(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0124448
(43) 공개일자 2013년11월14일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04W 12/06* (2009.01)
(21) 출원번호 10-2012-0095438(분할)
(22) 출원일자 2012년08월30일
심사청구일자 없음
(62) 원출원 특허 10-2012-0047793
원출원일자 2012년05월06일
심사청구일자 2012년05월06일

(71) 출원인
주식회사 씽크풀
서울특별시 영등포구 국제금융로 70, 미원빌딩 1106호 (여의도동)
(72) 발명자
김동진
서울특별시 서초구 서초중앙로 200, 12동 901호 (서초동, 삼풍아파트)
이왕근
서울특별시 영등포구 여의도동 한양아파트 H동 308호
(뒷면에 계속)
(74) 대리인
심충섭

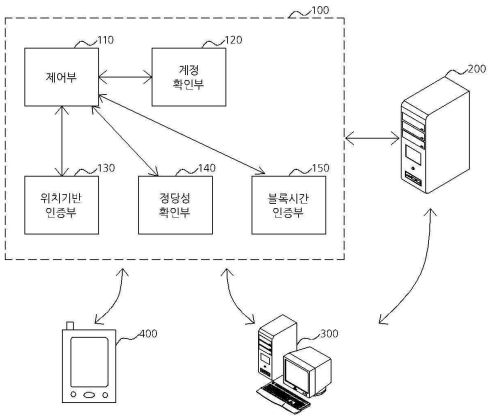
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 **정당성 확인 로그인 인증 시스템 및 그 방법**

(57) 요 약

정당성 확인 로그인 인증 시스템 및 그 방법이 개시된다. 상기 정당성 확인 로그인 인증 시스템은 사용자 단말기가 웹 서비스를 제공하는 웹 서버의 소정의 계정에 로그인 요청을 하는 경우, 상기 로그인 요청에 상응하는 계정 정보를 확인하기 위한 계정 확인부, 상기 로그인 요청에 상응하는 계정의 정당 사용자의 단말기로 소정의 확인신호를 전송하기 위한 정당성 확인부, 및 전송된 확인신호에 기초하여 상기 정당 사용자의 단말기로부터 응답신호가 수신되는지 여부에 기초하여 로그인된 상기 사용자 단말기의 로그인을 유지하거나 상기 사용자 단말기를 로그아웃 시키기 위한 제어부를 포함하며, 상기 제어부는 상기 웹 서버에 미리 저장된 로그인 정보에 기초한 로그인 정보 기반 인증이 성공한 모든 로그인 요청에 대해 로그인을 허락하며, 상기 정당성 확인부는 로그인이 허락된 계정에 상응하는 상기 정당 사용자의 단말기로 상기 확인신호를 전송하여 로그인이 허락된 모든 로그인 요청에 대해 정당성 확인절차를 수행하는 것을 특징으로 한다.

대 표 도 - 도1



(72) 발명자

이항기

서울특별시 구로구 신도림동 e편한세상대림5차아파트 706동 201호

허선주

서울특별시 중구 신당2동 432-457

심충섭

서울특별시 용산구 효창원로15길 16, 102동 307호 (신창동, 세방리버하이빌)

특허청구의 범위

청구항 1

사용자 단말기가 웹 서비스를 제공하는 웹 서버의 소정의 계정에 로그인 요청을 하는 경우, 상기 로그인 요청에 상응하는 계정정보를 확인하기 위한 계정 확인부;

상기 로그인 요청에 상응하는 계정의 정당 사용자의 단말기로 소정의 확인신호를 전송하기 위한 정당성 확인부; 및

전송된 확인신호에 기초하여 상기 정당 사용자의 단말기로부터 응답신호가 수신되는지 여부에 기초하여 로그인된 상기 사용자 단말기의 로그인을 유지하거나 상기 사용자 단말기를 로그아웃 시키기 위한 제어부를 포함하며,

상기 제어부는,

상기 웹 서버에 미리 저장된 로그인 정보에 기초한 로그인 정보 기반 인증이 성공한 모든 로그인 요청에 대해 로그인을 허락하며,

상기 정당성 확인부는,

로그인이 허락된 계정에 상응하는 상기 정당 사용자의 단말기로 상기 확인신호를 전송하여 로그인이 허락된 모든 로그인 요청에 대해 정당성 확인절차를 수행하는 것을 특징으로 하는 정당성 확인 로그인 인증 시스템.

청구항 2

제 1항에 있어서, 상기 정당성 확인 로그인 인증 시스템은,

소정의 블록 시간 정보를 저장하고, 상기 블록 시간 동안에 요청되는 로그인 요청에 대해서는 상기 로그인 정보 기반 인증과는 별개의 추가인증을 로그인을 요청한 단말기로 요청하기 위한 블록 시간 인증부를 더 포함하며,

상기 제어부는,

상기 블록 시간 인증부에 의해 요청된 상기 추가인증이 성공하여야만 상기 블록 시간 동안에 요청된 상기 로그인 요청을 허용하는 정당성 확인 로그인 인증 시스템.

청구항 3

제 1항에 있어서, 상기 정당 사용자의 단말기는,

상기 웹 서버에 상응하는 애플리케이션을 통해 상기 블록 시간 정보를 입력받으며,

입력받은 상기 블록 시간 정보를 상기 정당성 확인 로그인 인증 시스템에 포함되는 블록 시간 인증부로 전송하는 정당성 확인 로그인 인증 시스템.

청구항 4

제 2항에 있어서, 상기 블록 시간 인증부는,

로그인된 상기 사용자 단말기로부터 로그아웃 요청이 있는 경우 블록 설정 여부를 확인하는 정보를 상기 사용자 단말기로 전송하고, 상기 사용자 단말기에 의해 블록 설정 요청이 수신되는 경우 상기 사용자 단말기가 로그 아웃이 된 시점부터 상기 블록이 시작되도록 설정하는 것을 특징으로 하는 정당성 확인 로그인 인증 시스템.

청구항 5

정당성 확인 로그인 인증 방법에 있어서,

정당성 확인 로그인 인증 시스템이 사용자 단말기가 웹 서비스를 제공하는 웹 서버의 소정의 계정에 로그인 요청을 하는 경우, 상기 로그인 요청에 상응하는 계정정보를 확인하는 단계;

상기 정당성 확인 로그인 인증 시스템이 상기 정당 사용자의 단말기로 소정의 확인신호를 전송하는 단계; 및

상기 정당성 확인 로그인 인증 시스템이 전송된 확인신호에 기초하여 상기 정당 사용자의 단말기로부터 응답신호가 수신되는지 여부에 기초하여 로그인된 상기 사용자 단말기의 로그인을 유지하거나 상기 사용자 단말기를 로그아웃 시키는 로그인 제어를 수행하는 단계를 포함하며,

상기 정당성 확인 로그인 인증 방법은,

상기 웹 서버에 미리 저장된 로그인 정보에 기초한 로그인 정보 기반 인증이 성공한 모든 로그인 요청에 대해 로그인을 허락한 후, 로그인이 허락된 계정에 상응하는 상기 정당 사용자의 단말기로 상기 확인신호를 전송하여 로그인이 허락된 모든 로그인 요청에 대해 정당성 확인절차를 수행하는 것을 특징으로 하는 정당성 확인 로그인 인증 방법.

청구항 6

제 5항에 있어서, 상기 정당성 확인 로그인 인증 방법은,

상기 정당성 확인 로그인 인증 시스템이 계정별로 소정의 블록 시간 정보를 저장하는 단계;

상기 정당성 확인 로그인 인증 시스템이 상기 블록 시간 동안에 요청되는 로그인 요청에 대해서는 상기 로그인 정보 기반 인증과는 별개의 추가인증을 로그인을 요청한 단말기로 요청하는 단계; 및

상기 정당성 확인 로그인 인증 시스템이 요청된 상기 추가인증이 성공하여야만 상기 블록 시간 동안에 요청된 상기 로그인 요청을 허용하는 단계를 더 포함하는 정당성 확인 로그인 인증 방법.

청구항 7

제 5항 또는 제 6항 중 어느 한 항에 기재된 방법을 수행하기 위한 프로그램을 기록한 컴퓨터 판독 가능한 기록매체.

명 세 서

기 술 분 야

[0001] 본 발명은 정당성 확인 로그인 인증 시스템 및 그 방법에 관한 것으로, 보다 상세하게는 로그인 정보 기반의 인증 및/또는 위치기반의 로그인 인증을 수행할 수 있고 이러한 인증이 수행되었을 때의 인증결과를 정당 사용자가 원격에서 확인할 수 있는 시스템 및 이로 인해 발생할 수 있는 문제점을 해결할 수 있는 시스템 및 그 방법에 관한 것이다.

배 경 기 술

[0002] 인터넷의 발달과 함께 많은 사람이 웹 사이트 또는 특정 웹 서비스(예컨대, 인스턴트 메신저 등)를 위한 소정의 애플리케이션 등에 접속하여 다양한 서비스를 제공받고 있다. 이때 웹 사이트, 웹 서비스, 또는 웹 애플리케이션은 사용자를 식별하기 위해 로그인(log-in)이라는 절차를 수행하곤 한다. 로그인을 하기 위해서는 사용자는 사용자별로 할당된 계정(account)에 맞는 로그인 정보(예컨대, 아이디, 패스워드 등)를 입력하여야 한다.

[0003] 하지만, 이러한 로그인 정보에 기반한 인증은 로그인 정보가 유출되는 경우에는 그 인증기능이 유명무실하게 되는데, 최근에 다양하고 지능적인 사이버 공격에 의해 사용자들의 로그인 정보가 유출되는 사고가 발생하고 있어

로그인 정보에 기반한 인증방법의 안정성이 크게 위협받고 있다.

[0004] 본 출원인은 이러한 문제점을 해결하기 위해 위치기반의 인증을 통해 본인인증을 수행할 수 있는 다양한 기술적 사상을 제공한바 있다. 예컨대, 한국특허출원(출원번호 10-2009-0125293, "로그인 제어 시스템 및 그 방법"), 한국특허출원(출원번호 10-2010-0007524, "서비스 보안시스템 및 그 방법"), 한국특허출원(출원번호 10-2010-0124252, "위치기반의 서비스 보안 시스템 및 그 방법") 등이 그러한 일 예들이다.

[0005] 위치기반의 인증은 기본적으로 로그인이 요청되는 위치와 요청된 로그인의 계정에 상응하는 정당 사용자의 위치를 비교함으로써 인증을 수행하는 방식을 의미할 수 있다. 위치기반의 인증을 수행하는 경우에는 로그인 정보에 기반한 인증이 성공한 경우라도 정당 사용자의 위치와 동일성이 있는 위치에서 로그인 요청을 수행하지 않는 한 위치기반의 인증을 성공할 수 없으므로, 로그인 정보가 유출되는 경우에도 안전하게 정당 사용자의 계정을 보호할 수 있는 해결책을 제공해줄 수 있다.

[0006] 한편, 이러한 위치기반의 인증 및/또는 로그인 정보 기반의 인증을 수행하는 경우에 실제로 로그인을 제어하는 방식은 크게 두 가지가 존재할 수 있다. 먼저, 인증이 실패하는 경우에는 로그인을 아예 시켜주지 않는 로그인 거부 방식이 존재할 수 있다. 이처럼 로그인 거부 방식의 경우는 전통적으로 로그인 정보 기반의 가장 기본적인 인증에 많이 사용되어 왔다.

[0007] 또 다른 인증방식은 인증의 성공 또는 실패와 무관하게 일단 로그인을 허용한 후, 정당 사용자에 의해 해당 로그인을 유지시킬지 여부를 판단토록 하는 정당 사용자에 의한 정당성 판단 방식이 존재할 수 있는데, 이러한 경우를 본 명세서에서는 정당성 확인 방식이라고 정의하기로 한다.

[0008] 예컨대, 정당성 확인방식은 인증이 실패하거나 성공한 로그인에 대해 정당 사용자에게 확인신호 또는 메시지를 전송하고, 이에 응답하여 정당 사용자가 상기 로그인을 로그아웃 시키라는 응답이 오면 해당 로그인을 강제로 로그아웃 시키는 방식일 수 있다.

[0009] 정당성 확인방식을 통한 로그인 제어의 경우에는 정당 사용자가 본인이 로그인을 하는 경우에는 상기의 확인신호가 정당 사용자에게 가지 않거나 가더라도 응답을 하지 않을 수 있고, 타인이 로그인을 하는 경우에도 자신이 허락한 로그인인 경우에는 응답을 하지 않음으로써 로그인을 유지시킬 수 있다. 반면, 자신이 알지 못하는 로그인이 발생한 경우에는 응답을 통해 강제로 로그아웃을 시킴으로써 자신의 계정을 보호할 수 있게 된다. 또한, 정당성 확인방식은 인증이 성공한 로그인 요청에 대해서도 수행될 수 있는데, 웹 서버에 의해 인증이 성공하더라도 정당 사용자에 의해 별도로 로그인 요청의 정당성을 확인받는 절차는 매우 유용한 절차일 수 있기 때문이다.

[0010] 하지만, 이러한 정당성 확인방식의 경우 의외의 문제점이 발생할 수 있다. 예컨대, 정당 사용자가 자고 있는 경우나 자고 있지 않더라도 응답을 하기 곤란한 경우가 존재할 수 있는데, 이러한 경우에는 인증이 실패한 로그인 요청에 대해서 로그인을 일단 허용한 후에도 로그아웃을 시킬 수 없는 문제점이 존재할 수 있다.

발명의 내용

해결하려는 과제

[0011] 따라서, 본 발명이 이루고자 하는 기술적인 과제는 정당성 확인방식을 이용한 로그인 제어를 수행할 때 발생할 수 있는 문제점 즉, 정당 사용자가 응답을 할 수 없는 경우의 문제점을 개선할 수 있는 시스테 및 그 방법을 제공하는 것이다.

과제의 해결 수단

[0012] 상기 기술적 과제를 해결하기 위한 정당성 확인 로그인 인증 시스템은 사용자 단말기가 웹 서비스를 제공하는 웹 서버의 소정의 계정에 로그인 요청을 하는 경우, 상기 로그인 요청에 상응하는 계정정보를 확인하기 위한 계정 확인부, 상기 사용자 단말기의 위치와 상기 로그인 요청에 상응하는 계정의 정당 사용자의 위치에 기반한 위치기반 인증을 수행하기 위한 위치기반 인증부, 상기 정당 사용자의 단말기로 소정의 확인신호를 전송하기 위한 정당성 확인부, 및 전송된 확인신호에 기초하여 상기 정당 사용자의 단말기로부터 응답신호가 수신되는지 여부에 기초하여 로그인된 상기 사용자 단말기의 로그인을 유지하거나 상기 사용자 단말기를 로그아웃 시키기 위한

제어부를 포함하며, 상기 제어부는 상기 정당 사용자에 의해 설정되며 블록 시간을 특정할 수 있는 블록 시간 정보에 상응하는 블록 시간 동안에 요청된 로그인 요청에 대해서는, 상기 웹 서버에 미리 저장된 로그인 정보에 기초한 로그인 정보 인증 및 상기 위치기반 인증이 성공할 수 있는 로그인 요청에 대해서도, 로그인을 허용하지 않는다.

[0013] 상기 정당성 확인 로그인 인증 시스템은 상기 블록 시간 정보를 저장하고, 상기 블록 시간 동안에 요청되는 로그인 요청에 대해서는 상기 로그인 정보 인증 및 상기 위치기반 인증과는 별개의 추가인증을 로그인을 요청한 단말기로 요청하기 위한 블록 시간 인증부를 더 포함하며, 상기 제어부는 상기 블록 시간 인증부에 의해 요청된 상기 추가인증이 성공하여야만 상기 블록 시간 동안에 요청된 상기 로그인 요청을 허용할 수 있다.

[0014] 상기 정당 사용자의 단말기는 상기 웹 서버에 상응하는 애플리케이션을 통해 상기 블록 시간 정보를 입력받으며, 입력받은 상기 블록 시간 정보를 상기 정당성 확인 로그인 인증 시스템에 포함되는 블록 시간 인증부로 전송할 수 있다.

[0015] 상기 애플리케이션이 제공하는 소정의 UI가 선택되면 선택된 시점부터 상기 블록 시간이 시작되는 것을 특징으로 할 수 있다.

[0016] 상기 블록 시간 인증부는 로그인된 상기 사용자 단말기로부터 로그아웃 요청이 있는 경우 블록 설정 여부를 확인하는 정보를 상기 사용자 단말기로 전송하고, 상기 사용자 단말기에 의해 블록 설정 요청이 수신되는 경우 상기 사용자 단말기가 로그 아웃이 된 시점부터 상기 블록이 시작되도록 설정하는 것을 특징으로 할 수 있다.

[0017] 상기 정당성 확인부는 선택적으로 설정된 확인설정 정보에 기초하여, 상기 위치기반 인증이 실패한 경우에만 상기 정당 사용자의 단말기로 확인신호를 전송하거나 또는 상기 계정으로 로그인이 요청될 때마다 상기 확인신호를 전송하는 것을 특징으로 할 수 있다.

[0018] 상기 위치기반 인증부는 상기 사용자 단말기의 IP 주소를 확인하고, IP 주소별 위치정보에 기초하여 확인된 IP 주소에 상응하는 상기 사용자 단말기의 위치를 확인하기 위한 단말기 위치 판단 모듈 및 상기 서비스 요청에 상응하는 정당 사용자의 위치를 판단하기 위한 사용자 위치 판단 모듈을 포함하며, 상기 단말기 위치 판단 모듈이 판단한 제1위치와 상기 사용자 위치 판단 모듈이 판단한 제2위치를 비교하고, 비교결과에 기초하여 상기 위치기반 인증을 수행할 수 있다.

[0019] 상기 단말기 위치 판단 모듈은 IP 주소별로 위치정보를 저장하는 IP 주소별 위치정보 DB로부터 상기 제1위치를 확인하며, 상기 IP주소별 위치정보 DB는 소정의 단말기가 소정의 IP와 소정의 사용자 식별자를 이용하여 소정의 네트워크 시스템에 정당 접속한 경우, 상기 사용자 식별자에 대응되는 정당 사용자의 모바일 폰의 위치에 기초하여 IP별로 위치정보를 저장하는 것을 특징으로 할 수 있다.

[0020] 상기 정당성 확인부는 상기 확인신호를 메시지로 상기 정당 사용자의 단말기에 전송하도록 제어하거나, 상기 확인신호를 상기 웹 서버에 상응하며 상기 정당 사용자의 단말기에 설치된 애플리케이션으로 전송할 수 있다.

[0021] 상기 기술적 과제를 해결하기 위한 정당성 확인 로그인 인증 시스템은 사용자 단말기가 웹 서비스를 제공하는 웹 서버의 소정의 계정에 로그인 요청을 하는 경우, 상기 로그인 요청에 상응하는 계정정보를 확인하기 위한 계정 확인부, 상기 정당 사용자의 단말기로 소정의 확인신호를 전송하기 위한 정당성 확인부, 및 전송된 확인신호에 기초하여 상기 정당 사용자의 단말기로부터 응답신호가 수신되는지 여부에 기초하여 로그인된 상기 사용자 단말기의 로그인을 유지하거나 상기 사용자 단말기를 로그아웃 시키기 위한 제어부를 포함하며, 상기 정당성 확인부는 상기 로그인 요청에 상응하는 계정으로 로그인이 요청될 때마다 상기 확인신호를 전송하며, 상기 제어부는 상기 정당 사용자에 의해 설정된 블록 시간 정보를 저장하며, 상기 블록 시간 정보에 상응하는 블록 시간 동안에 요청된 로그인 요청에 대해서는, 상기 웹 서버에 미리 저장된 로그인 정보에 기초한 로그인 정보가 성공할 수 있는 로그인 요청에 대해서도, 로그인을 허용하지 않는다.

[0022] 상기 기술적 과제를 해결하기 위한 정당성 확인 로그인 인증 시스템은 사용자 단말기가 웹 서비스를 제공하는 웹 서버의 소정의 계정에 로그인 요청을 하는 경우, 상기 로그인 요청에 상응하는 계정정보를 확인하기 위한 계정 확인부, 상기 사용자 단말기의 위치와 상기 로그인 요청에 상응하는 계정의 정당 사용자의 위치에 기반한 위치기반 인증을 수행하기 위한 위치기반 인증부, 상기 정당 사용자의 단말기로 소정의 확인신호를 전송하기 위한 정당성 확인부, 및 전송된 확인신호에 기초하여 상기 정당 사용자의 단말기로부터 응답신호가 수신되는지 여부에 기초하여 로그인된 상기 사용자 단말기의 로그인을 유지하거나 상기 사용자 단말기를 로그아웃 시키기 위한 제어부를 포함하며, 상기 정당 사용자의 단말기는 상기 웹 서버에 상응하는 애플리케이션을 통해 블록 시간 정보를 입력받으며, 상기 애플리케이션은 입력된 상기 블록 시간 정보에 상응하는 블록 시간 동안에는 상기 확인

신호가 수신되면 자동으로 상기 응답신호를 전송할 수 있다.

[0023] 상기 기술적 과제를 해결하기 위한 정당성 확인 로그인 인증 방법은 정당성 확인 로그인 인증 시스템이 사용자 단말기가 웹 서비스를 제공하는 웹 서버의 소정의 계정에 로그인 요청을 하는 경우, 상기 로그인 요청에 상응하는 계정정보를 확인하는 단계, 상기 정당성 확인 로그인 인증 시스템이 상기 정당 사용자의 단말기로 소정의 확인신호를 전송하는 단계, 및 상기 정당성 확인 로그인 인증 시스템이 전송된 확인신호에 기초하여 상기 정당 사용자의 단말기로부터 응답신호가 수신되는지 여부에 기초하여 로그인된 상기 사용자 단말기의 로그인을 유지하거나 상기 사용자 단말기를 로그아웃 시키는 로그인 제어를 수행하는 단계를 포함하며, 상기 정당성 확인 로그인 인증 방법은 상기 정당성 확인 로그인 인증 시스템이 상기 정당 사용자에 의해 설정되며 블록 시간을 특정할 수 있는 블록 시간 정보에 상응하는 블록 시간 동안에 요청된 로그인 요청에 대해서는, 상기 웹 서버에 미리 저장된 로그인 정보에 기초한 로그인 정보 인증 및 상기 위치기반 인증이 성공할 수 있는 로그인 요청에 대해서도, 로그인을 허용하지 않는 단계를 더 포함한다.

[0024] 상기 정당성 확인 로그인 인증 시스템이 상기 정당 사용자의 단말기로 소정의 확인신호를 전송하는 단계는 상기 정당성 확인 로그인 인증 시스템이 선택적으로 설정된 확인설정 정보에 기초하여, 상기 위치기반 인증이 실패한 경우에만 상기 정당 사용자의 단말기로 확인신호를 전송하거나 또는 상기 계정으로 로그인이 요청될 때마다 상기 확인신호를 전송하는 단계를 포함할 수 있다.

[0025] 상기 기술적 과제를 해결하기 위한 정당성 확인 로그인 인증 방법은 정당성 확인 로그인 인증 시스템이 사용자 단말기가 웹 서비스를 제공하는 웹 서버의 소정의 계정에 로그인 요청을 하는 경우, 상기 로그인 요청에 상응하는 계정정보를 확인하는 단계, 상기 정당성 확인 로그인 인증 시스템이 상기 사용자 단말기의 위치와 상기 로그인 요청에 상응하는 계정의 정당 사용자의 위치에 기반한 위치기반 인증 또는 로그인 정보에 기반한 로그인 인증 중 적어도 하나를 수행하는 단계, 및 상기 정당성 확인 로그인 인증 시스템이 상기 정당 사용자의 단말기로 소정의 확인신호를 전송하고, 전송된 확인신호에 기초하여 상기 정당 사용자의 단말기로부터 응답신호가 수신되는지 여부에 기초하여 로그인된 상기 사용자 단말기의 로그인을 유지하거나 상기 사용자 단말기를 로그아웃 시키기 위한 로그인 제어를 수행하는 단계를 포함하며, 상기 정당 사용자의 단말기는 상기 웹 서버에 상응하는 애플리케이션을 통해 블록 시간 정보를 입력받으며, 상기 애플리케이션은 입력된 상기 블록 시간 정보에 상응하는 블록 시간 동안에는 상기 확인신호가 수신되면 자동으로 상기 응답신호를 전송할 수 있다.

[0026] 상기 기술적 과제를 해결하기 위한 정당성 확인 로그인 인증 방법은 프로그램을 기록한 컴퓨터 판독 가능한 기록매체에 저장될 수 있다.

발명의 효과

[0027] 따라서, 본 발명의 기술적 사상에 따르면 사용자가 자신이 정당성 확인에 대한 응답을 하지 못할 상황(예컨대, 취침 등)에 처할 경우에는 사용자가 원하는 시간 동안 아예 로그인을 차단할 수 있도록 함으로써, 정당성 확인 방식에 의한 로그인 제어의 취약점을 개선할 수 있는 효과가 있다.

[0028] 또한, 로그인이 차단된 상태에서도 정당 사용자는 소정의 추가 인증(예컨대, 공인인증서 또는 OTP 등)을 통해 로그인을 하거나, 로그인 차단을 해제할 수 있음으로써 정당 사용자 본인의 로그인 사용은 보장할 수 있는 효과가 있다.

[0029] 또한, 정당 사용자가 본인이 일정 기간 동안 로그인을 할 계획인 없는 경우에는 선택적으로 로그인을 차단시키거나 응답을 자동으로 발송할 수 있도록 함으로써 정당성 확인방식에 의한 로그인 제어의 취약점을 개선할 수 있는 효과가 있다. 또한, 이러한 경우에는 본인이 로그인을 하고자 할 때 추가인증을 할 필요가 없게 되는 효과가 있다.

[0030] 또한, 특별히 높은 보안성을 요구하는 시스템 또는 서비스의 경우에는 로그인 정보 기반의 인증이 성공한 모든 로그인에 대해서도 정당성 확인을 수행할 수 있도록 하고, 이때에도 정당성 확인 방식의 취약점을 개선하도록 함으로써 보안성이 높은 서비스를 제공할 수 있는 효과가 있다.

도면의 간단한 설명

[0031] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 간단한 설명이 제공된다.

도 1은 본 발명의 실시 예에 따른 정당성 확인 로그인 인증 방법을 구현하기 위한 개략적인 시스템 구성을 나타낸다.

도 2는 본 발명의 실시 예에 따른 정당성 확인 로그인 인증 시스템에 포함된 위치기반 인증부의 개략적인 구성을 나타낸다.

도 3은 본 발명의 실시 예에 따른 정당성 확인 로그인 인증 방법에서 블록 시간을 설정할 수 있는 방법을 개략적으로 설명하기 위한 도면이다.

도 4는 본 발명의 실시 예에 따른 정당성 확인 로그인 인증 방법에서 정당 사용자가 로그아웃을 수행하면서 블록설정을 할 수 있는 방법을 설명하기 위한 도면이다.

도 5는 본 발명의 실시 예에 따른 정당성 확인 로그인 인증 방법에서 추가인증을 통해 정당 사용자가 로그인을 수행할 수 있는 방법을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0032] 본 발명과 본 발명의 동작상의 이점 및 본 발명의 실시에 의하여 달성되는 목적을 충분히 이해하기 위해서는 본 발명의 바람직한 실시 예를 예시하는 첨부 도면 및 첨부 도면에 기재된 내용을 참조하여야만 한다.

[0033] 또한, 본 명세서에 있어서는 어느 하나의 구성요소가 다른 구성요소로 데이터를 '전송'하는 경우에는 상기 구성요소는 상기 다른 구성요소로 직접 상기 데이터를 전송할 수도 있고, 적어도 하나의 또 다른 구성요소를 통하여 상기 데이터를 상기 다른 구성요소로 전송할 수도 있는 것을 의미한다.

[0034] 반대로 어느 하나의 구성요소가 다른 구성요소로 데이터를 '직접 전송'하는 경우에는 상기 구성요소에서 다른 구성요소를 통하지 않고 상기 다른 구성요소로 상기 데이터가 전송되는 것을 의미한다.

[0035] 이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시 예를 설명함으로써, 본 발명을 상세히 설명한다. 각 도면에 제시된 동일한 참조부호는 동일한 부재를 나타낸다.

[0036] 우선, 본 발명의 기술적 사상은 정당성 확인방식 즉, 정당 사용자에게 로그인이 본인에 의한(또는 본인이 허락한) 로그인인지 여부를 확인하고 이를 제어할 수 있도록 하는 방식을 통한 로그인 제어에 유용한 효과가 있다.

[0037] 또한, 정당성 확인방식은 본 발명의 기술적 사상에서와 같이 기본적인 로그인 정보 기반의 인증과 함께 별도 인증(예컨대, 위치기반의 인증)이 수행될 때 유용할 수 있다. 즉, 로그인 정보 기반의 인증이 성공된 로그인 요청이 상기 별도 인증은 성공하지 못한 경우에, 상술한 바와 같이 로그인 거부 방식을 이용할 수도 있고 정당성 확인 방식을 이용할 수도 있는데, 이러한 경우에는 정당성 확인 방식이 더 유용할 수 있다.

[0038] 이처럼 로그인 거부 방식을 이용하지 않고 정당성 확인방식을 이용하는 이유로는 첫째, 웹 사이트 또는 웹 애플리케이션을 제공하는 기존의 대부분의 웹 서버들이 기본적으로 로그인 기반의 인증을 성공하면 로그인을 허용하도록 설계되어 있기 때문에, 위치기반의 인증과 같이 별도 인증기능을 추가하고 추가된 별도 인증의 성공 여부에 따라 로그인 허용 여부를 결정하기 위해서는 상당한 정도의 시스템 변경이 요구될 수 있다.

[0039] 둘째, 특히 위치기반의 인증과 같이, 특정 정보를 요청하는 공인인증서나 OTP 방식 등과 달리, 사실 상태에 기반한 인증이 별도의 인증방식으로 사용되는 경우에는 사용자가 인증에 참여하는 과정(예컨대, 공인인증서의 선택, 비밀번호 등의 입력 등)이 전혀 없이 바로 인증이 수행되어서, 사용자가 직접 참여하지도 않은 인증절차에 의해 로그인이 거부되는 경우에 느낄 수 있는 불쾌감이 클 수 있는 문제점이 존재할 수 있다.

[0040] 셋째, 사실 상태에 기반한 인증의 경우에는 사실 상태의 파악에 오류가 발생할 수 있는 위험이 존재할 수 있으며, 특히 위치기반의 인증에서는 로그인이 요청된 위치 및/또는 정당 사용자의 위치 파악에 일정한 오차 또는 오류가 발생할 가능성이 있다. 따라서, 실제로 정당 사용자임에도 불구하고 인증이 실패할 수 있는 위험이 있는데, 정당 사용자임에도 인증이 성공되지 않는 경우가 발생한 경우, 로그인을 거부하게 되면 서비스의 완성도나 사용자가 느끼는 서비스 신뢰도에 악영향을 미치게 될 수 있다. 따라서 기본적인 로그인 정보 기반의 인증이 성공된 경우에는 별도의 인증이 실패하더라도 일단은 로그인을 허용한 후 정당 사용자가 자신이 로그인을 한 것이 아니라면 강제로 로그아웃을 시킬 수 있도록 시스템 또는 서비스를 설계하는 것이 보다 안정적이고 신뢰성이 높을 수 있다.

[0041] 넷째, 로그인 거부 방식을 채택하게 되는 경우에는, 로그인 정보 기반의 인증과 함께 위치기반의 인증이 수행되

는 경우에는 로그인 정보 기반의 인증이 성공되는지 판단된 후에 위치기반의 인증이 성공하는지 여부까지 기다린 후 로그인을 허용하거나 거부하게 되는 문제점이 발생한다. 특히, 위치기반의 인증이 성공하지 못할 경우(예컨대, 부정 사용자에 의한 로그인)가 위치기반의 인증이 성공할 경우(예컨대, 정당 사용자에 의한 로그인)보다 수적으로 현저하게 적음에도 불구하고, 모든 케이스의 로그인 인증의 시간을 일률적으로 늦추는 것은 매우 비효율적인 서비스 설계방식일 수 있다.

[0042] 따라서, 이하에서는 이처럼 정당성 확인 방식에서 유용할 수 있는 본 발명의 기술적 사상을 보다 구체적으로 설명하도록 한다.

[0043] 도 1은 본 발명의 실시 예에 따른 정당성 확인 로그인 인증 방법을 구현하기 위한 개략적인 시스템 구성을 나타낸다.

[0044] 도 1을 참조하면, 본 발명의 실시 예에 따른 정당성 확인 로그인 인증 시스템(100)은 소정의 웹 사이트 또는 웹 애플리케이션을 제공하는 웹 서버(200)와 유무선 네트워크를 통해 연결될 수 있다. 또한, 상기 정당성 확인 로그인 인증 시스템(100)은 필요한 경우 사용자 단말기(300)와 유무선 네트워크를 통해 통신을 수행할 수도 있다. 또한, 상기 정당성 확인 로그인 인증 시스템(100)은 정당 사용자의 단말기(400)와 유무선 네트워크를 통해 통신을 수행할 수도 있다.

[0045] 상기 정당성 확인 로그인 인증 시스템(100)은 상기 웹 서버(200)에 포함되도록 설치되거나, 상기 웹 서버(200)와는 별도의 물리적 장치로 구현되되 상기 웹 서버(200)와 유기적으로 결합하여 본 발명의 기술적 사상을 구현할 수 있다. 물론, 상기 정당성 확인 로그인 인증 시스템(100)이 상기 웹 서버(200)와 별도의 물리적 장치로 구현되는 경우에는, 상기 웹 서버(200)에는 상기 정당성 확인 로그인 인증 시스템(100)과 소정의 데이터를 송수신하면서 본 발명의 기술적 사상을 구현하기 위한 소정의 소프트웨어가 설치될 수도 있다. 또한, 다른 구현 예에 의하면, 상기 정당성 확인 로그인 인증 시스템(100)에 포함된 일부의 구성 또는 기능은 상기 웹 서버(200)에 설치 또는 수행되고, 나머지 구성 또는 기능은 상기 정당성 확인 로그인 인증 시스템(100)에 포함 또는 수행될 수도 있다.

[0046] 한편, 상기 정당성 확인 로그인 인증 시스템(100)이 상기 웹 서버(200)와 별도의 물리적 장치로 구현되는 경우, 상기 정당성 확인 로그인 인증 시스템(100)은 상기 웹 서버(200)뿐만 아니라, 복수의 웹 서버와 유무선 네트워크를 통해 연결되어 본 발명의 기술적 사상을 제공할 수도 있다.

[0047] 이하에서는, 설명의 편의를 위해 상기 정당성 확인 로그인 인증 시스템(100)은 상기 웹 서버(200)와는 별도의 물리적 장치로 구현되는 경우를 일 예로 설명하기로 한다.

[0048] 상기 사용자 단말기(300)는 상기 웹 사이트 또는 웹 애플리케이션에 접속하여, 즉, 상기 웹 서버(200)에 접속하여 로그인 요청을 수행할 수 있다. 그러면, 상기 웹 서버(200)는 상기 로그인 요청에 대한 정보를 상기 정당성 확인 로그인 인증 시스템(100)으로 전송할 수 있다. 상기 웹 서버(200)는 이미 구현된 로그인 정보 기반의 인증을 수행할 수 있다. 예컨대, 상기 사용자 단말기(300)가 로그인 요청을 하는 계정의 아이디와 패스워드가 미리 저장된 아이디 및 패스워드와 일치하는지 여부를 판단하는 인증이 수행될 수 있다. 물론, 로그인을 위해 다른 방식의 인증(예컨대, 공인인증서 또는 OTP 등)이 필요할 수도 있다.

[0049] 한편, 상기 로그인 정보 인증이 성공하면, 상기 웹 서버(200)는 상기 정당성 확인 로그인 인증 시스템(100)으로 계정정보를 전송할 수 있다. 그러면 상기 정당성 확인 로그인 인증 시스템(100)은 상기 계정정보를 이용해 위치기반 인증을 수행할 수 있다. 상기 계정정보는 상기 로그인 요청에 상응하는 계정의 정당 사용자를 식별할 수 있는 정보가 포함될 수 있다. 또한, 상기 계정정보는 상기 사용자 단말기(300)가 상기 웹 서버(200)에 접속할 때 이용된 IP(Internet Protocol)의 주소에 대한 정보를 포함할 수도 있다.

[0050] 구현 예에 따라서는, 상기 웹 서버(200)는 상기 로그인 정보 인증을 수행하지 않고, 상기 계정정보를 전송할 수도 있다. 즉, 로그인 정보 인증을 수행하기 전에 상기 위치기반 인증을 수행할 수도 있고, 로그인 정보 인증은 하지 않고 위치기반 인증만 수행할 수도 있다.

[0051] 한편, 상기 정당성 확인 로그인 인증 시스템(100)은 위치기반 인증을 수행하고, 상기 위치기반 인증이 실패하면 상기 정당 사용자의 단말기(400)로 소정의 확인신호를 전송하여 정당성 확인절차를 수행할 수 있다. 즉, 상기 정당성 확인절차는 로그인 정보 인증이 성공하고 위치기반 인증이 실패하는 경우에 수행될 수 있다. 다른 실시 예에 의하면, 상기 사용자 단말기(300)를 로그인 시키기 위해서는 위치기반 인증만 수행되고, 위치기반 인증이 실패한 로그인 요청에 대해서만 또는 모든 로그인 요청에 대해서 상기 정당성 확인절차가 수행될 수도 있다. 또 다른 실시 예에 의하면, 상기 로그인 정보 인증이 성공한 모든 로그인 요청에 대해 상기 정당성 확인절차가 수

행될 수도 있다. 로그인 정보 인증이 실패한 로그인 요청은 로그인을 허용하지 않도록 상기 웹 서버(200) 및/또는 상기 정당성 확인 로그인 인증 시스템(100)이 구현되기 때문에 정당성 확인절차를 수행할 필요가 없기 때문이다. 다양한 경우에 대해서 한정적으로 또는 모든 로그인 요청에 대해 정당성 확인절차가 수행될 수 있다. 상기 정당성 확인 로그인 인증 시스템(100)이 확인신호를 전송한다고 함은, 상기 정당성 확인 로그인 인증 시스템(100)이 직접 확인신호를 전송하는 경우뿐만 아니라, 소정의 시스템(예컨대, 메시징 서버, 통신사 시스템 등)이 상기 확인신호를 전송하도록 제어하는 경우를 포함하는 의미일 수 있다.

[0052] 정당성 확인절차가 수행되면, 상기 정당성 확인 로그인 인증 시스템(100)은 소정의 확인신호를 정당 사용자의 단말기(400)로 전송할 수 있다. 그리고 전송된 확인신호에 기초하여 응답이 수신되면, 수신된 응답에 따라 로그인 제어(예컨대, 로그인을 유지시키거나 강제로 로그아웃을 시키기 위한 제어)가 수행될 수 있다.

[0053] 한편, 이처럼 정당성 확인절차를 통해 로그인 제어를 하는 경우에는 전술한 바와 같이 정당 사용자가 응답을 하지 못하는 경우가 존재할 수 있다. 즉, 소정의 인증을 통해 로그인 제어를 할 때 인증이 실패하는 경우 로그인 거부 방식이 아니라 정당성 확인방식을 적용하는데, 정당 사용자가 로그인 제어를 수행하지 못하는 경우에는 치명적인 약점이 존재할 수 있다.

[0054] 이러한 약점을 해결하기 위한 본 발명의 기술적 사상은 정당 사용자가 블록 시간을 설정할 수 있도록 하는 기술적 사상일 수 있다. 또 다른 기술적 사상은 자동으로 응답신호를 전송할 수 있도록 하는 기술적 사상일 수 있다.

[0055] 먼저, 상기 웹 서버(200) 및/또는 상기 정당성 확인 로그인 인증 시스템(100)은 정당 사용자가 소정의 블록 시간 정보를 설정할 수 있도록 할 수 있다. 그러면, 설정된 상기 블록 시간 정보에 상응하는 블록 시간 동안에는 원칙적으로 어떠한 로그인도 허용되지 않을 수 있다.

[0056] 상기 블록 시간 정보는 예컨대, 블록 시작 시간 및/또는 블록 종료 시간에 대한 정보를 포함할 수도 있다. 그러면, 상기 블록 시작 시간으로부터 블록 종료 시간 까지는 블록이 설정될 수 있다. 구현 예에 따라서는 상기 블록 시간 정보는 블록 시작 시간 및/또는 블록 종료 시간 중 적어도 하나를 특정할 수 있는 이벤트에 대한 정보를 포함할 수도 있다. 어떠한 경우든, 상기 블록 시간 정보는 상기 웹 서버(200)의 로그인이 블록으로 설정될 시간을 특정할 수 있는 정보를 포함하는 것이 바람직하다. 예컨대, 로그아웃 이벤트가 블록 시작 시간이 되도록 설정될 수도 있으며, 추가인증을 통한 로그인이 수행되면 자동으로 블록 종료가 될 수 있다. 이하에서는 블록 시간 정보는 시간에 대한 정보로 특정되는 경우를 일 예로 설명하지만 본 발명의 권리범위가 이에 한정되지는 않는다.

[0057] 예컨대, 블록 시간 즉, 정당 사용자가 응답을 하지 못하는 시간에 소정의 로그인 요청이 상기 정당성 확인 로그인 인증 시스템(100)으로 수신되면, 상기 정당성 확인 로그인 인증 시스템(100)은 상기 로그인 요청을 허용하지 않을 수 있다. 즉, 로그인을 시켜주지 않을 수 있다. 즉, 설정된 블록 시간에는 아예 로그인 정보 인증 및 위치기반 인증이 성공하더라도 로그인을 허용하지 않으므로 원칙적으로 아무도 상기 정당 사용자의 계정으로 로그인을 하지 못하도록 할 수 있다. 그러면, 정당 사용자는 자신이 설정한 블록 시간 동안에는 로그인 요청을 하지 않을 것이므로, 부정 사용자에 의한 로그인을 원천적으로 방지할 수 있다.

[0058] 상기 블록 시간은 예컨대, 정당 사용자가 자는 시간일 수 있다. 또는 기타 다양한 이유로 인해 정당 사용자가 확인신호에 응답을 하지 못하는 시간일 수 있다.

[0059] 블록 시간 이외의 시간에 부정 사용자가 로그인 요청을 하면, 설령 로그인 정보 인증이 성공하고 위치기반 인증은 실패하더라도, 경우에 따라서 로그인이 될 수 있다. 하지만, 이러한 로그인은 정당 사용자가 응답신호를 상기 정당성 확인 로그인 인증 시스템(100)에 전송함으로써 바로 로그아웃이 될 수 있다.

[0060] 상기 응답신호는 예컨대, 확인신호에 포함된 소정의 UI를 선택하는 경우 또는 확인신호에 포함된 소정의 안내정보에 따라 정당 사용자가 소정의 행위를 수행하는 경우(예컨대, 특정 버튼의 입력, 특정 정보를 포함하는 답장 등)에 상기 정당성 확인 로그인 인증 시스템(100)으로 전송될 수 있다. 예컨대, 소정의 행위가 정당 사용자에 의해 수행된 경우에 자동으로 상기 정당성 확인 로그인 인증 시스템(100)이 제공하는 소정의 모바일 웹 페이지에 상기 정당 사용자의 단말기(400)가 접속될 수 있으며, 이러한 모바일 웹 페이지를 통해 응답신호가 입력될 수 있다. 또는 상기 확인신호에 포함된 소정의 콜백 URL로 상기 응답신호가 전송될 수도 있다. 또는, 소정의 ARS 시스템으로 상기 정당 사용자의 단말기(400)가 호를 연결할 수 있으며, 상기 ARS 시스템을 통해 상기 응답신호를 입력할 수도 있다. 또는 상기 정당 사용자의 단말기(400)에 설치된 소정의 애플리케이션(10)을 통해 상기 확인신호가 수신된 경우에는, 상기 애플리케이션(10)에서 제공하는 소정의 UI를 통해 상기 응답신호가 상기

정당성 확인 로그인 인증 시스템(100)으로 출력될 수도 있다.

[0061] 한편, 블록 시간에서는 부정 사용자가 로그인을 한 경우에도 정당 사용자가 응답신호를 보낼 수 없으므로 정당성 확인방식의 로그인 제어에 취약점을 생성할 수 있다. 따라서, 이처럼 정당 사용자가 응답신호를 상기 정당성 확인 로그인 인증 시스템(100)으로 출력할 수 없는 상황에서는 어떠한 로그인 요청에 대해서도 로그인을 허용하지 않음으로써 이러한 문제점을 해결할 수 있다.

[0062] 한편, 정당 사용자는 자신이 설정한 블록 시간에 로그인을 해야 할 필요가 발생할 수도 있다. 이러한 경우에는 상기 정당성 확인 로그인 인증 시스템(100)은 소정의 추가인증을 통해 블록 시간임에도 로그인을 허용할 수 있다. 상기 추가인증은 로그인 정보 인증 및 상기 위치기반 인증과는 다른 인증방식인 것이 바람직하다. 예컨대, 공인인증서를 통해 방식, OTP를 통한 방식, 생체정보(예컨대, 지문 또는 홍체 등)를 이용한 인증방식 또는 소정의 오프라인 절차를 통한 인증 방식 등 다양한 방식이 상기 추가인증을 위한 인증방식으로 선택될 수 있다. 또한, 상기 추가인증을 수행하면, 블록 시간을 해제하거나 변경할 수도 있다.

[0063] 이러한 기술적 사상을 구현하기 위해 상기 정당성 확인 로그인 인증 시스템(100)은 제어부(110), 계정 확인부(120), 위치기반 인증부(130), 및 정당성 확인부(140)를 포함한다. 상기 정당성 확인 로그인 인증 시스템(100)은 블록 시간 인증부(150)를 더 포함할 수 있다.

[0064] 상기 정당성 확인 로그인 인증 시스템(100))은 본 발명의 기술적 사상을 구현하기 위해 필요한 하드웨어 리소스(resource) 및/또는 소프트웨어를 구비할 수 있으며, 반드시 하나의 물리적인 구성요소를 의미하거나 하나의 장치를 의미하는 것은 아니다. 즉, 상기 정당성 확인 로그인 인증 시스템(100)은 본 발명의 기술적 사상을 구현하기 위해 구비되는 하드웨어 및/또는 소프트웨어의 논리적인 결합을 의미할 수 있으며, 필요한 경우에는 서로 이격된 장치에 설치되어 각각의 기능을 수행함으로써 본 발명의 기술적 사상을 구현하기 위한 논리적인 구성들의 집합으로 구현될 수도 있다. 또한, 상기 정당성 확인 로그인 인증 시스템(100)은 본 발명의 기술적 사상을 구현하기 위한 각각의 기능 또는 역할별로 별도로 구현되는 구성들의 집합을 의미할 수도 있다.

[0065] 또한, 본 명세서에서 '~부'라 함은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 '~부'는 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스(resource)의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것은 아님은 본 발명의 기술분야의 평균적 전문가에게는 용이하게 추론될 수 있다.

[0066] 상기 제어부(110)는 본 발명의 기술적 사상을 구현하기 위하여 다른 구성요소들(예컨대, 계정 확인부(120), 위치기반 인증부(130), 정당성 확인부(140), 및/또는 상기 블록 시간 인증부(150) 등)의 기능 및/또는 리소스를 제어할 수 있다.

[0067] 상기 계정 확인부(120)는 로그인 요청이 된 계정의 계정정보를 확인할 수 있다. 상기 계정정보는 정당 사용자의 식별정보, 정당 사용자의 단말기(400)의 식별정보, 상기 정당 사용자의 단말기(400)의 IP 주소 정보(즉, 로그인 요청을 위해 상기 웹 서버(200)에 접속했을 때의 상기 정당 사용자의 단말기(400)의 IP 주소) 등을 포함할 수 있다. 상기 계정 확인부(120)는, 사용자 단말기(300)가 상기 웹 서버(200)에 로그인 요청을 하면, 로그인 요청에 상응하는 상기 계정정보를 상기 웹 서버(200)로부터 수신할 수 있다. 물론, 상기 정당성 확인 로그인 인증 시스템(100)이 상기 웹 서버(200)에 포함되어 설치되는 경우에는, 상기 계정 확인부(120)는 상기 계정정보를 직접 확인할 수도 있다.

[0068] 그러면, 상기 위치기반 인증부(130)는 확인된 상기 계정정보에 기초하여 상기 로그인 요청에 상응하는 계정의 정당 사용자의 위치와 상기 사용자 단말기의 위치를 확인할 수 있다. 그리고 확인된 위치를 비교하여 위치기반 인증을 수행할 수 있다. 상기 위치기반 인증부(130)의 상세한 구성은 도 2를 참조하여 설명하도록 한다.

[0069] 도 2는 본 발명의 실시 예에 따른 정당성 확인 로그인 인증 시스템에 포함된 위치기반 인증부의 개략적인 구성을 나타낸다.

[0070] 도 2를 참조하면 상기 위치기반 인증부(130)는 단말기 위치판단 모듈(131) 및 사용자 위치판단 모듈(132)을 포함한다.

[0071] 상기 단말기 위치판단 모듈(131)은 상기 웹 서버(200)로 로그인 요청을 수행한 단말기 즉, 사용자 단말기(300)의 위치를 판단할 수 있다. 또한, 상기 사용자 위치판단 모듈(132)은 상기 사용자 단말기(300)가 로그인 요청한 계정의 정당 사용자의 위치를 판단할 수 있다.

[0072] 일 실시 예에 의하면, 상기 단말기 위치 판단 모듈(131)은 상기 사용자 단말기(300)의 IP 주소에 기초하여 상기 사용자 단말기(300)의 위치를 판단할 수 있다. 예컨대, 상기 사용자 단말기(300)는 데스크톱 컴퓨터 등과 같이 고정된 데이터 프로세싱 장치 또는 모바일 폰과 같은 휴대용 단말기일 수 있다. 상기 단말기 위치 판단 모듈(131)은 로그인 요청을 하는 상기 사용자 단말기(300)의 IP(Internet Protocol) 주소를 획득하고, 획득된 상기 IP 주소에 기초하여 상기 사용자 단말기(300)의 위치를 알 수 있다.

[0073] IP(Internet Protocol) 주소는 실제 주소정보와 매칭될 수 있는데, 일반적으로 IP 주소는 ISP(Internet Service Provider)에 의해 할당, 등록, 및/또는 관리될 수 있다. 따라서, 상기 단말기 위치 판단 모듈(120)은 상기 사용자 단말기(300)에 대응하는 IP 주소를 획득하고, IP 주소별 위치정보를 저장하고 있는 소정의 시스템(예컨대, ISP 시스템(미도시))으로부터 상기 IP 주소에 대응되는 실제 주소정보를 획득할 수 있다. 상기 정당성 확인 로그인 인증 시스템(100)은 IP 주소별로 실제 주소 정보를 소정의 DB 즉, IP 주소별 위치정보 DB(미도시)에 저장하고 있을 수 있다.

[0074] 상기 정당성 확인 로그인 인증 시스템(100)에 포함된 상기 위치기반 인증부(130)는 상기 IP 주소별 위치정보 DB에 미리 저장하고 있거나, 주기적으로 또는 실시간으로 상기 IP 주소에 대응되는 실제 주소에 대한 정보를 수신할 수도 있다. 상기 실제 주소는 특정 행정구역(예컨대, 동 또는 구) 단위까지만을 갖는 정보일 수도 있고, 전체 주소일 수도 있다.

[0075] 상기 사용자 단말기(300)가 휴대용 단말기인 경우에는 상기 사용자 단말기(300)는 무선 인터넷 망을 통하여 무선 인터넷에 접속할 수 있는데, 이때에는 상기 무선 인터넷 서비스를 제공하는 통신사는 상기 사용자 단말기(300)에 할당되는 IP 주소 및/또는 상기 휴대용 단말기(210)가 접속한 액세스 포인트(AP)의 위치를 알 수 있다. 이때에는 상기 단말기 위치 판단 모듈(131)은 무선 인터넷 서비스를 제공하는 통신사 시스템으로부터 상기 액세스 포인트의 위치에 대한 정보를 수신할 수도 있다. 또한, 상기 사용자 단말기(300)의 위치는 종래의 다양한 위치추적방법(예컨대, 삼각측량, GPS 등)에 의해 파악될 수 있으며, 상기 단말기 위치 판단 모듈(131)은 이러한 정보들을 상기 통신사 시스템으로부터 수신할 수도 있다. 물론, 상기 사용자 단말기(300)가 소정의 LBS(location based service)를 사용하고 있는 경우에는, 상기 LBS 서비스를 제공하는 LBS 시스템(미도시)으로부터 상기 사용자 단말기(300)의 위치에 대한 정보를 수신할 수도 있다. 또는 구현 예에 따라, 상기 사용자 단말기(300)가 GPS 모듈과 같은 위치판단 수단을 포함하는 경우, 상기 단말기 위치 판단 모듈(131)은 상기 사용자 단말기(300)로부터 직접 상기 사용자 단말기(300)의 위치를 수신할 수도 있다. 이 밖에도 다양한 방법으로 상기 단말기 위치 판단 모듈(131)은 상기 사용자 단말기(300)의 위치를 판단할 수 있다.

[0076] 한편, 상기 IP 주소별 위치정보 DB는 전술한 바와 같이 ISP 시스템 등으로부터 수신된 정보에 기초하여 IP 주소 각각에 대응되는 위치정보를 저장할 수 있다. 하지만, 이러한 ISP 시스템으로부터 파악될 수 있는 위치 정보는 그 오차 범위가 클 뿐만 아니라, VPN(Virtual Private Network) 등과 같은 대규모의 사설 네트워크 등에서는 위치 정보가 정확하지 않다는 문제점이 있다.

[0077] 따라서 이러한 문제점을 해결하기 위해 본 발명의 실시 예에 따른 상기 IP 주소별 위치정보 DB는 사용자의 위치에 기초하여 IP별로 위치 정보를 저장하고 있는 DB일 수 있다. 이러한 기술적 사상은 본 출원인이 출원한 한국 특허출원(출원번호 10-2011-0081595, "네트워크 식별자 위치판단 시스템 및 그 방법", 이하 '이전출원')에 개시된 바 있다. 이전출원에 개시된 기술적 사상 및 그 기재는 본 발명의 레퍼런스로 포함되며, 본 명세서에 기재된 것으로 취급될 수 있다.

[0078] 결국, 상기 IP 주소별 위치정보 DB는 이전 출원에 개시된 바와 같이 정당 사용자의 위치에 기초하여 IP별로 위치정보가 매핑되어 있는 DB일 수 있다. 즉 정당 사용자가 소정의 네트워크 시스템(상기 웹 서버(200)일 수도 있고, 다른 웹 서버 등일 수도 있음)에 정당하게 접속하는 경우에 정당 사용자의 모바일 폰의 위치 값에 기초하여 상기 IP의 위치정보로 매핑할 수 있고, 이런 경우의 IP의 위치정보는 ISP 시스템으로부터 받는 위치정보에 비해 훨씬 오차범위가 줄어들고, 사설 네트워크 등에서 사용되는 IP의 경우에도 정확한 위치 정보를 파악할 수 있는 효과가 있다. 따라서, 위치 정보의 오차범위가 줄어듦에 따라 부정 사용자에 의한 로그인 요청임에도 IP에 상응하는 위치와 정당 사용자의 위치가 상응하는 것으로 잘못 판단되는 경우를 줄일 수 있으며, 대규모의 기업이나 아파트 단지 등과 같이 사설 네트워크나 DHCP(Dynamic Host Configuration Protocol)를 사용하는 경우에도 두 위치가 상응하는지를 정확하게 판단할 수 있다. 예컨대, 이전출원에 의하면 사설 네트워크나 DHCP를 사용하는 경우 동일한 IP(예컨대, IP 어드레스 등)에 대해 복수의 가능한 위치 정보가 매핑될 수 있다. 따라서, 본 발명의 실시 예에서 상기 위치기반 인증부(130)는 복수의 위치정보 중 어느 하나가 상기 정당 사용자의 위치와 상응하면 상기 사용자 단말기(300)에 상응하는 위치와 상기 정당 사용자의 위치가 동일성이 있다고 판단할 수도 있

다.

[0079] 결국, 종래의 IP에 해당하는 위치를 판단하는 방식은 단순히 네트워크 사업자(ISP)가 IP를 할당하는 방식, 규칙, 또는 네트워크 사업자의 정보에 의존하였던 방식임에 비해, 본 발명의 기술적 사상에 의하면, IP의 위치를 다른 파라미터(즉, 정당 사용자의 위치)를 이용하여 결정함으로써 보다 정확한 위치를 파악할 수 있는 효과가 있다. 특히, 종래의 방식은 IP별 위치를 동 단위 정도의 큰 오차를 가지는 정보로 파악할 수밖에 없음에 비해, 본 발명의 기술적 사상에 의하면 정당 사용자의 위치 정보의 오차 정도가 상기 IP별 위치의 오차로 결정되는 효과가 있다. 일반적으로 정당 사용자의 위치 정보를 정당 사용자의 단말기(400)의 위치로 파악하는 경우, 상기 정당 사용자의 위치정보는 GPS 값 또는 통신사 시스템으로부터 수신된 값을 포함하는데 이러한 경우의 오차는 수 미터에서 수백 미터 정도이므로 기존 방식에 비해 IP별 위치의 오차범위는 현격하게 줄어드는 효과가 있다.

[0080] 한편, 상기 사용자 위치 판단 모듈(132)은 상기 로그인 요청에 상응하는 계정의 정당 사용자의 위치를 판단할 수 있다. 이를 위해 상기 사용자 위치 판단 모듈(132)는 정당 사용자의 단말기(400)의 위치를 파악할 수 있다. 즉, 상기 사용자 위치 판단 모듈(132)은 정당 사용자의 위치를 상기 정당 사용자의 단말기(400)의 위치에 기초하여 판단할 수 있다. 상기 정당 사용자의 단말기(400)의 위치를 파악하는 방법은 상기 단말기 위치 판단 모듈(131)이 로그인 요청을 하는 휴대용 단말기의 위치 정보를 파악하는 방법과 유사하므로, 상세한 설명은 생략한다.

[0081] 상기 정당 사용자의 단말기(400)의 식별정보(예컨대, 휴대전화 번호)는 상기 정당성 확인 로그인 인증 시스템(100) 또는 상기 웹 서버(200)에 미리 저장되어 있을 수 있으며, 저장된 식별정보에 기초하여 상기 정당 사용자의 단말기(400)가 식별될 수 있다.

[0082] 그러면, 상기 위치기반 인증부(130)는 상기 단말기 위치 판단 모듈(131)이 판단한 상기 사용자 단말기(300)의 위치와 상기 사용자 위치 판단 모듈(132)이 판단한 상기 정당 사용자의 위치를 비교함으로써, 위치기반 인증을 수행할 수 있다.

[0083] 한편, 이처럼 위치기반 인증부(130)에 의해 위치기반 인증이 수행되는 경우는, 상기 웹 서버(200)에 의해 로그인 정보 인증이 성공된 로그인 요청에 한정될 수 있다. 예컨대, 아이디 및 패스워드를 통한 로그인 정보 인증이 통과하면, 상기 웹 서버(200)는 상기 계정 확인부(120)로 상기 계정정보를 전송할 수 있다. 그러면 상기 계정정보에 기초한 위치기반 인증이 수행될 수 있다.

[0084] 한편, 상기 정당성 확인부(140)는 상기 정당 사용자의 단말기(400)로 소정의 확인신호를 전송할 수 있다. 상기 확인신호는 예컨대, SMS 또는 MMS 등의 메시지일 수 있다. 또는, 상기 확인신호는 상기 정당 사용자의 단말기(400)에 설치된 소정의 애플리케이션으로 전송되는 푸시(push) 메시지일 수도 있다. 다양한 구현 예가 가능할 수 있다. 그리고, 상기 정당성 확인부(140)는 상기 확인신호에 기초하여 소정의 응답신호가 수신되는지를 판단할 수 있다. 상기 응답신호는 예컨대, 로그인된 상기 사용자 단말기(300)를 로그아웃시키기 위한 제어신호일 수 있다.

[0085] 그러면, 상기 제어부(110)는 상기 응답신호가 수신되는 경우, 상기 사용자 단말기(300)를 강제로 로그아웃 시킬 수 있다.

[0086] 한편, 전술한 바와 같이 본 발명의 실시 예에 따른 정당성 확인 로그인 인증 시스템(100)은 정당 사용자가 블록 시간을 설정할 수 있도록 하는 구성을 포함할 수 있다. 이를 위해서, 상기 정당성 확인 로그인 인증 시스템(100)은 블록 시간 인증부(150)를 더 포함할 수 있다. 본 명세서에서 블록 시간을 나타내는 블록 시간 정보에는 반드시 블록 종료 시간이 포함되는 경우를 의미하지는 않는다. 즉, 블록 시작을 나타내는 정보 또는 이벤트만 상기 블록 시간 정보에 포함될 수도 있다.

[0087] 사용자가 블록 시간을 설정할 수 있는 방식은 도 3 및 도 4를 참조하여 설명하도록 한다.

[0088] 먼저, 도 3은 본 발명의 실시 예에 따른 정당성 확인 로그인 인증 방법에서 블록 시간을 설정할 수 있는 방법을 개략적으로 설명하기 위한 도면이다.

[0089] 도 3a를 참조하면, 정당 사용자는 상기 웹 서버(200)에 접속하여 상기 웹 서버(200)가 제공하는 소정의 UI를 통해 블록 시간을 설정할 수 있다. 또한, 도 3b를 참조하면, 정당 사용자는 정당 사용자의 단말기(400)를 통해 상기 블록 시간을 설정할 수도 있다. 상기 정당 사용자의 단말기(400)를 통해 상기 블록 시간을 설정하기 위해서는 상기 웹 서버(200)에 상응하는 소정의 애플리케이션(10)이 상기 정당 사용자의 단말기(400)에 설치될 수 있

다. 즉, 상기 애플리케이션(10)은 상기 웹 서버(200)와 통신을 수행하여, 상기 애플리케이션(10)을 통해 입력된 블록 시간에 대한 정보를 상기 웹 서버(200)로 전송할 수 있다. 이처럼 상기 애플리케이션(10)을 통해 상기 블록 시간을 설정할 수 있는 경우에는, 사용자가 블록 시간을 설정하기 위해 상기 웹 서버(200)에 접속하여야 할 필요가 없는 효과가 있다.

[0090] 상기 웹 서버(200)에 접속하여 정당 사용자가 블록 시간을 설정하기 위해서는 상기 정당 사용자는 로그인 정보 인증 및/또는 위치기반 인증을 통해 로그인을 수행해야 할 수 있다. 그리고 상기 정당 사용자가 이용하는 단말기(상기 정당 사용자의 단말기(400)일 수도 있음)를 통해 블록 시간 설정 요청을 상기 웹 서버(200)로 전송하면, 상기 웹 서버(200)는 도 3a와 같은 소정의 UI를 제공할 수 있다.

[0091] 정당 사용자는 도 3에 도시된 바와 같이 예컨대, "지금부터"라는 UI를 선택할 수 있다. 그러면, 상기 UI가 선택된 시점부터 블록 시간이 시작될 수 있다. 한편, "해제" UI를 선택하면 블록 시간이 종료될 수 있다. 구현 예에 따라, 정당 사용자는 직접 블록 시간의 시작 시간 및 종료 시간을 입력할 수도 있다. 그러면, 입력된 시간이 블록 시간으로 설정될 수 있다.

[0092] 정당 사용자의 단말기(400)를 통해 블록 시간을 설정하는 경우에도 상기 애플리케이션(10)은 도 2a에서 설명한 바와 동일한 UI 또는 유사한 기능을 수행할 수 있는 UI를 제공할 수 있다. 그러면, 정당 사용자는 상기 애플리케이션(10)을 통해 블록 시간을 설정할 수 있다.

[0093] 한편, 블록 시간을 설정하지 않고도 블록 시간을 설정한 것과 유사한 효과를 나타낼 수 있는 기술적 사상이 본 명세서에 의해 개시된다.

[0094] 이러한 기술적 사상은 전술한 바와 같이 별도로 블록 시간을 설정함으로써 정당 사용자가 정당성 확인절차를 수행하기 위한 응답신호를 전송하지 못하는 경우를 대처하는 것과 달리, 정당 사용자가 직접 응답신호를 전송하지 못하는 경우에는 자동으로 응답신호를 전송하도록 함으로써 구현될 수 있다.

[0095] 예컨대, 상기 정당 사용자의 단말기(400)에는 상기 웹 서버(200)에 상응하는 애플리케이션(10)이 설치될 수 있다. 상기 애플리케이션(10)은 상기 정당성 확인 로그인 인증 시스템(100)으로부터 수신되는 확인신호를 식별할 수 있다. 그러면, 상기 확인신호가 수신되었음이 확인되면, 상기 애플리케이션(10)은 자동으로 상기 응답신호를 전송할 수 있다. 이를 통해 정당 사용자가 직접 응답신호를 전송하지 못하는 경우에도 정당 사용자는 자신이 원하는 시간 또는 상황에서는 자동으로 상기 응답신호를 전송하도록 할 수 있다.

[0096] 한편, 도 3a 또는 도 3b와 같은 경우에는 현재 정당 사용자가 상기 웹 서버(200)에 접속하고 있지 않은 경우에 상기 정당 사용자가 블록 시간을 설정하는 방식을 나타낼 수 있다. 한편, 블록 시간을 설정할 필요는 정당 사용자가 이미 상기 웹 서버(200)에 접속하고 있는 상태에서 자신은 로그아웃을 하고, 로그아웃 이후부터는 블록 시간으로 설정하고자 할 때 빈번히 발생할 수 있다.

[0097] 예컨대, 상기 웹 서버(200)가 제공하는 웹 서비스가 게임인 경우, 정당 사용자는 게임을 하다가 게임을 그만하고 로그아웃을 수행하고자 할 수 있다. 이러한 경우, 본 발명의 기술적 사상에 의하면 정당 사용자는 일일이 블록 시간 설정을 하기 위한 웹 페이지로 이동을 하여야할 필요 없이 로그아웃 절차와 함께 간편히 블록 시간을 설정할 수 있다.

[0098] 이러한 일 예는 도 4에 도시된다.

[0099] 도 4는 본 발명의 실시 예에 따른 정당성 확인 로그인 인증 방법에서 정당 사용자가 로그아웃을 수행하면서 블록설정을 할 수 있는 방법을 설명하기 위한 도면이다.

[0100] 도 4를 참조하면, 본 발명의 실시 예에 따른 정당성 확인 로그인 인증 시스템(100) 및/또는 상기 웹 서버(200)는 사용자 단말기(300)로부터 로그아웃 요청이 수신된 경우, 도 3에 도시된 바와 같은 소정의 로그아웃 확인 UI(20)를 사용자 단말기(300)로 제공할 수 있다. 상기 사용자 단말기(300)로부터의 로그아웃 요청은 상기 웹 서버(200)가 제공하는 소정의 로그아웃 요청 UI(미도시)를 선택한 경우일 수도 있고, 웹 클라이언트의 종료 요청일 수도 있다.

[0101] 상기 로그아웃 UI(20)는 도 4에 도시된 바와 같이 로그아웃 UI(21), 로그아웃 및 블록설정 UI(22), 및 로그아웃 취소 UI(23)를 포함할 수 있다. 상기 사용자 단말기(300)에 의해 로그아웃 UI(21)가 선택되면, 블록 시간 설정 없이 단순히 로그아웃만 수행될 수 있다. 상기 로그아웃 및 블록설정 UI(22)가 선택되면, 로그아웃이 수행됨과 동시에 로그아웃 후부터 블록 시간이 시작될 수 있다. 즉, 블록이 설정될 수 있다. 로그아웃 취소 UI(23)가 선

택되면 로그아웃이 되지 않고 로그인 상태가 유지될 수 있다.

[0102] 이처럼 로그아웃을 확인함과 동시에 간편하게 블록을 설정할 수 있다. 이후, 다시 정당 사용자가 로그인을 하기 위해서는 추가인증을 수행해야 할 수 있음은 물론이다. 추가인증이 수행되면 블록을 해제할 수도 있다. 구현 예에 따라서는, 도 4에 도시된 바와 같이 별도로 블록 설정 UI(예컨대, 22)를 제공할 필요가 없이, 로그아웃이 되면 자동으로 블록이 설정되도록 구현될 수도 있다.

[0103] 이렇게 사용자에 의해 블록 시간에 대한 정보 즉, 블록 시간 정보가 설정되면, 상기 블록 시간 인증부(150)는 블록 시간 정보를 저장할 수 있다. 그러면, 상기 제어부(110)는 상기 블록 시간 인증부(150)에 저장된 상기 블록 시간 정보를 확인할 수 있다. 그리고, 상기 블록 시간 동안에 요청되는 로그인 요청에 대해서는 원칙적으로 로그인을 허용하지 않을 수 있다.

[0104] 즉, 본 발명의 기술적 사상에 의하면, 상기 웹 서버(200)로 요청되는 로그인 요청에 대해서는 기본적으로는 로그인 정보 인증 및 위치기반 인증이 수행될 수 있다. 그리고 로그인 정보 인증이 성공하면 일단 로그인을 허용하되 위치기반 인증이 실패하는 경우에는 정당성 확인절차를 거칠 수 있다. 구현 예에 따라서는 위치기반 인증이 성공하여도 정당성 확인절차를 거칠 수 있다.

[0105] 하지만, 상기 제어부(110)는 블록 시간 동안에 요청된 로그인 요청에 대해서는, 설령 상기 로그인 요청이 상기 로그인 정보 인증이 성공될 수 있고, 위치기반 인증이 성공될 수 있는 로그인 요청이라 하더라도 로그인을 허용하지 않을 수 있다. 여기에서 로그인 정보 인증 및 위치기반 인증이 성공할 수 있는 로그인 요청의 로그인을 허용하지 않는다고 함은, 실제로 로그인 정보 인증 및 위치기반 인증을 수행하여야 하는 것을 의미하지는 않는다. 즉, 로그인 정보 인증 및 위치기반 인증을 수행하면, 모두 성공할 수 있는 로그인 요청이라 하더라도 로그인이 허용되지 않음을 의미하며 실제로 상기 정당성 확인 로그인 인증 시스템(100) 및/또는 상기 웹 서버(200)는 상기 로그인 정보 인증 및/또는 상기 위치기반 인증을 수행할 수도 있고 하지 않을 수도 있다.

[0106] 한편, 상기 블록 시간 동안에 로그인이 요청되면, 상기 블록 시간 인증부(150)는 소정의 추가 인증을 수행할 수 있다. 상기 추가 인증은 로그인 정보 인증 및 상기 위치기반 인증과는 별개의 인증 즉, 다른 방식의 인증일 수 있다. 그리고 이러한 추가 인증을 통과하여야만 블록 시간 동안에 로그인을 허용할 수 있다. 물론, 로그인 정보 인증 및 상기 위치기반 인증도 더 통과해야 블록 시간 동안의 로그인을 허용할 수도 있다.

[0107] 상기 추가 인증이 수행되는 과정은 도 5에 도시된 바와 같을 수 있다.

[0108] 도 5는 본 발명의 실시 예에 따른 정당성 확인 로그인 인증 방법에서 추가인증을 통해 정당 사용자가 로그인을 수행할 수 있는 방법을 설명하기 위한 도면이다.

[0109] 먼저, 도 5a를 참조하면, 사용자 단말기(300)는 웹 서버(200)에 제공할 수 있다. 도 5a에서는 소정의 웹 사이트에 접속하는 경우를 도시하고 있지만, 상기 웹 서버(200)가 제공하는 소정의 웹 애플리케이션을 이용하는 경우에도 본 발명의 기술적 사상이 제공될 수 있음은 물론이다.

[0110] 정당 사용자는 사용자 단말기(300)를 통해 상기 웹 사이트가 제공하는 소정의 로그인 UI에 로그인 정보(예컨대, ID, PWD)를 입력할 수 있다. 상기 로그인 정보를 통한 인증이 상기 웹 서버(200)에 의해 인증되면, 원칙적으로는 상기 웹 서버(200)는 상기 사용자 단말기(300)의 로그인을 허용할 수 있다.

[0111] 하지만, 상기 사용자 단말기(300)로부터의 로그인 요청이 전술한 바와 같은 블록 시간 동안에 요청된 경우에는 상기 정당성 확인 로그인 인증 시스템(100)은 도 5b와 같이 블록 시간임을 나타내는 정보 및/또는 추가인증을 통해 로그인을 수행하라는 안내 정보 등을 사용자 단말기(300)로 제공할 수 있다. 물론, 상기 정당성 확인 로그인 인증 시스템(100)은 추가인증을 수행하기 위한 소정의 UI를 상기 사용자 단말기(300)로 더 제공할 수 있다.

[0112] 한편, 본 발명의 기술적 사상에 의한 정당성 확인절차는 위치기반 인증이 실패한 경우에만 전송될 수 있다. 또한, 위치기반 인증이 실패하더라도 적어도 로그인 정보 인증은 성공하고, 위치기반 인증이 실패한 경우에 정당성 확인절차가 수행될 수 있다. 왜냐하면 로그인 정보 인증조차 실패한 경우에는 아예 로그인이 허용되지 않도록 구현되는 것이 일반적이기 때문이다.

[0113] 위치기반 인증이 실패하는 경우는 예컨대, 로그인 정보가 유출되어 부정 사용자가 로그인을 수행한 경우일 수도 있고, 정당 사용자가 타인에게 로그인을 허용하는 경우일 수도 있다. 일반적으로 회사 업무 등에서는 동료나 부하직원 등 특정한 계정을 복수의 사용자가 사용하는 경우가 빈번히 존재할 수 있다. 이러한 경우에는 로그인 정보 인증은 성공하더라도 상기 계정의 명의자의 위치와 현재 로그인을 수행하는 사용자의 위치가 다른 경우, 위치기반 인증이 실패할 수 있다. 따라서, 이러한 경우에는 정당 사용자는 자신의 단말기(400)로 수신된 확인신호

에 응답신호를 출력하지 않음으로써 해당 로그인의 정당성을 확인해줄 수도 있다.

[0114] 한편, 구현 예에 따라서는 웹 서버(200)의 제공주체는 반드시 소정의 계정은 상기 계정의 명의자만 사용할 수 있도록 구현되기를 바랄 수 있다. 이러한 일 예는 회사 내부의 시스템이나 특히 보안성이 요구되는 시스템 등일 수 있다. 이러한 경우에는 반드시 정당 명의자에게만 로그인을 허용하도록 상기 정당성 확인 로그인 인증 시스템(100)은 로그인 제어를 수행할 수도 있다. 이때에는 위치기반 인증이 성공한 경우에만 로그인을 허용하거나, 또는 위치기반 인증이 성공한 경우에도 정당성 확인절차를 수행하도록 구현됨으로써 가능할 수 있다.

[0115] 즉, 위치기반 인증이 실패하는 경우에는 당연히 정당성 확인절차를 거치는 것이 바람직할 수 있으며, 위치기반 인증이 성공하는 경우에도 보안성을 높이기 위해서는 정당성 확인절차를 수행할 수 있다.

[0116] 따라서, 결국, 상기 정당성 확인 로그인 인증 시스템(100)은 위치기반 인증이 실패하든 성공하든 관계없이 로그인 정보 인증이 성공한 모든 로그인 요청에 대해서 정당성 확인절차를 거칠 수도 있다. 이때에는 굳이 위치기반 인증을 수행할 필요가 없을 수도 있지만, 구현 예에 따라서는 수행할 수도 있다.

[0117] 따라서, 본 발명의 기술적 사상에 의하면 상기 정당성 확인 로그인 인증 시스템(100)은 로그인 정보 인증이 성공하고 위치기반 인증은 실패한 로그인 요청에 대해서 정당성 확인절차를 수행할 수도 있고, 로그인 정보 인증이 성공한 모든 로그인 요청에 대해서 수행할 수도 있다. 물론, 전술한 바와 같이 다른 케이스에 대해서도 정당성 확인절차가 수행될 수도 있다.

[0118] 어떠한 경우에 정당성 확인절차가 수행될지는 상기 정당 사용자에 의해 선택될 수도 있고, 상기 웹 서버(200)의 운영주체 또는 상기 정당성 확인 로그인 인증 시스템(100)의 운영주체에 의해 결정될 수도 있다. 상기 웹 서버(200) 및/또는 상기 정당성 확인 로그인 인증 시스템(100)은 정당성 확인절차를 어떤 경우에 설정할지에 대한 정보 즉, 확인설정 정보를 미리 저장할 수 있다. 그리고 저장된 확인설정 정보에 상응하도록 정당성 확인절차를 수행할 수 있다.

[0119] 상기 사용자 단말기(300)는 도 1에는 컴퓨터로 도시하였지만, 본 발명의 기술적 사상을 구현하기 위해 상기 정당성 확인 로그인 인증 시스템(100) 및/또는 웹 서버(200)에 소정의 로그인 요청을 출력할 수 있고, IP주소가 할당될 수 있는 모든 데이처 처리 시스템을 포함하는 의미로 정의될 수 있다.

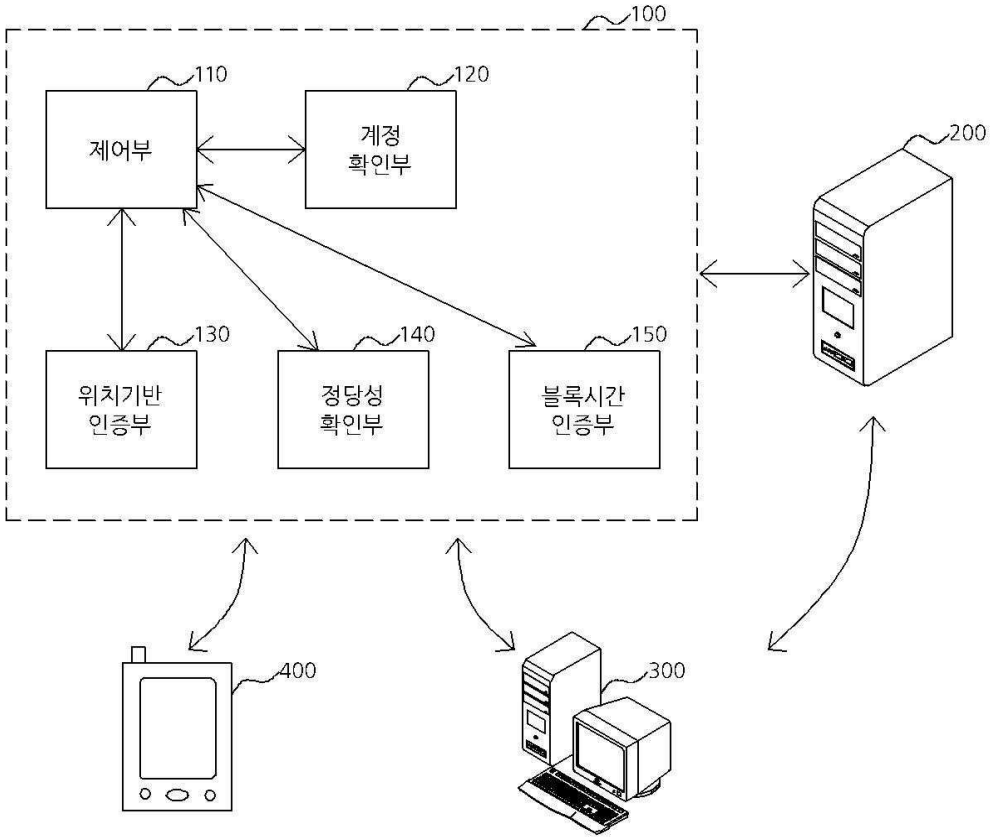
[0120] 또한, 상기 정당 사용자의 단말기(400) 역시 도 1에는 모바일 폰으로 도시하였지만, 본 발명의 기술적 사상을 구현하기 위해 상기 정당성 확인 로그인 인증 시스템(100)으로부터 확인신호를 수신하고 이에 응답하여 응답신호를 전송할 수 있는 모든 데이처 처리 시스템을 포함하는 의미로 정의될 수 있다.

[0121] 본 발명의 실시 예에 따른 정당성 확인 로그인 인증 방법은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 하드 디스크, 플로피 디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어, 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술분야의 프로그래머들에 의해 용이하게 추론될 수 있다.

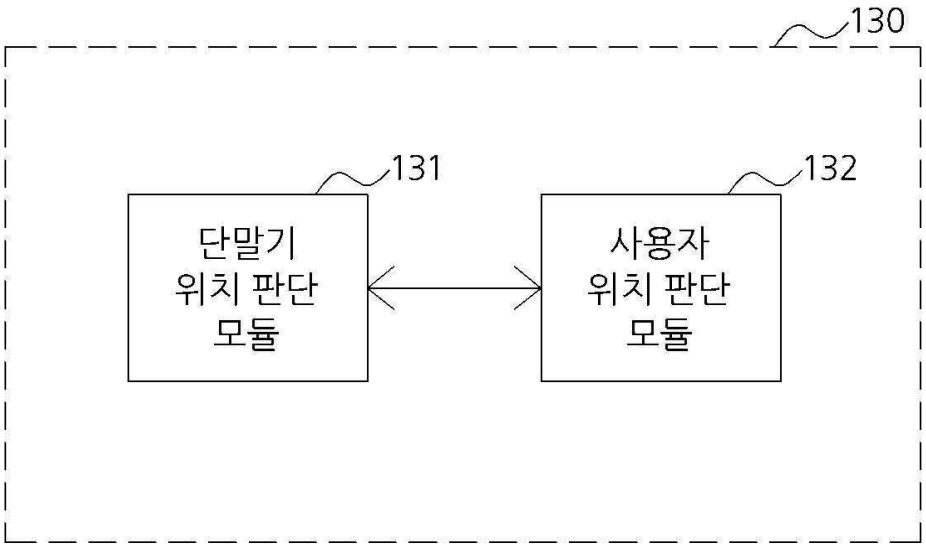
[0122] 본 발명은 도면에 도시된 일 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면

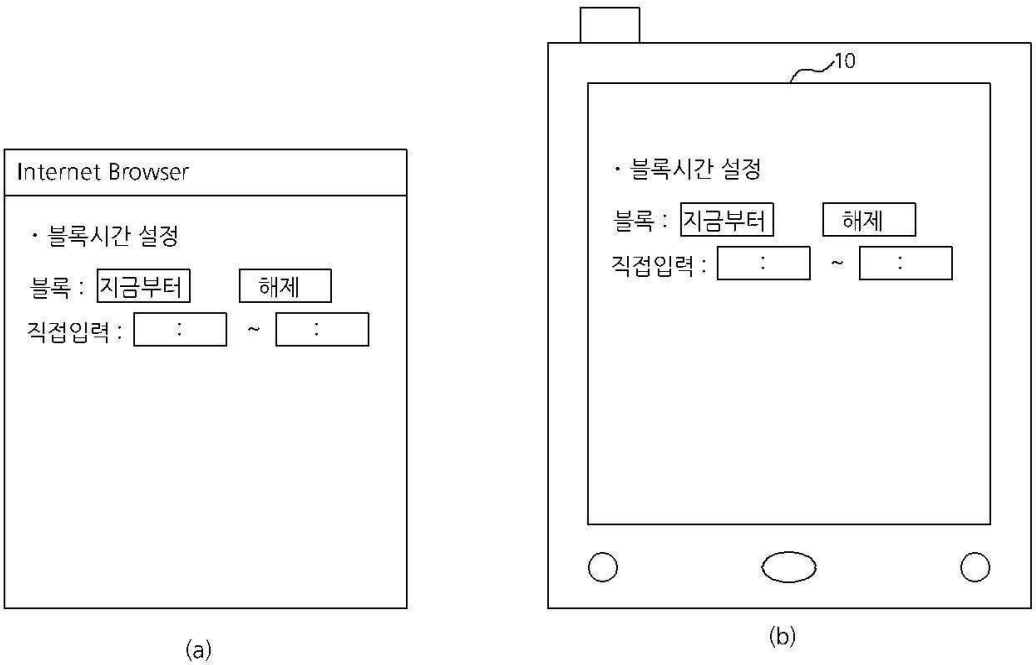
도면1


100
110
제어부
120
계정
확인부
200
130
위치기반
인증부
140
정당성
확인부
150
블록시간
인증부
400
300

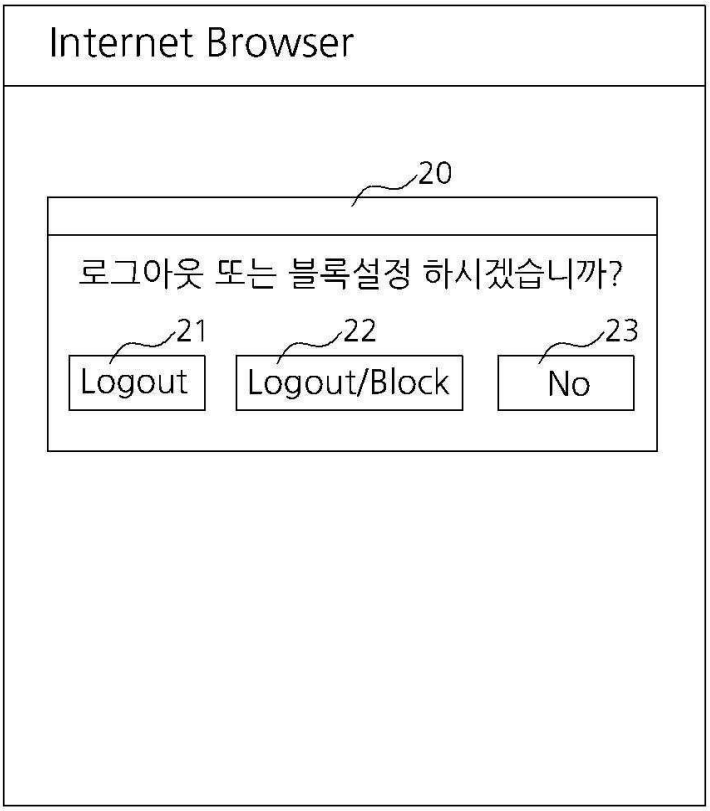
도면2


130
131
132
단말기
위치 판단
모듈
사용자
위치 판단
모듈

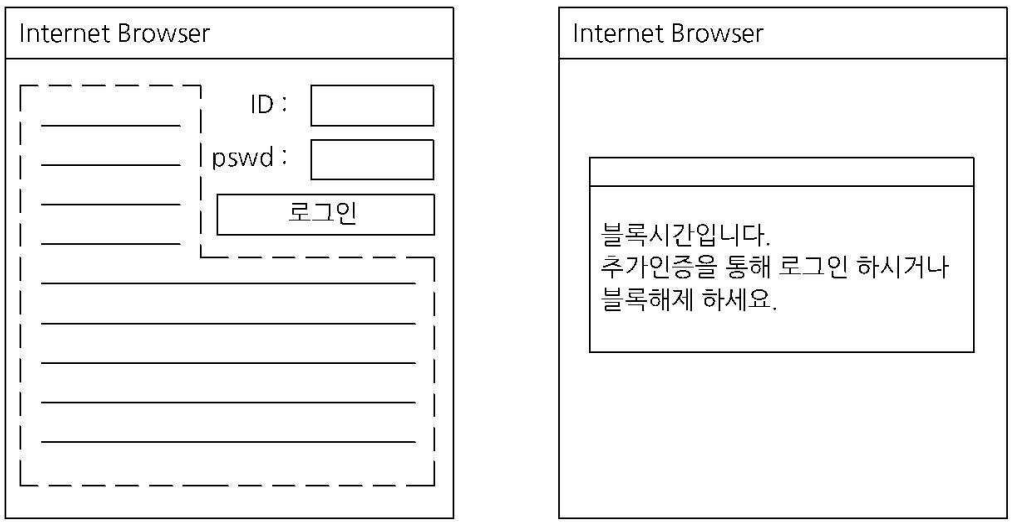
도면3


Internet Browser
· 블록시간 설정
블록 : 지금부터
해제
직접입력 :
:
~
:
(a)
10
· 블록시간 설정
블록 : 지금부터
해제
직접입력 :
:
~
:
(b)

도면4


Internet Browser
20
로그아웃 또는 블록설정 하시겠습니까?
21
22
23
Logout
Logout/Block
No

도면5


Internet Browser
ID :
pswd :
로그인
Internet Browser
블록시간입니다.
추가인증을 통해 로그인 하시거나
블록해제 하세요.

(a) (b)