(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0028309
(43) 공개일자 2013년03월19일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06F 21/22* (2006.01)
(21) 출원번호 10-2011-0091767
(22) 출원일자 2011년09월09일
심사청구일자 2011년09월09일

(71) 출원인
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
이문규
경기도 부천시 원미구 계남로 81, 2222동 702호 (상동, 진달래마을)
김진복
인천광역시 남구 경인남길118번길 58, 301호 (용현동, 우당원룸)
한태윤
인천광역시 남구 용현5동 신창미션힐아파트 103동 703호
(74) 대리인
특허법인무한

전체 청구항 수 : 총 12 항

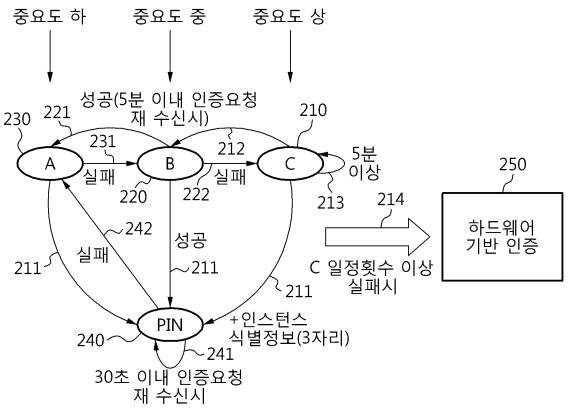
(54) 발명의 명칭 **다중 보안 설정에 기초한 사용자 인증 시스템 및 방법**

(57) 요 약

다중 보안 설정에 기초한 사용자 인증 시스템 및 방법이 개시된다.

다중 보안 설정에 기초한 사용자 인증 방법은 어플리케이션의 인증 요청을 수신하는 단계; 상기 어플리케이션의 중요도와 사용 빈도를 기초로 사용자 인증에 사용할 인증 수단을 결정하는 단계; 및 결정된 인증 수단을 사용하여 사용자를 인증하는 단계를 포함할 수 있다.

대 표 도 - 도2



이 발명을 지원한 국가연구개발사업

과제고유번호 10039180

부처명 지식경제부

연구사업명 산업융합원천기술개발사업

연구과제명 모바일 환경하에서 모바일 인증과 보안 강화를 위해 직관적이며 사용하기 편하고 안전한 인간-컴퓨터 상호작용(HCI) 기반 Usable Security 원천기술 개발

주관기관 세종대학교 산학협력단

연구기간 2011.05.01 ~ 2015.02.28

특허청구의 범위

청구항 1

모바일 단말기에서 수행되는 인증 방법에 있어서,

어플리케이션의 인증 요청을 수신하는 단계;

상기 어플리케이션의 중요도와 사용 빈도를 기초로 사용자 인증에 사용할 인증 수단을 결정하는 단계; 및

결정된 인증 수단을 사용하여 사용자를 인증하는 단계;

를 포함하는 인증 방법.

청구항 2

제1항에 있어서,

상기 결정하는 단계는,

상기 어플리케이션의 중요도와 사용 빈도를 기초로 사용자 인증에 사용할 인증 수단의 등급을 결정하는 단계;

인증 강도에 따라 결정한 등급으로 분류된 인증 수단 중 하나를 사용자 인증에 사용할 인증 수단으로 결정하는 단계

를 포함하는 것을 특징으로 하는 인증 방법.

청구항 3

제1항에 있어서,

상기 결정하는 단계는,

어플리케이션의 인증 요청을 재 수신하는 경우, 상기 어플리케이션의 중요도보다 낮은 등급의 인증 수단을 사용자 인증에 사용할 인증 수단으로 결정하는 것을 특징으로 하는 인증 방법.

청구항 4

제1항에 있어서,

상기 결정하는 단계는,

어플리케이션의 인증 요청을 재 수신하는 경우, 어플리케이션의 인증 요청을 수신한 시간과 어플리케이션의 인증 요청을 재 수신한 시간 간의 간격 및 상기 어플리케이션의 중요도를 기초로 인증 수단을 결정하는 것을 특징으로 하는 인증 방법.

청구항 5

제1항에 있어서,

상기 결정하는 단계는,

어플리케이션의 인증 요청을 수신한 횟수를 기초로 어플리케이션의 사용 빈도를 결정하는 것을 특징으로 하는 인증 방법.

청구항 6

제1항에 있어서,

사용자의 인증을 실패하는 경우, 상기 어플리케이션의 중요도보다 높은 등급의 인증 수단을 사용자 인증에 사용할 인증 수단으로 결정하는 단계

를 더 포함하는 인증 방법.

청구항 7

제1항에 있어서,

상기 인증부는,

인증을 성공한 경우 인스턴트 식별 정보를 사용자에게 제공하는 것을 특징으로 하는 인증 방법.

청구항 8

제7항에 있어서,

상기 인증하는 단계는,

어플리케이션의 인증 요청을 재 수신하는 경우, 인스턴트 식별 정보를 사용하여 사용자를 인증하는 것을 특징으로 하는 인증 방법.

청구항 9

제1항에 있어서,

사용자의 인증을 일정 회수 이상 실패하는 경우, 모바일 단말기를 락하고, 하드웨어를 사용한 인증 수단을 사용자 인증에 사용할 인증 수단으로 결정하는 단계

를 더 포함하는 인증 방법.

청구항 10

모바일 단말기에서 수행되는 인증 방법에 있어서,

어플리케이션의 인증 요청을 수신하는 단계;

상기 어플리케이션의 중요도와 사용 빈도를 기초로 인증 수단의 인증 강도를 결정하는 단계;

인증 강도가 결정된 인증 수단을 사용하여 사용자를 인증하는 단계;

를 포함하는 인증 방법.

청구항 11

제10항에 있어서,

상기 결정하는 단계는,

인증 수단의 파라미터를 변경하여 인증 수단의 인증 강도를 결정하는 것을 특징으로 하는 인증 방법.

청구항 12

모바일 단말기에서 수행되는 인증 시스템에 있어서,

어플리케이션의 인증 요청을 수신하는 인증 요청 수신부;

상기 어플리케이션의 중요도와 사용 빈도를 기초로 사용자 인증에 사용할 인증 수단을 결정하는 인증 수단 결정부; 및

결정된 인증 수단을 사용하여 사용자를 인증하는 사용자 인증부

를 포함하는 인증 시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 다중 보안 설정에 기초한 사용자 인증 시스템 및 방법에 관한 것으로, 보다 상세하게는 어플리케이션의 중요도와 사용 빈도에 따라 다른 인증 수단을 사용하여 인증을 수행함으로써, 보안성을 유지하면서도 자주

사용하는 어플리케이션은 보다 용이하게 인증하는 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 스마트 폰과 같은 모바일 단말기를 사용하는 사용자가 증가함에 따라 스마트 폰의 어플리케이션에 저장되는 개인 정보를 보호하기 위한 인증 방법이 발전하고 있다.

[0003] 이때, 각각의 어플리케이션이 사용하는 개인 정보의 중요도가 다르므로 중요도에 따라 인증 방법을 다르게 하는 방법이 개발되었다.

[0004] 그러나, 일반적으로 모바일 단말기에서 중요도가 높은 어플리케이션은 사용자의 사용 빈도가 높다.

[0005] 즉, 종래의 중요도에 따른 인증 방법은 사용자가 자주 사용하는 어플리케이션에 대하여 매번 복잡한 인증 방법을 요구하므로 사용자의 편의성을 저하하고 있는 실정이다.

[0006] 따라서, 어플리케이션의 중요도에 따른 보안성을 유지하면서도 사용자의 편의성을 높일 수 있는 인증 방법이 요청되고 있다.

발명의 내용

해결하려는 과제

[0007] 본 발명은 어플리케이션의 중요도와 사용 빈도에 따라 다른 인증 수단을 사용하여 인증을 수행함으로써, 보안성을 유지하면서도 자주 사용하는 어플리케이션은 보다 용이하게 인증하는 시스템 및 방법을 제공한다.

[0008] 또한, 본 발명은, 일정 이상 인증을 실패한 경우, 모바일 기기를 락하고, 하드웨어를 사용하여 인증을 수행한 경우에 모바일 기기의 락을 해제함으로써, 모바일 단말기를 분실하거나 도난 당했을 때에도 무차별 대입 공격 등에 쉽게 개인정보가 노출되지 않도록 하는 시스템 및 방법을 제공한다.

[0009] 그리고, 본 발명은 기 설정된 PC와 음향, 또는 이미지를 사용하여 하드웨어 인증을 수행함으로써 사용자가 별도의 기기를 소지하지 않아도 하드웨어를 사용한 인증을 수행하여 모바일 단말기의 락을 해제할 수 있는 시스템 및 방법을 제공한다.

과제의 해결 수단

[0010] 본 발명의 일실시예에 따른 다중 보안 설정에 기초한 사용자 인증 방법은 어플리케이션의 인증 요청을 수신하는 단계; 상기 어플리케이션의 중요도와 사용 빈도를 기초로 사용자 인증에 사용할 인증 수단을 결정하는 단계; 및 결정된 인증 수단을 사용하여 사용자를 인증하는 단계를 포함할 수 있다.

[0011] 본 발명의 일실시예에 따른 다중 보안 설정에 기초한 사용자 인증 시스템은 어플리케이션의 인증 요청을 수신하는 인증 요청 수신부; 상기 어플리케이션의 중요도와 사용 빈도를 기초로 사용자 인증에 사용할 인증 수단을 결정하는 인증 수단 결정부; 및 결정된 인증 수단을 사용하여 사용자를 인증하는 사용자 인증부를 포함할 수 있다.

발명의 효과

[0012] 본 발명의 일실시예에 의하면, 어플리케이션의 중요도와 사용 빈도에 따라 다른 인증 수단을 사용하여 인증을 수행함으로써, 보안성을 유지하면서도 자주 사용하는 어플리케이션은 보다 용이하게 인증할 수 있다.

[0013] 또한, 본 발명의 일실시예에 의하면, 일정 이상 인증을 실패한 경우, 모바일 기기를 락하고, 하드웨어를 사용하여 인증을 수행한 경우에 모바일 기기의 락을 해제함으로써, 모바일 단말기를 분실하거나 도난 당했을 때에도 무차별 대입 공격 등에 쉽게 개인정보가 노출되지 않도록 할 수 있다.

[0014] 그리고, 본 발명의 일실시예에 의하면, 기 설정된 PC와 음향, 또는 이미지를 사용하여 하드웨어 인증을 수행함으로써 사용자가 별도의 기기를 소지하지 않아도 하드웨어를 사용한 인증을 수행하여 모바일 단말기의 락을 해제할 수 있다.

도면의 간단한 설명

[0015] 도 1은 본 발명의 일실시예에 따른 다중 보안 설정에 기초한 사용자 인증 시스템을 도시한 블록

다이어그램이다.

도 2는 본 발명의 일실시예에 따른 다중 보안 설정에 기초한 사용자 인증 방법의 진행 과정의 일례이다.

도 3은 본 발명의 일실시예에 따른 다중 보안 설정에 기초한 사용자 인증 방법을 도시한 플로우차트이다.

도 4는 본 발명의 일실시예에 따른 사용자 인증 방법에서 인증 수단을 결정하는 방법을 도시한 플로우차트이다.

도 5는 본 발명의 일실시예에 따른 사용자 인증 방법에서 인증 수단을 재결정하는 방법을 도시한 플로우차트이다.

도 6은 본 발명의 다른 실시예에 따른 다중 보안 설정에 기초한 사용자 인증 방법을 도시한 플로우차트이다.

발명을 실시하기 위한 구체적인 내용

[0016] 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다. 본 발명의 일실시예에 따른 다중 보안 설정에 기초한 사용자 인증 방법은 다중 보안 설정에 기초한 사용자 인증 시스템에 의해 수행될 수 있다.

[0017] 도 1은 본 발명의 일실시예에 따른 다중 보안 설정에 기초한 사용자 인증 시스템을 도시한 블록 다이어그램이다.

[0018] 도 1을 참고하면, 본 발명의 일실시예에 따른 사용자 인증 시스템(100)은 인증 요청 수신부(110), 등급 결정부(120), 인증 수단 데이터베이스(130), 인증 수단 결정부(140) 및 사용자 인증부(150)를 포함할 수 있다. 이때, 사용자 인증 시스템(100)은 모바일 단말기에 설치된 어플리케이션의 인증을 수행하는 사용자 인증 시스템일 수 있다.

[0019] 인증 요청 수신부(110)는 어플리케이션의 인증 요청을 수신할 수 있다. 구체적으로, 사용자가 모바일 단말기에 설치된 어플리케이션 중 하나의 실행을 요청한 경우, 인증 요청 수신부(110)는 모바일 단말기의 제어부로부터 해당 어플리케이션의 인증 요청을 수신할 수 있다.

[0020] 등급 결정부(120)는 인증 요청을 수신한 어플리케이션의 중요도와 사용 빈도를 기초로 사용자 인증에 사용할 인증 수단의 등급을 결정할 수 있다. 이때, 등급 결정부(120)는 상기 어플리케이션에서 사용하는 사용자 개인 정보의 중요도에 따라 상기 어플리케이션의 중요도를 결정할 수 있다.

[0021] 이때, 등급 결정부(120)는 어플리케이션의 인증 요청을 재 수신하는 경우, 어플리케이션의 인증 요청을 수신한 횟수를 기초로 어플리케이션의 사용 빈도를 결정할 수 있다.

[0022] 일례로, 등급 결정부(120)는 인증 요청 수신부(110)가 어플리케이션의 인증 요청을 재 수신하는 경우, 어플리케이션의 중요도보다 낮은 등급의 인증 수단을 사용자 인증에 사용할 인증 수단의 등급으로 결정할 수 있다. 이때, 등급 결정부(120)는, 어플리케이션의 인증 요청을 수신한 시간과 어플리케이션의 인증 요청을 재 수신한 시간 간의 간격 및 상기 어플리케이션의 중요도를 기초로 인증 수단의 등급을 결정할 수 있다.

[0023] 즉, 등급 결정부(120)는 어플리케이션의 인증 요청을 재 수신하는 경우, 이미 인증을 한 사용자가 다시 어플리케이션을 사용하고자 하는 것으로 판단하고 어플리케이션에 대응하는 인증 수단의 등급을 낮출 수 있다. 다만, 일정 시간 이후에 인증 요청을 재 수신하는 경우에는 인증을 한 사용자가 아닐 수 있으므로, 등급 결정부(120)는 미리 설정한 시간 안에 인증 요청을 재 수신한 경우에만 인증 수단의 등급을 낮출 수 있다.

[0024] 그리고, 등급 결정부(120)는, 사용자의 인증을 실패하는 경우, 어플리케이션의 중요도보다 높은 등급의 인증 수단을 사용자 인증에 사용할 인증 수단으로 결정할 수 있다.

[0025] 인증 수단 데이터베이스(130)는 복수의 인증 수단을 인증 강도에 따라 결정한 등급 별로 분류하여 저장할 수 있다. 이때, 인증 수단 데이터베이스(130)는 파라미터에 따라 인증 강도가 변경되는 인증 수단의 경우, 인증 수단과, 인증 강도에 따른 파라미터를 저장할 수도 있다.

[0026] 일례로, 엿보기 공격에 강한 선형 PIN 입력 방법은 사용자가 모바일 단말기의 화면에 표시되는 “pass-object”를 좌우로 이동시켜 원하는 숫자를 선택함으로써 정해진 위치를 터치하지 않고 사용자 인증을 위한 PIN(personal identification number)를 입력하는 방법이다. 이때, 상기 선형 PIN 입력 방법은 도형을 좌우로 움직여 PIN을 입력 하므로 다른 엿보기 공격에 강한 PIN 입력 방법 보다 인증 강도는 약하지만, PIN 입력 시간이 짧으며 작은 화면에서도 구현이 가능하여 제한된 모바일 기기 상에서도 사용 가능한 장점이 있다.

[0027] 따라서, 인증 수단 데이터베이스(130)는 상기 선형 PIN 입력 방법을 사용한 인증 수단은 인증 강도가 약한 대신

사용자의 편이성이 높으므로 낮은 등급으로 분류하여 저장할 수 있다.

[0028] 다른 예로, 엿보기 공격에 강한 터치 위치 기반 PIN 입력 방법은 모바일 단말기에서 문자 또는 숫자의 입력 시 같은 버튼을 누르더라도 사용자마다 누르는 정확한 위치 좌표는 모두 다르다는 점을 이용하여 해당 좌표 정보를 추가로 인증에 활용하는 방법이다. 구체적으로, 상기 터치 위치 기반 사용자 인증 방법은 1) PIN의 자리 수를 나타내는 K; 2) 터치한 위치좌표와 인증 기준 위치 간의 거리차이의 허용범위를 나타내는 파라미터 t; 3) 사용자가 터치한 위치와 기준 위치 간의 거리차이가 t안으로 들어온 경우가 K자리의 PIN 숫자들 중 몇 개 이상이어야 인증 성공으로 인정할지를 나타내는 파라미터 Θ(Θ≤K)를 사용하여 PIN을 입력 받을 수 있다. 이때, 상기 터치 위치 기반 사용자 인증 방법은 파라미터 t를 작게 설정할수록 사용자가 정확한 위치를 선택해야만 인증하므로 인증강도는 강해질 수 있다. 또한, 상기 터치 위치 기반 사용자 인증 방법은 파라미터 Θ 를 작게 설정할수록 정확한 위치를 선택하지 않은 PIN 숫자를 인증하는 범위가 증가하므로 인증강도는 약해진다. 일례로, 사용자가 "1234"라는 PIN 숫자들을 입력하면서 1을 평소와 다른 위치에서 터치한 경우, Θ가 PIN 숫자들의 자리수인 4인 경우에는 4개가 모두 정확한 위치에서 터치한 경우만 인증 가능하므로 인증 실패가 되지만, Θ가 PIN 숫자들의 자리수인 3인 경우에는 3개만 정확한 위치에서 터치하면 인증 가능하므로 인증 성공이 될 수 있다.

[0029] 즉, 상기 터치 위치기반 PIN 입력 방법은 사용자 별 입력 습관을 사용하여 사용자를 인증하므로 인증 강도는 강하지만, 사용자가 정확한 PIN 번호를 선택하더라도 평소에 누르는 위치와 다른 곳을 터치한 경우 인증 실패로 판단할 수 있으므로 사용자의 편이성이 낮다. 또한, 사용자가 누르는 위치와의 오차 범위 또는 오차 범위 안에 포함되는 PIN의 개수에 따라 인증 강도와 편이성이 변경될 수 있다.

[0030] 따라서, 인증 수단 데이터베이스(130)는 상기 터치 위치 기반 PIN 입력 방법을 사용한 인증 수단은 인증 강도가 다양하고 강한 대신 사용자의 편이 성이 낮으므로, 중간 또는 높은 등급으로 분류하여 저장할 수 있다.

[0031] 예를 들어 파라미터 Θ를 K-1이 되도록 설정한 터치 위치 기반 PIN 입력 방법을 사용한 인증 수단은 중간 등급으로 분류하고, 파라미터 Θ를 K가 되도록 설정한 터치 위치 기반 PIN 입력 방법을 사용한 인증 수단은 상위 등급으로 분류할 수 있다.

[0032] 인증 수단 결정부(140)는 인증 수단 데이터베이스(130)에서 등급 결정부(120)가 결정한 등급에 대응하는 인증 수단 중 하나를 사용자 인증에 사용할 인증 수단으로 결정할 수 있다.

[0033] 이때, 인증 수단 결정부(140)는 사용자 인증부(150)가 사용자의 인증을 일정 회수 이상 실패하는 경우, 사용자 인증 시스템(100)이 설치된 모바일 단말기를 락(lock)하고, 하드웨어를 사용한 인증 수단을 사용자 인증에 사용할 인증 수단으로 결정할 수 있다.

[0034] 사용자 인증부(150)는 인증 수단 결정부(140)가 결정한 인증 수단을 사용하여 사용자를 인증할 수 있다.

[0035] 이때, 사용자 인증부(150)는 인증을 성공한 경우 인스턴트 식별 정보를 사용자에게 제공할 수 있다. 그리고, 사용자 인증부(150)는 어플리케이션의 인증 요청을 재 수신하는 경우, 인스턴트 식별 정보를 사용하여 사용자를 인증할 수 있다. 이때, 인스턴스 식별 정보는 인증 수단 데이터베이스에 포함된 인증 수단이 사용하는 PIN보다 자리수가 적은 instant PIN일 수 있다.

[0036] 즉, 사용자 인증부(150)는 어플리케이션의 인증 요청을 재 수신하는 경우, 사용자에게 제공한 인스턴트 식별 정보를 사용하여 사용자를 인증함으로써, 이미 인증을 한 사용자가 다시 어플리케이션을 사용하고자 하는 것인지를 판단하고, 인증을 한 사용자인 경우 짧은 PIN인 instant PIN을 사용하여 간편하게 인증할 수 있다.

[0037] 또한, 사용자 인증부(150)는 사용자가 하드웨어를 사용한 인증 수단으로 인증을 성공하면, 모바일 단말기의 락을 해제하고, 사용자가 어플리케이션의 인증을 성공한 것으로 판단할 수 있다.

[0038] 이때, 하드웨어를 사용한 인증 수단은 사용자가 모바일 단말기에 대응하는 하드웨어 토큰과 같이 특정 하드웨어를 모바일 단말기에 접촉하거나 근거리에 위치 시켜 사용자를 인증하는 인증 수단, OTP(One time password) 생성장치 등과 같이 별도의 장치로부터 생성되는 정보를 입력하게 인증 수단, 및 사용자가 기 설정한 고정 PC를 이용하여 모바일 단말기를 인증하는 인증 수단 중 하나일 수 있다. 일례로, 사용자 인증부(150)는 모바일 단말기가 기 설정된 특정 PC에 근접한 것을 확인하면 모바일 단말기의 락을 해제할 수 있다. 이때, 하드웨어를 사용한 인증 수단은 모바일 단말기를 다른 사용자가 주웠을 때 락이 풀리는 것을 방지하기 위해서 하드웨어와 모바일 단말기가 매우 근접한 경우에만 인증이 수행되도록 할 수 있다.

[0039] 이때, 사용자가 기 설정한 고정 PC를 이용하여 모바일 단말기를 인증하는 인증 수단은 웹 캠을 사용한 인증 수

단과 음향을 사용한 인증 수단 중 적어도 하나를 포함할 수 있다.

[0040] 일례로, 웹 캠을 사용한 인증 수단은 먼저, 락된 모바일 단말기가 랜덤 챌린지를 생성하여 화면에 디스플레이 하면, 기 설정된 PC에 장착된 카메라가 디스플레이 된 이미지를 촬영한다. 이때, 기 설정된 PC는 촬영한 이미지로부터 챌린지 코드를 추출하고, 사전에 모바일 단말기와 공유하였던 키와 추출한 챌린지 코드를 이용하여 계산한 응답 값을 모바일 단말기에 전송하여 인증을 수행할 수 있다.

[0041] 또한, PC와 모바일 단말기 간의 거리가 가까운 경우에만 모바일 단말기가 디스플레이 한 챌린지의 이미지를 정확하게 촬영할 수 있으므로, 응답 값이 정답이면 해당 PC가 공유된 키를 알고 있는 기 설정된 PC가 맞으며 PC와 모바일 단말기가 근접해 있다는 사실을 보장할 수 있다.

[0042] 다른 일례로, 음향을 사용한 인증 수단은 모바일 단말기의 스피커에서 일정한 주파수의 비프(Beep)음을 발생시킨 경우, 기 설정된 PC에 장착된 마이크를 통해 전달하여 사용자 인증을 수행할 수 있다. 이때, 음향 신호는 특성상 짧은 시간 내에 많은 챌린지 데이터를 보낼 수 없으므로, 챌린지를 실제로 가지고 있는 제3의 기기(서버)의 정보(주소 및 포트번호 등)만을 음향으로 전달하고, PC는 음향으로 전달될 서버에 접속하여 모바일 기기와 PC간의 인증에 필요한 추가적인 데이터를 수신할 수 있다. 이때, 서버에서 수신하는 데이터들은 사전에 공유된 키를 통해 암호화된 데이터일 수 있다.

[0043] 또한, 음향은 거리가 멀수록 소리가 작아지며 잡음으로 인한 간섭이 일어나므로 음향을 통하여 서버에 대한 정보가 정확하게 전달되면, 해당 PC가 공유된 키를 알고 있는 기 설정된 PC가 맞으며 PC와 모바일 단말기가 근접해 있다는 사실을 보장할 수 있다.

[0044] 본 발명의 일실시예에 따른 다중 보안 설정에 기초한 사용자 인증 시스템은 중요도가 낮은 어플리케이션은 간편하고 인증 강도가 낮은 인증 수단으로 사용자를 인증하고, 중요도가 높은 어플리케이션은 복잡하더라도 인증 강도가 높은 인증 수단으로 사용자를 인증함으로써, 어플리케이션의 보안성을 확보하면서도 최대한 사용자가 사용하기 용이하도록 할 수 있다.

[0045] 도 2는 본 발명의 일실시예에 따른 다중 보안 설정에 기초한 사용자 인증 방법의 진행 과정의 일례이다.

[0046] 본 발명의 일실시예에 따른 사용자 인증 시스템(100)은 어플리케이션의 중요도에 따라 인증 수단 A(230), B(220), C(210)을 설정할 수 있다. 이때, 중요도가 하인 어플리케이션에 대응하는 인증 수단 A(230)는 선형 PIN 입력 방법을 사용하는 인증 수단이고, 중요도가 중, 상인 어플리케이션에 대응하는 인증 수단 B(220), C(210)는 터치 위치 기반 PIN 입력 방법을 사용한 인증 수단일 수 있다. 이때, 중요도가 상인 어플리케이션에 대응하는 인증 수단 C(210)는 파라미터 Θ를 K가 되도록 설정함으로써 인증 강도를 높이고, 중요도가 중인 어플리케이션에 대응하는 인증 수단 B(220)는 파라미터 Θ를 K-1이 되도록 설정함으로써 사용자의 인증을 용이하게 할 수 있다.

[0047] 사용자가 선택한 어플리케이션의 중요도가 상인 경우, 인증 수단 결정부(140)는 사용자를 인증하기 위한 인증 수단으로 C(210)를 결정할 수 있다. 이때, 사용자 인증부(150)는 사용자가 인증에 성공하면, 사용자에게 3자리의 인스턴스 식별 정보를 제공할 수 있다(211).

[0048] 이때, 사용자가 30초 안에 상기 어플리케이션을 재 실행하여 상기 어플리케이션에 대한 인증 요청을 재 수신하는 경우(241), 인증 수단 결정부(140)는 상기 어플리케이션을 재실행한 사용자가 인증된 사용자일 가능성이 높다고 판단할 수 있다.

[0049] 따라서, 인증 수단 결정부(140)는 상기 어플리케이션의 중요도와 무관하게 PIN과 인스턴스 식별 정보를 단순히 입력하는 인증 수단(240)을 사용자 인증 수단으로 결정할 수 있다. 이때, 30초는 사용자가 인스턴스 식별 정보를 기억하고 있을 수 있는 시간이며, 다른 사용자가 모바일 단말기를 획득하여 다시 인증을 하고자 할 확률이 낮은 시간이므로 설정에 따라 변경될 수 있다.

[0050] 이때, 사용자가 인증 수단(240)를 사용하여 인증을 실패한 경우(242), 인증 수단 결정부(140)는 사용자가 인스턴스 식별 정보를 잊은 것으로 판단하고 인증 강도가 가장 낮은 A(230)를 사용자 인증 수단으로 결정할 수 있다.

[0051] 즉, 인증 수단 결정부(140)는 다른 사용자가 모바일 단말기를 사용할 가능성이 낮고, 사용자가 인스턴스 식별 정보를 기억하고 있을 시간인 30초 안에 사용자가 다시 상기 어플리케이션을 실행하는 경우, A(230), B(220), C(210)와 같이 인증 강도가 있는 인증 수단을 대신, 단순히 PIN 번호와 인스턴스 식별 정보를 입력하는 인증 수

단(240)을 사용자 인증 수단으로 결정함으로써, 사용자가 인증하기 쉽도록 할 수 있다.

[0052] 또한, 인증 수단 결정부(140)는 사용자가 5분 안에 상기 어플리케이션을 재 실행하여 상기 어플리케이션에 대한 인증 요청을 재 수신하는 경우(212), 상기 어플리케이션을 재실행한 사용자가 인증된 사용자일 가능성은 높으나. 30초 안에 재실행한 경우보다는 인증된 사용자일 가능성이 낮다고 판단할 수 있다.

[0053] 따라서, 인증 수단 결정부(140)는 단순히 PIN 번호와 인스턴스 식별 정보를 입력하는 인증 수단(240) 대신 인증 강도가 있는 인증 수단을 사용자 인증 수단으로 결정할 수 있다. 다만, 상기 어플리케이션을 재실행한 사용자가 인증된 사용자일 가능성은 높으므로 인증 수단 결정부(140)는 C(210)보다 인증 강도가 낮아서 사용자가 용이하게 인증 받을 수 있는 B(220)를 사용자 인증 수단으로 결정할 수 있다. 구체적으로, 등급 결정부(120)는 인증 요청을 수신한 시간과 인증 요청을 재 수신한 시간 간의 간격이 5분 이하인 경우, 중요도가 상인 상기 어플리케이션의 등급을 중간으로 결정할 수 있다. 그리고, 인증 수단 결정부(140)는 등급 결정부(120)가 결정한 등급에 대응하는 B(220)를 사용자 인증 수단으로 결정할 수 있다.

[0054] 또한, B(220)를 사용하여 인증한 사용자가 5분 안에 상기 어플리케이션을 재 실행하여 상기 어플리케이션에 대한 인증 요청을 재 수신하는 경우(221), 인증 수단 결정부(140)는 B(220)보다 인증 강도가 낮은 A(230)를 사용자 인증 수단으로 결정할 수도 있다. 구체적으로 등급 결정부(120)는 인증 요청을 수신한 시간과 인증 요청을 재 수신한 시간 간의 간격이 5분+5분인 10분 이하이고 인증 요청을 재 수신한 횟수가 2인 경우, 중요도가 상인 상기 어플리케이션의 등급을 하로 결정할 수 있다. 그리고, 인증 수단 결정부(140)는 등급 결정부(120)가 결정한 등급에 대응하는 A(210)를 사용자 인증 수단으로 결정할 수 있다.

[0055] 그리고, 인증 수단 결정부(140)는 사용자가 5분 이상 시간이 경과한 후에 상기 어플리케이션을 재 실행하여 상기 어플리케이션에 대한 인증 요청을 재 수신하는 경우(213), 상기 어플리케이션을 재실행한 사용자가 인증된 사용자일 가능성이 낮다고 판단하여 기존과 같이 C(210)를 사용자 인증 수단으로 결정할 수 있다.

[0056] 또한, 인증 수단 결정부(140)는 사용자 인증부(150)가 사용자의 인증을 실패한 경우, 상위 등급의 인증 수단을 사용자 인증 수단으로 결정할 수 있다.

[0057] 일례로, 사용자가 A(230)를 사용하여 인증을 실패한 경우(231), 인증 수단 결정부(140)는 사용자가 모바일 단말기의 소유자가 아닐 가능성이 있다고 판단하고 인증 강도가 더 높은 B(220)를 사용자 인증 수단으로 결정할 수 있다. 구체적으로, 등급 결정부(120)는 사용자가 A(230)를 사용하여 인증을 실패한 경우(231), 중요도가 하인 상기 어플리케이션의 등급을 중간으로 결정할 수 있다. 그리고, 인증 수단 결정부(140)는 등급 결정부(120)가 결정한 등급에 대응하는 B(220)를 사용자 인증 수단으로 결정할 수 있다.

[0058] 이때, 사용자가 B(220)를 사용해서도 인증을 실패한 경우(222), 인증 수단 결정부(140)는 인증 강도가 더 높은 A(210)를 사용자 인증 수단으로 결정할 수 있다.

[0059] 그리고, 사용자가 C(210)에서 일정 회수 이상 실패한 경우(214), 인증 수단 결정부(140)는 사용자가 모바일 단말기의 소유자가 아닐 가능성이 높다고 판단하여, 사용자 인증 시스템(100)이 설치된 모바일 단말기를 락(lock)하고, 하드웨어를 사용한 인증 수단(250)을 사용자 인증에 사용할 인증 수단으로 결정할 수 있다.

[0060] 본 발명에 따른 사용자 인증 시스템(100)은 모바일 단말기에 락이 걸리면 사용자의 기억에 의존한 사용자 인증 방법 대신 하드웨어를 사용한 인증 수단으로 모바일 단말기의 락을 해제하도록 함으로써, 모바일 단말기를 분실하거나 도난 당했을 때에도 무차별 대입 공격 등에 쉽게 개인정보가 노출되지 않도록 할 수 있다.

[0061] 도 3은 본 발명의 일실시예에 따른 다중 보안 설정에 기초한 사용자 인증 방법을 도시한 플로우차트이다.

[0062] 단계(S310)에서 인증 요청 수신부(110)는 어플리케이션의 인증 요청을 수신할 수 있다. 구체적으로, 사용자가 모바일 단말기에 설치된 어플리케이션 중 하나의 실행을 요청한 경우, 인증 요청 수신부(110)는 모바일 단말기의 제어부로부터 해당 어플리케이션의 인증 요청을 수신할 수 있다.

[0063] 단계(S320)에서 인증 수단 결정부(140)는 단계(S310)에서 인증 요청을 수신한 어플리케이션의 중요도를 기초로 사용자 인증에 사용할 인증 수단을 결정할 수 있다. 인증 수단을 결정하는 과정은 이하 도 4를 참조로 상세히 설명한다.

[0064] 단계(S330)에서 사용자 인증부(150)는 단계(S320)에서 결정된 인증 수단을 사용하여 사용자를 인증할 수 있다.

[0065] 단계(S340)에서 사용자 인증부(150)는 단계(S330)의 인증 결과가 실패인지 여부를 판별할 수 있다.

[0066] 인증 결과가 실패인 경우, 단계(S350)에서 인증 수단 결정부(140)는 사용자 인증 수단을 다시 결정할 수 있다. 인증 수단 결정부(140)가 인증 수단을 다시 결정하는 과정은 이하 도 5를 참조로 상세히 설명한다. 이때, 사용자 인증부(150)는 단계(S350)에서 재결정된 인증 수단을 사용하여 사용자를 인증할 수 있다.

[0067] 인증 결과가 성공인 경우, 단계(S360)에서 사용자 인증부(150)는 인스턴트 식별 정보를 사용자에게 제공할 수 있다.

[0068] 도 4는 본 발명의 일실시예에 따른 사용자 인증 방법에서 인증 수단을 결정하는 방법을 도시한 플로우차트이다. 이때, 도 4의 단계(S410) 내지 단계(S440)는 도 3에 도시된 단계(S320)에 포함될 수 있다.

[0069] 단계(S410)에서 등급 결정부(120)는 단계(S310)에서 수신한 인증 요청이 일정 시간 전에 수신하였던 인증 요청의 재 수신인지 여부를 판별할 수 있다.

[0070] 단계(S420)에서 등급 결정부(120)는 단계(S410)에서 재 수신이 아닌 것으로 판별된 경우, 단계(S310)에서 인증 요청을 수신한 어플리케이션의 중요도를 기초로 사용자 인증에 사용할 인증 수단의 등급을 결정할 수 있다.

[0071] 단계(S430)에서 등급 결정부(120)는 단계(S410)에서 재 수신으로 판별된 경우, 전에 어플리케이션의 인증 요청을 수신한 시간과 단계(S310)에서 어플리케이션의 인증 요청을 재 수신한 시간 간의 간격 및 상기 어플리케이션의 중요도, 또는 어플리케이션의 인증 요청을 수신한 횟수를 기초로 인증 수단을 결정할 수 있다.

[0072] 단계(S440)에서 인증 수단 결정부(130)는 단계(S420), 또는 단계(S430)에서 결정한 등급으로 분류된 인증 수단 중 하나를 사용자 인증에 사용할 인증 수단으로 결정할 수 있다.

[0073] 도 5는 본 발명의 일실시예에 따른 사용자 인증 방법에서 인증 수단을 재결정하는 방법을 도시한 플로우차트이다. 이때, 도 5의 단계(S510) 내지 단계(S540)는 도 3에 도시된 단계(S350)에 포함될 수 있다.

[0074] 단계(S510)에서 등급 결정부(120)는 단계(S320)에서 결정된 인증 수단의 등급보다 상위 등급이 있는지 여부를 판별할 수 있다.

[0075] 단계(S520)에서 등급 결정부(120)는 단계(S510)에서 상위 등급이 있는 것으로 판별된 경우, 상기 어플리케이션의 등급을 상향할 수 있다.

[0076] 단계(S530)에서 인증 수단 결정부(130)는 단계(S520)에서 결정한 등급으로 분류된 인증 수단 중 하나를 사용자 인증에 사용할 인증 수단으로 결정할 수 있다.

[0077] 단계(S530)에서 인증 수단 결정부(130)는 단계(S510)에서 상위 등급이 없는 것으로 판별된 경우, 하드웨어를 사용한 인증 수단을 사용자 인증에 사용할 인증 수단으로 결정할 수 있다.

[0078] 도 6은 본 발명의 다른 실시예에 따른 다중 보안 설정에 기초한 사용자 인증 방법을 도시한 플로우차트이다.

[0079] 도 6은 인증 강도를 변경할 수 있는 하나의 인증 수단을 사용한 사용자 인증 방법을 도시한 것이다.

[0080] 단계(S610)에서 인증 요청 수신부(110)는 어플리케이션의 인증 요청을 수신할 수 있다.

[0081] 단계(S620)에서 인증 수단 결정부(140)는 단계(S310)에서 인증 요청을 수신한 어플리케이션의 중요도를 기초로 사용자 인증에 사용할 인증 강도를 결정할 수 있다. 구체적으로 등급 결정부(120)가 단계(S310)에서 인증 요청을 수신한 어플리케이션의 중요도를 기초로 사용자 인증에 사용할 인증 수단의 등급을 결정하면, 인증 수단 결정부(130)는 인증 수단의 인증 강도가 등급 결정부(120)가 결정한 등급에 대응하는 인증 강도가 되도록 인증 수단의 파라미터를 설정할 수 있다.

[0082] 단계(S630)에서 사용자 인증부(150)는 단계(S620)에서 파라미터가 설정되어 인증 강도가 결정된 인증 수단으로 사용자를 인증할 수 있다.

[0083] 단계(S640)에서 사용자 인증부(150)는 단계(S630)의 인증 결과가 실패인지 여부를 판별할 수 있다.

[0084] 인증 결과가 실패인 경우, 단계(S650)에서 인증 수단 결정부(140)는 인증 수단의 인증 강도를 다시 결정할 수 있다. 구체적으로 인증 수단 결정부(140)는 인증 강도가 높아지도록 인증 수단의 파라미터를 수정할 수 있다. 이때, 사용자 인증부(150)는 단계(S650)의 재 결정된 인증 강도에 따라 수정된 인증 수단으로 사용자를 인증할 수 있다.

[0085] 인증 결과가 성공인 경우, 단계(S660)에서 사용자 인증부(150)는 인스턴트 식별 정보를 사용자에게 제공할 수

있다.

[0086] 본 발명은 어플리케이션의 중요도와 사용 빈도에 따라 다른 인증 수단을 사용하여 인증을 수행함으로써, 보안성을 유지하면서도 자주 사용하는 어플리케이션은 보다 용이하게 인증할 수 있다. 또한, 어플리케이션을 실행한 후 재실행할 때까지의 시간 간격에 따라 인증 수단의 인증 강도를 변경시킴으로써 자주 사용하는 어플리케이션은 사용자 인증 방법이 점차 쉬워지도록 할 수 있다. 그리고, 인증을 실패한 경우, 인증 강도를 높임으로써 보안성을 높일 수 있다.

[0087] 또한, 일정 이상 인증을 실패한 경우, 모바일 기기를 락하고, 하드웨어를 사용하여 인증을 수행한 경우에 모바일 기기의 락을 해제함으로써, 모바일 단말기를 분실하거나 도난 당했을 때에도 무차별 대입 공격 등에 쉽게 개인정보가 노출되지 않도록 할 수 있다. 그리고, 기 설정된 PC와 음향, 또는 이미지를 사용하여 하드웨어 인증을 수행함으로써 사용자가 별도의 기기를 소지하지 않아도 하드웨어를 사용한 인증을 수행하여 모바일 단말기의 락을 해제할 수 있다.

[0088] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0089] 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0090] 110: 인증 요청 수신부

120: 등급 결정부

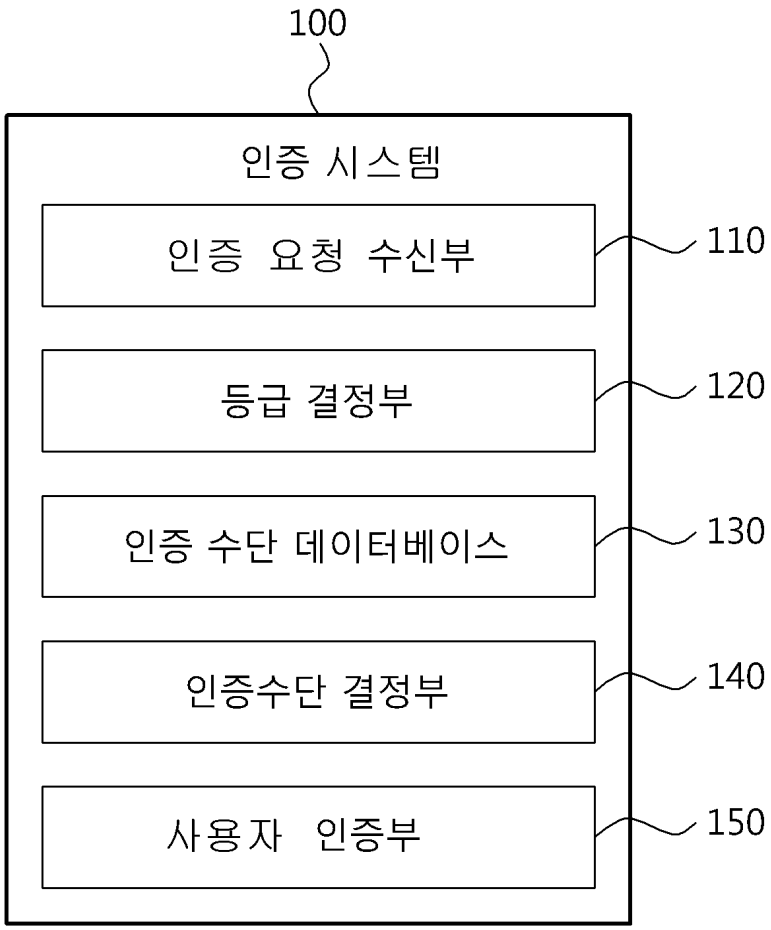
130: 인증 수단 데이터베이스

140: 인증 수단 결정부

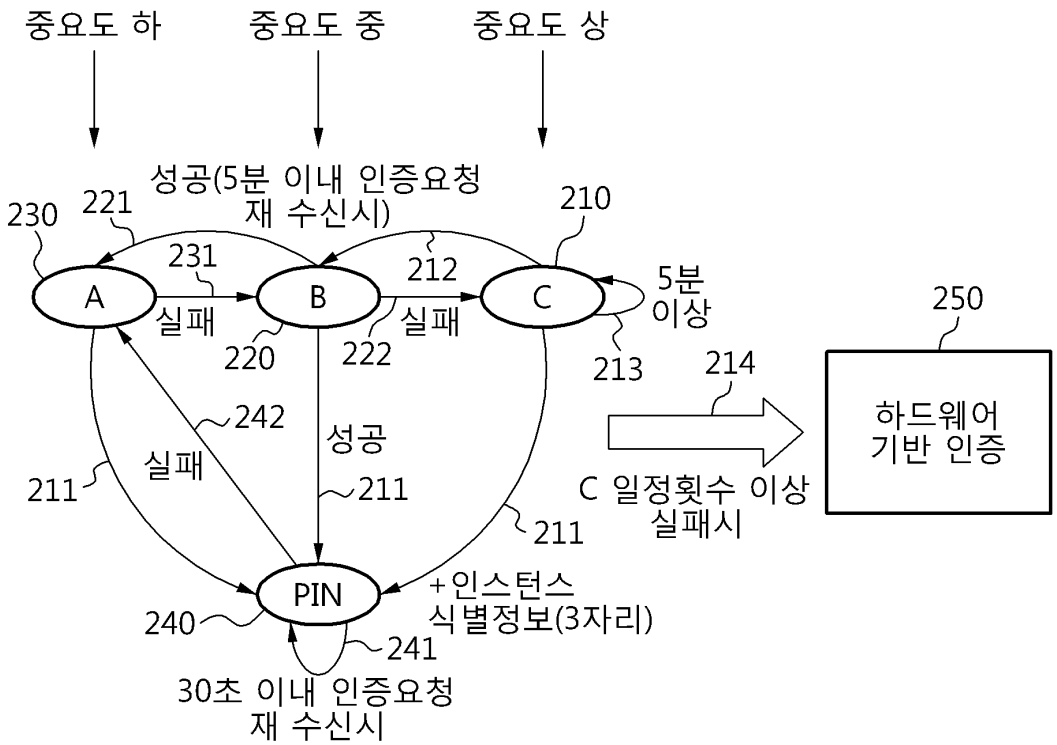
150: 사용자 인증부

도면

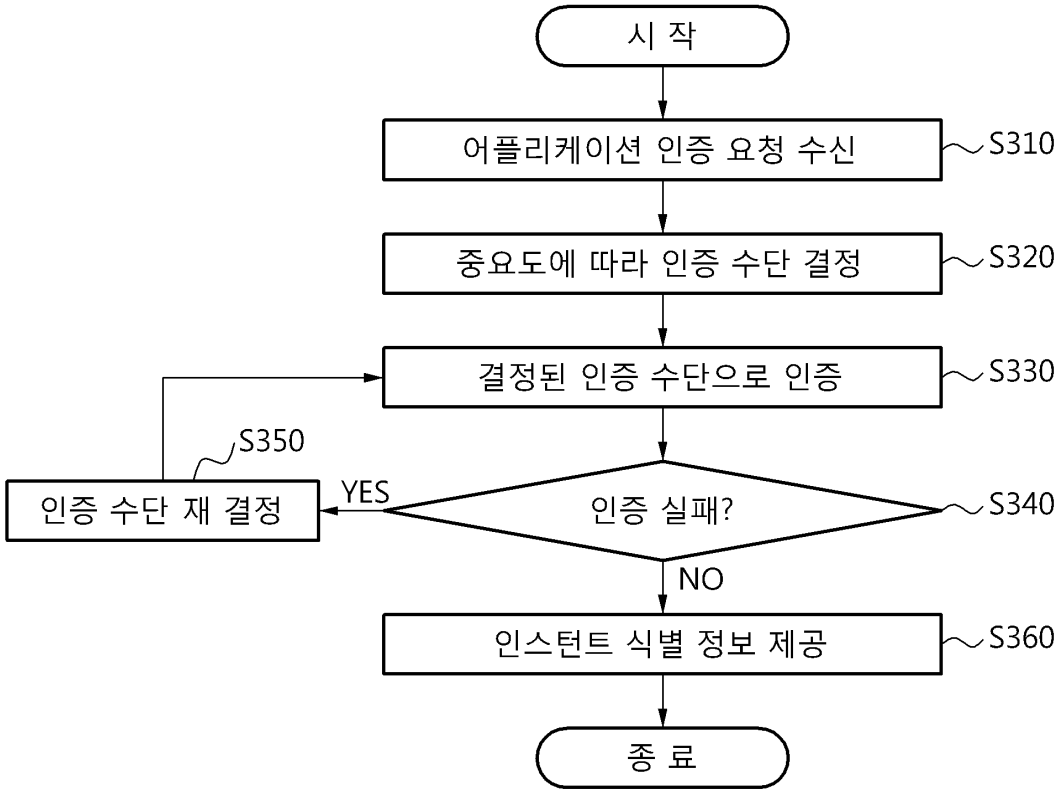
도면1


100
인증 시스템
인증 요청 수신부
110
등급 결정부
120
인증 수단 데이터베이스
130
인증수단 결정부
140
사용자 인증부
150

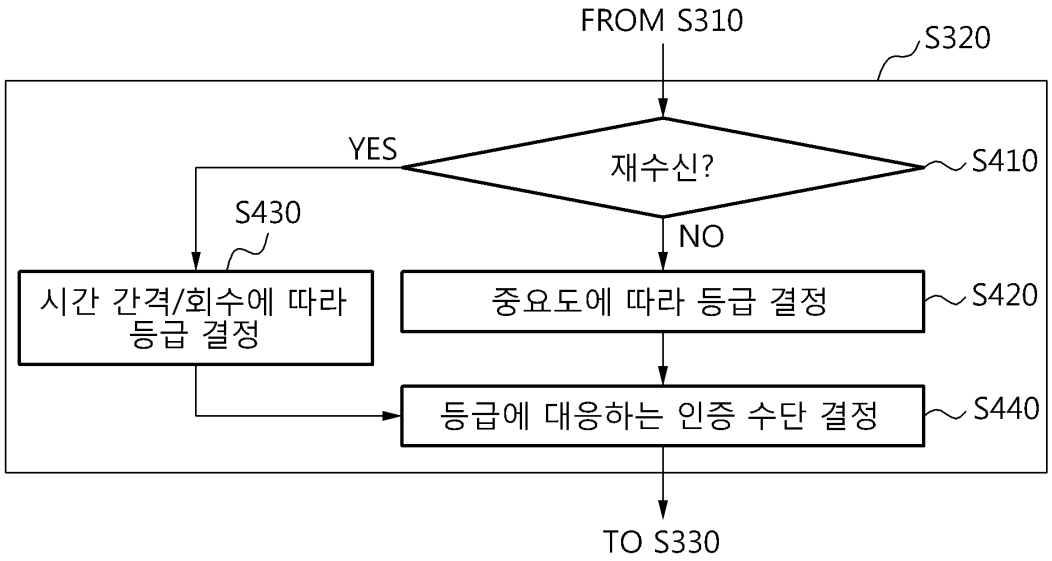
도면2


중요도 하
중요도 중
중요도 상
성공(5분 이내 인증요청
재 수신시)
230
221
210
231
212
A
B
C
5분
이상
실패
실패
220
222
213
214
250
하드웨어
기반 인증
242
성공
211
실패
211
211
C 일정횟수 이상
실패시
PIN
+인스턴스
식별정보(3자리)
240
241
30초 이내 인증요청
재 수신시

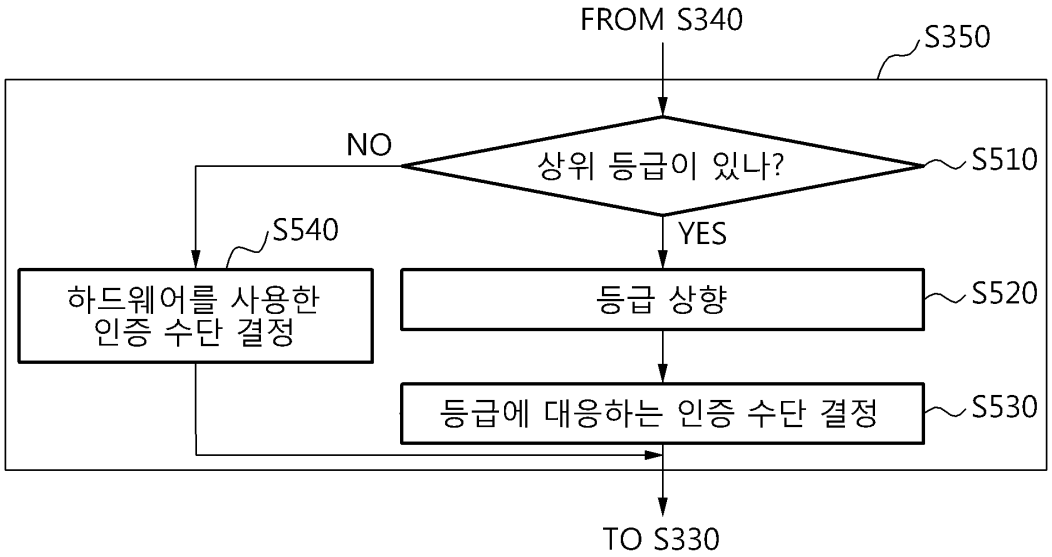
도면3


시 작
어플리케이션 인증 요청 수신
S310
중요도에 따라 인증 수단 결정
S320
결정된 인증 수단으로 인증
S330
S350
인증 수단 재 결정
YES
인증 실패?
S340
NO
인스턴트 식별 정보 제공
S360
종 료

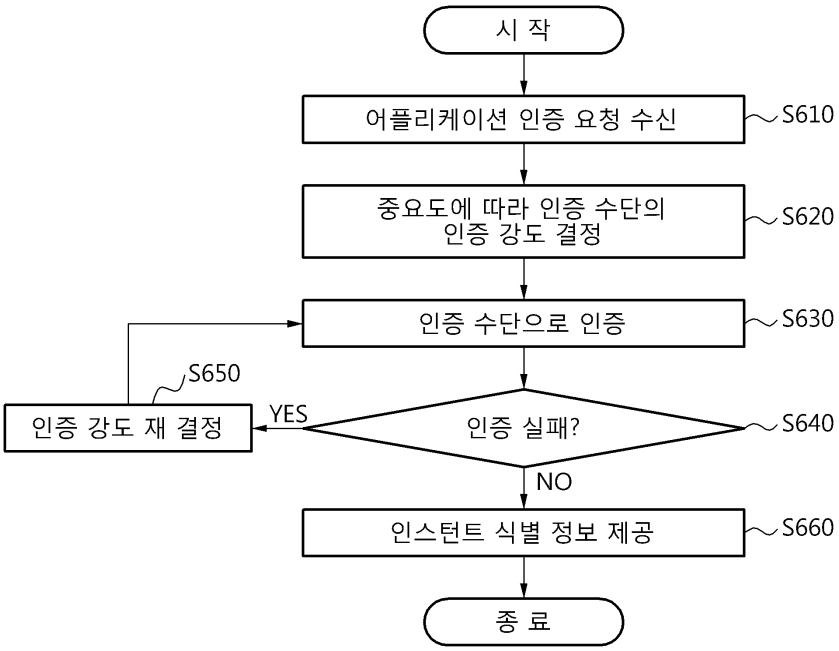
도면4


FROM S310
S320
YES
재수신?
S410
S430
NO
시간 간격/회수에 따라 등급 결정
중요도에 따라 등급 결정
S420
등급에 대응하는 인증 수단 결정
S440
TO S330

도면5


FROM S340
S350
NO
상위 등급이 있나?
S510
S540
YES
하드웨어를 사용한 인증 수단 결정
등급 상향
S520
등급에 대응하는 인증 수단 결정
S530
TO S330

도면6


시 작
어플리케이션 인증 요청 수신
S610
중요도에 따라 인증 수단의
인증 강도 결정
S620
인증 수단으로 인증
S630
S650
인증 강도 재 결정
YES
인증 실패?
S640
NO
인스턴트 식별 정보 제공
S660
종 료