(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0126727
(43) 공개일자 2022년09월16일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01)
(52) CPC특허분류
H04L 63/0876 (2013.01)
H04L 63/0421 (2013.01)
(21) 출원번호 10-2022-7023967
(22) 출원일자(국제) 2020년12월07일
심사청구일자 2022년08월09일
(85) 번역문제출일자 2022년07월12일
(86) 국제출원번호 PCT/EP2020/084951
(87) 국제공개번호 WO 2021/116046
국제공개일자 2021년06월17일
(30) 우선권주장
19215850.9 2019년12월12일
유럽특허청(EPO)(EP)

(71) 출원인
노센도 게엠바하
독일 47198 뒤스부르크 쾨닉스트라세 34
(72) 발명자
클란제트, 세바스찬
독일 46519 알펜 퓌어스트-벤타임-슈트라세50
헤니히, 레네
독일 42115 부페어탈 돌렌벡27
스티븐스, 필립
독일 46519 알펜 노이에 슈트라세 26
(74) 대리인
특허법인 정안

전체 청구항 수 : 총 20 항

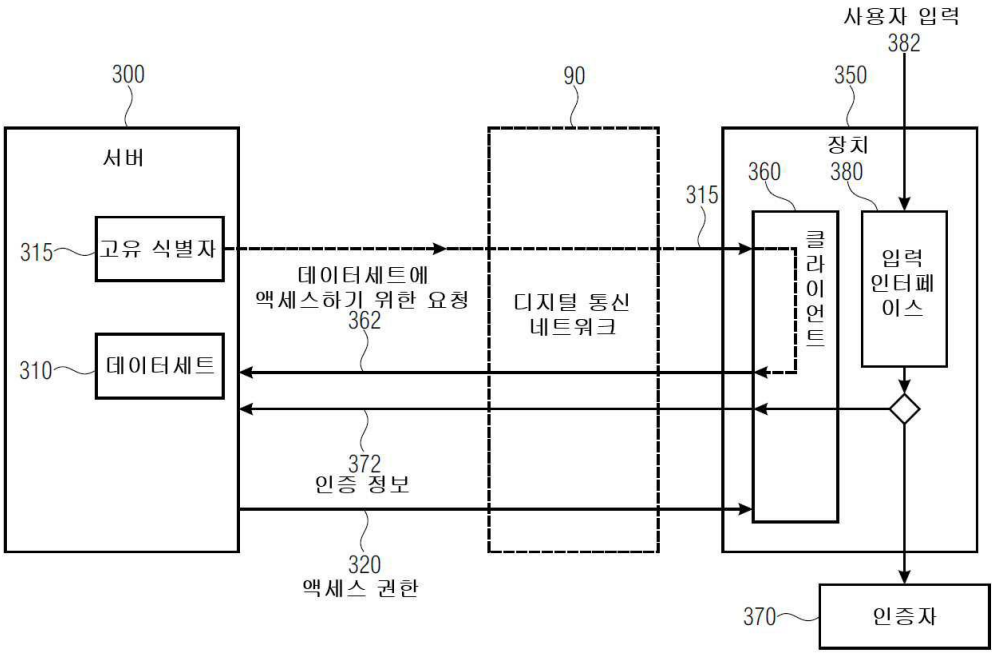
(54) 발명의 명칭 **디지털 통신 네트워크를 통한 하나 이상의 데이터 세트의 획득 및 제공**

(57) 요 약

디지털 통신 네트워크를 통해 하나 이상의 데이터세트를 제공하기 위한 서버는: 고유 식별자를 식별된 데이터세트와 연관시키고 - 상기 고유 식별자는 디지털 통신 네트워크를 통해 식별된 데이터세트에 액세스하기 위한 네트워크 주소를 나타내고, 고유 식별자는 식별된 데이터세트에 고유함- ; 고유 식별자를 통해 서버에 접근을 요청하

(뒷면에 계속)

대 표 도 - 도3



는 클라이언트의 인증자에 의해 제공된 인증 정보를 검증하고; 및 인증 정보가 인증자를 등록된 사용자와 연관된다고 식별하는 경우 클라이언트에 하나 이상의 데이터세트에 대한 액세스 권한을 선택적으로 제공하도록 구성된다. 디지털 통신 네트워크를 통해 데이터세트를 획득하기 위한 장치는 데이터세트의 고유 식별자를 획득하도록 구성되며, 고유 식별자는 디지털 통신망을 통해 데이터세트에 액세스하기 위한 네트워크 주소를 나타내며, 여기서 고유 식별자는 데이터세트에 고유하다. 상기 장치는 데이터세트를 제공하는 서버에 데이터세트에 액세스하기 위한 요청을 전송하기 위해 고유 식별자를 사용하도록 구성된 클라이언트를 포함한다. 클라이언트는 서버에 대해 클라이언트를 인증하기 위한 인증자의 인증 정보를 서버에 제공하도록 구성되며, 인증자는 등록된 사용자와 연관된다.

(52) CPC특허분류
H04L 63/062 (2013.01)
H04L 63/0823 (2013.01)
H04L 63/0861 (2013.01)

명 세 서

청구범위

청구항 1

디지털 통신 네트워크(90)를 통해 하나 이상의 데이터세트를 제공하기 위한 서버(100;200;300)에 있어서, 상기 서버(100;200;300)는:

고유 식별자(115;215;315)를 식별된 데이터세트(110;210;310)와 연관시키고 - 상기 고유 식별자(115;215;315)는 상기 디지털 통신 네트워크(90)를 통해 상기 식별된 데이터세트(110;210;310)에 액세스하기 위한 네트워크 주소를 나타내고, 상기 고유 식별자(115;215;315)는 상기 식별된 데이터세트(110;210;310)에 고유함 - ;

상기 고유 식별자(115;215;315)를 통해 상기 서버(100;200;300)에 대한 액세스를 요청하는 클라이언트(160;260;360)의 인증자(170;270;370)에 의해 제공되는 인증 정보(172;272;372)를 검증하고; 및

상기 인증 정보(172;272;372)가 상기 인증자(170;270;370)를 등록된 사용자와 관련된다고 식별한 경우, 하나 이상의 데이터세트에 대한 액세스 권한을 상기 클라이언트(160;260;360)에게 선택적으로 제공하도록

구성되는, 서버(100;200;300).

청구항 2

제 1 항에 있어서,

상기 서버(100;200;300)는 상기 고유 식별자(115;215;315)를 통해 상기 식별된 데이터세트(110;210;310)에 대한 액세스를 요청하는 상기 클라이언트(160;260;360)의 상기 인증자(170;270;370)에 의해 제공되는 상기 인증 정보(172;272;372)를 검증하도록 구성되고;

상기 서버(100;200;300)는 상기 식별된 데이터세트(110;210;310)에 대한 액세스 권한을 상기 클라이언트(160;260;360)에게 선택적으로 제공하도록 구성되고;

상기 식별된 데이터세트(110;210;310)에 대한 상기 액세스 권한은 상기 인증자(170;270;370)와 관련된 상기 등록된 사용자에 고유한, 서버(100;200;300).

청구항 3

디지털 통신 네트워크(90)를 통해 데이터세트(110;210;310)를 제공하기 위한 서버(100;200;300)에 있어서, 상기 서버(100;200;300)는:

고유 식별자(115;215;315)를 데이터세트(110;210;310)와 연관시키는 단계 - 상기 고유 식별자(115;215;315)는 디지털 통신 네트워크(90)를 통해 상기 데이터세트(110;210;310)에 액세스하기 위한 네트워크 주소를 나타내고, 상기 고유 식별자(115;215;315)는 상기 데이터세트(110;210;310)에 고유함 - ;

상기 고유 식별자(115;215;315)를 통해 상기 데이터세트(110;210;310)에 대한 액세스를 요청하는 클라이언트(160;260;360)의 인증자(170;270;370)에 의해 제공되는 인증 정보(172;272;372)를 검증하는 단계; 및

상기 클라이언트(160;260;360)에게 상기 데이터세트(110;210;310)에 대한 액세스 권한을 선택적으로 제공하는 단계 - 상기 액세스 권한은 상기 인증자(170;270;370)와 연관되는 등록된 사용자에게 고유함 -

를 포함하는, 서버(100;200;300).

청구항 4

선행 항들 중 어느 한 항에 있어서,

상기 서버(100;200;300)는 상기 인증자(170;270;370)를 상기 등록된 사용자를 식별하는 신원 정보와 연관시킴으로써 상기 인증자(170;270;370)를 등록하도록 구성되는, 서버(100;200;300).

청구항 5

선행 항들 중 어느 한 항에 있어서, 상기 서버(100;200;300)는 액세스 정보를 포함하고, 상기 액세스 정보는 상기 등록된 사용자를 상기 식별된 데이터세트(110;210;310)에 대한 상기 액세스 권한과 연관시키는, 서버(100;200;300).

청구항 6

선행 항들 중 어느 한 항에 있어서,

상기 서버(100;200;300)는 상기 서버(100; 200; 300)에 대한 액세스를 요청하는 상기 클라이언트(160;260;360)를 상기 식별된 데이터세트(110;210;310)에 연결하도록 구성되는, 서버(100;200;300).

청구항 7

선행 항들 중 어느 한 항에 있어서,

상기 서버(100;200;300)는 상기 인증 정보(172;272;372)를 검증하기 위해 암호화 시스템을 사용하도록 구성되고,

상기 서버(100;200;300)는 상기 인증자(170;270;370)를 상기 인증자(170;270;370)에 고유한 암호화 키와 연관시키도록 구성되는, 서버(100;200;300).

청구항 8

디지털 통신 네트워크(90)를 통해 데이터세트(110;210;310)를 획득하기 위한 장치(150;250;350)에 있어서,

상기 장치는 상기 데이터세트(110;210;310)의 고유 식별자(115;215;315)를 획득하도록 구성되고, 상기 고유 식별자(115;215;315)는 상기 디지털 통신 네트워크(90)를 통해 상기 데이터세트(110;210;310)에 액세스하기 위한 네트워크 주소를 나타내며, 상기 고유 식별자(115;215;315)는 상기 데이터세트(110;210;310)에 고유하며,

상기 장치는 상기 데이터세트(110;210;310)에 액세스하기 위한 요청을 상기 데이터세트(110;210;310)를 제공하는 서버(100;200;300)에 전송하기 위해 상기 고유 식별자(115;215;315)를 사용하도록 구성된 클라이언트(160;260;360)를 포함하고,

상기 클라이언트(160;260;360)는 상기 서버(100;200;300)에 대해 상기 클라이언트(160;260;360)를 인증하기 위한 인증자(170;270;370)의 인증 정보(172;272;372)를 상기 서버(100;200;300)에 제공하도록 구성되고, 상기 인증자(170;270;370)는 등록된 사용자와 연관되는, 장치(150;250;350).

청구항 9

제 8 항에 있어서, 상기 장치는 상기 인증자(170;270;370)를 포함하는, 장치(150;250;350).

청구항 10

제 8 항에 있어서, 상기 장치는 디지털 인터페이스를 통해 상기 인증자(170;270;370)에 대한 액세스를 갖도록 구성되는, 장치(150;250;350).

청구항 11

제 8 항 내지 제 10 항 중 어느 한 항에 있어서, 상기 장치는 사용자 입력(382)을 수신하기 위한 입력 인터페이스(380)를 포함하고,

상기 장치는 상기 사용자 입력(382)에 의존하여 상기 인증 정보(172;272;372)를 상기 서버(100;200;300)에 선택적으로 제공하도록 구성되는, 장치(150;250;350).

청구항 12

제 8 항 내지 제 11 항 중 어느 한 항에 있어서, 상기 장치는 사용자에 대한 생체 정보를 획득하도록 구성되고,

상기 장치는 상기 생체 정보가 상기 사용자를 상기 인증자(170;270;370)와 연관된다고 식별하는 경우, 상기 인증 정보(172;272;372)를 상기 서버(100;200;300)에 선택적으로 제공하도록 구성되는, 장치(150;250;350).

청구항 13

제 8 항 내지 제 12 항 중 어느 한 항에 있어서, 상기 장치는 상기 고유 식별자(115;215;315)를 나타내는 그래픽 패턴으로부터 상기 고유 식별자(115;215;315)를 검색하도록 구성되는, 장치(150;250;350).

청구항 14

제 8 항 내지 제 13 항 중 어느 한 항에 있어서,

상기 인증자(170;270;370)는 암호화 키를 포함하고,

상기 인증자(170;270;370)는 상기 인증 정보(172;272;372)를 상기 서버(100;200;300)에 제공하기 위해 상기 암호화 키를 사용하도록 구성되는, 장치(150;250;350).

청구항 15

제 8 항 내지 제 14 항 중 어느 한 항에 있어서, 상기 인증 정보(172;272;372)는 상기 서버(100;200;300)에 대해 상기 등록된 사용자의 익명 인증을 허용하는, 장치(150;250;350).

청구항 16

디지털 통신 네트워크(90)를 통해 하나 이상의 데이터세트를 제공하기 위한 서버(100;200;300)에 있어서, 상기 서버(100;200;300)는:

고유 식별자(115;215;315)를 식별된 데이터세트(110;210;310)와 연관시키고 - 상기 고유 식별자(115;215;315)는 상기 디지털 통신 네트워크(90)를 통해 상기 식별된 데이터세트(110;210;310)에 액세스하기 위한 네트워크 주소를 나타내고, 상기 고유 식별자(115;215;315)는 상기 식별된 데이터세트(110;210;310)에 고유함 - ;

상기 고유 식별자(115;215;315)를 통해 상기 서버(100;200;300)에 대한 액세스를 요청하는 클라이언트(160;260;360)의 인증자(170;270;370)에 의해 제공되는 인증 정보(172;272;372)를 검증하고; 및

상기 인증 정보(172;272;372)가 상기 인증자(170;270;370)를 등록된 사용자와 관련된다고 식별한 경우, 하나 이상의 데이터세트에 대한 액세스 권한을 상기 클라이언트(160;260;360)에게 선택적으로 제공하도록

구성되고,

상기 인증 정보는 상기 등록된 사용자의 사용자 이름, 비밀번호 및 개인 데이터를 포함하지 않으므로, 상기 인증 정보는 상기 서버에 대한 상기 등록된 사용자의 익명 인증을 허용하는, 서버(100;200;300).

청구항 17

제 16 항에 있어서, 상기 인증 정보는 상기 인증자를 사용하여 생성된 암호화된 메시지를 포함하고,

상기 인증자는 개인 데이터 또는 상기 인증자와 관련된 상기 등록된 사용자의 개인 데이터에 대한 힌트를 포함하지 않는 정보로 표시되는, 서버(100;200;300).

청구항 18

디지털 통신 네트워크(90)를 통해 하나 이상의 데이터세트를 제공하는 방법(500)에 있어서, 상기 방법(500)은:

고유 식별자(115;215;315)를 식별된 데이터세트(110;210;310)와 연관시키는 단계(501) - 상기 고유 식별자(115;215;315)는 상기 디지털 통신 네트워크(90)를 통해 상기 식별된 데이터세트(110;210;310)에 액세스하기 위한 네트워크 주소를 나타내고, 상기 고유 식별자(115;215;315)는 상기 식별된 데이터세트에 고유함 - ;

상기 고유 식별자(115;215;315)를 통해 하나 이상의 데이터세트에 대한 액세스를 요청하는 클라이언트(160;260;360)의 인증자(170;270;370)에 의해 제공되는 인증 정보(172;272;372)를 검증하는 단계(502); 및

상기 인증 정보(172;272;372)가 상기 인증자(170;270;370)를 등록된 사용자와 관련된다고 식별한 경우, 하나 이상의 데이터세트에 대한 액세스 권한을 상기 클라이언트(160;260;360)에게 선택적으로 제공하는 단계(503)

를 포함하는, 방법(500).

청구항 19

디지털 통신 네트워크(90)를 통해 데이터세트(110;210;310)를 획득하기 위한 방법(600)에 있어서,

데이터세트(110;210;310)의 고유 식별자(115;215;315)를 획득하는 단계(601) - 상기 고유 식별자(115;215;315)는 상기 디지털 통신 네트워크(90)를 통해 상기 데이터세트(110;210;310)에 액세스하기 위한 네트워크 주소를 나타내고, 상기 고유 식별자(115;215;315)는 상기 데이터세트(110;210;310)에 고유함 - ,

상기 데이터세트(110;210;310)를 호스팅하는 서버(100;200;300)에 액세스하기 위한 요청을 전송하기 위해 상기 고유 식별자(115;215;315)를 사용하는 단계(602), 및

상기 서버(100; 200; 300)에 대하여 상기 클라이언트(160;260;360)를 인증하기 위한 인증자(170;270;370)의 인증 정보(172;272;372)를 상기 서버(100;200;300)에 제공하는 단계(603) - 상기 인증자(170;270;370)는 등록된 사용자와 연관됨 -

를 포함하는, 방법(600).

청구항 20

컴퓨터 또는 신호 프로세서에서 실행될 때 제 18 항 또는 제 19 항의 방법 중 어느 하나를 구현하기 위한 컴퓨터 프로그램.

발명의 설명

기 술 분 야

[0001] 본 발명에 따른 실시 예는 디지털 통신 네트워크를 통해 데이터를 전송하는 분야에 관한 것이다. 보다 구체적으로, 본 발명의 실시 예는 디지털 통신 네트워크를 통해 하나 이상의 데이터세트를 제공하기 위한 서버 및 방법에 관한 것이다. 본 발명의 추가 실시 예는 디지털 통신 네트워크를 통해 데이터세트를 획득하기 위한 장치 및 방법에 관한 것이다. 추가 실시 예는 인터넷, 인트라넷 등과 같은 디지털 통신 네트워크를 통해 분석된 데이터에 대한 정보를 안전하게 검색하기 위한 방법 및 시스템에 관한 것이다.

[0002] 본 발명의 추가 실시 예는 인터넷을 통해 분석된 데이터에 대한 액세스를 안전하게 허가하기 위한 컴퓨터 방법 및 시스템에 관한 것이다.

배 경 기 술

[0003] 정보, 예를 들어, 분석된 데이터의 정보를 제공하거나 전송하는 것은 프린트아웃 보고서를 통한 전통적인 방식과 같이 별개의 방식으로 발생할 수 있다. 이렇게 하면 a) 수신자가 적절한 시간에 적절한 보안 기능과 적절한 편의를 갖추고, 메시지를 수신한다는 것을 보장하기 쉽다. 대부분의 경우 등기 우편을 사용하는 기존 우편 배달 시스템이 이러한 요구 사항을 충족하는 데 사용된다. 예를 들어, 공증인 등록 서신 또는 분석 보고서/진단 결과가 고객/환자에게 발송된다.

[0004] 그러나 다르게 오늘날 정보는 월드 와이드 웹/인터넷을 활용하여 전세계로 전송된다. 여기에 많은 편의성이 작용한다. 인터넷 또는 일반적으로 디지털 통신 네트워크를 사용하여 거의 모든 사람에게 빠르고 쉽게, 그리고 요청자의 위치에 관계없이 정보에 대한 액세스를 제공 및/또는 생성할 수 있다. 인터넷은 전세계 서버 네트워크를 사용하여 모든 종류의 정보를 클라이언트에 보낼 수 있다. 오늘날 인터넷은 소셜 네트워킹, 금융 거래 처리 또는 산업 기기 제어와 같이 무제한으로 사용된다. 모든 영역에서 보급률이 높아짐에 따라 보안에 대한 관심이 높아지고 있다. 대부분의 사람들은 이미 인터넷에 액세스할 수 있으며 여러 가지 방법을 통해 사용할 수 있다. 그 중 하나가 이메일이다. 정보 교환의 "어디서나" 사용할 수 있는 기능인 전자 메일은 의심할 여지 없이 문서에서 비디오, 사진 등에 이르기까지 모든 종류의 정보를 교환하는 데 가장 자주 사용되는 방법이다. 오늘날 스마트폰의 보급으로 인해 거의 모든 곳에서 자신에 대한 새로운 정보나 자신을 둘러싼 프로세스를 확인할 수 있다. 그러나m 특히 의료 분야에서 이 정보는 대부분 이메일과 인스턴트 메신저, 사진/포토 또는 비디오 공유 플랫폼 또는 문서 교환 소프트웨어와 같은 대부분의 다른 정보 공유 제품이 이러한 종류의 정보에 적합하지 않다는 소중하고 사적 성격을 띠고 있다.

[0005] 지난 몇 년 동안 중요한 개인 정보 까지, 정보를 클라우드에 저장할 수 있는 안전하고 여전히 매우 편리한 장소를 만들기 위해 엄청난 노력을 기울였다. 미사용중, 즉 전송 중이 아닌 동안 데이터의 보안은 주로 어떤 암호화

알고리즘이 사용되는지가 관건이다. 이것은 일종의 컴퓨터 하드웨어 상에 지속되는 데이터에 대해서도 마찬가지이다. 그러나 대부분의 경우 오늘날에도 일부 사용자 자격 증명의 인증 프로세스는 그다지 안전하지 않다. 다시 말하지만, 데이터베이스의 해싱 암호가 (이 데이터베이스는 일부 컴퓨터 하드웨어에서 유지되기 때문에) 이 정보를 보관하는 다소 안전한 방법이다. 로그인(자격 증명 확인) 및 데이터 조회 과정에서, 특히 의료 데이터의 경우, 적절한 권한이 있는 사람만 분석 데이터에 액세스하는 것을 사용자에게 보장하기 위해 추가적인 후속 권한 확인이 필요한다.

[0006] IT 시스템 설계에는 보안 대 편의성에 대한 지속적인 평가가 있다. 전부는 아니지만 많은 사람들이 개인 데이터(특히 의료 데이터)가 어디에 저장되든 안전하고 안전하기를 원한다. 그러나 허용되는 데이터를 사용하기 위해서는 데이터에 액세스하는 가장 편리하면서도 가장 안전한 액세스 방법이 있어야 한다.

[0007] 인터넷을 통해 개인 데이터와 같은 민감한 정보에 액세스하려면 보안 전송 채널과 보안 인증 메커니즘이 필요하다. 실제 표준은 사용된 암호의 강도에 크게 의존하는 사용자 이름과 암호를 통한 인증이다. 약한 암호는 추측하기 쉽지만 강력한 암호는 기억하기 어렵다. 그 외에도 사용자 이름은 종종 자신을 인증하려는 사람의 일부 또는 전체 이름으로 구성된다. 대부분의 시나리오에서 인증자는 데이터가 속한 사람이다. 그러나 특히 점점 더 디지털화되고 있는 의료 환경에서, 개인의 개인 데이터 요청자는 서비스 제공자이다. 이는 의료 환경에서 의사, 임상의 또는 실험실 서비스 제공자가 될 수 있다. 설명된 대로 데이터 전송은 가장 자주 안전하게 수행되지만 로그인 자격 증명(즉, 사용자 이름 및 암호)이 제출되고 전송되기 때문에 특정(건강) 데이터를 요청하는 개인에 관한 정보는 보호되지 않는다. 따라서 로그인 자격 증명 외에도 실제 지리적 위치(IP 주소를 통해)도 추적할 수 있기 때문에 그러한 개인의 신원을 추적할 수 있다. 이는 데이터가 관련된 개인에게도 취약성을 제공한다. 인터넷을 통해 정보에 액세스할 때의 또 다른 문제는 해당 정보의 식별이다. 예를 들어 특정 제품에 대한 자세한 정보를 요청하면 다른 제품에 대한 다른 정보가 나타날 수 있다.

발명의 내용

해결하려는 과제

[0008] 본 발명의 실시 예들의 목적은 정보를 전달하기 위한 개념을 제공하는 것이고, 이 개념은 전송된 정보와 사용자에 대한 정보 모두의 사용자 편의성과 데이터 보안 간의 개선된 절충점을 제공한다.

과제의 해결 수단

[0009] 본 발명에 따르면, 이러한 개념은 정보에 고유한 고유 식별자로 서버가 제공한 데이터세트와 같은 정보를 식별하고, 정보에 대한 액세스를 요청하는 사용자의 액세스 권한을 확인하기 위해 등록된 사용자와 연계된 인증자를 이용하여 제공된다. 이러한 기능을 조합하면 정보를 안전하고 구체적으로 제공하고 정보에 대한 액세스를 요청하는 사용자의 신원에 대한 정보를 비밀로 유지할 수 있다.

[0010] 본 발명에 따른 실시 예는 인터넷 또는 인트라넷과 같은 디지털 통신 네트워크를 통해 하나 이상의 데이터세트를 제공하기 위한 서버를 제공한다. 서버는 고유 식별자를 식별된 데이터세트, 예를 들어 하나 이상의 데이터세트의 특정 데이터세트와 연관시키도록 구성되며, 특정 데이터세트는 고유 식별자로 식별된다. 고유 식별자는 디지털 통신망을 통해 식별된 데이터세트에 액세스하기 위한 네트워크 주소를 나타내며, 고유 식별자는 식별된 데이터세트에 고유하다. 서버는 서버에 대한 액세스를 요청하는, 예를 들어 예를 들어 고유 식별자를 통해 서버가 호스팅하거나 제공하는 하나 이상의 데이터세트에 대한 액세스를 요청하는 클라이언트의 인증자에 의해 제공되는 인증 정보를 검증하도록 추가로 구성된다. 예를 들어, 인증 정보를 검증하는 것은 인증자의 신원을 획득하거나 검증하기 위한 인증 정보의 평가를 포함한다. 인증 정보가 인증자를 등록된 사용자, 예를 들어 이전에 등록된 사용자와 연관된다고 식별하는 경우, 서버는 하나 이상의 데이터세트에 대한 액세스 권한을 클라이언트에 선택적으로 제공하도록 구성된다. 예를 들어, 인증 정보를 검증하는 단계는 인증자가 등록된 사용자와 연결되는지에 대한 검증을 포함할 수 있다.

[0011] 예를 들어, 서버는 등록된 사용자에게 고유 식별자를 제공하도록 구성된다. 식별된 데이터세트의 고유 식별자를 갖게 되면, 사용자가 식별된 데이터세트를 식별할 수 있도록 하고 사용자가 원하는 데이터세트를 요청하도록 하여 잘못된 정보를 방지할 수 있다. 등록된 사용자는 클라이언트를 사용하여 서버에 액세스하도록 하기 위해 고유 식별자가 나타내는 네트워크 주소를 사용할 수 있다. 클라이언트가 서버에 대해 인증하기 위해 인증자를 사용하기 때문에, 등록된 사용자는 등록된 사용자의 ID에 대한 정보를 포함하는 자격 증명을 사용하여 서버에 대해 인증할 필요가 없다. 따라서, 서버에 있는 데이터세트에 액세스하기 위해, 클라이언트와 서버 간에 등록된

사용자의 신원을 전달할 필요가 없으므로 서버에 대한 액세스를 요청하는 등록된 사용자의 신원이 안전하다. 즉, 이러한 인증을 사용하면 클라이언트와 서버 간에 개인 데이터를 교환할 필요가 없다. 또한, 등록된 사용자의 인증을 위해 인증자를 사용함으로써, 등록된 사용자는 반드시 개별 자연인을 나타낼 필요는 없고, 사용자의 개체, 예를 들어 사람의 그룹을 나타낼 수도 있으므로, 여러 사람 또는 사용자가 등록된 사용자와 연결된 동일한 인증자를 사용한다. 따라서 인증자를 사용하면 예를 들어 제공된 데이터세트와 관련된 작업을 여러 사람이 공유하는 상황에서 유연성과 사용자 편의성이 향상된다. 하나 이상의 데이터세트에 대한 액세스 권한은 예를 들어 식별된 데이터세트에 대한 액세스 권한을 포함하지만, 서버에서 호스팅하는 추가 데이터세트에 대한 액세스 권한을 포함하므로, 사용자가 사용하는 클라이언트가 등록된 사용자로 인증된 경우, 사용자는 서버에 의해 호스팅되는 복수의 데이터세트에 액세스할 수 있다. 따라서 등록된 사용자에게 하나 이상의 데이터세트에 대한 액세스 권한을 부여하면 데이터 제공의 사용자 편의성이 향상된다.

[0012] 일 실시 예에 따르면, 서버는 고유 식별자를 통해 식별된 데이터세트에 대한 액세스를 요청하는 클라이언트의 인증자가 제공한 인증 정보를 검증하도록 구성되며; 서버는 식별된 데이터세트에 대한 액세스 권한을 클라이언트에 선택적으로 제공하도록 구성되고, 여기서 식별된 데이터세트에 대한 액세스 권한은 인증자와 관련된 등록된 사용자에 고유하다. 사용자 특정 액세스 권한은 식별된 데이터세트를 특정 등록된 사용자에게 제공할 수 있다. 따라서, 서버는 식별된 데이터세트가 특정 액세스 권한이 부여된 등록된 사용자에게 구체적이고 선택적으로 제공되는 것을 보장할 수 있다. 따라서 서버는 식별된 데이터세트에 대한 개별 액세스 권한을 여러 사용자에게 부여할 수 있다. 따라서 사용자 특정 액세스 권한은 식별된 데이터세트의 데이터 보안을 강화하는데, 한 명 이상의 특정 등록 사용자만이 식별된 데이터세트에 액세스할 수 있기 때문이다.

[0013] 본 발명에 따른 실시 예는 예를 들어 식별된 데이터세트로 지정된 데이터세트를 디지털 통신 네트워크를 통해 제공하기 위한 서버를 제공한다. 서버는 고유 식별자를 데이터세트와 연결하도록 구성되고, 고유 식별자는 디지털 통신망을 통해 데이터세트에 액세스하기 위한 네트워크 주소를 나타내며, 여기서 고유 식별자는 데이터세트에 고유하다. 서버는 고유 식별자를 통해 데이터세트에 대한 액세스를 요청하는 클라이언트의 인증자에 의해 제공되는 인증 정보를 검증하도록 추가로 구성된다. 서버는 클라이언트에게 데이터세트에 대한 액세스 권한을 선택적으로 제공하도록 구성되며, 액세스 권한은 인증자와 연결된 등록된 사용자에게만 적용된다. 서버는 전술한 실시 예의 기능과 장점을 결합한다.

[0014] 일 실시 예에 따르면, 서버는 인증자를 사용자를 식별하는 신원 정보와 연관시킴으로써 인증자를 등록하도록 구성된다. 예를 들어, 등록된 사용자는 사용자의 신원을 확인하기 위한 신원 정보를 제공함으로써 이전에 등록했을 수 있는 사용자일 수 있다. 예를 들어, 등록된 사용자는 예를 들어 인증 정보를 제공함으로써 인증자를 지정하는 정보를 제공함으로써 인증자를 등록할 수 있다. 예를 들어, 서버는 인증자를 사용자의 신원 정보와 연관시키기 위해, 예를 들어 인증 정보에 기초하거나 그로부터 유도될 수 있는 인증자를 식별하는 정보를 저장하도록 구성된다. 인증자 등록 후, 서버는 예를 들어 인증 정보를 수신하거나 평가함으로써 인증자를 통해 등록된 사용자를 식별할 수 있으므로, 서버에 대해 등록된 사용자를 인증하기 위한 신원 정보의 반복적인 제공 또는 전송이 불필요할 수 있다. 예를 들어, 서버는 여러 인증자를 등록된 사용자와 연관시키도록 구성될 수 있다. 예를 들어, 여러 자연인이 등록된 사용자와 관련된 여러 인증자를 사용할 수 있으므로, 시스템의 유연성과 사용자 편의성이 향상된다.

[0015] 일 실시 예에 따르면, 서버는 예를 들어 사용자에 대한 신원 정보를 저장함으로써 사용자를 등록하도록 구성된다. 서버가 사용자를 등록하도록 구성되어 있으므로, 새로운 사용자가 편리하게 시스템에 가입할 수 있다.

[0016] 일 실시 예에 따르면, 서버는 액세스 정보를 포함하고, 액세스 정보는 등록된 사용자를 식별된 데이터세트에 대한 액세스 권한과 연관시키고, 선택적으로 추가 데이터세트에 대한 액세스 권한과 연관시킨다. 예를 들어, 액세스 정보는 특정 데이터세트에 대한 개별 액세스 권한을 소유하도록 등록된 한 명 이상의 사용자를 정의할 수 있다. 액세스 정보가 있으면 서버가 하나 이상의 데이터세트에 대한 액세스 권한을 매우 효율적으로 구성할 수 있다.

[0017] 일 실시 예에 따르면, 서버는 서버에 대한 액세스를 요청하는 클라이언트를 식별된 데이터세트, 예를 들어, 클라이언트에 의해 서버에 액세스하기 위해 사용되는 고유 식별자로 식별되는 데이터세트로 연결하도록 구성된다. 클라이언트를 식별된 데이터세트로 연결하는 것은 식별된 데이터세트에 대한 액세스를 요청하는 사용자에게 매우 편리한다.

[0018] 일 실시 예에 따르면, 서버는 인증 정보를 검증하기 위해 암호화 시스템을 사용하도록 구성되며, 여기서 상기 서버는 상기 인증자를 상기 인증자에 고유한 암호화 키와 연관시키도록 구성된다. 예를 들어, 암호 시스템은 비

대칭 암호 시스템을 기반으로 할 수 있다. 서버는 인증자를 인증자의 공개 키 정보와 연관시킬 수 있다. 암호화를 사용하면 인증자의 신원을 안전하고 효율적이며 사용자가 편리하게 확인할 수 있다.

[0019] 본 발명에 따른 실시 예는 예를 들어 식별된 데이터세트로 지정된 데이터세트를 디지털 통신 네트워크를 통해 획득하기 위한 장치를 제공한다. 장치는 예를 들어 데이터세트의 고유 식별자를 획득, 예를 들어, 수신하거나 인식하도록 구성되며, 상기 고유 식별자는 디지털 통신망을 통해 데이터세트에 액세스하기 위한 네트워크 주소를 나타내며, 여기서 고유 식별자는 데이터세트에 고유하다. 장치는 데이터세트를 제공하는 서버에 데이터세트에 액세스하기 위한 요청을 전송하기 위해 고유 식별자를 사용하도록 구성된 클라이언트를 포함한다. 클라이언트는 서버에 대해 클라이언트를 인증하기 위한 인증자의 인증 정보를 서버에 제공하도록 구성되며, 여기서 인증자는 등록된 사용자와 연관된다. 데이터세트에 고유한 고유 식별자를 사용하여 데이터세트 액세스 요청을 전송함으로써, 서버에서 다른 데이터세트와 같은 잘못된 정보를 검색하는 것을 피할 수 있다. 예를 들어, 장치는 앞에서 설명한 서버에 대한 상대 역할을 할 수 있다. 예를 들어, 사용자는 서버에서 데이터세트를 검색하거나 요청하기 위해 장치를 사용할 수 있다. 따라서 서버의 세부 사항, 기능 및 이점과 그 특징은 적용 가능한 경우 장치에 동일하게 적용된다.

[0020] 일 실시 예에 따르면, 장치는 인증자를 포함한다. 따라서, 장치 및 클라이언트에 대한 인증자의 가용성이 특히 높아서, 사용자 편의성이 향상된다.

[0021] 일 실시 예에 따르면, 장치는 디지털 인터페이스를 통해 인증자에 액세스하도록 구성된다. 예를 들어 인증자는 디지털 인터페이스를 통해 장치에 연결된 외부 장치의 일부이다. 따라서, 인증자를 포함하는 외부 장치가 장치로부터 제거되므로, 장치는 서버에 대해 인증되지 않도록 할 수 있다. 따라서 인증자를 포함하는 외부 장치를 소유하거나 인증자에 대한 액세스 권한이 있는 사람만이 데이터세트를 요청하기 위해 장치를 사용할 수 있다. 승인되지 않은 사람이 장치를 사용하는 것을 방지하여 데이터 보안성을 향상시킬 수 있다.

[0022] 일 실시 예에 따르면, 장치는 사용자 입력을 수신하기 위한 입력 인터페이스를 포함하고, 여기서 장치는 사용자 입력에 따라 인증 정보를 서버에 선택적으로 제공하도록 구성된다. 예를 들어, 장치는 사용자의 존재 또는 사용자의 신원의 검증에 따라 인증 정보를 제공하기 위한 인증자의 사용을 허용하도록 구성될 수 있다. 따라서, 입력 인터페이스는 장치를 사용하기 위한 사용자의 승인을 보장할 수 있으며, 이는 데이터세트를 요청하기 위한 데이터 보안을 증가시킨다.

[0023] 일 실시 예에 따르면, 장치는 사용자에 대한 생체 정보를 획득하도록 구성되며, 여기서 상기 장치는 생체 정보가 인증자와 관련된 사용자를 식별하는 경우, 인증 정보를 서버에 선택적으로 제공하도록 구성된다. 예를 들어, 생체 정보는 사용자 입력 또는 입력 인터페이스를 통한 사용자 상호작용으로부터 획득될 수 있다. 생체 정보는 자연인을 식별하는 특히 안전하고 편리한 방법이다.

[0024] 일 실시 예에 따르면, 장치는 고유 식별자, 예를 들어 바코드 또는 QR 코드를 나타내는 그래픽 패턴에서 고유 식별자를 검색하도록 구성된다. 장치에 고유 식별자를 그래픽 패턴으로 제공하는 것은 사용자가 장치에 고유 식별자를 입력하는 편리한 방법이다. 또한, 고유 식별자를 그래픽 패턴으로 제공하면 고유 식별자의 잘못된 입력이나 장치에 대한 잘못된 고유 식별자의 제공을 피할 수 있으므로, 올바른 데이터세트가 요청된 것을 확인할 수 있다.

[0025] 일 실시 예에 따르면, 인증자는 암호 키, 예를 들어 비밀 키 또는 개인 키를 포함하고, 인증자는 인증 정보를 서버에 제공하기 위해 암호화 키를 사용하도록 구성된다. 예를 들어, 서버에 알려진 인증자의 암호화 키 및 추가 암호화 키, 예를 들어 서버가 인증자와 연관시키는 암호화 키(예: 공개 키)는 비대칭 암호화 시스템의 일부일 수 있다. 예를 들어, 각각의 암호화 키는 각각의 다른 키로 암호화된 메시지를 해독하도록 적응될 수 있다. 인증 정보를 제공하기 위해 암호화 키를 사용하면 서버에 대한 인증자의 안전한 유효성 검증이 가능한다.

[0026] 일 실시 예에 따르면, 인증 정보는 예를 들어 인증 정보, 예를 들어 암호화된 메시지가 인증자, 예를 들어 등록된 특정 사용자의 암호화 키를 포함하는 인증자를 사용하여 생성되었다는 검증에 따라, 예를 들어 사용자 이름 데이터 또는 암호 데이터를 전송하지 않고 서버에 대해 등록된 사용자의 익명 인증을 허용한다. 예를 들어 인증자는 익명으로 처리된다. 예를 들어, 인증자는 개인 데이터, 예를 들어 인증자와 관련된 등록된 사용자의 이름 또는 연락처 정보에 대한 힌트를 포함하지 않는 정보로 나타낼 수 있다.

[0027] 본 발명에 따른 실시 예는 디지털 통신 네트워크를 통해 하나 이상의 데이터세트를 제공하는 방법을 제공한다. 방법은 고유 식별자를 식별된 데이터세트와 연관시키는 단계를 포함하고, 고유 식별자는 디지털 통신 네트워크를 통해 식별된 데이터세트에 액세스하기 위한 네트워크 주소를 나타내며, 여기서 고유 식별자는 식별된 데이터

세트에 고유하다. 방법은 고유 식별자를 통해 하나 이상의 데이터세트에 대한 액세스를 요청하는 클라이언트의 인증자에 의해 제공되는 인증 정보를 검증하는 단계를 더 포함한다. 방법은 인증 정보가 인증자를 등록된 사용자와 연결된다고 식별하는 경우, 하나 이상의 데이터세트에 대한 액세스 권한을 클라이언트에 선택적으로 제공하는 단계를 더 포함한다.

[0028] 본 발명에 따른 실시 예는 디지털 통신 네트워크를 통해 데이터세트를 획득하기 위한 방법을 제공한다. 방법은 데이터세트의 고유 식별자를 획득하는 단계를 포함하고, 고유 식별자는 디지털 통신망을 통해 데이터세트에 액세스하기 위한 네트워크 주소를 나타내며, 여기서 고유 식별자는 데이터세트에 고유하다. 방법은 데이터세트를 호스팅하는 서버에 액세스하기 위한 요청을 전송하기 위해 고유 식별자를 사용하는 단계를 더 포함한다. 방법은 서버에 대해 클라이언트를 인증하기 위한 인증자의 인증 정보를 서버에 제공하는 단계를 더 포함하고, 여기서 인증자는 등록된 사용자와 연관된다.

[0029] 설명된 방법은 장치, 즉 상술된 데이터세트를 얻기 위한 서버 및 장치와 동일한 아이디어에 의존하고, 상기 방법은 동등한 기능과 이점을 제공한다. 방법은 대응하는 장치와 관련하여 본 명세서에서 설명된 특징, 기능 및 세부 사항 중 임의의 것과 선택적으로 결합되거나 이에 의해 보완될 수 있다. 방법은 개별적으로 또는 이들의 임의의 조합으로 언급된 특징, 기능 및 세부사항과 선택적으로 결합될 수 있다.

도면의 간단한 설명

[0030] 본 출원에 따른 실시 예들은 첨부된 도면들을 참조하여 후속하여 설명될 것이다:

도 1은 일 실시 예에 따른 서버의 개략도를 도시하고;

도 2는 일 실시 예에 따른 데이터세트를 획득하기 위한 장치의 개략도를 도시하고;,

도 3은 일 실시 예에 따른 데이터세트를 획득하기 위한 서버 및 장치의 개략도를 도시하고;

도 4는 일 실시 예에 따른 사용자 등록 방법에 대한 흐름도를 도시하고;

도 5는 일 실시 예에 따른 하나 이상의 데이터세트를 제공하기 위한 방법의 흐름도를 도시하고;

도 6은 일 실시 예에 따른 데이터세트를 획득하기 위한 방법의 흐름을 도시하고; 및

도 7은 다른 실시 예에 따라 데이터세트를 획득하기 위한 장치와 서버 사이에서 데이터세트를 전송하기 위한 방법의 흐름도를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0031] 이하, 상이한 본 발명의 실시 예 및 양태가 설명될 것이다. 또한, 추가 실시 예는 첨부된 청구범위에 의해 정의될 것이다.

[0032] 청구범위에 의해 정의된 바와 같은 임의의 실시 예는 본 명세서에 기재된 임의의 세부사항(특징 및 기능)에 의해 보완될 수 있음에 유의해야 한다. 또한, 본 명세서에 기재된 실시 예는 개별적으로 사용될 수 있고, 또한 청구범위에 포함된 세부사항(특징 및 기능) 중 임의의 것에 의해 선택적으로 보완될 수도 있다. 또한, 본 명세서에서 설명된 개별 측면은 개별적으로 또는 조합하여 사용될 수 있다는 점에 유의해야 한다. 따라서, 상기 측면 중 다른 하나에 세부 사항을 추가하지 않고 상기 개별 측면 각각에 세부 사항을 추가할 수 있다. 또한, 본 개시 내용은 정보를 전송, 제공, 검색, 요청 또는 수신하는 데 사용할 수 있는 기능을 명시적으로 또는 암시적으로 설명한다는 점에 유의해야 한다.

[0033] 본 발명은 아래에 주어진 상세한 설명 및 본 발명의 실시 예의 첨부 도면으로부터 더 완전하게 이해될 것이지만, 이것은 설명된 특정 실시 예로 본 발명을 제한하기 위한 것이 아니고 단지 설명 및 이해를 위한 것이다.

[0034] 도면에서, 더 나은 이해를 돕기 위해 점선으로 그려진 요소가 도시되어 있지만, 이러한 요소는 반드시 도시된 실시 예의 일부는 아니다.

[0035] 1. 도 1에 따른 하나 이상의 데이터세트를 제공하기 위한 서버의 실시 예

[0036] 도 1은 일 실시 예에 따른 서버(100)의 개략도를 도시한다. 서버(100)는 디지털 통신 네트워크(90)를 통해 하나 이상의 데이터세트를 제공하도록 구성된다. 또한, 서버(100)는 고유 식별자(115)를 하나 이상의 데이터세트의

일부일 수 있는 식별된 데이터세트(110)와 연관시키도록 구성된다. 고유 식별자(115)는 디지털 통신 네트워크(90)를 통해 식별된 데이터세트(110)에 액세스하기 위한 네트워크 주소를 나타내며, 여기서 고유 식별자(115)는 식별된 데이터세트(110)에 고유하다. 서버(100)는 고유 식별자(115)를 통해 서버(100)에 대한 액세스를 요청하는 클라이언트(160)의 인증자(170)에 의해 제공되는 인증 정보(172)를 검증하도록 추가로 구성된다. 서버는 인증 정보(172)가 인증자를 등록된 사용자와 연관된다고 식별하는 경우, 하나 이상의 데이터세트에 대한 액세스 권한(120)을 클라이언트(160)에 선택적으로 제공하도록 구성된다.

[0037] 일 실시 예에 따르면, 서버(100)는 고유 식별자(115)를 통해 식별된 데이터세트(110)에 대한 액세스를 요청하는 클라이언트(160)의 인증자(170)에 의해 제공되는 인증 정보(172)를 검증하도록 구성된다. 따라서, 서버는 하나 이상의 데이터세트, 예를 들어 데이터세트(110)의 특정 데이터세트에 액세스하기 위한 요청을 처리하도록 구성될 수 있다. 추가적으로, 서버(100)는 식별된 데이터세트(100)에 대한 액세스 권한(120)을 클라이언트(160)에게 선택적으로 제공하도록 구성될 수 있고, 여기서 식별된 데이터세트에 대한 액세스 권한(120)은 인증자와 연관된 등록된 사용자에 고유하다. 따라서, 서버는 클라이언트(160)가 인증 정보(172)를 전송하여 서버에 대해 인증하는 인증자(170)의 신원에 따라 다른 액세스 권한을 클라이언트(160)에게 제공할 수 있고, 여기서 인증자(170)의 신원은 등록된 사용자와 연관된다.

[0038] 대안적인 실시 예에 따르면, 서버(100)는 디지털 통신 네트워크(90)를 통해 식별된 데이터세트(110)라고도 하는 데이터세트(110)를 제공하도록 구성된다. 또한, 서버(100)는 고유 식별자(115)를 데이터세트(110)와 연관시키도록 구성되며, 고유 식별자(115)는 디지털 통신 네트워크(90)를 통해 데이터세트(110)에 액세스하기 위한 네트워크 주소를 나타내며, 여기서 고유 식별자(115)는 데이터세트(110)에 고유하다. 서버(100)는 고유 식별자(115)를 통해 데이터세트(110)에 대한 액세스를 요청하는 클라이언트(160)의 인증자(170)에 의해 제공되는 인증 정보(172)를 검증하도록 추가로 구성된다. 이 실시 예에 따르면, 서버(100)는 데이터세트(110)에 대한 액세스 권한(120)을 클라이언트(160)에 선택적으로 제공하도록 추가로 구성되며, 이 때 액세스 권한(120)은 인증자(160)와 관련된 등록된 사용자에 고유하다.

[0039] 서버(100)의 추가 세부사항은 다음 도면에 따른 추가 실시 예의 맥락에서 설명된다. 특히, 명확성을 위해, 서버(100)의 추가 세부사항은 데이터세트를 획득하기 위한 서버와 장치 사이의 상호작용의 맥락에서 설명된다. 서버의 실시 예는 선택적으로 다른 실시 예와 관련하여 본 명세서에 설명된 특징, 기능 및 세부사항 중 임의의 것에 의해 개별적으로 또는 조합하여 보완될 수 있다는 점에 유의해야 한다.

[0040] 2. 도 2에 따른 데이터세트를 획득하기 위한 장치

[0041] 도 2는 디지털 통신 네트워크(90)를 통해 데이터세트(210)를 획득하기 위한 장치(250)의 실시 예의 개략도를 도시한다. 데이터세트(210)는 데이터세트(110) 또는 식별된 데이터세트(110)와 유사할 수 있고 서버(200), 예를 들어 서버(100)에 의해 제공될 수 있다. 장치(250)는 데이터세트(210)의 고유 식별자(215)를 획득하도록 구성되며, 고유 식별자(215)는 디지털 통신 네트워크(90)를 통해 데이터세트(210)에 액세스하기 위한 네트워크 주소를 나타내고, 여기서 고유 식별자(215)는 데이터세트(210)에 고유하다. 예를 들어, 고유 식별자(215)는 서버(200)에 의해 제공될 수 있다. 장치(250)는 클라이언트(160)와 유사할 수 있는 클라이언트(260)를 포함한다. 예를 들어, 클라이언트(360)는 인터넷 브라우저 또는 파일 브라우저 또는 디지털 통신망(90)과 통신하도록 구성된 다른 유닛일 수 있다. 클라이언트(260)는 데이터세트(210)를 제공하는 서버(200)에 데이터세트(210)에 액세스하기 위한 요청(262)을 전송하기 위해 고유 식별자(215)를 사용하도록 구성된다. 클라이언트(260)는 서버(200)에 대해 클라이언트(260)를 인증하기 위한 인증자(270)의 인증 정보(272)를 서버(200)에 제공하도록 더 구성되고, 여기서 인증자(270)는 등록된 사용자와 연관된다. 예를 들어, 인증부(270) 및 인증 정보(272)는 각각 인증자(170) 및 인증 정보(172)와 유사할 수 있다.

[0042] 장치(250)의 추가 세부사항은 다음 도면에 따른 추가 실시 예의 맥락에서 설명된다. 특히, 명료함을 위해, 장치(250)의 추가 세부사항은 데이터세트를 획득하기 위한 서버와 장치 사이의 상호작용의 맥락에서 설명된다. 장치(250)의 실시 예는 선택적으로 다른 실시 예와 관련하여 본 명세서에 설명된 특징, 기능 및 세부사항 중 임의의 것에 의해 개별적으로 또는 조합하여 보완될 수 있다는 점에 유의해야 한다.

[0043] 3. 도 3에 따른 데이터세트를 얻기 위한 서버와 장치 간의 상호 작용

[0044] 도 3은 서버(100, 200)와 유사할 수 있는 서버(300)와 장치(150, 250)와 유사할 수 있는 데이터세트를 획득하기 위한 장치(350) 사이의 상호작용을 개략적으로 도시한다. 서버(300)와 장치(350)는 디지털 통신망(90), 예를 들어 인터넷을 통해 통신할 수 있다. 서버(300)는 데이터세트(310)를 포함하는 하나 이상의 데이터세트를 제공할

수 있고, 예를 들어, 서버(300)는 하나 이상의 데이터세트를 호스팅할 수 있거나 서버(300)는 다른 곳에서 호스팅되는 하나 이상의 데이터세트에 대한 액세스를 제공할 수 있다. 서버는 데이터세트(310)를 고유 식별자(315), 예를 들어 고유 식별자(115;215)와 연관시키도록 구성된다. 고유 식별자(315)는 디지털 통신 네트워크(90)를 통해 서버에 액세스할 때 데이터세트(310, 110)를 구체적으로 어드레싱하는 것을 허용할 수 있는 네트워크 주소를 나타낸다. 예를 들어, 데이터세트(310)를 검색하려는 사용자는 장치(350)의 클라이언트(360)를 사용하여 고유 식별자(315)를 호출함으로써 데이터세트(310)를 구체적으로 요청하기 위해 장치(350)를 사용할 수 있다. 따라서 데이터세트(310)에 액세스하기 위해 서버(300)에 요청(362)을 전송한다.

[0045] 예를 들어, 고유 식별자(315)는 서버(300)의 네트워크 주소 및 서버(300)에 의해 제공된 정보 또는 데이터세트의 엔티티 내에서 데이터세트(310)를 고유하게 식별하는 고유 데이터세트 식별자를 포함할 수 있다. 고유 데이터세트 식별자는 식별자의 특정 엔터티 내에서 전역적으로 고유할 수도 있다. 고유 식별자(315)는 고유 데이터세트 식별자에 대한 신택스 또는 유형 또는 방식에 대한 정보를 더 포함할 수 있다. 추가적으로, 고유 식별자(315)는 고유 식별자(315)의 신택스에 대한 정보를 포함할 수 있다.

[0046] 일 실시 예에 따르면, 고유 식별자(315)는 통합 자원 식별자(URI)로 표현된다. 즉, 요청된 데이터, 예를 들어 데이터세트(310)는 특별히 구성된 URI를 사용하여 식별된다. URI는 네 부분, SCHEME, BASEURL, IDENTIFIERTYPE 및 IDENTIFIER 자체으로 구성된다. SCHEME는 RFC 3986[1]의 IETF에 의해 정의된다. BASEURL은 사용자 요청을 수신할 서버의 도메인 이름, 예를 들어, example.com이다[1]. IDENTIFIERTYPE은 다음 식별자의 유형, 이상적으로는 GS1 GDTI(문서용)와 같은 국제 표준을 정의하지만, 내부적으로 정의된 식별자 유형 또는 유사한 기술적 액세스 방식일 수도 있다. 식별자 유형이 분석된 데이터에 대한 링크를 나타내는 고유 문자열로 구성된, IDENTIFIER 자체를 따르는 경우, IDENTIFIER는 내재한 시스템이거나 IDENTIFIERTYPE 전역 고유 문자열과 조합되어야 한다. 가능한 유효한 URI는 모든 부분을 결합하면 다음과 같다:

[0047] https://example.com/gdti/408980809ADHJKCGGHBKN

[0048] 예를 들어, 식별자가 요청된 모든 데이터 개체에 대해 고유한 문자열이라는 것이 중요할 수 있다. 이 식별자의 고유성을 보장하는 가능한 방법, 예를 들어 고유 식별자(315)는 EU 의료기기 규정(MDR) 및 체외 진단 규정(IVDR)에도 언급된 GS1과 같은 국제 표준을 중계하는 것이다. 위에서 설명된 URI 형식을 사용함으로써, 데이터 객체, 예를 들어 데이터세트(310)는 고유하게 식별되고 액세스 가능하게 될 수 있다.

[0049] 클라이언트(360)는 클라이언트(160, 260)와 유사할 수 있다. 예를 들어, 클라이언트(360)는 예를 들어 서버(100) 또는 서버에 의해 호스팅되는 데이터세트 중 하나에 액세스하기 위해 사용자에 의해 이용될 수 있는, 인터넷 브라우저 또는 파일 브라우저 또는 디지털 통신 네트워크에서 탐색하기 위한 다른 유닛을 포함하거나 그 일부일 수 있다.

[0050] 서버(300)는 서버(300)에 액세스하기 위해 클라이언트(360)를 사용하는 사용자의 신원에 따라 데이터세트(310) 및 선택적 추가 데이터세트에 대한 액세스를 선택적으로 부여하도록 구성될 수 있다. 이를 위해, 서버(300)는 데이터세트에 대한 액세스 요청(362)이 등록된 사용자로부터 시작되었는지 증명하고, 선택적으로, 서버(300)는 서버에 대한 액세스를 요청하는 등록된 사용자의 신원을 확인할 수 있다.

[0051] 등록된 사용자로 인증하기 위해 사용자는 인증자(370)로 대표될 수 있다. 예를 들어, 등록된 사용자는 단순히 이전에 등록된 인증자(370)로 표시될 수 있다. 인증자(370)는 암호화 시스템 내에서 인증자(370)의 고유한 식별을 허용하는 암호화 엔티티를 포함할 수 있다. 예를 들어, 인증자는 한 쌍의 암호화 키, 예를 들어 인증자에게 비밀인 개인 키와 공개 키를 포함할 수 있다.

[0052] 일 실시 예에 따르면, 서버(300)는 인증자(370)를 등록된 사용자를 식별하는 신원 정보와 연관시킴으로써 인증자(370)를 등록하도록 구성된다.

[0053] 예를 들어, 등록된 사용자는 인증자(370)를 등록하여 등록 후에 인증자(370)가 등록된 사용자와 연관되도록 할 수 있다. 예를 들어, 서버(300)는 인증자(370)를 등록하기 위한 인증자(370)의 공개 키를 저장할 수 있다.

[0054] 예를 들어, 서버(300)는 인증 정보(372)를 검증하기 위해 암호화 시스템을 사용하도록 구성되고, 여기서 서버(300)는 인증자(370)를 인증자(370)에 고유한 암호화 키와 연관시키도록 구성된다.

[0055] 일 실시 예에 따르면, 등록된 사용자는 하나 이상의 인증자를 등록할 수 있다. 인증자를 등록하기 위한 가능한 방식은 도 4와 관련하여 설명되어 있다.

[0056] 클라이언트(360)는 서버에 대한 액세스 요청이 등록된 사용자를 대신하여 발생하는지 확인하고 및/또는 서버에

대한 액세스를 요청하는 등록된 사용자의 신원을 확인하기 위해 등록된 사용자와 연결된 인증자(370)를 사용할 수 있다. 예를 들어, 인증자(370)의 신원 인증은 서버(300)와 클라이언트(360) 간의 암호화된 메시지 교환에 기초한다.

[0057] 일 실시 예에 따르면, 인증자(370)는 암호화 키를 포함할 수 있고, 인증자(370)는 인증 정보(372)를 서버에 제공하기 위해 암호화 키를 사용하도록 구성될 수 있다.

[0058] 예를 들어, 서버(300)는 검증 정보를 장치(350)로 전송할 수 있다. 장치(350)는 인증 정보(372)를 획득하기 위해 인증자(370)의 비밀 키, 예를 들어 키 쌍 중 개인 키를 사용하여 검증 정보를 암호화하거나 서명할 수 있다. 클라이언트(360)는 인증 정보(372)를 서버(300)로 전송할 수 있다. 서버(300)는 인증 정보의 서명이 개인 키를 사용하여 생성된 경우, 인증자(370)의 공개 키를 사용하여 인증 정보(372)를 복호화하면 클라이언트(370)에 원래 전송된 유효성 검사 정보가 생성되는지 테스트함으로써 또는 테스트를 위해 공개 키를 사용함으로써 인증자(370)의 신원을 검증할 수 있다. 서버는 인증자(370)를 등록된 사용자와 연관시킬 수 있으므로, 이 인증 절차를 통해 사용자 ID에 대한 정보를 전송하지 않고 서버에 대해 등록된 사용자를 인증할 수 있다. 따라서, 인증 정보(372)는 서버에 대해 등록된 사용자의 익명화된 인증을 허용할 수 있다.

[0059] 대안적으로, 암호화 시스템은 대칭적일 수 있다. 즉, 서버(300)는 인증자(370)와 관련된 암호키를 포함하고, 여기서 공통 암호 키는 인증자(370) 및 서버(300)에 대한 비밀이고, 서버(300)는 인증 정보(372)를 복호화하기 위해 공통 암호화 키를 사용하고, 인증 정보(372)는 공통 암호화 키를 사용하여 검증 정보를 복호화함으로써 장치(350)에 의해 획득된다.

[0060] 즉, 요청된 정보, 예를 들어 데이터세트에 액세스하기 위해, 요청자는 이 정보를 보유하고 있는 시스템 또는 서버에 대해 인증해야 할 수 있다. 예를 들어 인증 자체는 WebAuthn 표준을 기반으로 할 수 있으며 소위 인증 장치가 필요할 수 있다. 시스템의 모든 사용자는 기존 사용자 이름-암호 인증을 위한 대체 방법으로 이러한 장치 중 하나 이상을 등록할 수 있다. 이러한 종류의 인증을 사용하면 클라이언트와 서버 간에 개인 데이터를 교환할 필요가 없을 수 있다. 예를 들어, 교환되는 유일한 데이터는 사용자 인증 장치를 기반으로 하는 공개 키이다.

[0061] 도 1 내지 도 3의 인증자(370)의 구성은 개략적이고 예시적이다. 장치(350) 또는 클라이언트(360)는 인증자(370)를 포함할 수 있다. 따라서 장치는 예를 들어 작동 중 언제든지 인증자에 액세스할 수 있다.

[0062] 일 실시 예에 따르면, 장치(350)는 디지털 인터페이스를 통해 인증자(370)에 액세스하도록 구성된다. 예를 들어, 인증자(370)는 디지털 인터페이스를 통해 장치(350)에 연결된 외부 장치의 일부일 수 있다. 따라서, 장치(350)는 외부 장치가 장치(350)에 연결된 경우, 인증자(370)를 통해서만 인증할 수 있다.

[0063] 일 실시 예에 따르면, 서버는 액세스 정보를 포함하고, 이 액세스 정보는 등록된 사용자를 데이터세트(310)에 대한 액세스 권한과 연관시키고 선택적으로 추가 데이터세트에 대한 액세스 권한과 연관시킨다.

[0064] 예를 들어, 데이터세트(310)에 대한 액세스 권한은 데이터세트(310)에 대한 특정 허가, 예를 들어, 데이터세트(310)를 특정 형식으로 수신하거나 데이터세트(310)를 다운로드, 삭제 또는 수정할 수 있는 권리를 포함할 수 있다. 예를 들어, 액세스 권한은 특정 사용자 또는 특정 사용자 또는 역할 그룹에 대해 정의될 수 있다. 예를 들어, 액세스 정보는 등록된 사용자를 하나 이상의 역할 또는 사용자 그룹과 연과시킨다.

[0065] 일 실시 예에 따르면, 서버(300)는 등록된 사용자와 관련된 인증자로 인증하는 클라이언트에게 데이터세트(310)에 대한 액세스 및 선택적으로 추가 데이터세트, 예를 들어 서버(300)에 의해 제공되는 모든 데이터세트에 대한 액세스를 제공하도록 구성된다.

[0066] 일 실시 예에 따르면, 서버(300)는 서버(300)에 대한 액세스를 요청하는 클라이언트(360)를 식별된 데이터세트로 연결하도록 구성된다.

[0067] 예를 들어, 클라이언트(360)는 고유 식별자(315)를 이용하여 서버(300)에 접속할 수 있다. 인증 후에, 서버(300)는 클라이언트(360)를 고유 식별자(315)에 의해 식별되는 데이터세트(310)로 연결할 수 있다. 선택적으로, 서버(300)는 인증을 다시 요구하지 않고 추가 데이터세트에 대한 액세스를 클라이언트(360)에게 제공할 수 있다.

[0068] 일 실시 예에 따르면, 장치(350)는 사용자 입력(382)을 수신하기 위한 입력 인터페이스(380)를 포함하고, 여기서 장치(350)는 사용자 입력(372)에 의존하여 인증 정보(372)를 서버에 선택적으로 제공하도록 구성된다.

[0069] 예를 들어, 장치(350)는 사용자에게 데이터세트(310)에 액세스하기 위한 요청을 능동적으로 개시하거나 사용자

입력(382)에 의해 데이터세트(310)에 액세스하기 위한 요청의 개시를 확인하도록 요구할 수 있다. 예를 들어, 장치는 사용자로 하여금 사용자 입력(382)을 통해 사용을 개시하거나 확인한 후에만 클라이언트(360)가 인증자(370)를 사용하도록 허용할 수 있다. 예를 들어, 사용자 입력(382)은 키보드, 터치 스크린, 스캐너 유닛, 또는 카메라를 통한 입력을 포함할 수 있다.

[0070] 일 실시 예에 따르면, 장치(350)는 사용자에 대한 생체 정보를 획득하도록 구성되며, 여기서 장치(350)는 생체 정보가 인증자(372)와 연관된 것으로 사용자를 식별하는 경우, 인증 정보(372)를 서버(300)에게 선택적으로 제공하도록 구성된다.

[0071] 예를 들어, 사용자 입력은 사용자의 지문 또는 사용자의 얼굴 이미지를 포함한다. 장치(350)는 인증자(370)를 사용하도록 허용된 하나 이상의 사용자의 신원과 인증자(370)를 연관시킬 수 있다. 예를 들어, 장치는 연관된 사용자가 사용자 입력(382)을 통해 사용을 개시하거나 확인한 후에만 클라이언트(360)가 인증자(370)를 사용하도록 허용할 수 있다.

[0072] 일 실시 예에 따르면, 장치(300)는 고유 식별자(315)를 나타내는 그래픽 패턴으로부터 고유 식별자(315)를 검색하도록 구성된다. 예를 들어, 장치는 선택적으로 장치(350)의 일부일 수 있거나 외부 장치일 수 있는, 스캐너 유닛 또는 카메라로부터 고유 식별자(315)를 수신할 수 있다.

[0073] 예를 들어, 사용자 입력(382)은 그래픽 패턴을 스캐닝하는 것을 포함할 수 있다. 예를 들어, 그래픽 패턴을 스캐닝하는 사용자는 그래픽 패턴에 의해 표현되는 고유 식별자에 의해 식별된 데이터세트에 액세스하기 위한 요청을 시작할 수 있다.

[0074] 4. 도 4에 따른 인증자의 등록

[0075] 도 4는 실시 예에 따른 인증자, 예를 들어 인증자(170, 270, 370)를 등록하기 위한 방법(400)의 흐름도를 도시한다. 등록될 인증자는 데이터세트를 획득하기 위한 장치, 예를 들어, 장치(150;250;350)의 일부일 수 있거나, 그러한 장치에 연결될 수 있다. 등록을 위해서, 인증자는 다른 장치에 연결할 수도 있다.

[0076] 방법(400)은 인증자의 초기 등록에 적용될 수 있다. 단계(402)는 사용자 이름과 비밀번호를 사용하여 개인 관리 페이지에 대한, 사용자, 예를 들어, 등록된 사용자의 로그인을 포함한다. 예를 들어, 관리 페이지는 서버(100;200;300)에 의해 호스팅될 수 있다. 관리 페이지는 등록된 인증자에 대한 정보를 서버(100;200;300)와 공유하도록 구성된 다른 서버에서 호스팅될 수도 있다. 다른 단계(403)에서, 사용자는 새로운 인증자를 등록하기 위한 옵션을 선택할 수 있다. 그 후, 단계 404에서, 서버는 사용자에게 브라우저 또는 특정 앱(즉, 애플 앱스토어와 유사한 것과 같은 소프트웨어) 명령을 따르도록 요청한다. 그 후, 단계 405에서 사용자는 인증자 특정 등록 프로세스를 따른다. 단계 406에서, 서버는 인증자로부터 공개 키 정보를 수신하고 저장하여 인증자의 등록을 완료한다.

[0077] 예를 들어 인증 장치 등록은 WebAuthn 표준[2]에서 정의한 원칙을 따를 수 있다. 최초 로그인에 성공하면, 사용자는 새 보안 키/장치를 등록할 수 있다. WebAuthn 사양에 따라 보안 장치는 플랫폼 인증자 또는 로밍 인증자가 될 수 있다. 주요 차이점은 플랫폼 인증자가 클라이언트 장치(예: 스마트폰 또는 랩톱)에 물리적으로 바인딩되는 반면, 로밍 인증자(예: USB 보안 키)는 이동식이며 다른 클라이언트 장치에 연결할 수 있다는 점이다. 등록 프로세스 동안에, 서버 측 구성 요소는 인증자에 의해 제공된 공개 키를 사용자 정보와 연관시킨다.

[0078] 5. 도 5에 따른 하나 이상의 데이터세트 제공 방법

[0079] 도 5는 디지털 통신 네트워크를 통해 하나 이상의 데이터세트, 예를 들어 데이터세트(110;210;310)를 제공하기 위한 방법(500)의 실시 예의 흐름도를 도시한다.

[0080] 방법(500)은 고유 식별자(115,215,315)를 식별된 데이터세트(110,210,310)와 연관시키는 단계(501)를 포함하고, 이 때 고유 식별자(115,215,315)는 디지털 통신 네트워크(90)를 통해 식별된 데이터세트(110,210,310)에 액세스하기 위한 네트워크 주소를 나타내고, 또한 고유 식별자(115;215;315)는 식별된 데이터세트에 고유하다. 추가 단계(502)는 고유 식별자(115,215,315)를 통해 하나 이상의 데이터세트에 대한 액세스를 요청하는 클라이언트(160,260,360)의 인증자(170,270,370)에 의해 제공되는 인증 정보(172,272,372)를 검증하는 단계(502)를 포함한다. 방법(500)은 인증 정보(172;272;372)가 인증자(170;270;370)를 등록된 사용자와 연관된다고 식별하는 경우 하나 이상의 데이터세트에 대한 액세스 권한을 클라이언트(160, 260, 360)에 선택적으로 제공하는 추가 단계(503)를 포함한다.

[0081] 도 5에 도시된 바와 같은 방법(500)의 단계들의 순서는 예시적으로 선택된다. 예를 들어, 단계 502 및 단계 503

은 단계 501과 독립적으로 실행될 수 있다.

[0082] 6. 도 6에 따른 데이터세트를 획득하는 방법

[0083] 도 6은 디지털 통신 네트워크(90)를 통해 데이터세트(110, 210, 310)를 획득하기 위한 방법(600)의 실시 예의 흐름도를 도시한다.

[0084] 방법(600)은 데이터세트(110,210,310)의 고유 식별자(115,215,315)를 획득하는 단계(601)를 포함하고, 고유 식별자(115,215,315)는 디지털 통신 네트워크(90)를 통해 데이터세트(110,210,310)에 액세스하기 위한 네트워크 주소를 나타내며, 여기서 고유 식별자(115,215,315)는 데이터세트(110,210,310)에 고유하다. 방법은 데이터세트(110,210,310)를 호스팅하는 서버(100,200,300)에 액세스하기 위한 요청을 전송하기 위해 고유 식별자(115,215,315)를 사용하는 추가 단계(602)를 포함한다. 추가 단계(603)는 서버(100,200,300)에 대해 클라이언트(160,260,360)를 인증하기 위한 인증자(170,270,370)의 인증 정보(172,272,372)를 서버(100,200,300)에 제공하는 것을 포함하고, 여기서 인증자(170;270;370)는 등록된 사용자와 연관된다.

[0085] 도 6에 도시된 바와 같은 방법(600)의 단계들의 순서는 예시적으로 선택된다. 예를 들어, 고유 식별자를 획득한 후(601), 단계(602 및 603)는 반복적으로 및/또는 단계(601)와는 독립적으로 실행될 수 있다.

[0086] 7. 도 7에 따른 데이터세트를 전송하는 방법

[0087] 도 7은 데이터세트를 획득하기 위한 장치와 서버 사이에서 데이터세트를 전송하기 위한 방법(700)의 실시 예의 흐름도를 도시한다. 예를 들어, 방법(700)은 서버(100;200;300) 또는 장치(150;250;350)에 의해 실행될 수 있는 방법(500, 600)의 특징을 결합할 수 있다.

[0088] 방법(700)은 분석된 데이터 항목, 예를 들어 데이터세트(110;210;310)에 대한 고유 URI를 개방하는 단계(702)를 포함한다. 예를 들어, 단계(702)는 단계(602)를 포함할 수 있다. 예를 들어 URI는 서버, 예를 들어, 서버(100;200;300)로 연결된다. 이후 단계 703에서 서버는 인증을 요청한다. 다음 단계 704에서, 사용자는 인증자, 예를 들어 인증자(170;270;370)를 통해 자신을 인증한다. 예를 들어, 단계(704)는 단계(603)를 포함할 수 있다. 단계 705에서, 서버는 인증이 성공적인 경우, 예를 들어 사용자가 등록된 사용자로서 또는 요청된 데이터세트에 액세스하도록 승인된 등록된 사용자로서 인증하는지를 결정한다. 예를 들어, 단계(705)는 단계(502)를 포함할 수 있다. 인증에 성공하면, 단계 706이 실행되고, 그렇지 않으면 단계 707이 실행된다. 단계 706에서, 서버는 분석된 데이터 항목으로 응답한다. 예를 들어, 단계 706은 단계 503을 포함할 수 있다. 단계 707에서, 서버는 예를 들어, 서버 또는 데이터 항목 또는 데이터세트에 대한 액세스를 거부한다.

[0089] 즉, 인증자, 예를 들어 인증자(170;270;370)의 성공적인 등록 후, 사용자는 사용자 이름이나 암호를 제공하지 않고, 제공된 URI, 예를 들어 고유 식별자(115;215;315)를 통해 분석된 데이터, 예를 들어 데이터세트(110;210;310)에 액세스할 수 있다. 예를 들어 URI를 입력하거나 2차원 코드를 스캔하여 URI를 열 때, 사용자는 등록된 인증자를 사용하여 자신을 인증해야 할 수 있다. 인증 프로세스 자체는 WebAuthn 호환 공개 키 인증 메커니즘의 원칙을 따를 수도 있으며, 여기서 서버는 사용자 인증자가 자신의 개인 키로 주어진 메시지에 암호로 서명하고 이를 서버로 보내도록 하여 인증 정보를 검증한다. 그 후 서버는 전송된 메시지가 공개 키로 확인될 수 있고, 서버에 저장될 수 있고, 사용자와 연관될 수 있는지를 확인한다[3].

[0090] 일 실시 예에 따르면, 이러한 인증 방법을 이용하게 되면, 정보에 액세스하기 위해서 사용자를 식별하도록 개인 데이터를 전송할 필요가 없을 수 있다.

[0091] 8. 추가 측면 및 실시 예

[0092] 본 개시의 실시 예는 인터넷을 통해 분석된 (건강 관리) 데이터에 대한 정보를 안전하게 검색하기 위한 방법 및 시스템에 관한 것이다. 예를 들어, 분석된 데이터와 수집된 데이터에 대한 정보 간의 고유한 일대일 관계를 보장하는 국제 표준에 따라 잘 구성된 URI[4]를 호출하는 클라이언트가 정보를 요청한다. URI 자체는 QR 코드, GS1 데이터 매트릭스 또는 유사한 기술 액세스 방식과 같은 2차원 코드로 인코딩되어 표시될 수 있으며, 이는 핸드헬드 및 고정 장치를 통해 액세스할 수 있다.

[0093] 일 실시 예에 따르면, 정보를 검색하기 위해서, 클라이언트는 웹 인증 API 사양[2] 또는 유사한 기술 액세스 방식을 기반으로 하는 공개 키 암호화 메커니즘을 사용하여 서버에 대해 자신을 인증해야 한다. 예를 들어, 클라이언트에 의해 인증 정보를 수신한 후에, 서버는 HTML 또는 json과 같은 구조화된 데이터 형식으로 정보를 제공한다.

[0094] 본 개시의 실시 예들은 편리하면서도 안전한 방법을 통해 분석된(헬스케어) 데이터를 안전하게 검색하기 위한 방법 및 시스템에 관한 것이다.

[0095] 본 개시의 실시 예는 데이터 항목의 ID를 고유하게 유지하고 요청 당사자의 ID를 안전하게 유지하면서, 인터넷을 통해 분석된 데이터에 대한 액세스를 안전하게 부여하기 위한 시스템에 관한 것이다.

[0096] 본 발명의 실시 예는 원격 서비스 시스템에 대한 가명 액세스를 생성하고, 가명 데이터를 사용하여 원격 시스템에 대해 특정 사용자를 인증하고, 특정 액세스 권한, 즉 사용자의 역할에 기반하는 권한을 부여할 수 있는 방법, 장치 또는 시스템에 관한 것이다. 따라서 잘못된 정보를 방지하기 위해 요청된 데이터를 고유하게 식별할 수 있다.

[0097] 암호화된 전송 프로토콜을 사용하여 보안 채널을 통한 정보 전송을 보호하는 데 많은 진전이 있었지만, 사용자 이름이나 이메일 주소와 같은 개인 정보에 의존하지 않는 새로운 인증 메커니즘의 발명에는 초점을 맞추지 않았다.

[0098] 예를 들어 개인 데이터에 의존하지 않고 최종적으로 요청된 정보를 구조화된 방식으로 제시하지 않고, WebauthN 표준을 사용하여 사용자를 인증하는 개체 식별을 위해 고유 URI을 결합하게 되면, 모듈식의 고유한 방식으로 설명된 현재 솔루션의 문제를 해결할 수 있다.

[0099] 예를 들어, 요청된 상제 정보, 예를 들어, 요청된 객체 또는 데이터세트의 고유 식별은 특히 특정 개인에 대한 정보를 포함하는 임상 데이터의 맥락에서 불가피하다.

[0100] 일부 측면이 장치의 맥락에서 설명되었지만, 이러한 측면은 또한 해당 방법에 대한 설명을 나타내며, 여기서 블록 또는 장치는 방법 단계 또는 방법 단계의 기능에 해당한다. 유사하게, 방법 단계의 맥락에서 설명된 측면은 또한 대응하는 장치의 대응 블록 또는 항목 또는 특징의 설명을 나타낸다.

[0101] 방법 단계의 일부 또는 전부는 예를 들어 마이크로프로세서, 프로그램 가능한 컴퓨터 또는 전자 회로와 같은 하드웨어 장치에 의해 (또는 이를 사용하여) 실행될 수 있다. 일부 실시 예에서, 가장 중요한 방법 단계 중 하나 이상이 그러한 장치에 의해 실행될 수 있다.

[0102] 특정 구현 요건에 따라, 본 발명의 실시 예는 하드웨어 또는 소프트웨어로 구현될 수 있다. 구현은 각각의 방법이 수행되도록 프로그래밍 가능한 컴퓨터 시스템과 협력하는(또는 협력할 수 있는), 전자적으로 판독 가능한 제어 신호가 저장된 플로피 디스크, DVD, Blu-Ray, CD, ROM, PROM, EPROM, EEPROM 또는 FLASH 메모리와 같은 디지털 저장 매체를 사용하여 수행할 수 있다. 따라서, 디지털 저장 매체는 컴퓨터 판독 가능하다.

[0103] 본 발명에 따른 일부 실시 예는 프로그램 가능한 컴퓨터 시스템과 협력하여 본 명세서에 설명된 방법 중 하나가 수행되도록 할 수 있는 전자적으로 판독 가능한 제어 신호를 갖는 데이터 캐리어를 포함한다.

[0104] 일반적으로, 본 발명의 실시 예는 프로그램 코드를 갖는 컴퓨터 프로그램 제품으로서 구현될 수 있으며, 프로그램 코드는 컴퓨터 프로그램 제품이 컴퓨터 상에서 실행될 때 방법들 중 하나를 수행하기 위해 동작한다. 프로그램 코드는 예를 들어 기계 판독 가능한 캐리어에 저장될 수 있다.

[0105] 다른 실시 예는 기계 판독 가능한 캐리어에 저장된, 본 명세서에 설명된 방법 중 하나를 수행하기 위한 컴퓨터 프로그램을 포함한다.

[0106] 다시 말해, 본 발명의 방법의 실시 예는 컴퓨터 프로그램이 컴퓨터에서 실행될 때, 본 명세서에서 설명된 방법들 중 하나를 수행하기 위한 프로그램 코드를 갖는 컴퓨터 프로그램이다.

[0107] 따라서, 본 발명의 방법의 추가 실시 예는 본 명세서에 기술된 방법 중 하나를 수행하기 위한 컴퓨터 프로그램을 포함하며 여기에 기록되어 있는, 데이터 캐리어(또는 디지털 저장 매체, 또는 컴퓨터 판독 가능 매체)이다. 데이터 매체, 디지털 저장 매체 또는 기록 매체는 일반적으로 유형 및/또는 비일시적이다.

[0108] 따라서, 본 발명의 방법의 추가 실시 예는 본 명세서에서 설명된 방법들 중 하나를 수행하기 위한 컴퓨터 프로그램을 나타내는 데이터 스트림 또는 신호들의 시퀀스이다. 데이터 스트림 또는 신호의 시퀀스는 예를 들어 인터넷을 통해 데이터 통신 연결을 통해 전송되도록 구성될 수 있다.

[0109] 추가 실시 예는 본 명세서에 설명된 방법들 중 하나를 수행하도록 구성되거나 적응된 처리 수단, 예를 들어 컴퓨터, 또는 프로그램 가능 논리 장치를 포함한다.

[0110] 추가 실시 예는 본 명세서에 설명된 방법 중 하나를 수행하기 위한 컴퓨터 프로그램이 설치된 컴퓨터를 포함한

다.

[0111] 본 발명에 따른 추가 실시 예는 본 명세서에 기술된 방법들 중 하나를 수행하기 위한 컴퓨터 프로그램을 수신기에 (예를 들어, 전자적으로 또는 광학적으로) 전송하도록 구성된 장치 또는 시스템을 포함한다. 수신기는 예를 들어 컴퓨터, 모바일 장치, 메모리 장치 등일 수 있다. 장치 또는 시스템은 예를 들어 컴퓨터 프로그램을 수신기에 전송하기 위한 파일 서버를 포함할 수 있다.

[0112] 일부 실시 예에서, 프로그램 가능 논리 장치(예: 필드 프로그램 가능 게이트 어레이)는 본 명세서에서 설명된 방법의 기능 중 일부 또는 전부를 수행하는 데 사용될 수 있다. 일부 실시 예에서, 필드 프로그램 가능 게이트 어레이는 본 명세서에서 설명된 방법 중 하나를 수행하기 위해 마이크로프로세서와 협력할 수 있다. 일반적으로, 방법은 바람직하게는 임의의 하드웨어 장치에 의해 수행된다.

[0113] 본 명세서에 기술된 장치는 하드웨어 장치를 사용하거나 컴퓨터를 사용하거나 하드웨어 장치와 컴퓨터의 조합을 사용하여 구현될 수 있다.

[0114] 본 명세서에 설명된 방법은 하드웨어 장치를 사용하거나 컴퓨터를 사용하거나 하드웨어 장치와 컴퓨터의 조합을 사용하여 수행될 수 있다.

[0115] 본 개시는 예시적인 실시 예를 참조하여 설명되었지만, 이 설명은 제한적인 의미로 해석되어서는 안된다. 예시적인 실시 예의 다양한 수정 및 조합, 뿐만 아니라 본 개시의 다른 실시 예는 설명을 참조하면 당업자에게 명백할 것이다. 따라서 첨부된 청구범위는 이러한 수정 또는 실시 예를 포함하는 것으로 의도된다.

[0116] 참고문헌

[0117] [1] https://tools.ietf.org/html/rfc3986

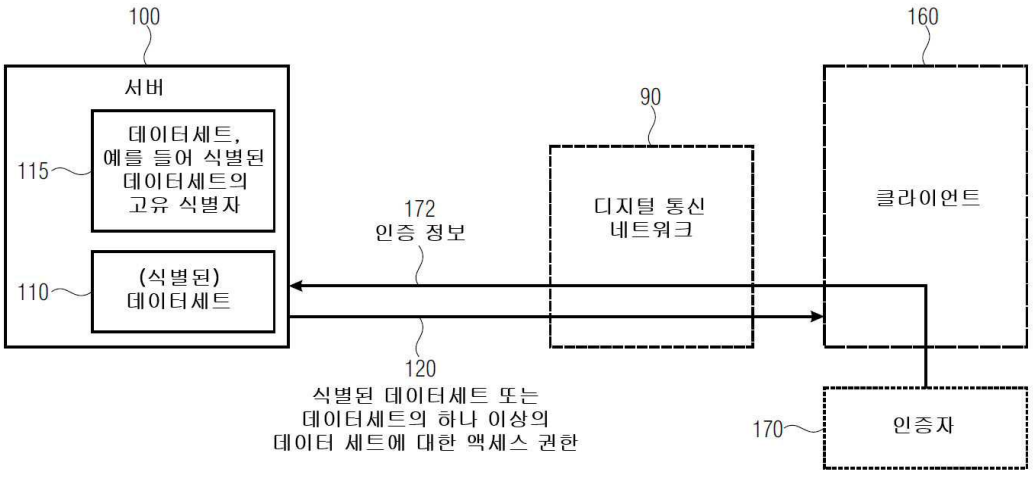
[0118] [2] https://w3c.github.io/webauthn/

[0119] [3] https://w3c.github.io/webauthn/#sctn-sample-authentication

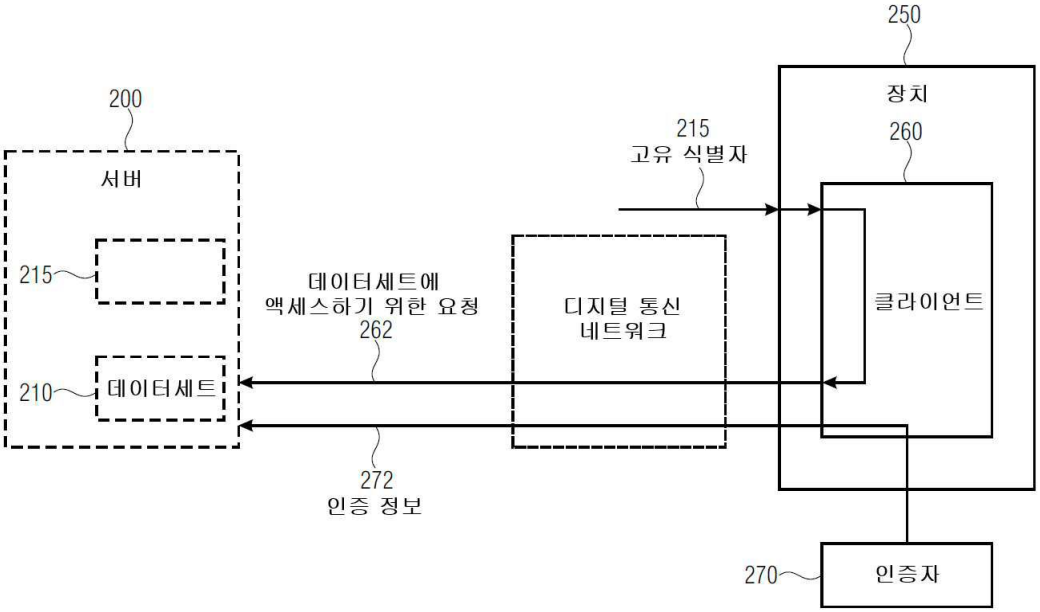
[0120] [4] https://tools.ietf.org/html/rfc1630

도면

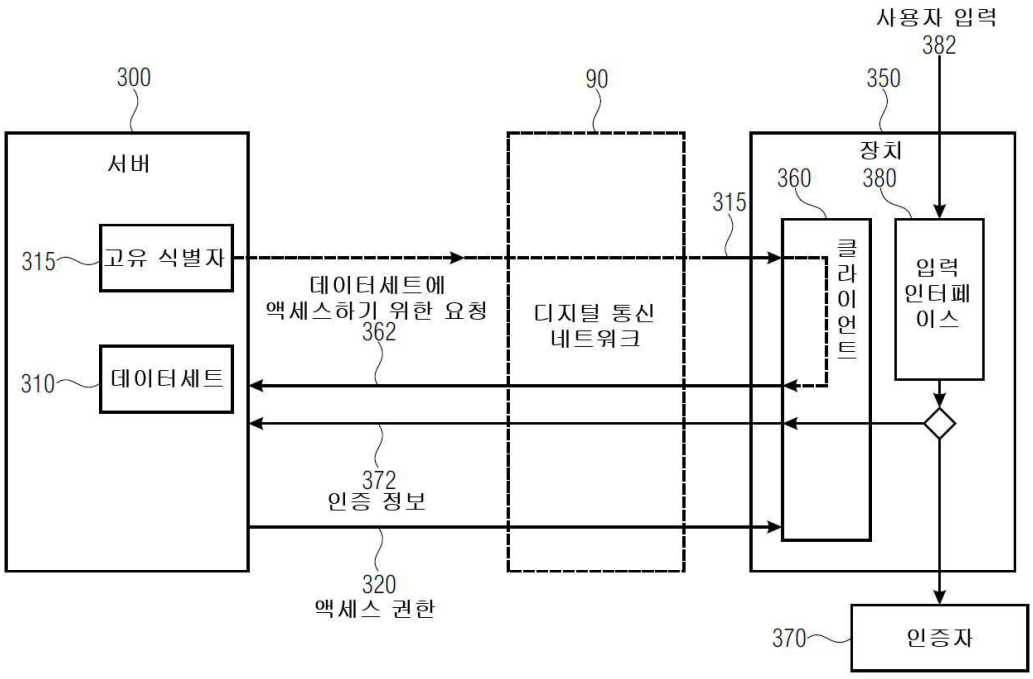
도면1



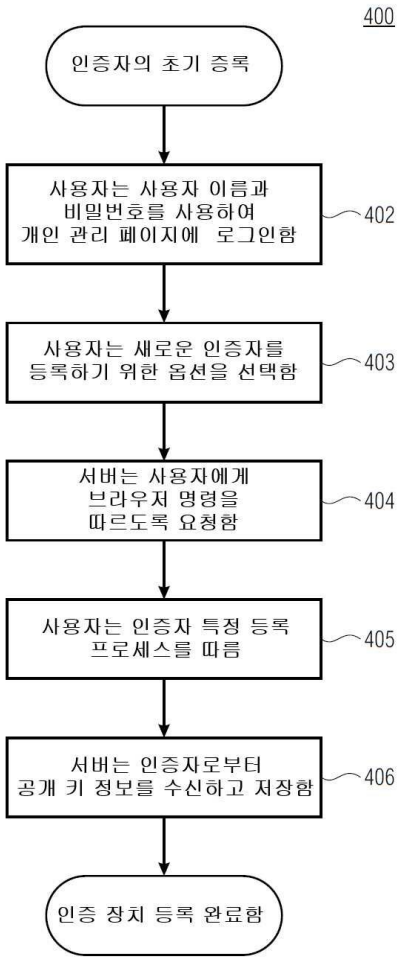
도면2


250
장치
200
서버
215
고유 식별자
260
215
데이터세트에
액세스하기 위한 요청
262
디지털 통신
네트워크
클라이언트
210
데이터세트
272
인증 정보
270
인증자

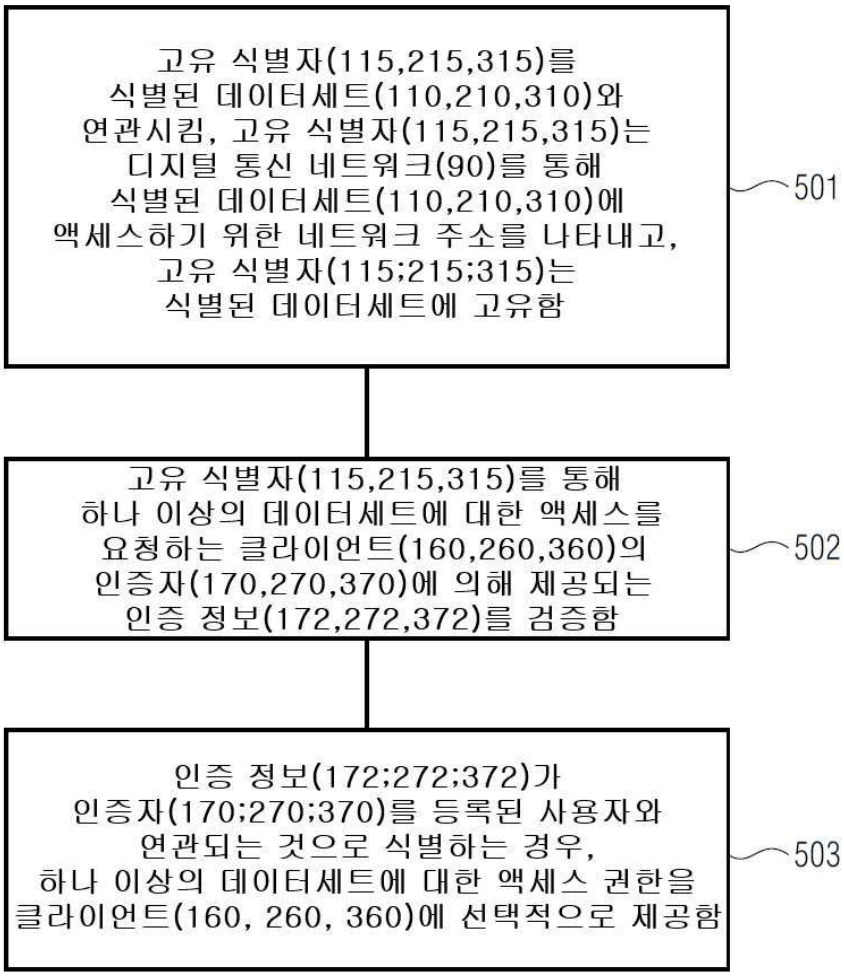
도면3


사용자 입력
382
300
90
350
서버
장치
360
380
315
315
고유 식별자
클라이언트
입력
인터페이스
데이터세트에
액세스하기 위한 요청
362
디지털 통신
네트워크
310
데이터세트
372
인증 정보
320
액세스 권한
370
인증자

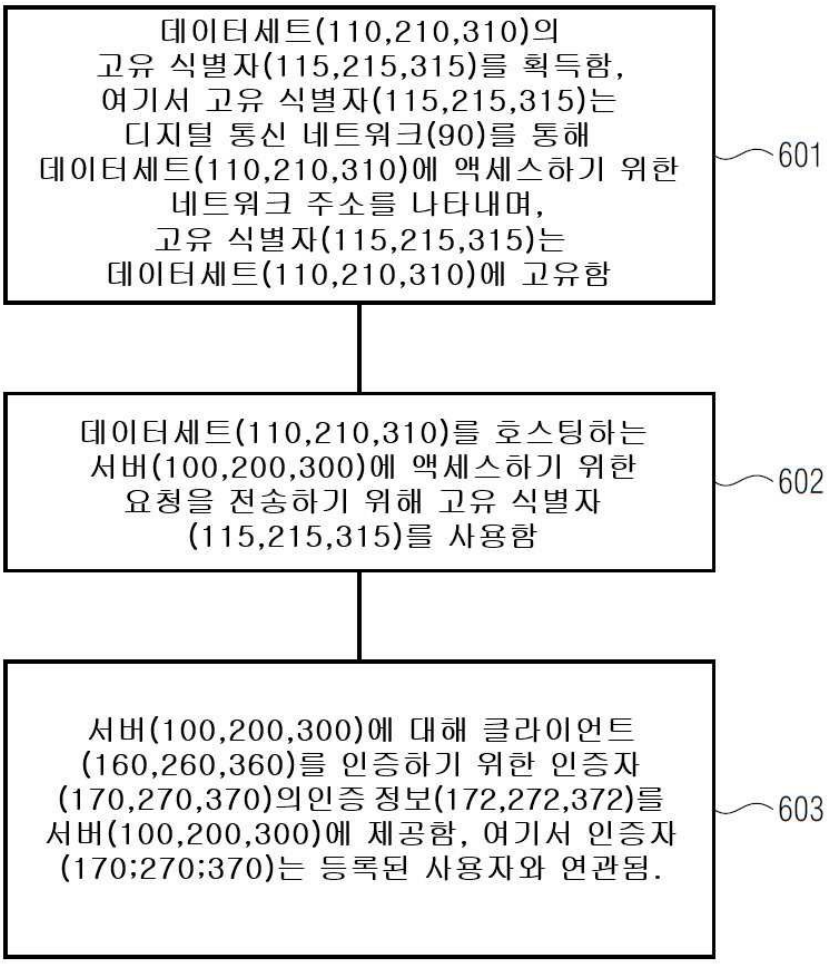
도면4


400
인증자의 초기 등록
사용자는 사용자 이름과 비밀번호를 사용하여 개인 관리 페이지에 로그인함
402
사용자는 새로운 인증자를 등록하기 위한 옵션을 선택함
403
서버는 사용자에게 브라우저 명령을 따르도록 요청함
404
사용자는 인증자 특정 등록 프로세스를 따름
405
서버는 인증자로부터 공개 키 정보를 수신하고 저장함
406
인증 장치 등록 완료함

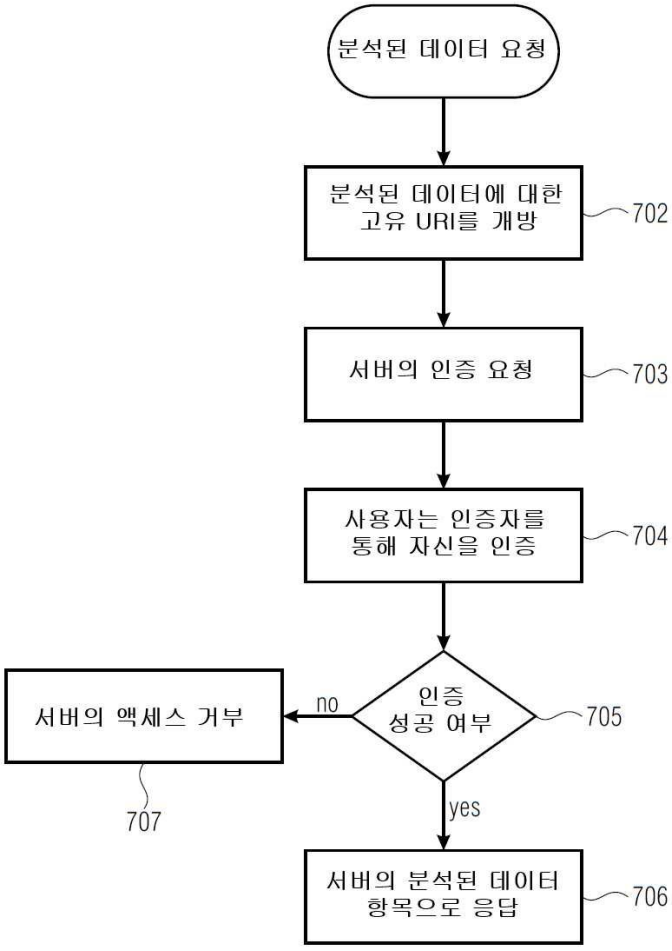
도면5


고유 식별자(115,215,315)를
식별된 데이터세트(110,210,310)와
연관시킴, 고유 식별자(115,215,315)는
디지털 통신 네트워크(90)를 통해
식별된 데이터세트(110,210,310)에
액세스하기 위한 네트워크 주소를 나타내고,
고유 식별자(115;215;315)는
식별된 데이터세트에 고유함
501
고유 식별자(115,215,315)를 통해
하나 이상의 데이터세트에 대한 액세스를
요청하는 클라이언트(160,260,360)의
인증자(170,270,370)에 의해 제공되는
인증 정보(172,272,372)를 검증함
502
인증 정보(172;272;372)가
인증자(170;270;370)를 등록된 사용자와
연관되는 것으로 식별하는 경우,
하나 이상의 데이터세트에 대한 액세스 권한을
클라이언트(160, 260, 360)에 선택적으로 제공함
503

도면6


데이터세트(110,210,310)의
고유 식별자(115,215,315)를 획득함,
여기서 고유 식별자(115,215,315)는
디지털 통신 네트워크(90)를 통해
데이터세트(110,210,310)에 액세스하기 위한
네트워크 주소를 나타내며,
고유 식별자(115,215,315)는
데이터세트(110,210,310)에 고유함
601
데이터세트(110,210,310)를 호스팅하는
서버(100,200,300)에 액세스하기 위한
요청을 전송하기 위해 고유 식별자
(115,215,315)를 사용함
602
서버(100,200,300)에 대해 클라이언트
(160,260,360)를 인증하기 위한 인증자
(170,270,370)의인증 정보(172,272,372)를
서버(100,200,300)에 제공함, 여기서 인증자
(170:270:370)는 등록된 사용자와 연관됨.
603

도면7


분석된 데이터 요청
분석된 데이터에 대한 고유 URI를 개방
702
서버의 인증 요청
703
사용자는 인증자를 통해 자신을 인증
704
인증 성공 여부
705
no
서버의 액세스 거부
707
yes
서버의 분석된 데이터 항목으로 응답
706