(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0067120
(43) 공개일자 2017년06월15일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 12/66* (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 63/105 (2013.01)
H04L 12/66 (2013.01)
(21) 출원번호 10-2016-0018230
(22) 출원일자 2016년02월17일
심사청구일자 2016년02월17일
(30) 우선권주장
1020150173095 2015년12월07일 대한민국(KR)

(71) 출원인
숭실대학교산학협력단
서울특별시 동작구 상도로 369 (상도동)
(72) 발명자
정수환
서울특별시 동작구 상도로 369, 형남공학관 1105호 (상도동, 숭실대학교)
박정수
서울특별시 동작구 상도로 369, 형남공학관 1102호 (상도동, 숭실대학교)
(뒷면에 계속)
(74) 대리인
특허법인엠에이피에스

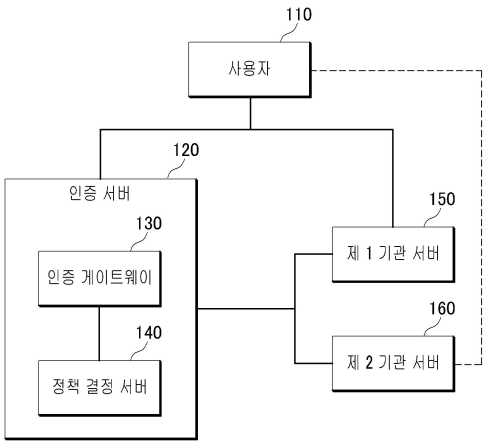
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 **인증 게이트웨이 및 인증 게이트웨이의 인증 방법**

(57) 요 약

본 발명은 통신 모듈, 사용자의 인증 및 접근을 관리하는 프로그램이 저장된 메모리 및 메모리에 저장된 프로그램을 실행하는 프로세서를 포함한다. 이때, 프로세서는 사용자가 비가입 기관 서버에 대한 접근을 요청하면, 사용자의 정보에 기초하여, 비가입 기관 서버에 대한 사용자의 인증을 수행하고, 인증을 수행한 비가입 기관 서버에 사용자의 접근을 허용한다. 그리고 사용자의 정보는 사용자의 가입 기관 서버의 인증 정보를 포함하고, 사용자의 가입 기관 서버는 사용자의 비가입 기관 서버와 상이하다.

대 표 도 - 도1



(52) CPC특허분류
H04L 63/0807 (2013.01)
H04L 63/0815 (2013.01)
H04L 63/0892 (2013.01)
H04L 9/3213 (2013.01)
(72) 발명자
김진욱
서울특별시 동작구 상도로 369, 형남공학관 1102호
(상도동, 숭실대학교)

윤권진
서울특별시 동작구 상도로 369, 형남공학관 1102호
(상도동, 숭실대학교)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711026579
부처명 미래창조과학부
연구관리전문기관 정보통신산업진흥원
연구사업명 정보통신기술인력양성
연구과제명 클라우드 환경의 스마트 기기와 서비스 보안 기술개발 및 연구 인력양성
기 여 율 1/1
주관기관 숭실대학교산학협력단
연구기간 2015.01.01 ~ 2015.12.31

명 세 서

청구범위

청구항 1

인증 게이트웨이에 있어서,

통신 모듈,

사용자의 인증 및 접근을 관리하는 프로그램이 저장된 메모리 및

상기 메모리에 저장된 프로그램을 실행하는 프로세서를 포함하되,

상기 프로세서는 상기 사용자가 비가입 기관 서버에 대한 접근을 요청하면,

상기 사용자의 정보에 기초하여, 상기 비가입 기관 서버에 대한 상기 사용자의 인증을 수행하고, 상기 인증을 수행한 비가입 기관 서버에 상기 사용자의 접근을 허용하되,

상기 사용자의 정보는 상기 사용자의 가입 기관 서버의 인증 정보를 포함하고,

상기 사용자의 가입 기관 서버는 상기 사용자의 비가입 기관 서버와 상이한, 인증 게이트웨이.

청구항 2

제 1 항에 있어서,

상기 프로세서는 상기 사용자의 가입 기관 서버로 상기 사용자의 정보를 전달하여, 상기 비가입 기관 서버에 대한 상기 사용자의 인증을 수행하는, 인증 게이트웨이.

청구항 3

제 2 항에 있어서,

상기 프로세서는 상기가입 기관 서버로부터 상기 사용자 인증에 대응하는 로그인 정보를 수신하고, 상기 수신한 로그인 정보에 기초하여, 상기 비가입 기관 서버에 대한 상기 사용자의 인증을 수행하되,

상기 로그인 정보는 상기 사용자의 식별자, 상기가입 기관 서버에서의 상기 사용자의 권한 레벨, 상기가입 기관 서버에서의 상기 사용자의 인증 시간, 상기 가입 기관의 정보 및 상기 비가입 기관 서버의 URL으로 구성된 것인, 인증 게이트웨이.

청구항 4

제 3 항에 있어서,

상기 프로세서는 정책 결정 서버를 통하여, 상기가입 기관 서버로부터 수신한 로그인 정보에 기초하여, 암호화된 토큰을 생성하고,

상기 생성된 암호화된 토큰을 상기 비가입 기관 서버로 전송하는, 인증 게이트웨이.

청구항 5

제 3 항에 있어서,

상기 비가입 기관 서버는 상기 로그인 정보에 포함된 상기 사용자의 권한 레벨에 기초하여, 상기 사용자의 접근 요청에 대응하는 상기 사용자의 권한 레벨을 설정하는 것인, 인증 게이트웨이.

청구항 6

제 1 항에 있어서,

상기 프로세서는 상기 사용자 정보에 포함된 상기 사용자의 가입 기관 서버 중 상기 사용자가 선택한 가입 기관

서버에 포함된 인증 정보에 기초하여, 상기 비가입 기관 서버에 대한 상기 사용자의 인증을 수행하는, 인증 게이트웨이.

청구항 7

제 1 항에 있어서,

상기 비가입 기관 서버 및 상기가입 기관 서버는 클라우드 서비스 서버인, 인증 게이트웨이.

청구항 8

인증 게이트웨이의 인증 방법에 있어서,

사용자가 비가입 기관 서버에 대한 접근을 요청하면, 상기 사용자의 정보에 기초하여, 상기 비가입 기관 서버에 대한 상기 사용자의 인증을 수행하는 단계; 및

상기 인증을 수행한 비가입 기관 서버에 상기 사용자의 접근을 허용하는 단계를 포함하되,

상기 사용자의 정보는 상기 사용자의 가입 기관 서버의 인증 정보를 포함하고,

상기 사용자의 가입 기관 서버는 상기 사용자의 비가입 기관 서버와 상이한, 인증 게이트웨이의 인증 방법.

청구항 9

제 8 항에 있어서,

상기 비가입 기관 서버에 대한 상기 사용자의 인증을 수행하는 단계는,

상기 사용자의 가입 기관 서버로 상기 사용자의 정보를 전달하는 단계; 및

상기 사용자의 가입 기관 서버를 통하여, 상기 비가입 기관 서버에 대한 상기 사용자의 인증을 수행하는 단계를 포함하는, 인증 게이트웨이의 인증 방법.

청구항 10

제 9 항에 있어서,

상기 비가입 기관 서버에 대한 상기 사용자의 인증을 수행하는 단계는,

상기가입 기관 서버로부터 상기 사용자 인증에 대응하는 로그인 정보를 수신하는 단계; 및

상기 수신한 로그인 정보에 기초하여, 상기 비가입 기관 서버에 대한 상기 사용자의 인증을 수행하는 단계를 포함하되,

상기 로그인 정보는 상기 사용자의 식별자, 상기가입 기관 서버에서의 상기 사용자의 권한 레벨, 상기가입 기관 서버에서의 상기 사용자의 인증 시간, 상기가입 기관의 정보 및 상기 비가입 기관 서버의 URL으로 구성된 것인, 인증 게이트웨이의 인증 방법.

청구항 11

제 8 항 내지 제 10 항 중 어느 한 항에 기재된 방법을 컴퓨터 상에서 수행하기 위한 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 인증 게이트웨이 및 인증 게이트웨이의 인증 방법에 관한 것이다.

배 경 기 술

[0002] 클라우드 서비스에서 계정 관리 솔루션은 통합 인증(signal sign-on; 이하, SSO), 통합 인증 관리(extranet access management; EAM) 및 통합 계정 관리(identity access management; IAM) 등이 있다.

[0003] 통합 인증은 한 번의 로그인으로 다양한 시스템 혹은 인터넷 서비스를 사용할 수 있게 하는 보안 솔루션이다. 통합 인증은 다수의 인증 절차를 거치지 않고도 하나의 계정만으로 다양한 시스템 및 서비스에 접속할 수 있다. 그러므로 통합 인증은 사용자의 편의성과 관리 비용을 절감할 수 있다는 장점이 있다.

[0004] 통합 인증 관리는 가트너 그룹(Gartner group)에서 정의한 용어이다. 통합 인증 관리는 통합 인증과 사용자의 인증을 세분화하여 관리한다. 통합 인증 관리는 애플리케이션 및 데이터에 대한 사용자 접근을 관리하기 위하여, 보안 정책 기반의 단일 메커니즘을 이용한다.

[0005] 이와 같이, 통합 인증 및 통합 인증 관리는 애플리케이션의 접근 권한 중심의 솔루션이다. 이에 비하여, 통합 계정 관리는 보다 포괄적으로 확장된 개념이다. 통합 계정 관리는 계정 관리 솔루션, 통합 계정 관리 및 통합 인증 관리 등의 여러 명칭으로 불리고 있다. 통합 계정 관리는 다양한 시스템에서의 식별자 및 권한 등을 통하여, 시스템 자원에 대한 사용자의 접근을 관리할 수 있다.

[0006] 이와 관련되어, 한국 공개특허공보 제10-2013-0046155호(발명의 명칭: "클라우드 컴퓨팅 서비스에서의 접근제어 시스템 ")는 퍼스널 클라우드 서비스 제공을 위한 접근 제어 및 권한 부여 정책을 개시하고 있다. 구체적으로 이 발명은 사용자 인증 서버, 복수의 클라우드 서비스 서버 및 협업 서비스 서버를 포함하고, 클라우드 서비스 서버를 통하여, 접근 토큰의 정보와 사용자 접근 제어 리스트를 비교하여 사용자의 서비스 접근을 승인한다.

발명의 내용

해결하려는 과제

[0007] 본 발명은 전술한 종래 기술의 문제점을 해결하기 위한 것으로서, 인터-클라우드 환경에서 기가입된 서버를 통하여, 비가입 서버의 인증을 수행하는 인증 게이트웨이 및 인증 게이트웨이의 인증 방법을 제공한다.

[0008] 다만, 본 실시예가 이루고자 하는 기술적 과제는 상기된 바와 같은 기술적 과제로 한정되지 않으며, 또 다른 기술적 과제들이 존재할 수 있다.

과제의 해결 수단

[0009] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 제 1 측면에 따른 인증 게이트웨이는 통신 모듈, 사용자의 인증 및 접근을 관리하는 프로그램이 저장된 메모리 및 메모리에 저장된 프로그램을 실행하는 프로세서를 포함한다. 이때, 프로세서는 사용자가 비가입 기관 서버에 대한 접근을 요청하면, 사용자의 정보에 기초하여, 비가입 기관 서버에 대한 사용자의 인증을 수행하고, 인증을 수행한 비가입 기관 서버에 사용자의 접근을 허용한다. 그리고 사용자의 정보는 사용자의 가입 기관 서버의 인증 정보를 포함하고, 사용자의 가입 기관 서버는 사용자의 비가입 기관 서버와 상이하다.

[0010] 또한, 본 발명의 제 2 측면에 따른 인증 게이트웨이의 인증 방법은 사용자가 비가입 기관 서버에 대한 접근을 요청하면, 사용자의 정보에 기초하여, 비가입 기관 서버에 대한 사용자의 인증을 수행하는 단계; 및 인증을 수행한 비가입 기관 서버에 사용자의 접근을 허용하는 단계를 포함한다. 이때, 사용자의 정보는 사용자의 가입 기관 서버의 인증 정보를 포함하고, 사용자의 가입 기관 서버는 사용자의 비가입 기관 서버와 상이하다.

발명의 효과

[0011] 본 발명은 인터-클라우드 환경에서 사용자가 기가입된 기관으로부터 수신한 최소한의 기가입된 기관의 정보 및 사용자의 정보에 기초하여, 비가입 기관의 정보에 접근할 수 있다. 그러므로 본 발명은 사용자에게 안전하고, 효율적으로 타 기관의 정보를 활용할 수 있도록 통합 계정 관리 서비스를 제공할 수 있다. 또한, 본 발명은 사용자에게 복수의 기관의 서비스를 끊김 없이 제공할 수 있다.

도면의 간단한 설명

[0012] 도 1 은 본 발명의 일 실시예에 따른 인증 시스템의 블록도이다.

도 2는 본 발명의 일 실시예에 따른 기본 인증 과정의 순서도이다.

도 3은 본 발명의 일 실시예에 따른 인증 서버의 인증 과정의 순서도이다.

도 4는 본 발명의 일 실시예에 따른 인증 게이트웨이의 블록도이다.

도 5는 본 발명의 일 실시예에 따른 인증 게이트웨이의 인증 방법의 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0013] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0014] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0015] 다음은 도 1 내지 도 4를 참조하여 본 발명의 일 실시예에 따른 인증 시스템(100)을 설명한다.

[0016] 도 1 은 본 발명의 일 실시예에 따른 인증 시스템(100)의 블록도이다.

[0017] 인증 시스템(100)은 인증 서버(120)를 통해 사용자(110)의 요청에 따라, 제 1 기관 서버(150) 및 제 2 기관 서버(160)에 대한 사용자(110) 인증을 수행한다. 그리고 인증 시스템(100)은 사용자(110) 인증에 따라, 제 1 기관 서버(150) 및 제 2 기관 서버(160)에 대한 사용자(110)의 접근을 허용한다.

[0018] 인증 서버(120)는 식별접근 관리(identity and access management) 서버일 수 있다. 또한, 인증 서버(120)는 계정 관리 솔루션 서버, 통합 계정 관리 서버 및 통합 인증 관리 서버일 수 있으나, 이에 한정된 것은 아니다.

[0019] 또한, 인증 서버(120)는 인증 게이트웨이(130) 및 정책 결정 서버(140)를 포함할 수 있다.

[0020] 인증 게이트웨이(130)는 제 1 기관 서버(150) 및 제 2 기관 서버(160)의 요청에 따라, 사용자(110)에 대한 인증을 수행한다.

[0021] 정책 결정 서버(140)는 사용자(110)의 인증 결과가 각각의 기관 서버에서 용이하게 사용될 수 있도록 미리 정해진 규칙에 따라, 사용자(110)의 인증 결과를 변환할 수 있다.

[0022] 제 1 기관 서버(150) 및 제 2 기관 서버(160)는 인터-클라우드(inter-cloud) 환경에서 서로 상이한 클라우드 서비스를 제공하는 서버이다. 이때, 제 1 기관 서버(150) 및 제 2 기관 서버(160)는 공공 클라우드 서비스 서버 또는 민간 클라우드 서비스 서버일 수 있으나, 이에 한정된 것은 아니다.

[0023] 제 1 기관 서버(150) 및 제 2 기관 서버(160)는 자체의 레거시 인증(lagacy authentication) 장치를 포함할 수 있다. 즉, 제 1 기관 서버(150) 및 제 2 기관 서버(160)는 자체의 레거시 인증 장치를 통하여, 사용자(110)의 인증을 수행할 수 있다.

[0024] 또한, 제 1 기관 서버(150) 및 제 2 기관 서버(160)는 인증 서버(120) 및 사용자(110)와 접속을 위한 에이전트(agent)를 포함할 수 있다. 그러므로 사용자(110)는 제 1 기관 서버(150) 및 제 2 기관 서버(160) 에 포함된 에이전트를 통하여, 인증 서버(120)에 접속할 수 있다.

[0025] 사용자(110)는 제 1 기관 서버(150) 및 제 2 기관 서버(160)를 사용하는 디바이스(device)일 수 있다. 예를 들어, 디바이스는 종류, 성능, 형태 등에 의해 특별히 제한되지 않고, 휴대용 단말기 또는 컴퓨터로 구현될 수 있다.

[0026] 인증 시스템(100)에서의 인증 과정은 도 2 및 도 3을 참조하여 설명한다.

[0027] 도 2는 본 발명의 일 실시예에 따른 기본 인증 과정의 순서도이다.

[0028] 도 2의 (a)와 같이, 제 1 기관 서버(150)는 사용자(110)가 기 가입한 기관 서버일 수 있다. 사용자(110)는 기 가입 기관 서버인 제 1 기관 서버(150)의 인증 정보를 이용하여, 제 1 기관 서버(150)에 정보 접근 요청 메시지를 전송할 수 있다(S200).

[0029] 제 1 기관 서버(150)는 제 1 기관 서버(150)에 포함된 레거시 인증 장치를 통하여, 사용자(110)의 제 1 기관 서버(150)의 인증 정보에 대한 기본 인증을 수행할 수 있다. 그리고 제 1 기관 서버(150)는 수행된 기본 인증에 대응하는 사용자(110)의 접근 허가 메시지를 사용자(110)에게 전송할 수 있다(S210).

[0030] 그리고 사용자(110)는 제 1 기관 서버(150)의 정보에 접근할 수 있다(S220).

[0031] 도 2의 (b)에서 제 2 기관 서버(160)는 사용자(110)가 가입하지 않은 기관의 서버일 수 있다. 이때, 사용자(110)는 비가입 기관 서버인 제 2 기관 서버(160)에 접근을 요청할 수 있다(S230).

[0032] 제 2 기관 서버(160)는 제 2 기관 서버(160)에 포함된 레거시 인증 장치를 통하여, 사용자(110)의 기본 인증을 수행할 수 있다. 이때, 사용자(110)는 제 2 기관 서버(160)에 대한 인증 정보를 보유하지 않기 때문에, 제 2 기관 서버(160)는 사용자(110)의 접근 불가 메시지를 사용자(110)에게 전송할 수 있다(S240).

[0033] 만약, 사용자(110)가 인증 서버(120)를 통하여, 비가입 서버에 대한 인증을 수행할 수 있도록 설정하였다면, 제 2 기관 서버(160)는 인증 서버(120)를 통하여, 사용자(110)의 접근을 허용할 수 있다.

[0034] 도 3은 본 발명의 일 실시예에 따른 인증 서버(120)의 인증 과정의 순서도이다.

[0035] 구체적으로 사용자(110)가 비가입 기관 서버인 제 2 기관 서버(160)에 접근을 요청하면(S300), 제 2 기관 서버(160)는 인증 서버(120)의 인증 게이트웨이(130)를 통하여, 사용자(110)에 대한 인증을 요청한다(S310).

[0036] 이때, 제 2 기관 서버(160)는 인증 게이트웨이(130)에 쿠키(cookie) 값 및 제 2 기관 서버(160)의 정보를 전달할 수 있다. 쿠키 값은 제 2 기관 서버(160)에 접근을 요청한 사용자(110)를 식별하기 위한 정보를 포함하도록 생성된 것이다. 또한, 제 2 기관 서버(160)의 정보는 사용자(110)에 대한 인증이 완료된 이후, 사용자(110) 다시 제 2 기관 서버(160)로 접근하기 위한 URL(uniform resource locator) 등의 정보를 포함할 수 있다.

[0037] 인증 게이트웨이(130)는 제 2 기관 서버(160)의 접근 요청에 따라, 제 2 기관 서버(160)로부터 수신한 쿠키 값에 포함된 사용자(110)의 정보에 기초하여, 사용자(110) 인증을 수행한다.

[0038] 이때, 사용자(110)의 정보는 사용자(110)의 가입 기관 서버의 인증 정보를 포함한다. 즉, 인증 게이트웨이(130)는 사용자(110)의 정보에 포함된 사용자(110)의 가입 기관 서버 중 제 1 기관 서버(150)에 대한 인증 정보를 통하여, 인증을 수행할 수 있다.

[0039] 또한, 제 2 기관 서버(160)의 인증을 위하여 선택된, 제 1 기관 서버(150)는 사용자(110)가 인증 시스템(100)에 미리 설정한 것일 수 있다. 또한, 제 1 기관 서버(150)는 제 2 기관 서버(160)에 인증을 요청할 때, 사용자(110)가 선택한 가입 기관 서버일 수 있다.

[0040] 구체적으로 인증 게이트웨이(130)는 사용자(110)의 제 1 기관 서버(150)에 대한 인증 정보를 제 1 기관 서버(150)에 전달할 수 있다. 그리고 인증 게이트웨이(130)는 제 1 기관 서버(150)에 사용자 인증을 요청할 수 있다(S320). 이때, 인증 게이트웨이(130)가 전달한 제 1 기관 서버(150)의 인증 정보는 사용자(110)의 식별자 및 제 2 기관 서버(160)의 정보를 포함할 수 있다. 예를 들어, 제 2 기관 서버(160)의 정보는 제 2 기관 서버(160)의 URL 정보가 될 수 있다.

[0041] 사용자(110)의 제 1 기관 서버(150)에 대한 인증 정보를 수신한 제 1 기관 서버(150)는 사용자(110)의 인증 정보에 기초하여, 사용자(110)의 인증을 수행할 수 있다. 그리고 제 1 기관 서버(150)는 사용자(110)의 인증 결과 및 제 2 기관 서버(160)에서 사용자(110)의 인증을 위하여 필요한 최소한의 사용자(110)의 로그인 정보를 인증 서버(120)로 전송할 수 있다(S330).

[0042] 예를 들어, 제 1 기관 서버(150)는 사용자(110)의 식별자, 제 1 기관 서버(150)에서의 사용자(110)의 권한 레벨, 제 1 기관 서버(150) 에서의 사용자의 인증 시간, 제 1 기관 서버(150)에 대한 정보 및 제 2 기관 서버(160)의 URL으로 구성된 사용자(110)의 로그인 정보를 생성할 수 있다. 이때, 제 1 기관 서버(150)에서의 사용자(110)의 인증 시간은 제 2 기관 서버(160)에 대한 인증을 위하여 제 1 기관 서버(150)에 로그인 한 시간이 될 수 있다.

[0043] 인증 게이트웨이(130)는 사용자(110)의 인증 결과 및 사용자(110)의 로그인 정보를 제 1 기관 서버(150)로부터 수신하여, 제 2 기관 서버(160)에 전송할 수 있다(S340).

[0044] 이때, 제 1 기관 서버(150)의 로그인 정보 및 제 2 기관 서버(160)의 로그인 정보의 형식은 서로 상이할 수 있다. 그러므로 인증 게이트웨이(130)는 인증 서버(120)에 포함된 정책 결정 서버(140)를 통하여 기관 서버 별로 정의된 접속 규약(access agreement)에 따라, 기관 서버에 대응되는 로그인 정보를 생성할 수 있다. 이때, 인증 게이트웨이(130)는 접속 규약에 포함된 미리 정해진 형식에 따라, XML(extensible markup language) 및 JSON(JavaScript object notation)를 이용하여 로그인 정보를 생성할 수 있으나, 이에 한정된 것은 아니다.

[0045] 예를 들어, 미리 정해진 형식이 JSON인 경우, 정책 결정 서버(140)는 사용자(110)의 로그인 정보를 JWT(JSON web token)로 생성할 수 있다. 그리고 정책 결정 서버(140)는 생성된 로그인 정보를 포함하는 JWT를 암호화하여, 인증 서버(120)의 인증 게이트웨이(130)로 전송할 수 있다.

[0046] 인증 게이트웨이(130)는 암호화된 JWT를 사용자(110)의 로그인 정보로 제 2 기관 서버(160)에 전송할 수 있다.

[0047] 제 2 기관 서버(160)는 인증 게이트웨이(130)로부터 수신한 사용자(110)의 JWT에 포함된 로그인 정보에 기초하여, 사용자(110)의 접근을 허가할 수 있다(S350).

[0048] 이때, 제 2 기관 서버(160)는 사용자(110)의 로그인 정보에 포함된 사용자(110)의 권한 레벨에 기초하여, 제 2 기관 서버(160)에 대한 접근 레벨을 설정할 수 있다. 그리고 제 2 기관 서버(160)는 사용자(110)에게 접근 허가 메시지를 전송할 수 있다.

[0049] 그리고 사용자(110)는 제 2 기관 서버(160)의 접근 허가에 따라, 제 2 기관 서버(160)의 정보에 접근할 수 있다(S360). 사용자(110)가 제 2 기관 서버(160)에 접근을 시도하면, 제 2 기관 서버(160)는 인증 게이트웨이(130)로부터 수신한 암호화된 사용자(110)의 로그인 정보에 기초하여, 사용자(110)의 인증을 수행할 수 있다. 그리고 제 2 기관 서버(160)는 사용자(110)의 로그인 정보에 기초하여, 사용자(110)에게 제공하는 정보 및 정보에 대한 권한 레벨 등을 설정할 수 있다.

[0050] 이와 같이, 사용자(110)는 인증 시스템(100)을 통하여, 기가입 기관 서버인 제 1 기관 서버(150)의 사용자 정보에 기초하여, 비가입 기관 서버인 제 2 기관 서버(160)에 접근할 수 있다.

[0051] 또한, 제 1 기관 서버(150)는 사용자(110)가 가입하지 않은 제 2 기관 서버(160)에 사용자(110)에 대한 최소한의 정보만을 제공할 수 있다. 그러므로 사용자(110)는 안전하고, 효율적으로 제 2 기관 서버(160)의 정보에 접근할 수 있다. 또한, 제 2 기관 서버(160)로 최소한의 정보만을 제공하므로, 제 2 기관 서버(160)가 사용자(110)의 정보를 악의적으로 사용하는 것을 미연에 방지할 수 있다.

[0052] 다음은 도 4를 참조하여, 본 발명의 일 실시예에 따른 인증 게이트웨이(130)를 설명한다.

[0053] 도 4는 본 발명의 일 실시예에 따른 인증 게이트웨이(130)의 블록도이다.

[0054] 인증 게이트웨이(130)는 사용자(110)의 요청에 따라, 복수의 기관 서버에 대한 인증을 수행한다. 이때, 인증 게이트웨이(130)는 통신 모듈(400), 메모리(410) 및 프로세서(420)를 포함한다.

[0055] 통신 모듈(400)은 복수의 기관 서버와 통신을 수행한다. 이때, 통신 모듈(400)은 복수의 기관 서버에 포함된 에이전트를 통하여, 사용자(110)와 통신을 수행할 수 있다.

[0056] 메모리(410)는 사용자(110)의 인증 및 접근을 관리하는 프로그램을 저장한다. 이때, 메모리(410)는 전원이 공급되지 않아도 저장된 정보를 계속 유지하는 비휘발성 저장장치 및 저장된 정보를 유지하기 위하여 전력이 필요한 휘발성 저장장치를 통칭하는 것이다.

[0057] 프로세서(420)는 사용자(110)가 비가입 기관 서버에 대한 접근을 요청하면, 사용자 정보에 기초하여, 사용자(110) 인증을 수행한다. 이때, 사용자 정보는 사용자(110)가 가입 기관 서버의 인증 정보를 포함한다.

[0058] 이때, 본 발명의 일 실시예에 따른 비가입 기관 서버 및 가입 기관 서버는 클라우드 서비스 서버일 수 있다.

[0059] 가입 기관 서버는 사용자(110)의 로그인 이력이 존재하거나, 사용자(110)가 가입한 기관 서버이다.

[0060] 또한, 비가입 기관 서버는 사용자(110)의 사용자(110)의 정보 또는 사용자(110)의 로그인 정보를 보유하지 않은, 사용자(110)가 가입하지 않은 기관 서버이다. 이때, 비가입 기관 서버 및 가입 서버는 서로 상이할 수 있다.

[0061] 이때, 가입 기관 서버는 사용자(110)가 가입한 기관 서버 중 사용자(110)가 선택한 기관 서버일 수 있다. 즉, 프로세서(420)는 사용자(110)의 비가입 기관 서버에 대한 접근 요청과 함께, 사용자(110)가 선택한 가입 기관 서버의 정보를 수신할 수 있다.

[0062] 프로세서(420)는 통신 모듈(400)을 통하여, 사용자(110)가 선택한 가입 기관 서버로 사용자 정보를 전달할 수 있다. 즉, 프로세서(420)는 사용자(110)가 선택한 가입 기관 서버를 통하여, 사용자(110)의 인증을 수행할 수 있다.

[0063] 가입 기관 서버가 사용자 정보를 인증하고, 인증에 대응하는 사용자(110)의 로그인 정보를 전송하면, 프로세서

(420)는 통신 모듈(400)을 통해, 사용자(110)의 로그인 정보를 수신할 수 있다.

[0064] 이때, 로그인 정보는 사용자(110)의 식별자, 가입 기관 서버에서의 사용자(110)의 권한 레벨, 가입 기관 서버에서의 사용자(110)의 인증 시간, 가입 기관의 정보 및 비가입 기관 서버의 URL으로 구성된 것일 수 있다.

[0065] 프로세서(420)는 정책 결정 서버(140)를 통하여, 가입 기관 서버로부터 수신한 로그인 정보에 기초하여, 암호화된 토큰을 생성할 수 있다. 그리고 프로세서(420)는 생성된 암호화된 토큰을 비가입 기관 서버로 전송할 수 있다.

[0066] 암호화된 토큰을 수신한 비가입 기관 서버는 암호화된 토큰을 이용하여, 사용자(110)의 인증을 수행할 수 있다. 이때, 비가입 기관 서버는 암호화된 토큰에 포함된 사용자(110)의 레벨에 기초하여, 비가입 기관 서버 상에서의 사용자(110) 권한 레벨을 설정할 수 있다.

[0067] 그리고 프로세서(420)는 인증을 수행한 비가입 기관 서버에 대한 사용자(110)의 접근을 허용한다.

[0068] 사용자(110)는 접근이 허용된 비가입 기관 서버에 접속하여, 사용자(110)의 권한에 따라, 정보를 열람할 수 있다.

[0069] 다음은 도 5를 참조하여, 본 발명의 일 실시예에 따른 인증 게이트웨이(130)의 인증 방법을 설명한다.

[0070] 도 5는 본 발명의 일 실시예에 따른 인증 게이트웨이(130)의 인증 방법의 순서도이다.

[0071] 사용자(110)가 비가입 기관 서버에 대한 접근을 요청하면(S500), 인증 게이트웨이(130)는 사용자(110)의 정보에 기초하여, 비가입 기관 서버에 대한 사용자(110)의 인증을 수행한다. 이때, 사용자 정보는 사용자(110)의 가입 기관 서버의 인증 정보를 포함한다. 그리고 사용자(110)의 가입 기관 서버는 사용자(110)의 비가입 기관 서버와 상이하다.

[0072] 구체적으로 인증 게이트웨이(130)는 사용자(110)가 이미 가입한 가입 기관 서버로 사용자(110)의 정보를 전달할 수 있다(S510).

[0073] 인증 게이트웨이(130)는 사용자(110)의 가입 기관 서버를 통하여, 비가입 기관 서버에 대한 사용자(110)의 인증을 수행할 수 있다(S520).

[0074] 이때, 인증 게이트웨이(130)는 비가입 기관 서버에 대한 사용자(110)의 인증을 수행하기 위하여, 가입 기관 서버로부터 사용자 인증에 대응하는 로그인 정보를 수신할 수 있다. 사용자(110)의 로그인 정보는 사용자(110)의 식별자, 가입 기관 서버에서의 사용자(110)의 권한 레벨, 가입 기관 서버에서의 사용자(110)의 인증 시간, 가입 기관의 정보 및 비가입 기관 서버의 URL으로 구성된 것일 수 있다.

[0075] 그리고 인증 게이트웨이(130)는 가입 기관 서버로부터 수신한 사용자(110)의 로그인 정보에 기초하여, 비가입 기관 서버에 대한 사용자(110)의 인증을 수행할 수 있다.

[0076] 사용자(110)의 인증에 성공하면, 인증 게이트웨이(130)는 인증을 수행한 비가입 기관 서버에 사용자(110)의 접근을 허용한다(S530).

[0077] 본 발명의 일 실시예에 따른 인증 게이트웨이(130) 및 인증 게이트웨이(130)의 인증 방법은 인터 클라우드 환경에서 사용자(110)가 최소한의 기가입된 기관의 정보 및 사용자(110)의 정보에 기초하여, 비가입 기관의 정보에 접근할 수 있다.

[0078] 그러므로 인증 게이트웨이(130) 및 인증 게이트웨이(130)의 인증 방법은 사용자(110)에게 안전하고, 효율적으로 타 기관의 정보를 활용할 수 있도록 통합 계정 관리 서비스를 제공할 수 있다. 인증 게이트웨이(130) 및 인증 게이트웨이(130)의 인증 방법은 사용자에게 복수의 기관의 서비스를 끊김 없이 제공할 수 있다.

[0079] 본 발명의 일 실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다. 통신 매체는 전형적으로 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 메커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.

[0080] 본 발명의 방법 및 시스템은 특정 실시예와 관련하여 설명되었지만, 그것들의 구성 요소 또는 동작의 일부 또는 전부는 범용 하드웨어 아키텍처를 갖는 컴퓨터 시스템을 사용하여 구현될 수 있다.

[0081] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0082] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

[0083] 100: 인증 시스템

110: 사용자

120: 인증 서버

130: 인증 게이트웨이

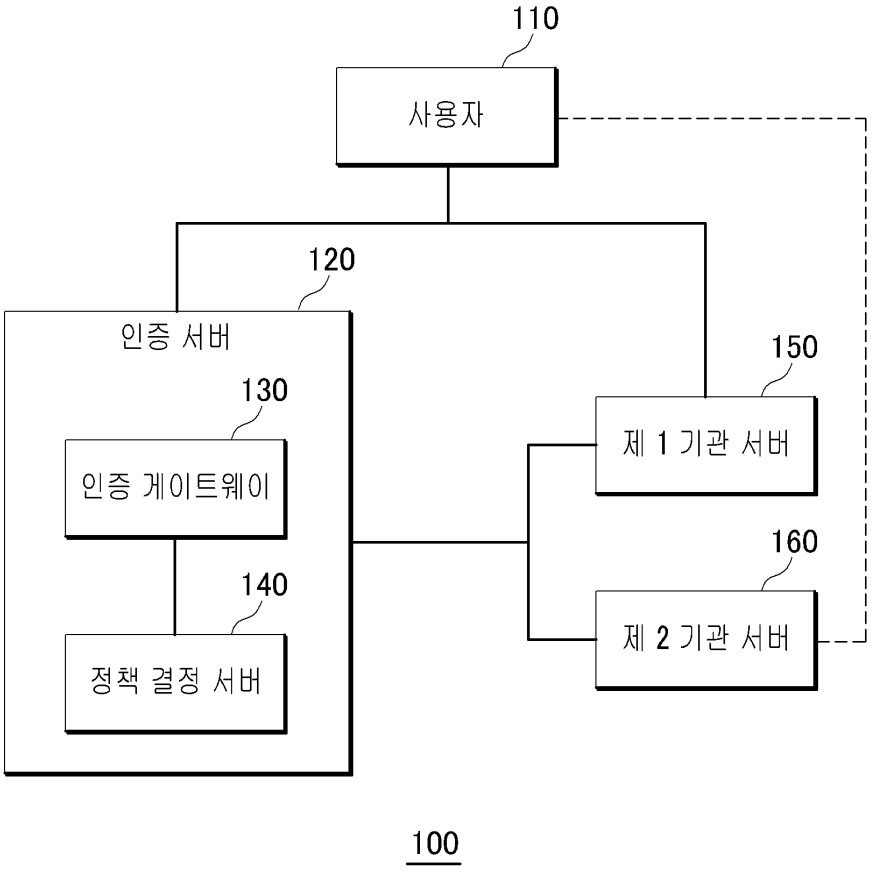
140: 정책 결정 서버

150: 제 1 기관 서버

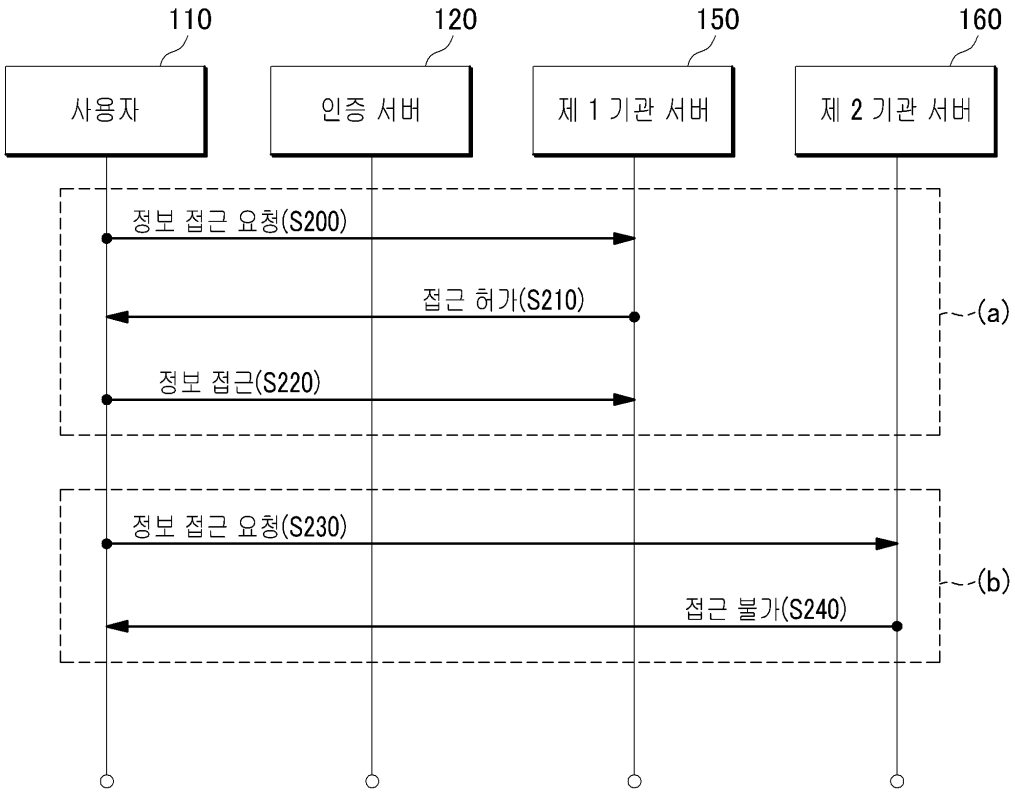
160: 제 2 기관 서버

도면

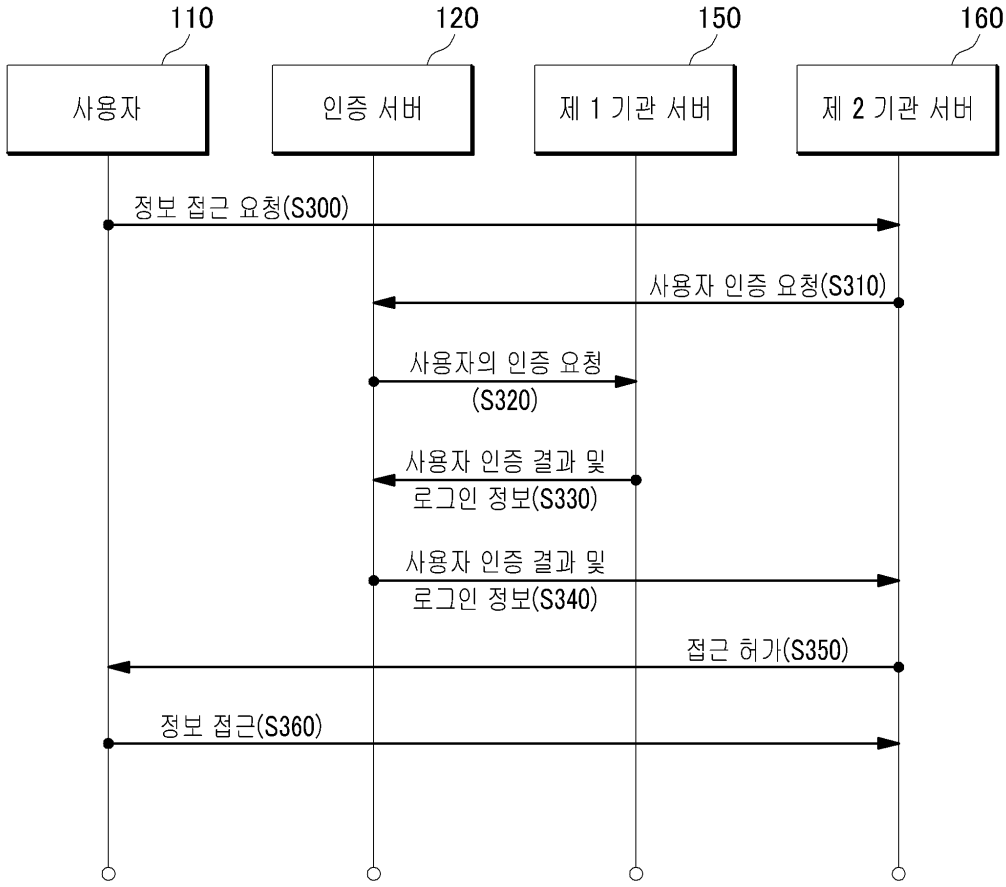
도면1


110
사용자
120
인증 서버
130
인증 게이트웨이
140
정책 결정 서버
150
제 1 기관 서버
160
제 2 기관 서버
100

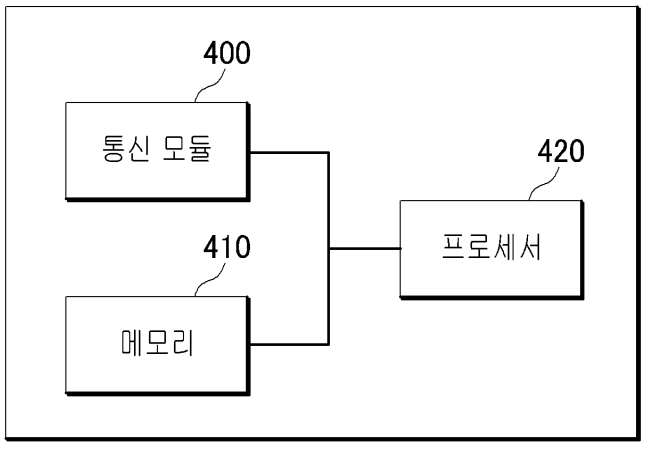
도면2


110
120
150
160
사용자
인증 서버
제 1 기관 서버
제 2 기관 서버
정보 접근 요청(S200)
접근 허가(S210)
정보 접근(S220)
(a)
정보 접근 요청(S230)
접근 불가(S240)
(b)

도면3

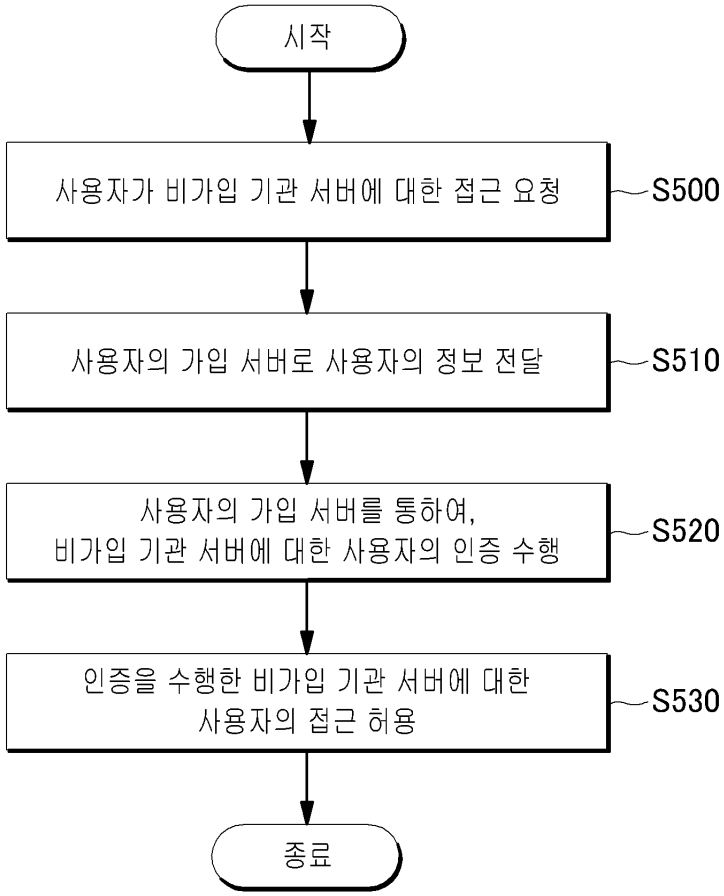

110
120
150
160
사용자
인증 서버
제 1 기관 서버
제 2 기관 서버
정보 접근 요청(S300)
사용자 인증 요청(S310)
사용자의 인증 요청
(S320)
사용자 인증 결과 및
로그인 정보(S330)
사용자 인증 결과 및
로그인 정보(S340)
접근 허가(S350)
정보 접근(S360)

도면4


400
통신 모듈
420
프로세서
410
메모리

130

도면5


시작
사용자가 비가입 기관 서버에 대한 접근 요청
S500
사용자의 가입 서버로 사용자의 정보 전달
S510
사용자의 가입 서버를 통하여,
비가입 기관 서버에 대한 사용자의 인증 수행
S520
인증을 수행한 비가입 기관 서버에 대한
사용자의 접근 허용
S530
종료