



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년05월20일
(11) 등록번호 10-1980483
(24) 등록일자 2019년05월14일

(51) 국제특허분류(Int. Cl.)
G06F 21/46 (2013.01) G06F 21/31 (2013.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
G06F 21/46 (2013.01)
G06F 21/31 (2013.01)
(21) 출원번호 10-2018-0025582
(22) 출원일자 2018년03월05일
심사청구일자 2018년03월05일
(56) 선행기술조사문헌
KR101054096 B1*
KR1020150092441 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인하대학교 산학협력단
인천광역시 미추홀구 인하로 100(용현동, 인하대학교)
(72) 발명자
양대현
서울특별시 서초구 서초중앙로 200, 17동 901호(서초동, 삼풍아파트)
정창훈
경기도 부천시 중동로 107, 125동 804호(중동, 팰리스카운터)
(뒷면에 계속)
(74) 대리인
양성보

전체 청구항 수 : 총 5 항

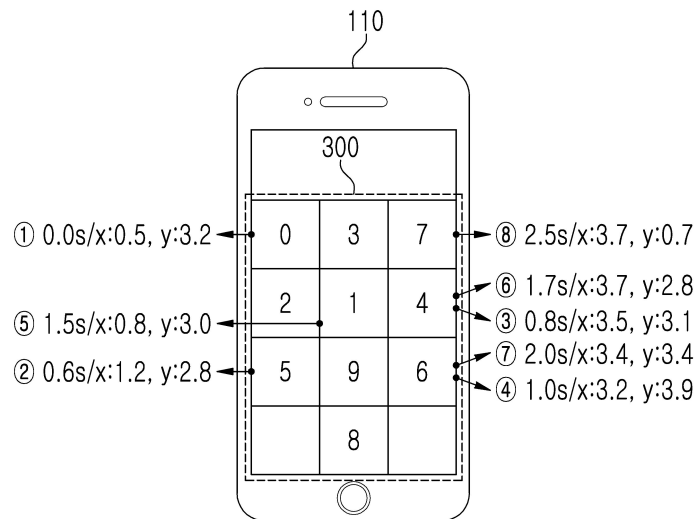
심사관 : 문남두

(54) 발명의 명칭 머신러닝을 이용한 사용자 행동 인식 기반의 PIN 입력 방법 및 시스템

(57) 요약

머신러닝을 이용한 사용자 행동 인식 기반의 PIN 입력 방법 및 시스템이 개시된다. 일 실시예에 따른 사용자 인증 방법은, 전자 기기에 사용자 인증을 위한 인증 화면을 표시하는 단계; 사용자로부터 상기 인증 화면을 통하여 입력되는 패스워드 데이터, 상기 패스워드 데이터와 관련된 시간 데이터 및 상기 패스워드 데이터와 관련된 위치 데이터를 포함하는 입력 정보를 수신하는 단계; 및 상기 입력 정보와 상기 사용자로부터 입력된 입력 정보에 기반하여 학습된 학습 데이터의 비교를 통하여 사용자 인증을 수행하는 단계를 포함할 수 있다.

대표도 - 도3



(52) CPC특허분류

H04L 9/3226 (2013.01)

(72) 발명자

장룡호

인천광역시 남구 인하로 100, 하이테크센터 1008
호(용현동, 인하대학교)

이현석

인천광역시 연수구 술샘로43번길 15, 107동 901호
(청학동, 성호아파트)

이 발명을 지원한 국가연구개발사업

과제고유번호 20160000970022002

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 방송통신산업기술개발사업

연구과제명 [IITP-Ezbaro] 비대면 본인확인을 위한 바이오 공개키 기반 구조 기술 개발(2차년도)

기 여 율 1/1

주관기관 한국전자통신연구원

연구기간 2017.01.01 ~ 2017.12.31

명세서

청구범위

청구항 1

사용자 인증 방법에 있어서,

전자 기기에 사용자 인증을 위한 인증 화면을 표시하는 단계;

사용자로부터 상기 인증 화면을 통하여 입력되는 패스워드 데이터, 상기 패스워드 데이터와 관련된 시간 데이터 및 상기 패스워드 데이터와 관련된 위치 데이터를 포함하는 입력 정보를 수신하는 단계; 및

상기 입력 정보와 상기 사용자로부터 입력된 입력 정보에 기반하여 학습된 학습 데이터의 비교를 통하여 사용자 인증을 수행하는 단계

를 포함하고,

상기 사용자로부터 사용자 인증을 위한 인증 정보를 등록하는 단계

를 더 포함하고,

상기 사용자로부터 사용자 인증을 위한 인증 정보를 등록하는 단계는,

상기 사용자로부터 상기 사용자 인증을 위한 패스워드 데이터, 상기 패스워드 데이터가 입력되는 시간 데이터 및 상기 패스워드 데이터가 입력되는 위치 데이터를 인증 정보로 등록하고, 상기 등록된 패스워드 데이터에 기반하여 상기 패스워드 데이터가 입력되는 시간 데이터 및 상기 패스워드 데이터가 입력되는 위치 데이터에 대한 학습을 수행함에 따라 학습 데이터를 획득하고, 상기 패스워드 데이터를 데이터베이스에 저장하고, 상기 패스워드 데이터가 입력되는 시간 데이터 및 상기 패스워드 데이터가 입력되는 위치 데이터에 대한 머신러닝 학습을 위하여 TRUE 라벨을 부가하고, 상기 사용자로부터 입력되는 인증 정보 이외의 다른 데이터를 랜덤하게 생성하여 FALSE 라벨을 부가하여 상기 머신러닝 학습을 통하여 모델을 생성하는 단계

를 포함하는 사용자 인증 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 전자 기기에 사용자 인증을 위한 인증 화면을 표시하는 단계는,

상기 전자 기기에 상기 사용자 인증을 위한 키패드를 랜덤으로 배열하고, 상기 랜덤으로 배열된 키패드를 인증 화면에 표시하는 단계

를 포함하고,

상기 입력 정보를 수신하는 단계는,

상기 키패드에서 상기 패스워드 데이터에 설정된 패스워드 길이에 기초하여 첫 번째 자리의 패스워드를 입력하는 시간 데이터를 기준으로, 상기 패스워드 데이터의 첫 번째 자리의 패스워드부터 상기 패스워드 데이터의 마지막 자리의 패스워드를 터치할 때까지의 각각의 터치 시간 데이터를 포함하는 시간 데이터와 상기 패스워드 데이터를 터치하는 각각의 x 좌표, y 좌표를 포함하는 위치 데이터를 식별하는 단계

를 포함하는 사용자 인증 방법.

청구항 5

제1항에 있어서,

상기 사용자 인증을 수행하는 단계는,

상기 사용자로부터 입력된 패스워드 데이터로부터 획득되는 시간 데이터 및 위치 데이터를 식별함에 따라 상기 사용자로부터 입력된 패스워드 데이터가 기 저장된 패스워드와 일치하는지 여부를 판단하는 단계

를 포함하는 사용자 인증 방법.

청구항 6

제5항에 있어서,

상기 사용자 인증을 수행하는 단계는,

상기 사용자로부터 입력된 패스워드 데이터가 기 저장된 패스워드와 일치함에 따라 상기 사용자로부터 입력된 패스워드 데이터와 관련된 시간 데이터, 위치 데이터를 상기 사용자로부터 입력된 입력 정보에 기반하여 학습된 학습 데이터와 비교하여 0내지 1 사이의 소수값을 인증 결과로서 도출하고, 상기 도출된 인증 결과를 기 설정된 기준에 기초하여 인증 성공 또는 인증 실패로 분류하는 단계

를 포함하는 사용자 인증 방법.

청구항 7

사용자 인증을 수행하는 사용자 인증 시스템에 있어서,

사용자로부터 사용자 인증을 위한 인증 정보를 등록하는 등록부;

전자 기기에 사용자 인증을 위한 인증 화면을 표시하는 표시부;

상기 사용자로부터 상기 인증 화면을 통하여 입력되는 패스워드 데이터, 상기 패스워드 데이터와 관련된 시간 데이터 및 상기 패스워드 데이터와 관련된 위치 데이터를 포함하는 입력 정보를 수신하는 수신부; 및

상기 입력 정보와 상기 사용자로부터 입력된 입력 정보에 기반하여 학습된 학습 데이터의 비교를 통하여 사용자 인증을 수행하는 수행부

를 포함하고,

상기 등록부는,

상기 사용자로부터 상기 사용자 인증을 위한 패스워드 데이터, 상기 패스워드 데이터가 입력되는 시간 데이터 및 상기 패스워드 데이터가 입력되는 위치 데이터를 인증 정보로 등록하고, 상기 등록된 패스워드 데이터에 기반하여 상기 패스워드가 입력되는 시간 데이터 및 상기 패스워드가 입력되는 위치 데이터에 대한 학습을 수행함에 따라 학습 데이터를 획득하고, 상기 패스워드 데이터를 데이터베이스에 저장하고, 상기 패스워드 데이터가 입력되는 시간 데이터 및 상기 패스워드 데이터가 입력되는 위치 데이터에 대한 머신러닝 학습을 위하여 TRUE 라벨을 부가하고, 상기 사용자로부터 입력되는 인증 정보 이외의 다른 데이터를 랜덤하게 생성하여 FALSE 라벨을 부가하여 상기 머신러닝 학습을 통하여 모델을 생성하는

사용자 인증 시스템.

발명의 설명

기술 분야

[0001]

아래의 설명은 전자 기기에서 PIN(Personal Identification Number)을 입력할 때에 보안성을 강화하기 위한 것으로, 사용자가 안전하게 PIN을 입력하는 방법 및 시스템에 관한 것이다.

배경 기술

- [0002] 도 1(a)를 참고하면, 랜덤 숫자 키패드를 이용하는 PIN 입력 기법은 사용자가 인증을 위해 PIN 입력을 시도할 때마다, 0부터 9까지 10개의 숫자들이 키패드에 랜덤하게 배치된다. 이에 따라 사용자는 매번 PIN을 입력하려고 숫자 버튼을 터치할 때, 일반적인 숫자 키패드와 다른 위치를 터치해야 한다. 이 기법은 이러한 특징으로 인해 일반적인 숫자 키패드를 이용하여 PIN을 입력하는 기법보다 낮은 사용성을 가지고 있다. 사용자는 매번 같은 PIN을 입력하더라도 매번 다른 위치의 숫자 버튼을 터치하여 PIN을 입력해야 하기 때문이다. 그러나 이러한 특징은 한편으로 일반적인 숫자 키패드 보다 높은 보안성을 가질 수 있게 해주는 특징이기도 하다. 공격자가 스머지 공격을 이용하여 스마트폰 스크린 표면의 묻은 지문의 흔적을 보고 사용자가 어느 위치를 터치하였는지는 알 수 있지만, 랜덤 숫자 키패드이기 때문에 어떠한 번호를 터치하였는지는 정확하게 알 수 없으므로 스머지 공격에는 강한 특징을 가지고 있다. 또한 공격자가 키로깅 공격을 이용하여 사용자가 스마트폰 스크린상의 터치한 위치 데이터를 탈취한다고 하더라도, 랜덤 숫자 키패드이기 때문에 사용자가 터치한 위치에 어떤 번호가 위치해 있었는지는 정확하게 알 수 없으므로 키로깅 공격에도 강한 특징을 가지고 있다. 그러나 솔더 서핑 공격에는 여전히 약한 특징을 가지고 있는데, 사용자가 지하철, 버스, 강의실 등의 공개된 장소에서 결제를 하려고 PIN을 입력할 때, 공격자가 솔더 서핑 공격으로 사용자가 PIN을 입력하는 과정을 본다면, 공격자는 사용자가 터치한 PIN을 그대로 알 수 있기 때문에 솔더 서핑 공격에 약한 특징을 가지고 있다. 그러므로 솔더 서핑 공격에도 강한 PIN 입력 기법이 필요한 상황이다.
- [0003] 도 1(b)를 참고하면, 2011년 김진복, 이문규님이 한국정보보호학회 논문지에 게재한 "터치스크린을 이용한 터치 위치기반 사용자 인증" 논문과, 등록번호 10-1054096 "터치스크린을 이용한 안전한 패스워드 입력 방법 및 그 방법을 구현하는 프로그램"을 기록한 컴퓨터로 읽을 수 있는 기록매체 특허"에서는 사용자 인증을 위해 PIN을 입력할 때 터치 위치 데이터를 사용하여 안전성을 높인 PIN 입력 기법을 제안하였다. 터치 위치 데이터는 도 1(b)와 같이 하나의 숫자 버튼을 기준으로 좌측상단의 (0, 0)부터 우측하단의 (X_MAX, Y_MAX)로 표현될 수 있다. 이 기법은 먼저 올바른 사용자가 여러 번 PIN을 입력하여 하나의 숫자 버튼에 대하여 여러 개의 터치 위치 데이터를 저장시킨 후, 그 데이터들의 평균값을 기준으로 정의한다. 그리고 사용자 인증을 위해 PIN을 입력할 때 터치 위치 데이터도 같이 입력으로 받아서, 터치 위치 데이터들이 기준이 되는 터치 위치 데이터의 평균값보다 어느 정도 떨어져 있는지 확인하여, 인증 성공 여부를 판단한다. 그러므로 공격자가 솔더 서핑 공격 등으로 사용자의 PIN을 탈취하여도, 사용자가 PIN을 입력할 때의 터치한 위치 데이터를 모르고 있으면 인증을 할 수 없게 된다.
- [0004] 머신러닝이란, 인공지능의 한 분야로서 사람이 컴퓨터에 일일이 명시적인 코드로 프로그래밍을 하지 않아도, 컴퓨터가 데이터로부터 학습하여 새로운 지식을 얻어내거나 자동적으로 프로그램을 실행시키는 것을 말한다. 머신러닝은 50년대 이후부터 시작되어 오래되었지만 80~90년대까지 발전 후 체자리결음을 하다가 2000년대 들어와서 빅데이터(Big Data)와 결합되었고, 그로 인해 엄청난 발전을 보였다. 머신러닝은 빅데이터로부터 학습에 필요한 많은 데이터를 획득함으로써 딥러닝(Deep Learning)으로 이어졌고, 딥러닝은 컴퓨터공학 분야 내에서 주목할 만한 분야 중 하나로 인식되고 있다.
- [0005] 이에 따라 사용자가 전자 기기에서 PIN을 입력할 때, PIN뿐만 아니라 PIN을 입력함에 따라 식별된 전자 기기의 스크린을 터치하는 시간 데이터와 위치 데이터를 머신러닝을 이용하여 사용자 인증을 수행하는 기술이 제안될 필요가 있다.

발명의 내용

해결하려는 과제

- [0006] 전자 기기에서 사용자가 보다 안전하게 사용자 인증을 수행하는데 목적이 있다. 스머지 공격, 키로깅 공격, 솔더 서핑 공격에 대하여 보다 안전하게 PIN을 입력하는 방법 및 시스템을 제공할 수 있다.

과제의 해결 수단

- [0007] 사용자 인증 방법은, 전자 기기에 사용자 인증을 위한 인증 화면을 표시하는 단계; 사용자로부터 상기 인증 화면을 통하여 입력되는 패스워드 데이터, 상기 패스워드 데이터와 관련된 시간 데이터 및 상기 패스워드 데이터

와 관련된 위치 데이터를 포함하는 입력 정보를 수신하는 단계; 및 상기 입력 정보와 상기 사용자로부터 입력된 입력 정보에 기반하여 학습된 학습 데이터의 비교를 통하여 사용자 인증을 수행하는 단계를 포함할 수 있다.

[0008] 상기 사용자 인증 방법은, 상기 사용자로부터 사용자 인증을 위한 인증 정보를 등록하는 단계를 더 포함하고, 상기 사용자로부터 사용자 인증을 위한 인증 정보를 등록하는 단계는, 상기 사용자로부터 상기 사용자 인증을 위한 패스워드 데이터, 상기 패스워드 데이터가 입력되는 시간 데이터 및 상기 패스워드 데이터가 입력되는 위치 데이터를 인증 정보로 등록하고, 상기 등록된 패스워드 데이터에 기반하여 상기 패스워드가 입력되는 시간 데이터 및 상기 패스워드가 입력되는 위치 데이터에 대한 학습을 수행함에 따라 학습 데이터를 획득하는 단계를 포함할 수 있다.

[0009] 상기 사용자로부터 사용자 인증을 위한 인증 정보를 등록하는 단계는, 상기 패스워드 데이터를 데이터베이스에 저장하고, 상기 패스워드 데이터가 입력되는 시간 데이터 및 상기 패스워드 데이터가 입력되는 위치 데이터에 대한 머신러닝 학습을 위하여 TRUE 라벨을 부가하고, 상기 사용자로부터 입력되는 인증 정보 이외의 다른 데이터를 랜덤하게 생성하여 FALSE 라벨을 부가하여 상기 머신러닝 학습을 통하여 모델을 생성하는 단계를 포함할 수 있다.

[0010] 상기 전자 기기에 사용자 인증을 위한 인증 화면을 표시하는 단계는, 상기 전자 기기에 상기 사용자 인증을 위한 키패드를 랜덤으로 배열하고, 상기 랜덤으로 배열된 키패드를 인증 화면에 표시하는 단계를 포함하고, 상기 입력 정보를 수신하는 단계는, 상기 키패드에서 상기 패스워드 데이터에 설정된 패스워드 길이에 기초하여 첫 번째 자리의 패스워드를 입력하는 시간 데이터를 기준으로, 상기 패스워드 데이터의 첫 번째 자리의 패스워드부터 상기 패스워드 데이터의 마지막 자리의 패스워드를 터치할 때까지의 각각의 터치 시간 데이터를 포함하는 시간 데이터와 상기 패스워드 데이터를 터치하는 각각의 x 좌표, y 좌표를 포함하는 위치 데이터를 식별하는 단계를 포함할 수 있다.

[0011] 상기 사용자 인증을 수행하는 단계는, 상기 사용자로부터 입력된 패스워드 데이터로부터 획득되는 시간 데이터 및 위치 데이터를 식별함에 따라 상기 사용자로부터 입력된 패스워드 데이터가 기 저장된 패스워드와 일치하는지 여부를 판단하는 단계를 포함할 수 있다.

[0012] 상기 사용자 인증을 수행하는 단계는, 상기 사용자로부터 입력된 패스워드 데이터가 기 저장된 패스워드와 일치함에 따라 상기 사용자로부터 입력된 패스워드 데이터와 관련된 시간 데이터, 위치 데이터를 상기 사용자로부터 입력된 입력 정보에 기반하여 학습된 학습 데이터와 비교하여 0내지 1 사이의 소수값을 인증 결과로서 도출하고, 상기 도출된 인증 결과를 기 설정된 기준에 기초하여 인증 성공 또는 인증 실패로 분류하는 단계를 포함할 수 있다.

[0013] 사용자 인증을 수행하는 사용자 인증 시스템은, 사용자로부터 사용자 인증을 위한 인증 정보를 등록하는 등록부; 상기 전자 기기에 사용자 인증을 위한 인증 화면을 표시하는 표시부; 상기 사용자로부터 상기 인증 화면을 통하여 입력되는 패스워드 데이터, 상기 패스워드 데이터와 관련된 시간 데이터 및 상기 패스워드 데이터와 관련된 위치 데이터를 포함하는 입력 정보를 수신하는 수신부; 및 상기 입력 정보와 상기 사용자로부터 입력된 입력 정보에 기반하여 학습된 학습 데이터의 비교를 통하여 사용자 인증을 수행하는 수행부를 포함할 수 있다.

발명의 효과

[0014] 일 실시예에 따른 사용자 인증 시스템은 사용자가 PIN을 입력할 때, PIN, 터치 시간 데이터, 터치 위치 데이터를 이용하여 머신러닝 학습에 기반한 패스워드 인증을 수행함으로써 기존보다 더욱 신뢰성 있는 사용자 검증 및 인증이 가능한 것은 물론, 기존의 스마트폰,패드, 도어락 등의 단말기와 인증 서버에 별도의 하드웨어 추가 없이, 소프트웨어 적으로 쉽게 구현이 가능하므로 구현 비용의 절감 하는 효과를 획득 수 있다.

[0015] 또한, 일 실시예에 따른 사용자 인증 시스템은 기존의 PIN 입력 방식을 간편하게 대체할 수 있고 사용자 설정 및 등록 과정을 간소화할 경우 사용성과 보안성을 동시에 높일 수 있다. 아울러 사용자의 행동을 인식할 수 있도록 스마트 폰 등에 탑재된 센서들과 융합하여 기능을 보강할 경우, 더욱 강력한 보안 성능을 제공할 수 있을 것으로 기대된다. 그로 인해 사용자들은 모바일 상의 금전 거래를 더욱 더 안전하게 사용할 수 있으며, 사용자의 금전을 목적으로 하는 보안 사고를 예방할 수 있다.

도면의 간단한 설명

- [0016] 도 1은 PIN 입력 방법을 설명하기 위한 예이다.
- 도 2는 일 실시예에 따른 사용자 인증 시스템의 구성을 설명하기 위한 블록도이다.
- 도 3은 일 실시예에 따른 사용자 인증 시스템에서 사용자 인증을 수행하기 위한 유저 인터페이스를 나타낸 예이다.
- 도 4는 일 실시예에 따른 사용자 인증 시스템에서 사용자 등록 방법을 설명하기 위한 흐름도이다.
- 도 5는 일 실시예에 따른 사용자 인증 시스템에서 사용자 등록 과정에서 의사코드 알고리즘을 기재한 것이다.
- 도 6은 일 실시예에 따른 사용자 인증 시스템에서 사용자 인증 방법을 설명하기 위한 흐름도이다.
- 도 7은 일 실시예에 따른 사용자 인증 시스템에서 사용자 인증 과정의 의사코드 알고리즘을 기재한 것이다.

발명을 실시하기 위한 구체적인 내용

- [0017] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.
- [0018] 도 2는 일 실시예에 따른 사용자 인증 시스템의 구성을 설명하기 위한 블록도이다.
- [0019] 사용자 인증 시스템(100)은 등록부(210), 표시부(220), 수신부(230) 및 수행부(240)를 포함할 수 있다.
- [0020] 등록부(210)는 사용자로부터 사용자 인증을 위한 인증 정보를 등록할 수 있다. 등록부(210)는 사용자로부터 상기 사용자 인증을 위한 패스워드 데이터, 패스워드 데이터가 입력되는 시간 데이터 및 패스워드 데이터가 입력되는 위치 데이터를 인증 정보로 등록하고, 등록된 패스워드 데이터에 기반하여 패스워드가 입력되는 시간 데이터 및 패스워드가 입력되는 위치 데이터에 대한 학습을 수행함에 따라 학습 데이터를 획득할 수 있다. 등록부(210)는 패스워드 데이터를 데이터베이스에 저장하고, 패스워드가 입력되는 시간 데이터 및 패스워드가 입력되는 위치 데이터에 대한 머신러닝 학습을 위하여 TRUE 라벨을 부가하고, 사용자로부터 입력되는 인증 정보 이외의 다른 데이터를 랜덤하게 생성하여 FALSE 라벨을 부가하여 머신러닝 학습을 통하여 모델을 생성할 수 있다.
- [0021] 표시부(220)는 전자 기기에 사용자 인증을 위한 인증 화면을 표시할 수 있다. 표시부(220)는 전자 기기에 상기 사용자 인증을 위한 키패드를 랜덤으로 배열하고, 랜덤으로 배열된 키패드를 인증 화면에 표시할 수 있다.
- [0022] 수신부(230)는 사용자로부터 인증 화면을 통하여 입력되는 패스워드 데이터, 패스워드 데이터와 관련된 시간 데이터 및 패스워드 데이터와 관련된 위치 데이터를 포함하는 입력 정보를 수신할 수 있다. 수신부(230)는 패스워드 데이터에 설정된 패스워드 길이에 기초하여 첫 번째 자리의 패스워드를 입력하는 시간 데이터를 기준으로, 패스워드 데이터의 첫 번째 자리의 패스워드부터 패스워드 데이터의 마지막 자리의 패스워드를 터치할 때까지의 각각의 터치 시간 데이터를 포함하는 시간 데이터와 패스워드 데이터를 터치하는 각각의 x 좌표, y 좌표를 포함하는 위치 데이터를 식별할 수 있다.
- [0023] 수행부(240)는 입력 정보와 사용자로부터 입력된 입력 정보에 기반하여 학습된 학습 데이터의 비교를 통하여 사용자 인증을 수행할 수 있다. 수행부(240)는 사용자로부터 입력된 패스워드 데이터로부터 획득되는 시간 데이터 및 위치 데이터를 식별함에 따라 사용자로부터 입력된 패스워드 데이터가 기 저장된 패스워드와 일치하는지 여부를 판단할 수 있다. 수행부(240)는 사용자로부터 입력된 패스워드 데이터가 기 저장된 패스워드와 일치함에 따라 사용자로부터 입력된 패스워드 데이터와 관련된 시간 데이터, 위치 데이터를 사용자로부터 입력된 입력 정보에 기반하여 학습된 학습 데이터와 비교하여 0내지 1 사이의 소수값을 인증 결과로서 도출하고, 상기 도출된 인증 결과를 기 설정된 기준에 기초하여 인증 성공 또는 인증 실패로 분류할 수 있다.
- [0024] 도 3은 일 실시예에 따른 사용자 인증 시스템에서 사용자 인증을 수행하기 위한 유저 인터페이스를 나타낸 예이다.
- [0025] 전자 기기(110)에 키패드(300)가 랜덤으로 배열되어 표시될 수 있다. 예를 들면, 키패드는 문자, 숫자, 기호 중 어느 하나 이상 또는 두 개 이상이 결합된 형태로 구성될 수 있다. 도 3에서는 0 내지 9로 구성된 키패드를 예를 들어 설명하기로 한다.

- [0026] 전자 기기(110)는 예를 들면, 스마트폰(smart phone), 휴대폰, 내비게이션, 컴퓨터, 노트북, 디지털방송용 단말, PDA(Personal Digital Assistants), PMP(Portable Multimedia Player), 태블릿 PC 등이 있다. 전자 기기(110)는 무선 또는 유선 통신 방식을 이용하여 네트워크를 통하여 서버와 통신할 수 있다. 일례로, 전자 기기(110)에 사용자 인증을 수행하기 위한 어플리케이션이 설치되어 동작될 수 있다.
- [0027] 실시예에서는, 전자 기기(110)에 사용자 인증을 수행함에 있어서, 사용자 식별자로 패스워드 데이터뿐만 아니라 사용자로부터 패스워드 데이터를 입력할 때의 전자 기기(110)의 스크린을 터치하는 시간 데이터 및 패스워드 데이터를 터치하는 위치 데이터를 식별자로 사용할 수 있다. 이러한, 시간 데이터 및 위치 데이터를 머신러닝을 이용하여 올바른 사용자인지 올바르게 않은 사용자인지 사용자를 판단할 수 있다. 여기서, 패스워드 데이터를 입력할 때, 패스워드 데이터에 설정된 패스워드 길이에 기초하여 첫 번째 자리의 패스워드를 입력하는 시간 데이터를 기준으로, 패스워드 데이터의 첫 번째 자리의 패스워드로부터 패스워드 데이터의 마지막 자리의 패스워드 패스워드를 터치할 때까지의 각각의 터치 시간 데이터를 포함하는 시간 데이터와 패스워드 데이터를 터치하는 각각의 x 좌표, y 좌표를 포함하는 위치 데이터를 식별할 수 있다. 다시 말해서, 시간 데이터는 패스워드 데이터를 입력할 때, 패스워드 데이터의 첫 번째 자리를 입력하기 위하여 숫자 버튼을 터치하는 시간을 시작 기준으로 하여 패스워드 데이터의 마지막 자리의 숫자 버튼을 터치할 때까지, 숫자 버튼의 터치와 터치 사이의 시간을 기록한 데이터를 의미한다. 첫 번째 시간 데이터는 기준이기 때문에 항상 0.0초이다. 그리고, 위치 데이터는 패스워드 데이터를 입력하려면 숫자 버튼을 터치해야 하는데, 이때, 각 숫자의 버튼 범위 내에서 사용자가 터치한 위치의 x 좌표, y좌표를 기록한 데이터를 의미한다.
- [0028] 더욱 상세하게는, 키패드에 각각의 패스워드 데이터를 입력하기 위한 유저 인터페이스가 구성될 수 있다. 예를 들면, 0 내지 9의 숫자로 구성된 키패드에 사용자의 터치를 감지하기 위한 0 내지 9에 대응하는 10개의 유저 인터페이스로 구성될 수 있으며, 각각의 유저 인터페이스의 크기는 동일 또는 비동일할 수 있다. 사용자 인증 시스템은 이와 같이 키패드에 구성된 10개의 유저 인터페이스에 대응하는 숫자 중 일부가 입력됨에 따라 숫자가 터치된 위치 데이터를 식별할 수 있다. 이때, 사용자는 키패드의 유저 인터페이스를 입력함에 있어서, 패스워드 데이터에 대응하는 유저 인터페이스의 크기 내에서 입력될 수 있다.
- [0029] 사용자로부터 입력된 입력 정보에 기반하여 사용자를 인증하기 위하여 머신러닝을 수행할 수 있다. 머신러닝은 예를 들면, 로지스틱 리그레션(Logistic Regression), 시그모이드 함수(Sigmoid Function), 렐루(ReLU) 등의 이론을 사용하여 사용자 데이터를 기반으로 모델을 생성한 후, 생성된 모델을 이용하여 올바른 사용자와 올바르게 않은 사용자를 분류할 수 있다. 이때, 모델을 생성하기 위해서는 사용자의 데이터(예를 들면, 패스워드 데이터, 패스워드 데이터와 관련된 시간 데이터, 패스워드 데이터와 관련된 위치 데이터 등)가 필요하다.
- [0030] 이러한 랜덤으로 표시되는 키패드에서 '05461467'인 PIN을 입력하는 동작을 설명하기로 한다. 사용자가 패스워드 데이터를 입력하기 위하여 숫자 버튼을 터치하면, 자동으로 시간 데이터와 위치 데이터가 기록될 수 있다. 또한, 스머지 공격, 키로깅 공격에 강한 특징을 갖기 위하여 일반 숫자 키패드보다 보안성이 더 높은 랜덤 숫자 키패드를 사용할 수 있다. 이때, 키패드의 랜덤한 숫자 배치는 사용자 의존성을 가지고 있어 사용자마다 숫자 키가 다르게 배치될 수 있다. 예를 들면, 키패드는 사용자로부터 하나의 숫자 키를 누를 때마다 숫자 키가 랜덤으로 변경될 수 있고, 패스워드 데이터가 모두 입력된 후, 인증 과정을 수행함에 따라 숫자 키가 랜덤으로 변경될 수 있다. 도 3을 참고하면, 사용자가 '05461467'을 입력하였을 때 기록된 터치 시간 데이터와 터치된 위치 데이터의 예이다. 예를 들면, 0이 입력되었을 때의 시간 데이터(예를 들면, 0.0s), 0이 입력된 위치 데이터(x:0.5, y:3.2)가 식별될 수 있다.
- [0031] 사용자 인증 시스템은 인증을 위하여 입력 정보를 수집하는 등록 과정 및 사용자의 인증을 수행하는 인증 과정을 수행할 수 있다. 도 4를 참고하면, 일 실시예에 따른 사용자 인증 시스템에서 사용자 등록 방법을 설명하기 위한 흐름도이다. 사용자로부터 전자 기기의 인증 화면을 통하여 패스워드 데이터, 패스워드 데이터가 입력되는 시간 데이터 및 패스워드 데이터가 입력되는 위치 데이터가 서버로 전송될 수 있다. 먼저, 사용자는 사전 훈련이 필요하다. 예를 들면, 사용자는 패스워드 데이터를 설정한 후, 패스워드 데이터를 복수 번 반복하여 입력할 수 있다. 이때, 기 설정된 기준의 일정하게 터치되는 시간 데이터 및 위치 데이터에 대한 패턴을 획득하기 위하여 매번 최대한 비슷하게 터치되는 시간 데이터 및 위치 데이터의 패턴을 유지해야 한다. 이를 위하여, 사용자가 패스워드 데이터를 입력하기 위하여 전자 기기의 스크린에 표시된 키패드를 터치할 때, 사용자만이 터치되는 시간 데이터 및 위치 데이터에 대한 패턴을 인지하고 있어야 한다. 사용자가 어느 정도 패스워드 데이터를 입력하는 것이 익숙해짐에 따라 다시 복수 번 패스워드 데이터를 입력할 수 있다. 이와 같이, 사용자로부터 복수 번 패스워드 데이터가 입력됨으로써 머신러닝을 통하여 사용자로부터 입력된 패스워드 데이터와 관련된 입력 정보를 학습할 수 있다. 전자 기기는 사용자로부터 복수 번 입력된 패스워드 데이터, 패스워드 데이터와

관련된 시간 데이터 및 패스워드 데이터와 관련된 위치 데이터를 인증 서버에게 전송하고, 인증 서버는 사용자로부터 전송받은 데이터 중 패스워드 데이터를 데이터베이스에 저장할 수 있다. 이때, 패스워드 데이터를 입력한 시간 데이터 및 패스워드 데이터를 입력한 위치 데이터에 머신러닝 학습을 위하여 패스워드 데이터를 입력한 시간 데이터 및 패스워드 데이터를 입력한 위치 데이터에 TRUE 라벨을 부가할 수 있다. TRUE 라벨을 부가하는 데이터는 올바른 사용자의 데이터임을 의미한다. 그리고, 사용자로부터 입력된 입력 정보 이외의 다른 데이터를 랜덤하게 생성하여 FALSE 라벨을 부가할 수 있다. FALSE 라벨이 부가된 데이터는 올바르지 않은 사용자의 데이터임을 의미한다. TRUE 라벨이 부가된 데이터에 기반하여 머신러닝 학습을 수행할 수 있고, 머신러닝 학습이 수행된 학습 데이터에 대한 모델을 생성할 수 있다. 예를 들면, TRUE 라벨이 부가된 데이터에 기반하여 추후에 사용자로부터 입력된 입력 정보를 비교하기 위한 기준값이 도출될 수 있다. TRUE 라벨이 부가된 데이터에 기반하여 올바른 사용자로 인증하기 위한 범위가 설정될 수 있으며, 이러한 범위에 기초하여 인증 성공 여부를 판단할 수 있다. 이와 같은 과정을 수행함에 따라 사용자 등록 과정이 완료될 수 있다. 도 5를 참고하면, 사용자 등록 과정에서 의사코드 알고리즘을 기재한 것이다. 여기서 T(Time)는 시간 데이터, L(Location)은 위치 데이터를 의미한다.

[0032] 도 6를 참고하면, 사용자 인증 방법을 설명하기 위한 흐름도이다. 사용자 등록 과정이 완료됨에 따라 사용자는 인증을 시도할 수 있다. 사용자는 인증을 수행하기 위하여 전자 기기의 인증 화면에 랜덤으로 표시된 키패드에 입력 정보를 입력할 수 있다. 예를 들면, 사용자는 인증 화면에 표시된 키패드에 기반하여 패스워드 데이터를 입력할 수 있다. 이때, 사용자는 패스워드 데이터를 입력함에 있어서, 평상적으로 패스워드 데이터를 입력할 때와 비슷하게 터치되는 시간 데이터, 터치되는 위치 데이터의 패턴을 인지하면서 입력을 진행할 수 있다. 사용자로부터 입력 정보의 입력이 완료됨에 따라 사용자로부터 입력된 패스워드 데이터, 패스워드 데이터가 입력된 시간 데이터 및 패스워드 데이터가 입력된 위치 데이터를 서버로 전송할 수 있다. 이때, 인증 방법에 따라 사용자가 인증 화면에 패스워드 데이터를 각각 터치함으로써 입력 정보를 입력할 수 있고, 패스워드 데이터를 연속적으로 각각 연결함으로써 입력 정보를 입력할 수 있다. 서버는 사용자로부터 전송받은 입력 정보에 포함된 패스워드 데이터가 데이터베이스에 저장되어 있는 패스워드가 일치하는지 여부를 비교할 수 있다. 만약, 입력 정보에 포함된 패스워드 데이터가 데이터베이스에 저장되어 있는 패스워드와 일치할 경우, 패스워드 데이터가 입력된 시간 데이터 및 위치 데이터를 기 생성된 모델(인증 과정에서 생성된 모델)과 비교할 수 있다. 구체적으로, 사용자로부터 입력된 패스워드 데이터와 관련된 시간 데이터, 위치 데이터를 사용자로부터 입력된 입력 정보에 기반하여 학습된 학습 데이터에 대한 모델과 비교하여 0내지 1 사이의 소수값을 인증 결과로서 도출하고, 도출된 인증 결과를 기 설정된 기준에 기초하여 인증 성공 또는 인증 실패로 분류할 수 있다. 이때, 모델은 사용자로부터 입력된 입력 정보가 TRUE에 근접한 것인지 FALSE에 근접한 것인지 계산한 후 인증 결과로서 0과 1 사이의 소수값을 서버로 반환할 수 있다. 서버는 0과 1사이에서 인증 성공과 인증 실패를 나누는 기준값(인증 성공 기준)을 설정한 후, 모델로부터 반환된 인증 결과를 기준 값에 적용함에 따라 인증 성공 여부를 전자 기기에게 통보할 수 있다. 예를 들면, 서버에서 인증 성공 기준이 0.9이고, 인증 결과가 0.6일 경우 인증 실패로 판단할 수 있고, 인증 결과가 0.95일 경우 인증 성공이 된다. 도 7을 참고하면, 사용자 인증 과정의 의사코드 알고리즘을 기재한 것이다. 여기서, T(Time)은 패스워드 데이터가 입력된 시간 데이터이고, L(Location)은 패스워드 데이터가 입력된 위치 데이터를 의미한다. 그리고 도 7의 PIN은 데이터베이스에 저장

되어 있는 사용자의 패스워드를 의미하고, θ 는 0과 1사이의 소수값으로서 서버에서 설정한 인증 성공 기준을 의미할 수 있다.

[0033] 일 실시예에 따른 사용자 인증 시스템은 사용자가 PIN을 입력할 때, 공격자로부터 스머지 공격에 대하여 안전하게 PIN 입력 가능하다. 공격자가 일반적인 숫자 키패드를 사용하는 사용자를 스머지 공격으로 공격한다면, 전자 기기(예를 들면, 스마트폰) 스크린 표면의 묻은 지문의 흔적으로부터 사용자의 PIN을 알아낼 수 있다. 그러나 본 발명은 일단 사용자마다 다른 랜덤 숫자 키패드를 사용하고 있기 때문에, 공격자가 스머지 공격을 이용하여 사용자가 어느 숫자 키를 터치했는지 알기 어렵고, 뿐만 아니라 스머지 공격으로는 터치 시간 데이터까지 알아낼 수 없으므로 일반적으로 사용되는 숫자 키패드보다 스머지 공격에 강하다.

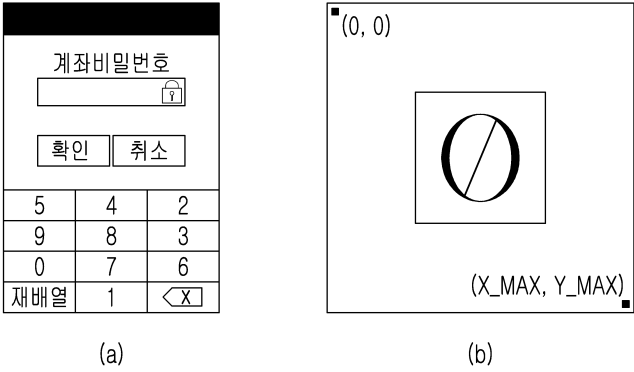
[0034] 또한, 일 실시예에 따른 사용자 인증 시스템은 사용자가 PIN을 입력할 때, 공격자로부터 키로깅 공격에 대하여 안전하게 PIN 입력 가능하다. 공격자는 사용자가 PIN을 입력하기 위해 전자 기기(예를 들면, 스마트폰)를 터치할 때에 키로깅 공격으로 터치 위치 데이터를 탈취할 수 있다. 그러나 본 발명은 일단 사용자마다 다른 랜덤 숫자 키패드를 사용하고 있기 때문에, 탈취당한 터치 위치 데이터에 어떤 번호가 위치해 있었는지 알 수 없으므로 공격자는 사용자의 PIN을 정확히 알아낼 수 없을 것이다. 뿐만 아니라 공격자는 사용자가 PIN을 입력할 때

숫자 버튼을 터치한 시간 데이터를 여전히 모르고 있기 때문에, 공격자는 인증에 성공할 수 없다. 이에 따라, 일반적으로 사용되는 숫자 키패드보다 키로깅 공격에 강하다.

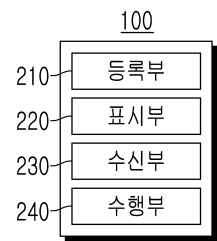
- [0035] 또한, 일 실시예에 따른 사용자 인증 시스템은 사용자가 PIN을 입력할 때, 솔더 서핑 공격에 대하여 안전하게 PIN 입력 가능하다. 사용자가 PIN을 입력하려고 할 때, 공격자는 솔더 서핑 공격으로 사용자가 어떤 번호를 터치하였는지 쉽게 알 수 있으며 그로 인해 사용자의 PIN을 알아낼 수 있다. 그러나 공격자가 PIN을 쉽게 알아내더라도, 사용자가 정확히 어떠한 시간 패턴으로 터치를 했는지, 정확히 어느 위치를 터치 했는지 기억하지 못한다면 공격을 성공시키기 어려울 것이다. 그렇기 때문에 본 발명은 솔더 서핑 공격에 강한 특징을 가지고 있다.
- [0036] 일 실시예에 따른 사용자 인증 시스템은 사용자로 하여금 보다 안전하게 PIN을 입력하게 하는 기법으로서, 다양한 분야에 적용 및 응용을 시킬 수 있다. 특히, 스마트폰에서 금전을 이용하는 모바일 간편결제 서비스 및 모바일 뱅킹 서비스 등 적용될 수 있다. 뿐만 아니라 USIM 잠금 시스템 분야 또는 일반적으로 패스워드를 입력하는 분야 등에서 숫자를 입력할 때 적용될 수 있기 때문에, 보다 널리 사용될 수 있을 것이다.
- [0037] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.
- [0038] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embodiment)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.
- [0039] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.
- [0040] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.
- [0041] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

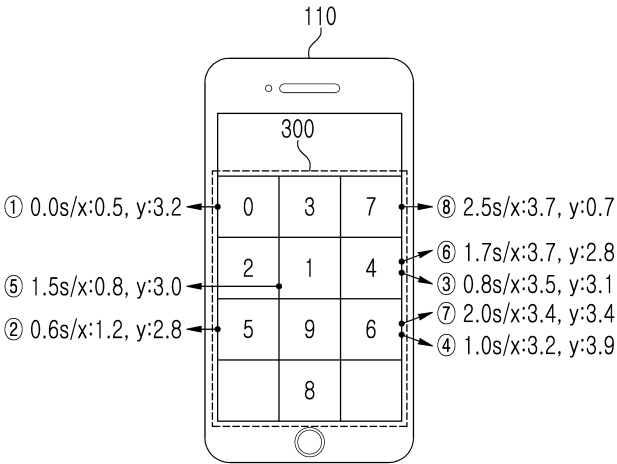
도면1



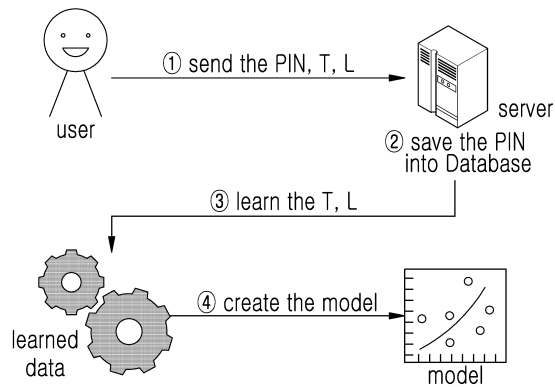
도면2



도면3



도면4



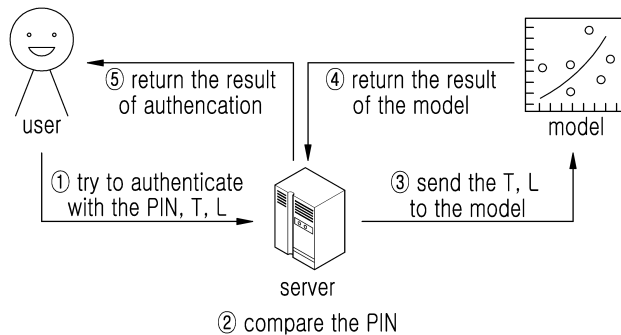
도면5

Input: PIN, T(Time), L(Location)
Output: Model

```

save(PIN)
var_L = Learning(T, L)
var_M = Modeling(var_L)
return var_M
  
```

도면6



도면7

Input: PIN, T(Time), L(Location)
Output: SUCCESS, FAIL

```

if PIN = PIN '
  var_Result = var_M(T, L)
  if var_Result ≥ θ
    return SUCCESS
  Else
    return FAIL
  
```