신하고; 상기 아이덴티티 데이터에 기초하여 상기 사용자의 아이덴티티를 확인하고; 상기 사용자의 아이덴티티의 긍정적인 확인에 기초하여 상기 사용자 계정을 생성하도록 구성되고, 상기 사용자 장치는 상기 고유 장치 프로파일에 기초하여 상기 사용자 계정과 연관된다.

[0012] 소정의 실시예에서, 사용자 등록시, 상기 서버 프로세싱 시스템은, 복수의 인덱스 키를 포함하는 상기 키맵을 상기 사용자 계정과 연관시키고; 상기 사용자 장치의 메모리에 저장하기 위하여 상기 키맵을 나타내는 데이터를 상기 사용자 장치로 전송하도록 구성된다.

[0013] 소정의 실시예에서, 상기 서버 프로세싱 시스템은, 상기 사용자로부터 개인 식별자 등록 요청을 수신하고; 상기 키맵으로부터의 선택 키를 나타내는 인덱스를 상기 사용자 장치 또는 사용자로 전송하고; 등록 코드를 수신하고 - 상기 사용자는 상기 사용자 장치에 의해 제시된 선택 키 및 원하는 개인 식별자에 기초하여 상기 등록 코드를 결정함 -; 상기 등록 코드 및 상기 선택 키에 기초하여 상기 원하는 개인 식별자의 해시 값을 결정하고; 상기 해시 값을 상기 사용자 계정에 저장하도록 구성된다.

[0014] 소정의 실시예에서, 상기 서버 프로세싱 시스템은, 상기 사용자로부터 개인 식별자 등록 요청을 수신하고; 상기

키맵으로부터의 제1 선택 키를 나타내는 제1 인덱스를 상기 사용자 장치 또는 사용자로 전송하고; 등록 코드를 수신하고 - 상기 사용자는 상기 사용자 장치에 의해 제시된 상기 제1 선택키 및 원하는 개인 식별자에 기초하여 상기 등록 코드를 결정함 -; 상기 등록 코드 및 상기 제1 선택 키에 기초하여 상기 원하는 개인 식별자의 제1 해시 값을 결정하고; 상기 키맵으로부터의 제2 선택 키를 나타내는 제2 인덱스를 상기 사용자 장치 또는 사용자로 전송하고; 제2 등록 코드를 수신하고 - 상기 사용자는 상기 제2 선택 키 및 상기 원하는 개인 식별자에 기초하여 상기 제2 등록 코드를 결정함 - ; 상기 제2 등록 코드 및 상기 키맵으로부터의 제2 인덱스에 대응하는 상기 제2 선택 키를 이용하여 제2 해시 값을 결정하고; 상기 제2 해시 값에 대응하는 제1 해시 값에 응답하여 상기 사용자 계정에 상기 제1 또는 제2 해시 값을 저장하도록 구성된다.

[0015] 소정의 실시예에서, 상기 서버 프로세싱 시스템은, 상기 사용자로부터 리셋 개인 식별자 요청을 수신하고; 상기 사용자의 아이덴티티의 확인을 가능하게 하고; 성공적인 확인에 응답하여, 상기 키맵으로부터의 선택 키의 인덱스를 상기 사용자 장치 또는 사용자로 전송하고; 리셋 코드를 수신하고 - 상기 사용자는 상기 사용자 장치에 의해 제시된 상기 선택 키 및 새로운 개인 식별자에 기초하여 상기 리셋 코드를 결정함 -; 상기 리셋 코드 및 상기 선택 키에 기초하여 상기 새로운 개인 식별자의 해시 값을 결정하고; 상기 새로운 개인 식별자의 해시 값을 상기 사용자 계정에 저장하도록 구성된다.

[0016] 소정의 실시예에서, 상기 서버 프로세싱 시스템은 상기 사용자의 디지털 증명서에 의해 지시된 사용자의 아이덴티티를 나타내는 데이터를 상기 사용자 계정에 저장하도록 구성된다.

[0017] 소정의 실시예에서, 상기 서버 프로세싱 시스템은 상기 사용자 장치로부터 인덱스 요청을 수신하도록 구성되고, 상기 인덱스 요청의 수신에 응답하여, 상기 서버 프로세싱 시스템은 상기 키맵으로부터의 선택 키의 인덱스를 상기 사용자 장치로 전송한다.

[0018] 제2 형태에 있어서, 원격 서버 프로세싱 시스템에 의해 제어되는 안전한 환경을 액세스하려고 시도하는 사용자를 인증하는 방법으로서, 상기 방법은, 상기 서버 프로세싱 시스템이, 상기 원격 서버 프로세싱 시스템으로부터 인증 요청을 수신하여 상기 안전한 환경을 액세스하려고 시도하는 사용자를 인증하는 단계; 상기 사용자 장치의 메모리 또는 서버 액세스가능 메모리에 저장된 키맵으로부터의 선택 키에 대응하는 인덱스를 상기 사용자 또는 상기 사용자와 연관된 사용자 장치로 전송하는 단계; 코드를 나타내는 데이터를 수신하는 단계 - 상기 사용자는 상기 사용자 장치에 의해 제시된 선택 키 및 개인 식별자에 기초하여 상기 코드를 결정함 -; 상기 코드 및 상기 서버 액세스가능 메모리에 저장된 선택 키를 이용하여 상기 개인 식별자의 해시 값을 결정하는 단계; 상기 결정된 해시 값을 상기 서버 액세스가능 메모리에 저장된 사용자 계정과 연관된 저장 해시 값과 비교하는 단계; 및 상기 비교에 기초하여 상기 안전한 환경에 액세스하기 위하여 사용자가 인증되었는지를 나타내는 인증 응답을 상기 원격 서버 프로세싱 시스템으로 전송하는 단계를 포함하는 방법이 제공된다.

[0019] 소정의 실시예에서, 상기 사용자는, 상기 사용자 장치와 독립적인 사용자 프로세싱 시스템, 또는 상기 사용자 장치 중의 하나로부터 상기 안전한 환경을 액세스하도록 시도한다.

[0020] 소정의 실시예에서, 상기 사용자 장치는 휴대용 프로세싱 시스템이다.

[0021] 소정의 실시예에서, 상기 방법은, 상기 서버 프로세싱 시스템이, 상기 사용자의 아이덴티티를 증명하려고 시도하는 아이덴티티 데이터, 및 상기 사용자 장치를 식별하는 고유 장치 프로파일을 나타내는 등록 요청을 수신하는 단계; 상기 아이덴티티 데이터에 기초하여 상기 사용자의 아이덴티티를 확인하는 단계; 및 상기 사용자의 아이덴티티의 긍정적인 확인에 기초하여 상기 사용자 계정을 생성하는 단계를 포함하고, 상기 사용자 장치는 상기 고유 장치 프로파일에 기초하여 상기 사용자 계정과 연관된다.

[0022] 소정의 실시예에서, 상기 방법은, 사용자 등록시, 상기 서버 프로세싱 시스템이, 복수의 인덱스 키를 포함하는 상기 키맵을 상기 사용자 계정과 연관시키는 단계; 및 상기 사용자 장치의 메모리에 저장하기 위하여 상기 키맵을 나타내는 데이터를 상기 사용자 장치로 전송하는 단계를 포함한다.

[0023] 소정의 실시예에서, 상기 방법은, 상기 서버 프로세싱 시스템이, 상기 사용자로부터 개인 식별자 등록 요청을 수신하는 단계; 상기 키맵으로부터의 선택 키를 나타내는 인덱스를 상기 사용자 장치 또는 사용자로 전송하는 단계; 등록 코드를 수신하는 단계 - 상기 사용자는 상기 사용자 장치에 의해 제시된 선택 키 및 원하는 개인 식별자에 기초하여 상기 등록 코드를 결정함 -; 상기 등록 코드 및 상기 선택 키에 기초하여 상기 원하는 개인 식별자의 해시 값을 결정하는 단계; 및 상기 해시 값을 상기 사용자 계정에 저장하는 단계를 포함한다.

[0024] 소정의 실시예에서, 상기 방법은, 상기 서버 프로세싱 시스템이, 상기 사용자로부터 개인 식별자 등록 요청을 수신하는 단계; 상기 키맵으로부터의 제1 선택 키를 나타내는 제1 인덱스를 상기 사용자 장치 또는 사용자로 전

송하는 단계; 제1 등록 코드를 수신하는 단계 - 상기 사용자는 상기 사용자 장치에 의해 제시된 상기 제1 선택 키 및 원하는 개인 식별자에 기초하여 상기 제1 등록 코드를 결정함 -; 상기 제1 등록 코드 및 상기 제1 선택 키에 기초하여 상기 원하는 개인 식별자의 제1 해시 값을 결정하는 단계; 상기 키맵으로부터의 제2 선택 키를 나타내는 제2 인덱스를 상기 사용자 또는 사용자 장치로 전송하는 단계; 제2 등록 코드를 수신하는 단계 - 상기 사용자는 상기 사용자 장치에 의해 제시된 상기 제2 선택 키 및 상기 원하는 개인 식별자에 기초하여 상기 제2 등록 코드를 결정함 -; 상기 제2 등록 코드 및 상기 키맵으로부터의 제2 인덱스에 대응하는 상기 제2 선택 키를 이용하여 제2 해시 값을 결정하는 단계; 및 상기 제2 해시 값에 대응하는 제1 해시 값에 응답하여 상기 사용자 계정에 상기 제1 또는 제2 해시 값을 저장하는 단계를 포함한다.

[0025] 소정의 실시예에서, 상기 방법은, 상기 서버 프로세싱 시스템이, 상기 사용자로부터 리셋 개인 식별자 요청을 수신하는 단계; 상기 사용자의 아이덴티티의 확인을 가능하게 하는 단계; 성공적인 확인에 응답하여, 상기 키맵으로부터의 선택 키의 인덱스를 상기 사용자 장치 또는 사용자로 전송하는 단계; 리셋 코드를 수신하는 단계 - 상기 사용자는 상기 선택 키 및 새로운 개인 식별자에 기초하여 상기 리셋 코드를 결정함 -; 상기 리셋 코드 및 상기 선택 키에 기초하여 상기 새로운 개인 식별자의 해시 값을 결정하는 단계; 및 상기 새로운 개인 식별자의 해시 값을 상기 사용자 계정에 저장하는 단계를 포함한다.

[0026] 소정의 실시예에서, 상기 방법은 서버 프로세싱 시스템이 상기 사용자의 디지털 증명서에 의해 지시된 사용자의 아이덴티티를 나타내는 데이터를 상기 사용자 계정에 저장하는 단계를 포함한다.

[0027] 소정의 실시예에서, 상기 방법은 상기 서버 프로세싱 시스템이 상기 사용자 장치로부터 인덱스 요청을 수신하는 단계를 포함하고, 상기 인덱스 요청의 수신에 응답하여, 상기 서버 프로세싱 시스템은 상기 키맵으로부터의 선택 키의 인덱스를 상기 사용자 장치로 전송한다.

[0028] 제3 형태에 있어서, 원격 서버 프로세싱 시스템에 의해 제어되는 안전한 환경을 액세스하려고 시도하는 사용자를 인증하도록 서버 프로세싱 시스템을 구성하는 컴퓨터 판독가능 매체로서, 상기 컴퓨터 판독가능 매체는, 실행시, 제2 형태의 방법을 수행하도록 상기 서버 프로세싱 시스템을 구성하는 실행가능 명령을 포함하는 컴퓨터 판독가능 매체가 제공된다.

[0029] 제4 형태에 있어서, 원격 서버 프로세싱 시스템에 의해 제어되는 안전한 환경을 액세스하려고 시도하는 사용자를 인증하는 시스템으로서, 상기 시스템은 서버 프로세싱 시스템 및 소프트웨어 애플리케이션을 포함하고, 상기 서버 프로세싱 시스템은, 상기 원격 서버 프로세싱 시스템으로부터 인증 요청을 수신하여 상기 안전한 환경을 액세스하려고 시도하는 사용자를 인증하고; 상기 사용자 장치의 메모리 또는 서버 액세스가능 메모리에 저장된 키맵으로부터의 선택 키에 대응하는 인덱스를 상기 사용자 또는 상기 사용자와 연관된 사용자 장치로 전송하고; 코드를 나타내는 데이터를 수신하고 - 상기 사용자는 상기 사용자 장치에 의해 제시된 선택 키 및 개인 식별자에 기초하여 상기 코드를 결정함 -; 상기 코드 및 상기 서버 액세스가능 메모리에 저장된 선택 키를 이용하여 상기 개인 식별자의 해시 값을 결정하고; 상기 결정된 해시 값을 상기 서버 액세스가능 메모리에 저장된 사용자 계정과 연관된 저장 해시 값과 비교하고; 상기 비교에 기초하여 상기 안전한 환경을 액세스하기 위하여 사용자가 인증되었는지를 나타내는 인증 응답을 상기 원격 서버 프로세싱 시스템으로 전송하도록 구성되고, 상기 소프트웨어 애플리케이션은 상기 사용자 장치에 의해 실행 가능하여, 상기 키맵을 수신하고, 상기 사용자 장치의 메모리에 상기 키맵을 저장하고, 상기 인덱스에 기초하여 상기 키맵으로부터의 상기 선택 키를 상기 사용자에게 제시하도록 상기 사용자 장치를 구성하는 시스템이 제공된다.

[0030] 제5 형태에 있어서, 원격 서버 프로세싱 시스템에 의해 제어되는 안전한 환경을 액세스하려고 시도하는 사용자를 인증하는데 사용되는 개인 식별자를 사용자가 리셋하도록 하는 서버 프로세싱 시스템으로서, 상기 서버 프로세싱 시스템은, 상기 사용자로부터 리셋 개인 식별자 요청을 수신하고; 상기 사용자의 아이덴티티의 확인을 가능하게 하고; 성공적인 확인에 응답하여, 사용자 계정과 연관된 키맵으로부터의 선택 키에 대응하는 인덱스를 상기 사용자 장치 또는 사용자에게 전송하고 - 상기 키맵은 상기 사용자 장치의 메모리 및 서버 액세스가능 메모리에 저장됨 -; 리셋 코드를 수신하고 - 상기 사용자는 상기 선택 키맵 및 새로운 개인 식별자에 기초하여 상기 리셋 코드를 결정함 -; 상기 리셋 코드 및 상기 선택 키에 기초하여 상기 새로운 개인 식별자의 해시 값을 결정하고; 상기 새로운 개인 식별자의 해시 값을 상기 사용자 계정에 저장하도록 구성되는 서버 프로세싱 시스템이 제공된다.

[0031] 제6 형태에 있어서, 원격 서버 프로세싱 시스템에 의해 제어되는 안전한 환경을 액세스하려고 시도하는 사용자를 인증하기 위하여 개인 식별자를 리셋하는 방법으로서, 상기 방법은, 상기 서버 프로세싱 시스템이, 상기 사용자로부터 리셋 개인 식별자 요청을 수신하는 단계; 상기 사용자의 아이덴티티의 확인을 가능하게 하는 단계;

성공적인 확인에 응답하여, 사용자 계정과 연관된 키맵으로부터의 선택 키에 대응하는 인덱스를 상기 사용자 장치 또는 사용자에게 전송하는 단계 - 상기 키맵은 상기 사용자 장치의 메모리 및 서버 액세스가능 메모리에 저장됨 -; 리셋 코드를 수신하는 단계 - 상기 사용자는 상기 선택 키맵 및 새로운 개인 식별자에 기초하여 상기 리셋 코드를 결정함 -; 상기 리셋 코드 및 상기 선택 키에 기초하여 상기 새로운 개인 식별자의 해시 값을 결정하는 단계; 및 상기 새로운 개인 식별자의 해시 값을 상기 사용자 계정에 저장하는 단계를 포함하는 방법이 제공된다.

[0032] 제7 형태에 있어서, 원격 서버 프로세싱 시스템에 의해 제어되는 안전한 환경을 액세스하려고 시도하는 사용자를 인증하는데 사용되는 개인 식별자를 사용자가 리셋하도록 하는 서버 프로세싱 시스템을 구성하는 컴퓨터 판독가능 매체로서, 상기 컴퓨터 판독가능 매체는, 실행시, 제6 형태의 방법을 수행하도록 상기 서버 프로세싱 시스템을 구성하는 실행가능 명령을 포함하는 컴퓨터 판독가능 매체가 제공된다.

[0033] 다른 형태 및 실시예는 상세한 설명을 통해 실현될 것이다.

도면의 간단한 설명

[0034] 예시적인 실시예는 첨부된 도면과 결합하여 적어도 하나의 바람직한 비제한 실시예의 예로서 주어지는 다음의 설명으로부터 명백해질 것이다.

도 1은 특정 실시예를 구현하거나 그에 효과를 제공하는데 이용될 수 있는 예시적인 프로세싱 시스템의 기능 블록도.

도 2는 특정 실시예를 구현하거나 그에 효과를 제공하는데 이용될 수 있는 예시적인 네트워크 인프라스트럭쳐를 나타내는 도면.

도 3은 안전한 환경으로의 액세스를 시도하는 사용자를 인증하는 시스템의 시스템 다이어그램.

도 4는 안전한 환경으로의 액세스를 시도하는 사용자를 인증하기 위하여 서버 프로세싱 시스템에 의해 수행되는 예시적인 방법을 나타내는 흐름도.

도 5는 서버 프로세싱 시스템에 의해 제공되는 인증 서비스를 이용하기 위하여 사용자가 등록하는 예시적인 방법을 나타내는 플로우챠트.

도 6a는 예시적인 키맵을 나타내는 도면.

도 6b는 키 및 식별자 참조의 그래픽 표시를 포함하는 예시적인 사용자 인터페이스를 나타내는 도면.

도 7은 사용자를 인증하는데 사용하기 위하여 사용자가 개인 식별자를 리셋하는 예시적인 방법을 나타내는 플로우챠트.

발명을 실시하기 위한 구체적인 내용

[0035] 바람직한 실시예 또는 실시예들의 주제를 더 정밀하게 이해하기 위하여 단지 예로서 주어지는 다음의 모드가 기재된다. 예시적인 실시예의 특징을 설명하도록 포함된 도면에서, 동일한 참조 번호는 도면에 걸쳐 동일한 부분을 확인하는데 사용된다.

[0036] 예시적인 프로세싱 시스템

[0037] 특정 실시예는 프로세싱 시스템을 이용하여 실현될 수 있고, 그 예는 도 1에 도시된다. 특히, 프로세싱 시스템(100)은 일반적으로 버스 또는 버스의 그룹(110)을 통해 접속된 적어도 하나의 프로세서(102) 또는 프로세싱 유닛 또는 복수의 프로세서, 메모리(104), 적어도 하나의 입력 장치(106) 및 적어도 하나의 출력 장치(108)를 포함한다. 소정의 실시예에서, 입력 장치(106) 및 출력 장치(108)는 동일한 장치일 수 있다. 인터페이스(112)는 또한 프로세싱 시스템(100)을 하나 이상의 주변 장치에 결합하기 위하여 제공될 수 있고, 예를 들어, 인터페이스(112)는 PCI 카드 또는 PC 카드일 수 있다. 적어도 하나의 데이터베이스(116)를 하우징하는 적어도 하나의 저장 장치(114)가 또한 제공될 수 있다. 메모리(104)는 임의의 형태의 메모리 장치, 예를 들어, 휘발성 또는 비휘발성 메모리, 솔리드 스테이트 저장 장치, 자기 장치 등일 수 있다. 프로세서(102)는 예를 들어 1보다 많은 개별 프로세싱 장치를 포함하여 프로세싱 시스템(100) 내의 상이한 기능을 처리할 수 있다.

[0038] 입력 장치(106)는 입력 데이터(118)를 수신하고 예를 들어 키보드, 펜형상 장치 또는 마우스 등의 포인터 장치, 마이크로폰 등의 보이스 제어 활성화를 위한 오디오 수신 장치, 모뎀 또는 무선 데이터 어댑터 등의 데이터 수

신기 또는 안테나, 데이터 획득 카드 등을 포함할 수 있다. 입력 데이터(118)는 예를 들어 네트워크를 통해 수신된 데이터와 결합하여 상이한 소스, 예를 들어, 키보드 명령으로부터 비롯될 수 있다. 출력 장치(108)는 출력 데이터(120)를 생성 또는 발생하고 예를 들어 출력 데이터(120)가 시각적으로 보이는 경우의 디스플레이 장치 또는 모니터, 출력 데이터(120)가 인쇄되는 경우의 프린터, 포트, 예를 들어, USB 포트, 주변 컴포넌트 어댑터, 모뎀 또는 무선 네트워크 어댑터 등의 데이터 송신기 또는 안테나 등을 포함할 수 있다. 출력 데이터(120)는 개별적이며, 상이한 출력 장치, 예를 들어, 네트워크로 송신되는 데이터와 결합하여 모니터 상의 시각 디스플레이로부터 도출될 수 있다. 사용자는 예를 들어 모니터 상에서 또는 프린터를 이용하여 데이터 출력 또는 데이터 출력의 해석(interpretation)을 볼 수 있다. 저장 장치(114)는 임의의 형태의 데이터 또는 정보 저장 수단, 예를 들어, 휘발성 또는 비휘발성 메모리, 솔리드 스테이트 저장 장치, 자기 장치 등일 수 있다.

[0039] 사용에 있어서, 프로세싱 시스템(100)은 유선 또는 무선 통신 수단을 통해 데이터 또는 정보가 적어도 하나의 데이터베이스(116) 및/또는 메모리(104)에 저장되고 및/또는 그로부터 검색(retrieve)되도록 적응된다. 인터페이스(112)는 프로세싱 유닛(102) 및 특수 목적을 제공할 수 있는 주변 컴포넌트 사이의 유선 및/또는 무선 통신을 허용할 수 있다. 프로세서(102)는 입력 장치(106)를 통해 입력 데이터(118)로서 명령을 수신하고 출력 장치(108)를 이용함으로써 사용자에게 프로세싱된 결과 또는 다른 출력을 디스플레이할 수 있다. 1보다 많은 입력 장치(106) 및/또는 출력 장치(108)가 제공될 수 있다. 프로세싱 시스템(100)은 임의의 형태의 단말, 서버, 특수 하드웨어 등일 수 있음을 인식해야 한다.

[0040] 프로세싱 장치(100)는 도 2에 도시된 바와 같이 네트워킹 통신 시스템(200)의 일부일 수 있다. 프로세싱 장치(100)는 네트워크(202), 예를 들어, 인터넷 또는 WAN에 접속될 수 있다. 입력 데이터(118) 및 출력 데이터(120)는 네트워크(202)를 통해 다른 장치에 전달될 수 있다. 다른 단말, 예를 들어, 씬 클라이언트(thin client)(204), 추가의 프로세싱 시스템(206, 209), 노트북 컴퓨터(210), 메인프레임 컴퓨터(212), PDA(214), 폰 기반 컴퓨터(216), 서버(218) 등이 네트워크(202)에 접속될 수 있다. 많은 다른 다양한 타입의 단말 또는 구성이 이용될 수 있다. 네트워크(202)를 통한 정보 및/또는 데이터의 전송은 유선 통신 수단(220) 또는 무선 통신 수단(222)을 이용하여 달성될 수 있다. 서버(218)는 네트워크(202) 및 하나 이상의 데이터베이스(224) 간의 데이터 전송을 가능하게 할 수 있다. 서버(218) 및 하나 이상의 데이터베이스(224)는 정보 소스의 예를 제공한다.

[0041] 다른 네트워크가 네트워크(202)와 통신할 수 있다. 예를 들어, 텔레커뮤니케이션 네트워크(230)는 무선 통신 수단(236) 및 수신/송신 스테이션(238)을 이용함으로써 네트워크(202) 및 모바일 또는 셀룰러 전화(232) 또는 PDA 타입 장치(234) 간의 데이터 전송을 가능하게 할 수 있다. 위성 통신 네트워크(240)는 위성(244)으로부터 데이터 신호를 수신하는 위성 신호 수신기(242)와 통신할 수 있고, 결과적으로, 위성 신호 송신기(246)와 원격 통신한다. 단말, 예를 들어, 추가의 프로세싱 시스템(248), 노트북 컴퓨터(250) 또는 위성 전화(252)는 네트워크(202)와 통신할 수 있다. 예를 들어 전용 네트워크, LAN 등일 수 있는 로컬 네트워크(260)가 또한 네트워크(202)에 접속될 수 있다. 예를 들어, 네트워크(202)는 단말(264), 데이터베이스(268)로 및/또는 로부터의 데이터의 전송을 제어하는 서버(266), 및 프린터(270)를 접속하는 이더넷(262)과 접속될 수 있다. 다양한 다른 타입의 네트워크가 사용될 수 있다.

[0042] 프로세싱 장치(100)는 데이터(118, 120)를 네트워크(202)로 및 로부터 송수신함으로써 다른 단말, 예를 들어, 추가의 프로세싱 시스템(206, 208)과 통신하도록 적응되어, 네트워킹 통신 시스템(200)의 다른 컴포넌트와의 가능한 통신을 가능하게 한다.

[0043] 따라서, 예를 들어, 네트워크(202, 230, 240)는 인터넷의 일부를 형성하거나 인터넷에 접속될 수 있고, 이 경우, 단말(206, 212, 218)은 예를 들어 웹 서버, 인터넷 단말 등일 수 있다. 네트워크(202, 230, 240, 260)는 LAN, WAN, 이더넷, 토큰 링, FDDI 링, 스타(star) 네트워크 등의 다른 통신 네트워크 또는 GSM, CDMA 또는 3G 네트워크 등의 모바일 전화 네트워크 등이거나 그 일부를 형성할 수 있고, 특정 구현예에 따라 예를 들어 광파이버 또는 무선 네트워크를 포함하여 전체적으로 또는 부분적으로 유선일 수 있다.

[0044] 시스템의 개요

[0045] 도 3을 참조하면, 안전한 환경(325)으로의 액세스를 시도하는 사용자(350)를 인증하는 예시적인 시스템(300)을 나타내는 시스템 다이어그램이 도시된다.

[0046] 특히, 시스템(300)은 데이터 통신 수단을 통해 원격 서버 프로세싱 시스템(320)과 데이터 통신하는 서버 프로세

싱 시스템(310)을 포함한다. 서버 프로세싱 시스템(310)은 데이터베이스의 형태로 제공되는 서버 액세스가능 메모리(315)와 연관되고, 서버 액세스가능 메모리는 사용자(350)를 인증하기 위한 계정(account) 데이터를 저장한다. 원격 프로세싱 시스템(320)은 허가된 사용자로 제한되는 안전한 환경(325)으로의 액세스를 제어한다. 안전한 환경(325)의 예는 안전한 웹사이트, 안전한 서버 서비스 등의 디지털 환경 또는 빌딩 내의 안전한 문 등의 잠재적으로 물리적인 환경을 포함한다.

[0047] 시스템(300)은 또한 데이터 통신 수단을 통해 원격 서버 프로세싱 시스템(320)과 데이터 통신하는 사용자 프로세싱 시스템(340)을 포함할 수 있다. 사용자(350)는 안전한 환경(325)으로 액세스하기 위하여 사용자 프로세싱 시스템(340)과 상호작용하여 원격 서버 프로세싱 시스템(320)으로 요청을 전송한다. 사용자 프로세싱 시스템(340)의 예는 데스크탑 단말, 랩탑, 태블릿 컴퓨터 등을 포함할 수 있다.

[0048] 시스템(300)은, 또한, 사용자 프로세싱 시스템(340)과 독립적이고, 사용자(350)와 연관되고 데이터 통신 수단을 통해 서버 프로세싱 시스템(310)과 데이터 통신하는 사용자 장치(330)를 포함한다. 사용자 장치(330)는 바람직하게 모바일 전화(즉, "스마트폰 등), 착용가능 프로세싱 시스템(즉, 구글 글래스(Google Glass)™) 또는 사용자 프로세싱 시스템(340)과 별개이고 사용자(350)와 연관된 임의의 다른 상호작용 장치 등의 사용자(350)와 연관된 휴대용 프로세싱 시스템이다. 사용자 장치(330)는 인증을 위해 사용자에게 인터페이스를 제시하는 소프트웨어 애플리케이션(335)(일반적으로 "앱(app)"라 함)을 메모리에 저장한다.

[0049] 하나의 형태에 있어서, 사용자 프로세싱 시스템이 필요하지 않다. 특히, 사용자는 안전한 환경(325)으로 액세스하기 위하여 사용자 장치와 상호 작용하여 원격 서버 프로세싱 시스템(320)에 요청을 전송할 수 있다.

[0050] 등록

[0051] 도 4를 참조하면, 원격 서버 프로세싱 시스템(320)에 의해 제어되는 안전한 환경(325)을 액세스할 때 사용자(350)를 인증하는 서버 프로세싱 시스템(310)에 사용자(350)가 등록하는 예시적인 방법(400)을 나타내는 플로우 챠트가 도시된다.

[0052] 특히, 단계(405)에서, 방법(400)은 사용자(350)가 등록 요청을 서버 프로세싱 시스템(310)으로 전송하는 단계를 포함한다. 등록 요청은 사용자(350)에 의해 동작하는 사용자 장치(330) 및/또는 사용자 프로세싱 시스템(340)으로부터 전송될 수 있다. 특히, 등록 요청이 적어도 부분적으로 사용자 장치(330)를 이용하여 제출되는 경우에, 이것은 사용자가 사용자 장치(330) 상에 소프트웨어 애플리케이션(335)을 설치하고 소프트웨어 애플리케이션(335)을 런칭(launch)하고 사용자가 소프트웨어 애플리케이션(335)과 상호 작용하여 등록 요청을 제출하는 것에 응답할 수 있다. 등록 요청은 사용자(350)의 아이덴티티를 증명하도록 시도하는 아이덴티티 데이터를 나타낼 수 있고, 고유한 장치 식별자는 사용자 장치(330)를 나타낼 수 있다. 아이덴티티 데이터는 크레딧 카드 번호, 패스포트 번호, 유틸리티 빌(utility bills), 어드레스 및 다른 유사한 정보를 나타낼 수 있다. 특정 실시예에서, 고유 장치 식별자는 소프트웨어 애플리케이션(335)에 의해 발생된 고유 장치 프로파일이다. 소프트웨어 애플리케이션(335)은 사용자 장치(330)의 다수의 특징을 결정하고 결정된 특징을 이용하여 고유 장치 프로파일을 생성한다. 결정된 특징은 사용자 장치(330)(CPU, 메모리 등)의 하드웨어, 사용자 장치(330)의 MAC 어드레스, 사용자와 연관된 디지털 증명서를 나타낼 수 있는 소프트웨어 프로파일 및 사용자 장치(330)와 연관된 하나 이상의 식별자 중의 하나 이상의 특징을 포함할 수 있다. 소프트웨어 애플리케이션(335)은 결정된 특징에 해싱(hashing) 알고리즘을 적용하여 해시 값의 형태로 고유 장치 프로파일을 생성한다. 그 후, 고유 장치 프로파일은 저장을 위해 서버 프로세싱 시스템으로 전송된다. 고유 장치 프로파일은 장치 서명(signature)으로서 동작하여 사용자 장치(330)의 다수의 특징에 기초하여 사용자 장치(330)를 고유하게 식별한다. 특정 실시예에서, 고유 장치 프로파일은 또한 사용자 장치(330)의 메모리에 저장되고 이하에서 상세히 설명하는 바와 같이 보안 검사(security check)를 구현하는데 사용될 수 있다.

[0053] 단계(410)에서, 방법(400)은 서버 프로세싱 시스템(310)이 아이덴티티 데이터에 기초하여 사용자(350)의 아이덴티티의 확인(verification)을 가능하게 하는 단계를 포함한다. 특히, 서버 프로세싱 시스템(310)은 정보의 세트가 단일 사용자와 연관된다는 것을 확인하려는 시도에서 아이덴티티 확인기(IDV; identity verifier)를 이용할 수 있다. 긍정적인 확인에 응답하여, 방법은 단계(415)로 진행한다. 그렇지 않으면, 서버 프로세싱 시스템(310)은 사용자(350)에게 추가의 식별 정보를 요청할 수 있다.

[0054] 단계(415)에서, 방법(400)은 서버 프로세싱 시스템(310)이 서버 프로세싱 시스템(310)과 연관된 메모리(315)에 사용자 계정을 생성하는 단계를 포함한다. 메모리(315)는 바람직하게 서버 프로세싱 시스템(310)에 의해 액세

스가능한 데이터베이스이다. 서버 프로세싱 시스템(310)은, 특정 실시예에서 고유 장치 프로파일인 고유 장치 식별자에 기초하여 사용자 장치(330)를 사용자 계정과 연관시킨다.

[0055] 단계(420)에서, 방법(400)은 서버 프로세싱 시스템(310)이 키맵(keymap)(600) 및 사용자 계정 간의 연관성을 저장하는 단계를 포함한다. 특히, 각각의 키맵(600)은 고유 인덱스 번호(610)(즉, 일련 번호)와 연관된 복수의 고유 키(620)를 포함한다. 복수의 키(620) 및 연관된 인덱스(660)를 포함하는 키맵(650)의 그래픽 표시의 예가 도 6a에 도시된다. 특히, 각각의 키(620)는 복수의 고유 키 부분(630)을 포함한다. 이 예에서, 각각의 키(620)는 알파벳 키 부분을 포함하지만, 다른 형태의 키가 이용될 수 있다.

[0056] 단계(425)에서, 방법(400)은 서버 프로세싱 시스템(310)이 사용자 계정과 연관된 키맵(600)의 복수의 인덱스 키를 나타내는 키맵 데이터를 사용자 장치(300)로 전송하는 단계를 포함한다.

[0057] 단계(430)에서, 방법(400)은 사용자 장치(330)가 키맵 데이터를 로컬 메모리에 저장하는 단계를 포함한다.

[0058] 단계(435)에서, 방법(400)은 서버 프로세싱 시스템(310)이 사용자(350)로부터 개인 식별자 등록 요청을 수신하는 단계를 포함한다. 개인 식별자 등록 요청은 사용자 프로세싱 시스템(340) 또는 사용자 장치(330)로부터 수신될 수 있다. 응답으로, 서버 프로세싱 시스템은 원하는 개인 식별자를 간접적으로 나타내는 코드를 사용자가 입력하도록 요청하는 코드 요청 인터페이스를 사용자에게 제시하기 위하여 사용자 프로세싱 시스템(340) 또는 사용자 장치(330)로 전송한다. 코드 요청 인터페이스는 웹 브라우저, 웹 가능 애플리케이션 등을 통해 제시될 수 있다. 코드 요청 인터페이스는 사용자(350)에 제시되는 웹 페이지 또는 웹 페이지의 일부일 수 있다. 예를 들어, 코드 요청 인터페이스는 원격 서버 프로세싱 시스템(320)에 의해 호스팅된 웹페이지 내에 위치하는 프레임 또는 윈도우일 수 있고, 코드 요청 인터페이스는 서버 프로세싱 시스템(325)에 의해 생성 및 호스팅될 수 있다. 이하에서 상세히 설명하는 바와 같이, 사용자(350)에 의해 코드 요청 인터페이스에 입력되는 코드는 서버 프로세싱 시스템(310)으로 전송된다.

[0059] 단계(437)에서, 방법(400)은 사용자가 사용자 장치(330)의 소프트웨어 애플리케이션(335)을 통해 서버 프로세싱 시스템에게 인덱스를 요청하는 단계를 포함한다. 여기에서, 요청은 인덱스 요청이라 한다. 인덱스 요청은 사용자 장치(330)로부터 서버 프로세싱 시스템으로 전송되고, 인덱스 요청은 사용자의 사용자 장치 프로파일 및/또는 아이덴티티를 나타낼 수 있다. 인덱스 요청은 이하에서 상세히 설명하는 바와 같이 사용자의 디지털 증명서와 연관된 개인키(private key)를 이용하여 디지털적으로 서명될 수 있다.

[0060] 단계(440)에서, 인덱스 요청의 수신에 응답하여, 방법(400)은 서버 프로세싱 시스템(310)이 사용자 계정과 연관된 키맵(600)으로부터의 선택 키(620)를 나타내는 인덱스(610)를 사용자 장치(330)로 전송하는 단계를 포함한다. 사용자 장치 프로파일 및/또는 사용자 아이덴티티는 서버 프로세싱 시스템(310)에 의해 사용되어 사용자 계정 및 적절한 키맵을 결정한다. 코드 요청 인터페이스가 사용자 프로세싱 시스템(340)을 통해 제시되고 사용자 장치(330)가 서버 프로세싱 시스템(310)과 통신하지 않는 상황에서, 서버 프로세싱 시스템(310)은 사용자 프로세싱 시스템(340)을 통해 인덱스(610)를 사용자에게 제공할 수 있다. 그 후, 사용자는 사용자 장치(330)의 입력 장치를 이용하여 인덱스(610)를 소프트웨어 애플리케이션(335)에 수동으로 입력할 수 있다. 사용자는, 사용자 프로세싱 시스템(340)과 상호 작용하여 사용자 프로세싱 시스템(340)으로의 인덱스(610)의 전송 및 제시를 요청하도록 요구될 수 있다.

[0061] 단계(445)에서, 방법은 사용자 장치(330)가 수신된 인덱스(610)에 기초하여 로컬 메모리에 저장된 키맵(600)으로부터 해당 키(620)를 검색하는 단계를 포함한다.

[0062] 단계(450)에서, 방법은 사용자 장치(330)가 사용자 장치(330) 상에서 사용자 인터페이스(640)를 생성하고 디스플레이하는 단계를 포함하고, 여기서, 소프트웨어 애플리케이션(335)의 사용자 인터페이스(640)는 키(620) 및 식별자 참조(650)의 그래픽 표시를 제시한다. 도 6b를 참조하면, 0 내지 9의 숫자에 대한 10개의 키를 포함하는 수치 디스플레이로서 식별자 참조(650)를 오름차순으로 제시하는 예시적인 사용자 인터페이스(640)가 도시된다. 도 6b에 도시된 바와 같이, 키(620)는 해당 수의 랜덤 알파벳 문자를 포함할 수 있다. 바람직하게, 도 6에 도시된 바와 같이, 사용자 인터페이스(640)는 해당 식별자 참조 부분(660)에 인접하여 각각의 키 부분(630)을 제시하여 식별자 참조(650)의 각 숫자가 키(620)의 해당 키 부분(630)과 정렬하고 인접하도록 한다. 키(620) 및 식별자 참조(650)에 알파벳과 문자로 이루어진 데이터의 다른 구성이 사용될 수 있음을 인식할 것이다.

[0063] 단계(455)에서, 방법(400)은 사용자(350)가 제시된 키 및 원하는 개인 식별자를 사용하여 코드를 결정하는 단계를 포함한다. 일 형태에 있어서, 사용자는 시각적으로 제시된 인터페이스(640)를 검사하고 코드를 결정한다.

예를 들어, 원하는 개인 식별자의 각각의 숫자에 대하여, 사용자(350)는 식별자 참조(650) 내의 이 숫자(660)에 대응하는 키 부분(630)을 식별한다. 키 부분(630)은 사용자에 의해 함께 연결되어 코드를 형성한다. 도 6b에 제시된 인터페이스에 기초하여, 사용자의 원하는 개인 식별자가 "1032"이면, 사용자(350)에 대한 코드는 "QRS L"이다. 사용자(350)가 사용자 장치(330)를 이용하여 개인 식별자를 설정하는 경우, 사용자는 사용자 장치(330)의 입력 장치와 상호 작용하여 코드를 코드 요청 인터페이스에 입력할 수 있고, 여기서, 코드는 원하는 개인 식별자를 간접적으로 나타낸다. 대안으로, 사용자가 사용자 프로세싱 시스템(340)을 이용하여 안전한 환경으로의 액세스를 얻으면, 사용자는 사용자 프로세싱 시스템(340)의 입력 장치를 이용하여 코드를 사용자 프로세싱 시스템(340)에 의해 제시된 코드 요청 인터페이스에 입력할 수 있다.

[0064] 단계(460)에서, 방법(400)은 사용자 장치(330) 또는 사용자 프로세싱 시스템(340)이 사용자(350)에 의해 코드 요청 인터페이스에 입력된 코드를 나타내는 응답을 서버 프로세싱 시스템(310)으로 전송하는 단계를 포함한다. 사용자 장치(330) 또는 사용자 프로세싱 시스템(340)에 의해 제시된 코드 요청 인터페이스는 제출 버튼을 포함할 수 있고, 여기서, 코드는 사용자 장치(330) 또는 사용자 프로세싱 시스템(340)으로부터 제출 버튼의 사용자 선택을 통해 서버 프로세싱 시스템(310)으로 전송될 수 있다.

[0065] 단계(465)에서, 방법(400)은 서버 프로세싱 시스템(310)이 코드 및 선택 키(620)에 기초하여 해시 값을 결정하는 단계를 포함한다. 특히, 서버 프로세싱 시스템(310)은 수신된 코드의 입력 변수, 단계(440)에서 전송된 인덱스(610)에 대응하는 키맵(600)으로부터의 선택 키(620) 및 사용자(350)와 연관된 솔트(salt) 값을 서버 프로세싱 시스템(310)에 의해 실행된 해싱 알고리즘에 제공하여 해시 값을 생성한다. 바람직하게, 해싱 알고리즘은 SHA-3, MD5 또는 그 변형 등의 단방향 해싱 알고리즘이다. 해싱 알고리즘은 개인 식별자가 서버 프로세싱 시스템(310)에 의해 식별될 필요가 없도록 가환성 암호 기술(commutative cipher techniques)을 이용할 수 있다.

[0066] 단계(470)에서, 방법(400)은 서버 프로세싱 시스템(310)이 사용자 계정 내의 해시 값을 데이터베이스에 저장하는 단계를 포함한다. 유리하게, 서버 프로세싱 시스템(310)은 사용자의 개인 식별자를 저장하지 않거나 서버 프로세싱 시스템(310)이 개인 식별자를 직접적으로 나타내는 데이터를 수신하지 않아, 상당한 보안 이득을 제공할 수 있다. 임의의 실시예에서, 이들 보안 이득은, 사용자(350)가 자신의 개인 식별자를 알고 있지만, 다른 어떤 누구도, 사용자(350)가 액세스를 시도하는 안전한 환경(325)의 고용인조차도 개인 식별자를 결정할 수 없는 결과를 포함한다.

[0067] 서버 프로세싱 시스템(310)이 단계(440 내지 465)를 반복하여 2개의 해시 값을 얻을 수 있음을 인식할 것이다. 특히, 서버 프로세싱 시스템(310)은 초기 인덱스와 상이한 다른 인덱스(610)를 사용자 장치(330)(또는 사용자 장치(330)가 서버 프로세싱 시스템(310)과 통신하지 않는 경우 사용자 프로세싱 시스템을 통해 사용자)로 전송할 수 있다. 그러면, 서버 프로세싱 시스템(310)은 사용자로부터 수신된 추가의 코드에 기초하여 제2 해시 값을 산출하고, 해시 값이 적절(congruent)(즉, 매칭)하는 경우, 해시 값(즉, 이들 값이 동일하기 때문에 제1 또는 제2 해시 값)이 데이터베이스에 저장된다. 해시 값이 매칭되지 않는 경우, 이것은 사용자(350)가 적절하지 않은(non-congruent) 원하는 개인 식별자를 잘못 표시한 것을 나타낸다. 이로써, 등록 프로세스가 종료되거나 사용자(350)가 등록 프로세스를 다시 반복하도록 요청될 수 있다.

[0068] 인증

[0069] 도 5를 참조하면, 서버 프로세싱 시스템(310)이 원격 서버 프로세싱 시스템(320)에 의해 호스팅된 안전한 환경(325)을 액세스하려고 시도하는 사용자(350)를 인증하는 예시적인 방법을 나타내는 플로우챠트가 도시된다.

[0070] 특히, 단계(505)에서, 방법(500)은 사용자(350)가 사용자 프로세싱 시스템(340) 또는 사용자 장치(330)를 동작하여 원격 서버 프로세싱 시스템(320)에게 안전한 환경(325)을 액세스하라는 요청을 전송하는 단계를 포함한다. 요청은 웹 브라우저, 웹 가능 애플리케이션 등을 통해 제출될 수 있다.

[0071] 단계(510)에서, 방법(500)은 원격 서버 프로세싱 시스템(320)이 인증 요청을 서버 프로세싱 시스템(310)으로 전송하여 사용자(350)를 인증하는 단계를 포함한다. 인증 요청은 사용자가 안정한 환경으로의 액세스를 요청하는 것을 나타낸다. 바람직한 형태에서, 원격 서버 프로세싱 시스템(320)은 서버 프로세싱 시스템(310)으로 원격 서버 프로세싱 시스템(320)의 아이덴티티를 확인하는 디지털 증명서를 이용하여 요청을 디지털적으로 서명할 수 있다. 그러면, 서버 프로세싱 시스템(310)은 디지털적으로 서명된 요청에 기초하여 원격 서버 프로세싱 시스템(320)의 아이덴티티의 확인을 가능하게 하여 요청이 식별가능한 엔티티로 수신되었음을 보증할 수 있다. 서버 프로세싱 시스템(310)은 사용자(350)에 대하여 인증 요청이 수신되었다는 것을 데이터베이스(315)에 기록하고

타임스탬프를 이 요청과 연관시킨다.

[0072] 원격 서버 프로세싱 시스템(320)에게 안전한 환경(325)으로의 액세스를 요청한 것에 응답하여, 원격 서버 프로세싱 시스템(320)은 서버 프로세싱 시스템(310)에 의해 호스팅된 코드 요청 인터페이스를 포함하는 인터페이스를 요청하는 장치(330 또는 340)로 전송한다. 코드 요청 인터페이스는 웹 브라우저, 웹 가능 애플리케이션을 통해 제시될 수 있다.

[0073] 단계(515)에서, 방법(500)은 사용자(350)가 사용자 장치(330)의 소프트웨어 애플리케이션(335)와 상호 작용하여 인덱스 요청을 서버 프로세싱 시스템(310)으로 전송하여 서버 프로세싱 시스템이 사용자(350)를 인증하기 위하여 사용자의 키맵(600)으로부터 키(620)의 인덱스(610)를 선택하도록 한다. 바람직한 형태에서, 서버 프로세싱 시스템(310)은 시간적인 임계 기간 내에 사용자(350)로부터 인덱스 요청을 수신하도록 요구되고, 그렇지 않으면, 서버 프로세싱 시스템(310)은 사용자(350)가 안전한 환경(325)을 액세스하도록 인증되지 않았다는 것을 나타내는 인증 응답을 원격 서버 프로세싱 시스템(320)으로 전송할 것이다. 요청을 전송하기 위하여, 사용자(350)는 사용자 장치(330) 상에 소프트웨어 애플리케이션(335)을 런칭하여 인덱스 요청의 전송을 개시할 수 있다. 이 때, 사용자 장치(330)는 또한 사용자의 디지털 증명서의 개인 키를 이용하여 인덱스 요청을 디지털적으로 서명하여 서버 프로세싱 시스템(310)이 해당 공공 키를 이용하여 사용자의 아이덴티티를 확인하도록 한다. 디지털 서명이 사용자(350)의 아이덴티티를 성공적으로 확인하지 못한 경우, 서버 프로세싱 시스템(310)은 사용자(350)가 안전한 환경(325)을 액세스하도록 인증되지 않았다는 것을 나타내는 인증 응답을 원격 서버 프로세싱 시스템(320)으로 전송할 수 있다.

[0074] 단계(520)에서, 방법(500)은 원격 서버 프로세싱 시스템(320)이 사용자 계정과 연관된 키맵(600)으로부터 선택 키(620)의 인덱스(610)를 나타내는 데이터를 사용자(350)와 연관된 사용자 장치(330)의 소프트웨어 애플리케이션으로 전송하는 단계를 포함한다. 서버 프로세싱 시스템(310)은 선택된 인덱스(610)를 나타내도록 발행된 챌린지(challenge)를 사용자 계정에 기록한다. 상술한 바와 같이, 사용자 장치(330)가 서버 프로세싱 시스템(310)과 데이터 통신하지 않는 경우에, 서버 프로세싱 시스템(310)은 사용자(350)로의 제시를 위해 선택된 인덱스(610)의 인덱스를 나타내는 데이터를 사용자 프로세싱 시스템(340)으로 전송할 수 있다. 그러면, 사용자(350)는 사용자 장치(330)의 입력 장치를 통해 제시된 인덱스를 소프트웨어 애플리케이션(335)으로 수동으로 입력하여 사용자 장치(330)가 인덱스를 성공적으로 수신하도록 한다. 사용자(350)는 사용자 프로세싱 시스템(340)과 상호 작용하여 사용자 프로세싱 시스템(340)으로의 인덱스(610)의 전송을 요청하도록 요구될 수 있다.

[0075] 선택적으로, 단계(522)에서, 방법은 사용자 장치(330)가 보안 검사를 수행하는 단계를 포함한다. 특히, 소프트웨어 애플리케이션(335)은 하나 이상의 사용자 장치 특징을 결정하여 본 문서에서 상술한 바와 같이 사용자 장치 프로파일을 생성한다. 그러면, 소프트웨어 애플리케이션(335)은 새롭게 생성된 사용자 장치 프로파일을 사용자 장치(330)의 메모리에 저장된 사용자 장치 프로파일과 비교한다. 성공적인 비교의 경우, 방법은 단계(525)로 진행하고, 그렇지 않으면, 방법은 종료한다. 이 프로세스는 사용자 장치(330)에 부당 변경(tampering)이 발생하는지를 확인할 수 있다.

[0076] 단계(525)에서, 방법(500)은 사용자 장치(330)의 소프트웨어 애플리케이션(335)이 키맵(600)으로부터 인덱스(610)에 대응하는 키(620)를 로컬 메모리로부터 검색하는 단계를 포함한다.

[0077] 단계(530)에서, 방법(500)은 사용자 장치(330)의 소프트웨어 애플리케이션(335)이 사용자 장치(330) 상에 사용자 인터페이스(600)를 생성 및 디스플레이하는 단계를 포함하고, 사용자 인터페이스(600)는 키(620) 및 식별자 참조(650)의 그래픽 표시를 제시한다. 이 프로세스는 상술한 단계(450)와 유사하게 수행된다.

[0078] 단계(535)에서, 방법(500)은 사용자(350)가 사용자 장치(330)에 의해 제시된 소프트웨어 애플리케이션(335)의 사용자 인터페이스(640)를 이용하여 코드를 결정한다. 단계는, 코드 요청 인터페이스를 통해 사용자가 원하는 개인 식별자보다는 오히려 설정된 개인 식별자의 일부에 대응하는 키 부분을 입력하는 것을 제외하고, 상술한 단계(455)와 유사하게 수행된다.

[0079] 단계(540)에서, 방법(500)은 사용자 프로세싱 시스템(340) 또는 사용자 장치(330)가 코드 요청 인터페이스를 통해 사용자(350)에 의해 입력된 코드를 나타내는 데이터를 서버 프로세싱 시스템으로 전송하는 단계를 포함한다.

[0080] 서버 프로세싱 시스템(310)은 수신된 초기 인증 요청 및/또는 발행된 챌린지 요청의 시간적 임계 기간 내에 챌린지 응답이 수신되는지를 결정하도록 구성될 수 있다. 응답이 시간적 임계 기간 내에 수신되지 않는 경우, 서버 프로세싱 시스템(310)은 안전한 환경(325)을 액세스하기 위하여 사용자가 인증되지 않음을 나타내는 인증 응답을 원격 서버 프로세싱 시스템(320)으로 전송할 수 있다.

[0081] 단계(545)에서, 방법(500)은 서버 프로세싱 시스템(310)이 코드 및 선택 키(620)에 기초하여 해시 값을 결정하는 단계를 포함한다. 특히, 서버 프로세싱 시스템(310)은 수신된 코드의 입력 변수, 사용자 장치(330)에 의해 수신된 인덱스(610)에 대응하는 선택 키(620) 및 사용자(350)와 연관된 솔트(salt) 값을 서버 프로세싱 시스템(310)에 의해 실행된 해싱 알고리즘에 제공하여 해시 값을 생성한다. 바람직하게, 해싱 알고리즘은 SHA-3, MD5 또는 그 변형 등의 단방향 해싱 알고리즘이다. 해싱 알고리즘은 개인 식별자가 서버 프로세싱 시스템(310)에 의해 식별될 필요가 없도록 가환성 암호 기술을 이용할 수 있다.

[0082] 단계(550)에서, 방법(500)은 서버 프로세싱 시스템(310)이 결정된 해시 값을 사용자 계정 내의 저장 해시 값과 비교하는 단계를 포함한다. 유리하게, 서버 프로세싱 시스템(310)은 사용자의 개인 식별자를 얻거나 수신하지 않아, 상당한 보안 이득을 제공할 수 있다. 임의의 실시예에서, 이들 보안 이득은, 사용자(350)가 자신의 개인 식별자를 알고 있지만, 다른 어떤 누구도, 사용자(350)가 액세스를 시도하는 안전한 환경(325)의 고용인조차도, 개인 식별자를 결정할 수 없는 결과를 포함한다.

[0083] 단계(555)에서, 방법(500)은 서버 프로세싱 시스템(310)이 인증 응답을 생성하여 원격 서버 프로세싱 시스템(320)으로 전송하는 단계를 포함하고, 인증 응답은 단계(550)의 비교에 기초하여 안전한 환경(325)을 액세스하기 위하여 사용자(350)가 인증되는지를 나타낸다. 특히, 해시 값이 단계(550)에서 수행되는 비교에 대응하지 않는 경우, 서버 프로세싱 시스템(310)은 사용자(350)가 원격 서버 프로세싱 시스템(320)에 의해 제어되는 안전한 환경(325)으로의 액세스를 승인받지 않아야 한다는 것을 나타내는 인증 응답을 생성하여 전송한다. 그러나, 해시 값이 단계(560)에서 수행된 비교에 대응하는 경우, 서버 프로세싱 시스템(310)은 사용자(350)가 원격 서버 프로세싱 시스템(320)에 의해 제어되는 안전한 환경(325)으로의 액세스을 승인받아야 한다는 것을 나타내는 응답을 생성하여 전송한다.

[0084] 단계(560)에서, 방법(500)은 서버 프로세싱 시스템(310)이 챌린지 응답이 수신되고 인증 응답이 원격 서버 프로세싱 시스템(320)으로 전송되었다는 것을 사용자 계정에 기록하는 단계를 포함한다.

[0085] 사용자(350)가 사용자 프로세싱 시스템(340)을 통해 코드를 부정확하게 입력하면, 서버 프로세싱 시스템(310)은 하나 이상의 추가의 챌린지 요청을 재발생할 수 있고, 고유 및 상이한 인덱스(610)가 각 챌린지 요청에서 전송됨을 인식할 것이다. 임계수의 부정확한 코드가 원격 서버 프로세싱 시스템(320)에 의한 단일 인증 요증을 위해 서버 프로세싱 시스템(310)에 의해 식별되면, 서버 프로세싱 시스템(310)은 사용자(350)가 안전한 환경(325)으로의 액세스를 승인받지 않아야 한다는 것을 지시하는 인증 응답을 생성하여 원격 서버 프로세싱 시스템(320)으로 전송할 수 있다.

[0086] 개인 식별자 리셋

[0087] 도 7을 참조하면, 사용자(350)가 리셋 요청을 서버 프로세싱 시스템(310)으로 전송하는 방법을 나타내는 플로우챠트가 도시된다.

[0088] 특히, 단계(705)에서, 방법은 사용자(350)가 리셋 요청을 서버 프로세싱 시스템(310)으로 전송하여 사용자의 개인 식별자를 리셋하는 단계를 포함한다. 리셋 요청은 사용자 프로세싱 시스템(340) 또는 사용자 장치(330)로부터 잠재적으로 소프트웨어 애플리케이션(335)을 통해 전송될 수 있다. 리셋 요청은 서버 프로세싱 시스템에 의해 사용될 수 있는 데이터 또는 IDV를 포함하여 사용자의 아이덴티티를 확인할 수 있다.

[0089] 단계(710)에서, 서버 프로세싱 시스템(310)은 사용자의 아이덴티티의 확인을 가능하게 한다. 사용자의 아이덴티티의 성공적인 확인에 응답하여, 서버 프로세싱 시스템에 의해 호스팅된 코드 요청 인터페이스가 사용자 장치(330) 또는 사용자 프로세싱 시스템(340)을 통해 사용자(350)에 제시되고 방법(700)은 단계(712)로 진행하고, 그렇지 않으면, 리셋 프로세스를 종료한다.

[0090] 단계(712)에서, 사용자(350)는 사용자 장치(335)의 소프트웨어 애플리케이션(335)과 상호 작용하여 인덱스 요청을 서버 프로세싱 시스템(340)으로 전송한다.

[0091] 단계(715)에서, 방법(700)은 서버 프로세싱 시스템(310)이 사용자 계정과 연관된 키맵(600)으로부터의 선택 키(620)의 인덱스(610)를 사용자 장치(330)로 전송하는 단계를 포함한다. 상술한 바와 같이, 사용자 장치(330)가 서버 프로세싱 시스템(310)과 데이터 통신하지 않는 경우에는, 사용자(350)에게 제시하기 위하여 서버 프로세싱 시스템(310)이 선택 키(620)의 인덱스(610)를 나타내는 데이터를 사용자 프로세싱 시스템(340)으로 전송할 수 있다. 그러면, 사용자(350)는 사용자 장치(330)의 입력 장치를 통해 소프트웨어 애플리케이션(335)으로 제시된

인덱스(610)를 수동으로 입력하여 사용자 장치(330)가 인덱스(610)를 성공적으로 수신하도록 한다. 사용자는 사용자 프로세싱 시스템(340)과 상호 작용하여 사용자 프로세싱 시스템(340)으로의 인덱스의 전송을 요청하도록 요구될 수 있다.

[0092] 서버 프로세싱 시스템(310)은 수신된 리셋 요청 및 사용자에게 전송된 인덱스(610)의 기록을 데이터베이스(315)에 저장할 수 있고, 이들 이벤트의 각각이 발생한 시간을 나타내는 타임스탬프가 데이터베이스(315)에 기록된다.

[0093] 단계(720)에서, 방법(700)은 사용자 장치(330)의 소프트웨어 애플리케이션(335)이 사용자 장치(330)의 메모리에 저장된 키맵(600)으로부터의 수신된 인덱스(610)와 대응하는 키(620)를 로컬 메모리로부터 검색하는 단계를 포함한다.

[0094] 단계(725)에서, 방법(700)은 사용자 장치(330)가 사용자 인터페이스(600)를 생성하여 사용자 장치(330)에 디스플레이하는 단계를 포함하고, 사용자 인터페이스(600)는 키(620) 및 식별자 참조(650)의 그래픽 표시를 제시한다. 이 단계는 상술한 단계(450)와 유사하게 수행된다.

[0095] 단계(730)에서, 방법(700)은 사용자(350)가 사용자 장치에 의해 제시된 사용자 인터페이스를 이용하여 리셋 코드를 결정하는 단계를 포함한다. 예를 들어, 새로운 개인 식별자의 각각의 숫자에 대하여, 사용자(350)는 식별자 참조(650) 내의 각각의 숫자에 대응하는 각각의 키 부분(630)을 식별하고 해당 키 부분(630)을 연결하여 리셋 코드를 형성한다. 도 6b에 제시된 인터페이스에 기초하여, 사용자의 새로운 개인 식별자가 "5732"이면, 사용자(350)에 의해 입력된 리셋 코드는 "XKSL"이다.

[0096] 단계(735)에서, 방법(700)은 사용자 프로세싱 시스템(340) 또는 사용자 장치가 사용자(350)에 의해 입력된 리셋 코드를 나타내는 응답을 코드 요청 인터페이스를 통해 서버 프로세싱 시스템(310)으로 전송하는 단계를 포함한다.

[0097] 서버 프로세싱 시스템(310)은 리셋 코드가 리셋 요청 또는 인덱스의 전송의 시간적 임계 기간 내에 수신되었는지를 결정하도록 구성될 수 있다. 리셋 코드가 시간적 임계 기간 내에서 수신되지 않은 경우에는, 서버 프로세싱 시스템(310)이 수신된 리셋 코드에 기초하여 개인 식별자를 리셋하는 것을 거절할 수 있다.

[0098] 단계(740)에서, 방법(700)은 서버 프로세싱 시스템(310)이 리셋 코드 및 선택 키에 기초하여 해시 값을 결정하는 단계를 포함한다. 특히, 서버 프로세싱 시스템(310)은 수신된 리셋 코드의 입력 변수, 사용자로 전송된 인덱스에 대응하는 키맵으로부터의 키 및 사용자(350)와 연관된 솔트 값을 서버 프로세싱 시스템(310)에 의해 실행될 해싱 알고리즘에 제공하여 해시 값을 생성한다. 바람직하게, 해싱 알고리즘은 SHA-3, MD5 또는 그 변형 등의 단방향 해싱 알고리즘이다..

[0099] 단계(745)에서, 방법(700)은 서버 프로세싱 시스템(310)이 사용자의 새로운 개인 식별자의 결정된 해시 값을 사용자 계정에 저장하고 사용자의 이전 개인 식별자에 대응하는 이전 해시 값을 삭제하는 단계를 포함한다. 유리하게, 서버 프로세싱 시스템(310)은 사용자의 새로운 개인 식별자를 저장하지 않거나 서버 프로세싱 시스템(310)이 새로운 개인 식별자를 직접적으로 나타내는 데이터를 수신하지 않아, 상당한 보안 이득을 제공한다. 임의의 실시예에서, 이들 보안 이득은 사용자(350)가 자신의 개인 식별자를 알지만, 다른 어느 누구도, 사용자(350)가 액세스를 시도하는 안전한 환경(325)의 고용인조차도, 개인 식별자를 결정할 수 없는 결과를 포함한다.

[0100] 사용자(350)가 간접적으로 동일한 새로운 개인 식별자를 식별했다는 것을 확인하기 위하여 단계(710 내지 740)가 반복될 수 있음을 인식해야 한다. 2개의 해시 값이 대응되는 경우에는, 새로운 개인 식별자에 대응하는 해시 값이 사용자 계정에 저장된다.

[0101] 상기 프로세스의 일부는 사용자가 사용자 프로세싱 시스템(340)과 상호 작용하는 것과 관련하여 설명하였지만, 사용자가 사용자 장치(330)를 이용하여 동일한 단계를 수행할 수 있다는 것을 인식할 것이다.

[0102] 변형

[0103] 도 3에 도시된 실시예는 단지 단일 사용자(350) 및 단일 원격 서버 프로세싱 시스템(320)만을 나타냄을 인식할 것이다. 서버 프로세싱 시스템(310)이 바람직하게 복수의 원격 서버 프로세싱 시스템(320)과 데이터 통신하고 각각의 원격 서버 프로세싱 시스템(320)이 각각의 안전한 환경(325)으로의 사용자 액세스를 제어하는 것을 인식할 것이다.

[0104] 서버 프로세싱 시스템(310)이 바람직하게 복수의 사용자(350)와 각각 연관된 복수의 사용자 장치(330)와 데이터 통신하고, 복수의 사용자(350)를 인증하기 위하여, 서버 프로세싱 시스템(310)과 연관된 메모리(325)가 복수의 사용자 계정을 저장하는 것을 인식할 것이다.

[0105] 서버 프로세싱 시스템(310)이 분배된 프로세싱 시스템 또는 단일 전용 프로세싱 시스템의 형태로 제공될 수 있다는 것을 인식할 것이다.

[0106] 시스템의 다양한 컴포넌트 사이에서 전송되는 데이터가 암호화 및 디지털 서명 기술을 이용할 수 있다는 것을 인식할 것이다.

[0107] 다른 해싱 프로세스가 서버 프로세싱 시스템(310)에 의해 적용될 수 있음을 인식할 것이다. 특히, 대안으로, 서버 프로세싱 시스템(310)은 요청에서 전송된 인덱스와 연관된 선택 키를 역으로 사용자 장치(330)에 적용함으로써 사용자의 개인 식별자를 결정할 수 있다. 결정시, 서버 프로세싱 시스템(310)은 사용자의 개인 식별자를 즉시 해싱할 수 있다. 그러면, 사용자의 개인 식별자는 서버 프로세싱 시스템(310)의 RAM으로부터 즉시 제거(purge)되어 사용자의 개인 식별자를 직접 나타내는 데이터가 서버 프로세싱 시스템(310)에 의해 저장되지 않는다.

[0108] IDV는 서버 프로세싱 시스템(310) 또는 서버 프로세싱 시스템(310)과 데이터 통신하는 개별 프로세싱 시스템의 일부일 수 있다.

[0109] 키 및 개인 식별자가 위에서 일련의 알파벳 문자 및/또는 숫자로서 예시되었지만, 고유 그래픽 아이콘, 컬러, 가청음 등의 다른 형태의 데이터가 이용될 수 있다.

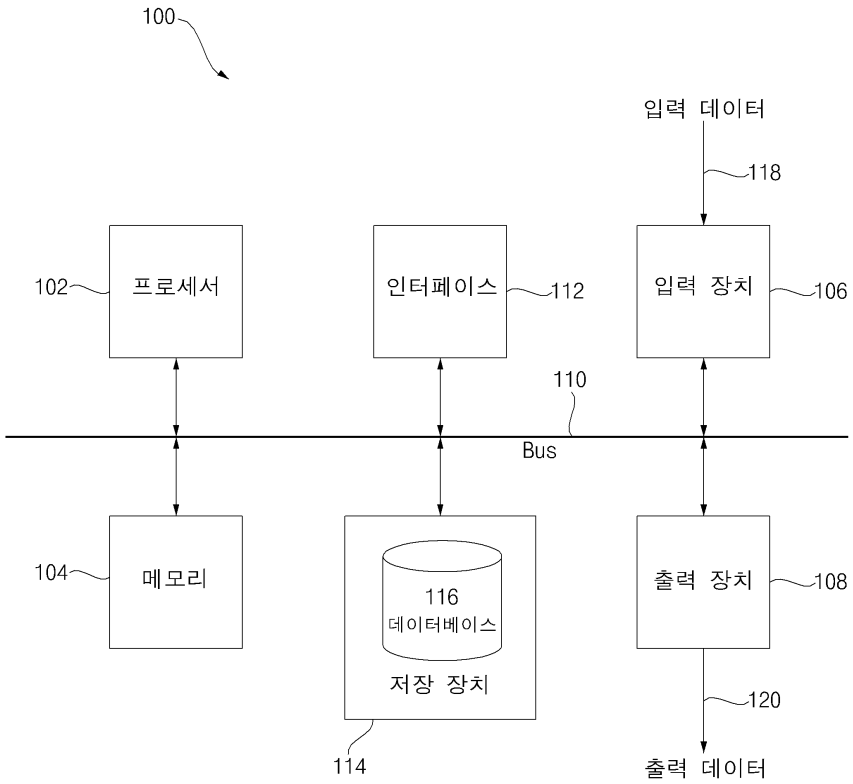
[0110] 단계(522)에서 수행되는 보안 검사 프로세스는 인증 프로세스와 관련하여 설명하였지만, 보안 검사 프로세스가 또한 방법(400 및 700)에서 수행되어 악의적 부당변경(malicious tampering)이 사용자 장치에 발생하지 않도록 보장할 수 있다.

[0111] 상기 실시예는 완전한 하드웨어 실시예, 완전한 소프트웨어 실시예, 펌웨어 또는 소프트웨어 및 하드웨어 형태를 조합한 실시예의 형태를 취할 수 있다.

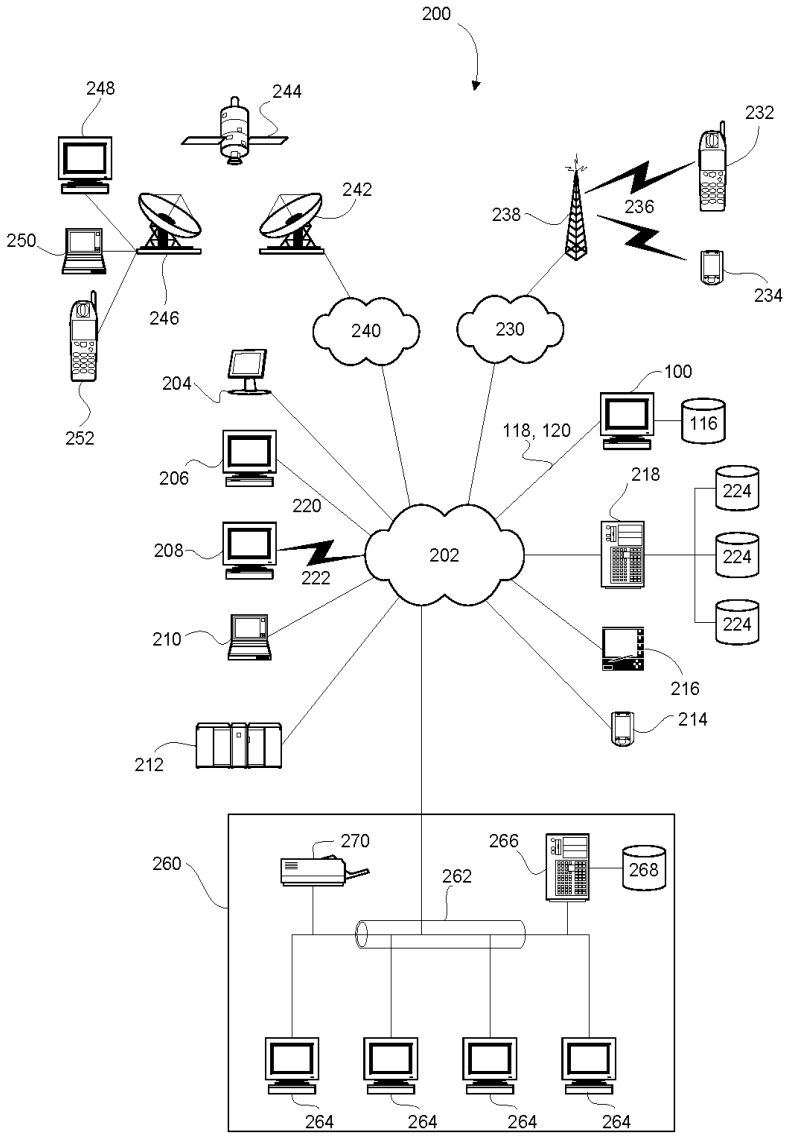
[0112] 본 발명의 범위를 벗어나지 않고 많은 변형이 가능함은 당업자에게 자명하다.

도면

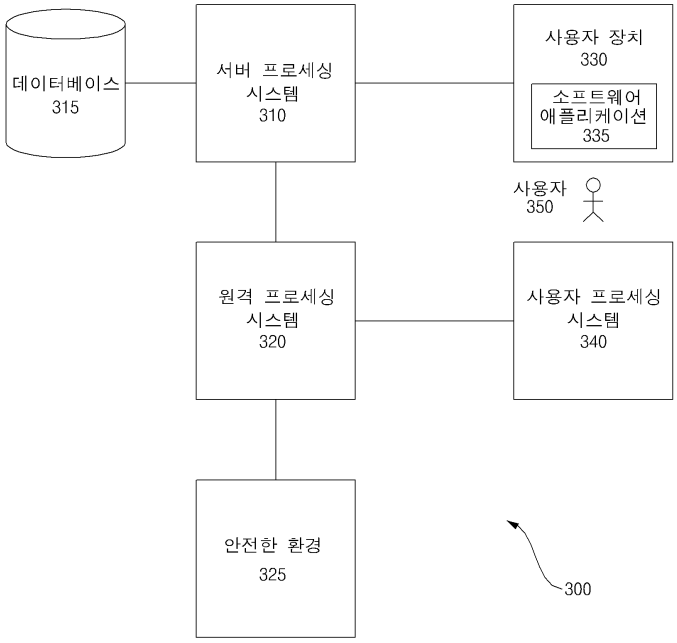
도면1


100
입력 데이터
118
102
프로세서
인터페이스
112
입력 장치
106
110
Bus
104
메모리
116
데이터베이스
저장 장치
출력 장치
108
120
114
출력 데이터

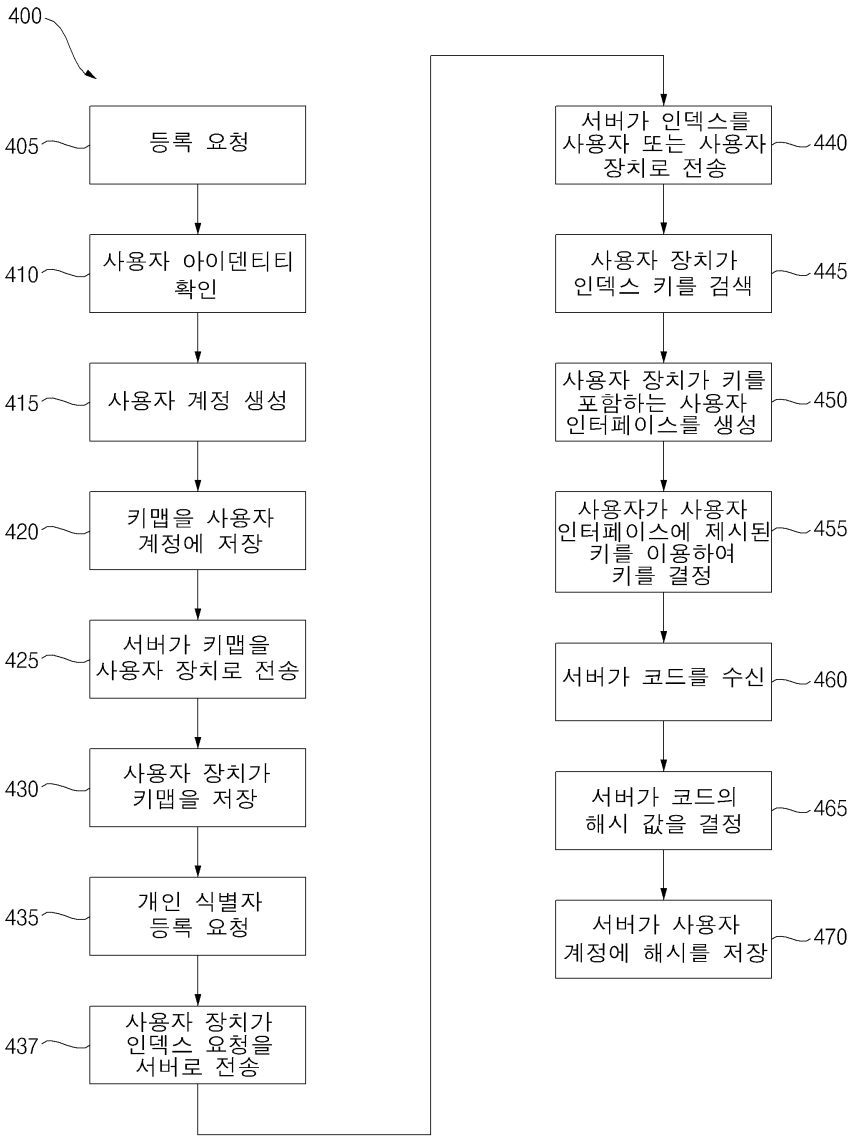
도면2


200
248
244
232
242
238
236
250
234
246
240
230
252
204
100
118, 120
116
206
218
220
224
208
202
222
224
210
224
216
214
212
270
266
260
262
268
264
264
264
264

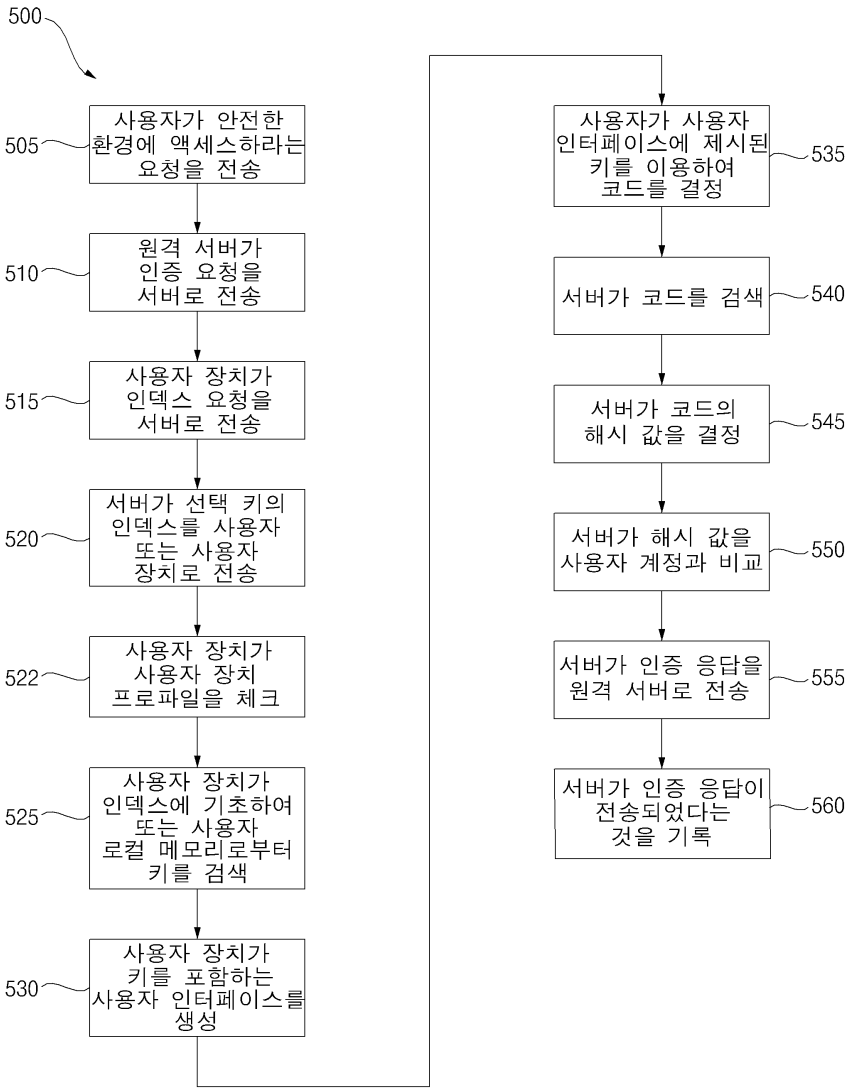
도면3


데이터베이스
315
서버 프로세싱
시스템
310
사용자 장치
330
소프트웨어
애플리케이션
335
사용자
350
원격 프로세싱
시스템
320
사용자 프로세싱
시스템
340
안전한 환경
325
300

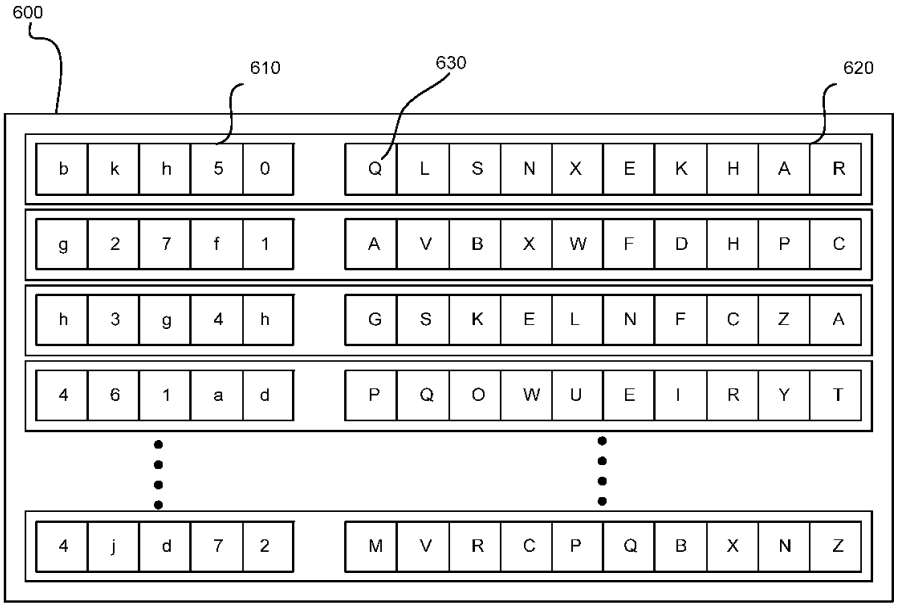
도면4


400
405
등록 요청
410
사용자 아이덴티티 확인
415
사용자 계정 생성
420
키맵을 사용자 계정에 저장
425
서버가 키맵을 사용자 장치로 전송
430
사용자 장치가 키맵을 저장
435
개인 식별자 등록 요청
437
사용자 장치가 인덱스 요청을 서버로 전송
440
서버가 인덱스를 사용자 또는 사용자 장치로 전송
445
사용자 장치가 인덱스 키를 검색
450
사용자 장치가 키를 포함하는 사용자 인터페이스를 생성
455
사용자가 사용자 인터페이스에 제시된 키를 이용하여 키를 결정
460
서버가 코드를 수신
465
서버가 코드의 해시 값을 결정
470
서버가 사용자 계정에 해시를 저장

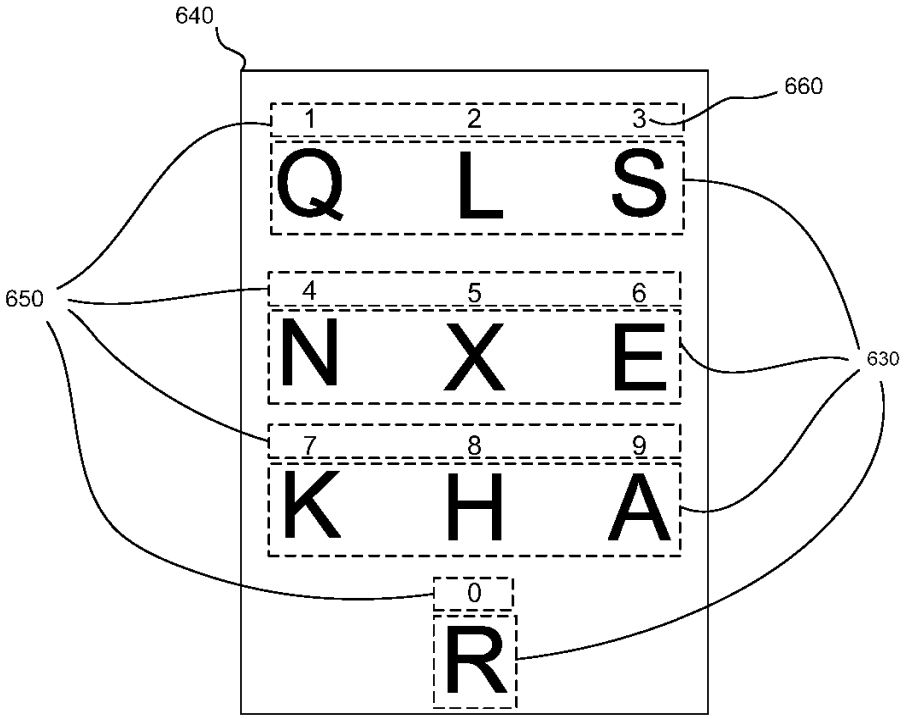
도면5


500
505
사용자가 안전한 환경에 액세스하라는 요청을 전송
510
원격 서버가 인증 요청을 서버로 전송
515
사용자 장치가 인덱스 요청을 서버로 전송
520
서버가 선택 키의 인덱스를 사용자 또는 사용자 장치로 전송
522
사용자 장치가 사용자 장치 프로파일을 체크
525
사용자 장치가 인덱스에 기초하여 또는 사용자 로컬 메모리로부터 키를 검색
530
사용자 장치가 키를 포함하는 사용자 인터페이스를 생성
535
사용자가 사용자 인터페이스에 제시된 키를 이용하여 코드를 결정
540
서버가 코드를 검색
545
서버가 코드의 해시 값을 결정
550
서버가 해시 값을 사용자 계정과 비교
555
서버가 인증 응답을 원격 서버로 전송
560
서버가 인증 응답이 전송되었다는 것을 기록

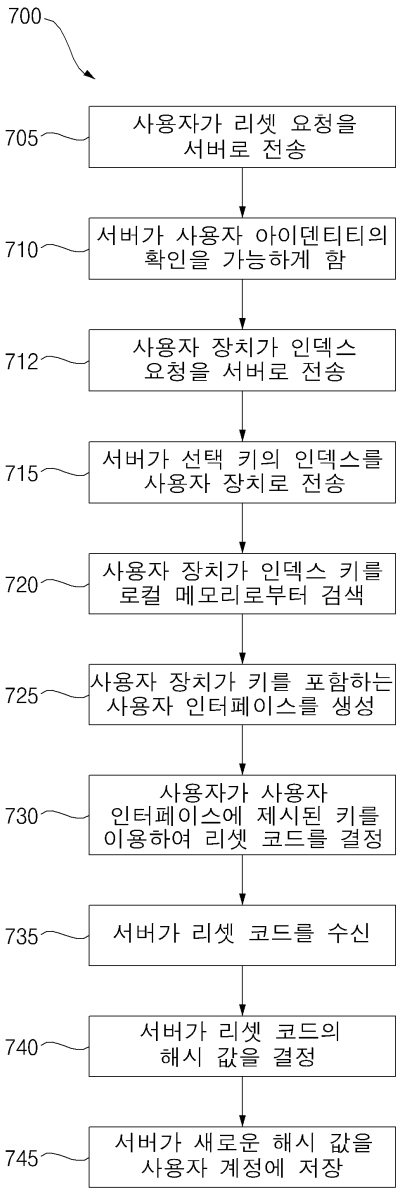
도면6a


600
610
630
620
b k h 5 0
Q L S N X E K H A R
g 2 7 f 1
A V B X W F D H P C
h 3 g 4 h
G S K E L N F C Z A
4 6 1 a d
P Q O W U E I R Y T
4 j d 7 2
M V R C P Q B X N Z

도면6b


640
660
650
630
1 2 3
Q L S
4 5 6
N X E
7 8 9
K H A
0
R

도면7


700
705
사용자가 리셋 요청을 서버로 전송
710
서버가 사용자 아이덴티티의 확인을 가능하게 함
712
사용자 장치가 인덱스 요청을 서버로 전송
715
서버가 선택 키의 인덱스를 사용자 장치로 전송
720
사용자 장치가 인덱스 키를 로컬 메모리로부터 검색
725
사용자 장치가 키를 포함하는 사용자 인터페이스를 생성
730
사용자가 사용자 인터페이스에 제시된 키를 이용하여 리셋 코드를 결정
735
서버가 리셋 코드를 수신
740
서버가 리셋 코드의 해시 값을 결정
745
서버가 새로운 해시 값을 사용자 계정에 저장