(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0032807
(43) 공개일자 2023년03월07일

(51) 국제특허분류(Int. Cl.)
G16H 70/00 (2018.01) *G16H 10/00* (2018.01)
H04L 9/32 (2006.01) *H04L 9/40* (2022.01)
(52) CPC특허분류
G16H 70/00 (2021.08)
G16H 10/00 (2021.08)
(21) 출원번호 10-2021-0135966
(22) 출원일자 2021년10월13일
심사청구일자 2021년10월13일
(30) 우선권주장
1020210115831 2021년08월31일 대한민국(KR)

(71) 출원인
고려대학교 세종산학협력단
세종특별자치시 조치원읍 세종로 2511 (고려대학교세종캠퍼스내)
(72) 발명자
문종섭
세종특별자치시 조치원읍 세종로 2511 (고려대학교세종캠퍼스내)
전승호
세종특별자치시 조치원읍 세종로 2511 (고려대학교세종캠퍼스내)
(74) 대리인
양성보

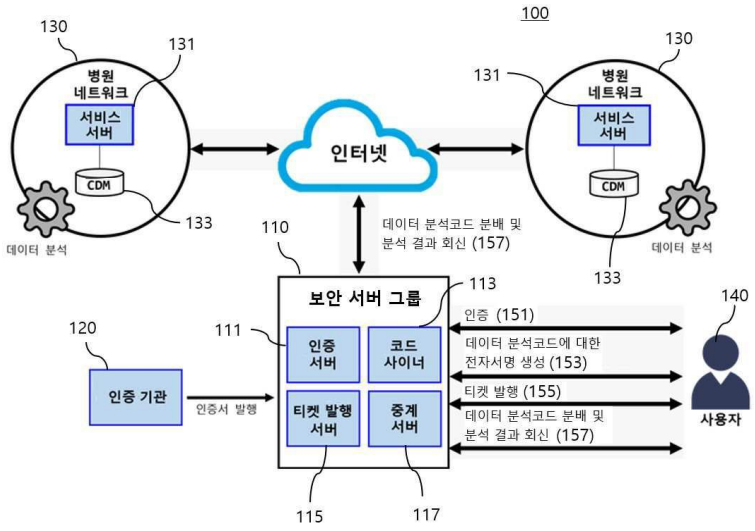
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **다기관 분산 환경에서 안전한 다기관 CDM 데이터를 분석하기 위한 플랫폼 시스템 및 그의 방법**

(57) 요 약

다양한 실시예들은 다기관 분산 환경에서 안전한 다기관 CDM 데이터를 분석하기 위한 플랫폼 시스템 및 그의 방법을 제공한다. 다양한 실시예들은, 인증 서버가 사용자를 위한 토큰을 생성하고, 코드 사이너가 사용자의 분석코드에 대한 전자서명을 생성하고, 티켓 발행 서버가 사용자를 위한 티켓을 발행하고, 각 병원의 서비스 서버가 티켓을 이용하여 사용자를 검증하고 전자서명을 이용하여 분석코드를 검증하고, 사용자 및 분석코드에 대한 검증에 성공 시, 서비스 서버가 분석코드를 실행하여, 병원의 CDM 데이터를 분석하며, 서비스 서버가 CDM 데이터에 대한 분석 결과를 사용자에게 회신하도록 구성된다.

대 표 도 - 도1



(52) CPC특허분류
H04L 63/0823 (2013.01)
H04L 63/083 (2013.01)
H04L 9/3213 (2013.01)
H04L 2209/88 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1465032868
과제번호	HI19C0791
부처명	보건복지부
과제관리(전문)기관명	한국보건산업진흥원
연구사업명	공익적 목적의 CDM 활용을 위한 제도 및 정보보호 기술연구
연구과제명	다기관 CDM 분산연구망을 위한 안전한 인증 및 데이터 분배 체계 연구
기 여 율	1/1
과제수행기관명	고려대학교 세종산학협력단
연구기간	2019.07.25 ~ 2021.12.31

명 세 서

청구범위

청구항 1

다기관 분산 환경에서 안전하게 다기관 CDM 데이터를 분석하기 위한 플랫폼 시스템에 있어서,

사용자를 위한 토큰을 생성하도록 구성되는 인증 서버;

상기 사용자의 분석코드에 대한 전자서명을 생성하도록 구성되는 코드 사이너;

상기 사용자를 위한 티켓을 발행하도록 구성되는 티켓 발행 서버; 및

각 병원에서, 상기 티켓을 이용하여 상기 사용자를 검증하고, 상기 전자서명을 이용하여 상기 분석코드를 검증하며, 상기 사용자 및 상기 분석코드에 대한 검증에 성공 시, 상기 분석코드를 실행하여, 상기 병원의 CDM 데이터를 분석하도록 구성되는 서비스 서버

를 포함하는,

플랫폼 시스템.

청구항 2

제 1 항에 있어서,

상기 인증 서버는,

상기 사용자로부터 상기 사용자의 식별 정보가 수신되면, 상기 식별 정보를 기반으로 상기 사용자를 인증하여, 상기 토큰을 생성하고,

상기 사용자에게 상기 토큰을 제공하도록 구성되는,

플랫폼 시스템.

청구항 3

제 1 항에 있어서,

상기 코드 사이너는,

상기 사용자로부터 상기 토큰 및 상기 분석코드가 수신되면, 개인키를 이용하여, 상기 분석코드에 대한 상기 전자서명을 생성하고,

상기 사용자에게 상기 전자서명을 제공하도록 구성되는,

플랫폼 시스템.

청구항 4

제 1 항에 있어서,

상기 분석코드는,

상기 사용자에 의해 작성되고, 각 병원의 CDM 데이터를 분석하기 위한 정보를 포함하는,

플랫폼 시스템.

청구항 5

제 1 항에 있어서,

상기 티켓 발행 서버는,

상기 사용자로부터 상기 토큰 및 상기 전자서명이 수신되면, 암호화 키를 이용하여, 상기 티켓을 생성하고,

상기 서비스 서버의 공개키를 이용하여, 상기 암호화 키를 암호화하고,

상기 사용자에게 상기 티켓을 상기 암호화 키와 함께 제공하도록 구성되는,

플랫폼 시스템.

청구항 6

제 1 항에 있어서,

상기 서비스 서버는,

상기 사용자에게 상기 CDM 데이터에 대한 분석 결과를 회신하도록 구성되는,

플랫폼 시스템.

청구항 7

제 6 항에 있어서,

상기 사용자와 상기 서비스 서버 간 통신을 중계하도록 구성되는 중계 서버

를 더 포함하고,

상기 중계 서버는,

상기 사용자로부터 상기 토큰, 상기 전자서명, 및 상기 티켓이 수신되면, 상기 토큰을 이용하여, 상기 사용자를 확인하고,

상기 서비스 서버에 상기 전자서명 및 상기 티켓을 전달하도록 구성되는,

플랫폼 시스템.

청구항 8

제 7 항에 있어서,

상기 서비스 서버는,

상기 분석 결과를 상기 중계 서버에 회신하도록 구성되고,

상기 사용자는,

상기 중계 서버로부터 상기 분석 결과를 다운로드하는,

플랫폼 시스템.

청구항 9

제 7 항에 있어서,

상기 서비스 서버는,

관리자의 승인을 기반으로, 상기 분석코드를 실행하여, 상기 CDM 데이터를 분석하고,

상기 관리자의 승인을 기반으로, 상기 분석 결과를 상기 사용자에게 회신하도록 구성되는,

플랫폼 시스템.

청구항 10

제 7 항에 있어서,

상기 서비스 서버는,

상기 사용자가 화이트리스트에 등록되어 있으면, 상기 분석 결과를 상기 사용자에게 회신하고,

상기 사용자가 상기 화이트리스트에 등록되어 있지 않으면, 관리자의 승인을 기반으로, 상기 분석 결과를 상기 사용자에게 회신하도록 구성되는,

플랫폼 시스템.

청구항 11

다기관 분산 환경에서 안전하게 다기관 CDM 데이터를 분석하기 위한 플랫폼 시스템의 방법에 있어서,

인증 서버가 사용자를 위한 토큰을 생성하는 단계;

코드 사이너가 상기 사용자의 분석코드에 대한 전자서명을 생성하는 단계;

티켓 발행 서버가 상기 사용자를 위한 티켓을 발행하는 단계;

각 병원의 서비스 서버가 상기 티켓을 이용하여 상기 사용자를 검증하고, 상기 전자서명을 이용하여 상기 분석코드를 검증하는 단계; 및

상기 사용자 및 상기 분석코드에 대한 검증에 성공 시, 상기 서비스 서버가 상기 분석코드를 실행하여, 상기 병원의 CDM 데이터를 분석하는 단계

를 포함하는,

플랫폼 시스템의 방법.

청구항 12

제 11 항에 있어서,

상기 토큰을 생성하는 단계는,

상기 사용자가 상기 인증 서버에 상기 사용자의 식별 정보를 전송하는 단계;

상기 인증 서버가 상기 식별 정보를 기반으로 상기 사용자를 인증하여, 상기 토큰을 생성하는 단계; 및

상기 인증 서버가 상기 사용자에게 상기 토큰을 제공하는 단계

를 포함하는,

플랫폼 시스템의 방법.

청구항 13

제 11 항에 있어서,

상기 전자서명을 생성하는 단계는,

상기 사용자가 상기 코드 사이너에 상기 코드 사이너에 상기 토큰 및 상기 분석코드를 전송하는 단계;

상기 코드 사이너가 개인키를 이용하여, 상기 분석코드에 대한 상기 전자서명을 생성하는 단계; 및

상기 코드 사이너가 상기 사용자에게 상기 전자서명을 제공하는 단계

를 포함하는,

플랫폼 시스템의 방법.

청구항 14

제 11 항에 있어서,

상기 분석코드는,

상기 사용자에 의해 작성되고, 각 병원의 CDM 데이터를 분석하기 위한 정보를 포함하는,

플랫폼 시스템의 방법.

청구항 15

제 11 항에 있어서,

상기 티켓을 발행하는 단계는,

상기 사용자가 상기 티켓 발행 서버에 상기 토큰 및 상기 전자서명을 전송하는 단계;

상기 티켓 발행 서버가 암호화 키를 이용하여, 상기 티켓을 생성하는 단계;

상기 티켓 발행 서버가 상기 서비스 서버의 공개키를 이용하여, 상기 암호화 키를 암호화하는 단계; 및

상기 티켓 발행 서버가 상기 사용자에게 상기 티켓을 상기 암호화 키와 함께 제공하는 단계

를 포함하는,

플랫폼 시스템의 방법.

청구항 16

제 11 항에 있어서,

상기 서비스 서버가 상기 사용자에게 상기 CDM 데이터에 대한 분석 결과를 회신하는 단계

를 더 포함하는,

플랫폼 시스템의 방법.

청구항 17

제 16 항에 있어서,

상기 사용자 및 상기 분석 코드를 검증하는 단계는,

상기 사용자가 중계 서버에 상기 토큰, 상기 전자서명, 및 상기 티켓을 전송하는 단계;

상기 중계 서버가 상기 토큰을 이용하여, 상기 사용자를 확인하는 단계;

상기 중계 서버가 상기 서비스 서버에 상기 전자서명 및 티켓을 전달하는 단계; 및

상기 서비스 서버가 상기 티켓을 이용하여 상기 사용자를 검증하고, 상기 전자서명을 이용하여 상기 분석코드를 검증하는 단계

를 포함하는,

플랫폼 시스템의 방법.

청구항 18

제 17 항에 있어서,

상기 분석 결과를 회신하는 단계는,

상기 서비스 서버가 상기 분석 결과를 상기 중계 서버에 회신하는 단계; 및

상기 사용자가 상기 중계 서버로부터 상기 분석 결과를 다운로드하는 단계

를 포함하는,

플랫폼 시스템의 방법.

청구항 19

제 17 항에 있어서,

상기 CDM 데이터를 분석하는 단계는,

상기 서비스 서버가 관리자의 승인을 기반으로, 상기 분석코드를 실행하여, 상기 CDM 데이터를 분석하는 단계

를 포함하고,

상기 분석 결과를 회신하는 단계는,

상기 관리자의 승인을 기반으로, 상기 분석 결과를 상기 사용자에게 회신하는 단계

를 포함하는,

플랫폼 시스템의 방법.

청구항 20

제 17 항에 있어서,

상기 분석 결과를 회신하는 단계는,

상기 사용자가 화이트리스트에 등록되어 있으면, 상기 서비스 서버가 상기 분석 결과를 상기 사용자에게 회신하는 단계; 및

상기 사용자가 상기 화이트리스트에 등록되어 있지 않으면, 상기 서비스 서버가 관리자의 승인을 기반으로, 상기 분석 결과를 상기 사용자에게 회신하는 단계

를 포함하는,

플랫폼 시스템의 방법.

발명의 설명

기 술 분 야

[0001] 다양한 실시예들은 의료 정보 시스템 및 그의 방법에 관한 것으로, 보다 세부적으로는 여러 병원의 의료 데이터

를 안전하고 편리하게 분석하기 위한 네트워크 보안 플랫폼 시스템 및 그의 방법에 관한 것이다.

배 경 기 술

[0002] 지난 수십년간 전세계 각 지역의 병원들은 환자에 대한 진료 및 관찰 데이터를 수집해 빅데이터를 형성했다. 하지만, 헬스 빅데이터는 병원별로 각기 다른 양식으로 보관되고 있기 때문에 다기관 연구에 적합하지 않다. 이에 국제 비영리 단체인 OHDSI(observational health data sciences and informatics)는 헬스 빅데이터 분석을 지원하기 위한 많은 소프트웨어를 제시했다.

[0003] 첫 번째로, OHDSI는 병원별로 상이한 데이터 양식을 표준화하기 위해 OMOP-CDM(observational medical outcomes partnership common data model)을 제공한다. OMOP-CDM은 진료 및 관찰 데이터를 저장하기 위한 공통된 데이터베이스 스키마이다. OMOP-CDM은 오라클(Oracle) 및 MS SQL 서버와 같은 대중적으로 사용되는 DBMS를 지원한다. 병원의 데이터 큐레이터는 ETL(extract-transform-load)을 통해 원내의 원본 의료 데이터를 OMOP-CDM으로 변환한다.

[0004] 두 번째로, OHDSI는 OMOP-CDM으로 변환된 의료 데이터를 분석하기 위한 플랫폼으로 아틀라스(Atlas)를 제공한다. 아틀라스는 웹 애플리케이션 형태로 구현되었으며, 코호트 정의와 같은 기능을 지원한다. 아틀라스의 가장 특징적인 기능은 데이터를 분석하기 위한 분석코드를 자동으로 생성하는 것이다. 이 분석코드는 R 언어로 작성되어 있다. 사용자는 아틀라스를 통해 생성한 분석코드를 자신의 로컬 컴퓨팅 환경에서 실행하여 의료 데이터를 분석한다. 이 분석코드는 실행 중 원격의 OMOP-CDM 데이터베이스에 접속하여 필요한 데이터를 읽는다. 또한, 2개 이상의 병원이 OMOP-CDM 데이터베이스를 마련했다면, 사용자는 동일한 분석코드를 통해 해당 병원들의 데이터를 손 쉽게 분석할 수 있다.

[0005] 이와 같이 OHIDS가 OMOP-CDM으로 표현된 의료 데이터를 분석하기 위한 다양한 소프트웨어를 지원하지만, 아틀라스와 OMOP-CDM은 여전히 몇 가지 문제들을 가지고 있다. 그들 중 하나는, OMOP-CDM 데이터가 의료 데이터에 대한 통일된 표현을 제공하지만, 병원들은 여전히 데이터베이스를 외부로부터 격리된 원내 네트워크에 보관한다는 것이다. 이러한 운영 환경은 외부 사용자의 데이터에 대한 접근성을 떨어뜨린다. 그들 중 다른 하나는, 사용자는 여전히 데이터에 접근하기 위해 각 병원에 개별적으로 신원을 증명해야 한다는 것이다. 다시 말해, 각 병원은 사용자를 인증하기 위한 계정 데이터베이스를 별도로 운영해야 한다.

[0006] 사용자에 대한 인증은 네트워크를 통한 원격 서비스 개발에 필수이다. 인가된 사용자에게만 서비스를 제공해야 하기 때문이다. 특히, 서비스들이 네트워크 상에 분산된 경우, 특별한 인증 프로토콜이 요구된다. 분산 환경에 대한 고려 없이, 인증 프로토콜을 설계할 경우, 서비스 별로 사용자의 계정 데이터베이스를 운영해야 한다. 커버로스(Kerberos)는 이를 해결하기 위해 고안되었다.

[0007] 커버로스는 사용자 인증과 서비스 접근 인가를 분리하는 것을 목표로 하며, 이를 위해 3개의 주요 구성요소들, 즉, 인증 서버, 티켓 발행 서버, 및 서비스 서버를 요구한다. 이들 중 서비스 서버는 앞서 언급한 네트워크 상에 분산된 서비스를 의미하며, 서비스를 제공하는 (CDM 데이터 분석하는) 서버로써, 여러 개이다. 인증 서버는 사용자의 계정 데이터베이스와 연동하여 사용자의 신원을 검증하는 역할을 수행한다. 신원이 확인된 사용자는 인증 서버로부터 티켓 발생 서버를 이용할 수 있는 티켓이 발행된다. 티켓 발행 서버는 신원이 확인된 사용자에게 서비스 서버를 이용할 수 있게 하는 티켓을 발행한다. 티켓 발행 서버가 발급한 티켓을 서비스 서버가 검증함으로써, 서비스 서버는 별도의 사용자 계정 데이터베이스 없이 사용자에게 서비스 접근을 인가할 수 있다. 또한 사용자가 새로운 서비스 서버에 접근할 경우, 인증 서버를 통해 처음부터 신원 증명을 수행하지 않고, 티켓 발행 서버에 인증 서버의 티켓만 제시함으로써, 서비스 서버에 대한 접근 권한을 획득할 수 있다.

[0008] 커버로스가 분산 네트워크 환경에서 편리한 사용자 인증을 제공하지만, 사용자가 한 번에 하나의 서비스에만 접근할 수 있도록 한다. 또한 커버로스는 사용자의 신원을 입증하기 위한 정보만 암호화되어 전달될 뿐, 추가적인 데이터를 안전하게 전달하기 위한 수단은 서비스에 의존한다.

발명의 내용

해결하려는 과제

[0009] 전술한 바와 같이, 병원들은 관리와 보안상의 이유로 의료 데이터를 기관의 로컬 네트워크 내에 보관한다. 이러한 세팅은 분석할 자원(의료 데이터)가 네트워크상에 분산되게 하기 때문에, 의료 데이터를 통합하기 위한 고민을 강구하게 한다. 한편, 일반적으로, 병원은 개별적으로 데이터를 누적해왔기 때문에 고유의 데이터를 저장하

기 위한 고유의 양식을 가지고 있다. 데이터 양식의 차이는 각 기관으로부터 수집된 의료 데이터를 병합하고, 나아가 분석할 때 걸림돌이 될 수 있다. 또한, 적절한 보안 없이 데이터를 병원 전산망 밖으로 전송하는 것은 환자의 프라이버시를 침해할 수 있다. 아울러, 기관들 간에 안전한 네트워크 채널을 통해 의료 데이터를 전달하더라도 환자들은 자신의 개인정보가 포함되는 것을 원치 않을 수 있다.

[0010] 따라서, 다양한 실시예들은, 인터넷상에 위치한 플랫폼의 보안 서버 그룹으로부터 인증된 사용자가 플랫폼에 연결된 병원들의 서버에 의료 데이터 분석코드를 안전하고 신속하게 전달하고, 분석 결과 또한 안전하고 신속하게 회신 받는데 그 목적이 있다.

과제의 해결 수단

[0011] 다양한 실시예들은 다기관 분산 환경에서 안전한 다기관 CDM 데이터를 분석하기 위한 플랫폼 시스템 및 그의 방법을 제공한다.

[0012] 다양한 실시예들에 따른 플랫폼 시스템은, 사용자를 위한 토큰을 생성하도록 구성되는 인증 서버, 상기 사용자의 분석코드에 대한 전자서명을 생성하도록 구성되는 코드 사이너, 상기 사용자를 위한 티켓을 발행하도록 구성되는 티켓 발행 서버, 및 각 병원에서, 상기 티켓을 이용하여 상기 사용자를 검증하고, 상기 전자서명을 이용하여 상기 분석코드를 검증하며, 상기 사용자 및 상기 분석코드에 대한 검증에 성공 시, 상기 분석코드를 실행하여, 상기 병원의 CDM 데이터를 분석하도록 구성되는 서비스 서버를 포함한다.

[0013] 다양한 실시예들에 따른 플랫폼 시스템의 방법은, 인증 서버가 사용자를 위한 토큰을 생성하는 단계, 코드 사이너가 상기 사용자의 분석코드에 대한 전자서명을 생성하는 단계, 티켓 발행 서버가 상기 사용자를 위한 티켓을 발행하는 단계, 각 병원의 서비스 서버가 상기 티켓을 이용하여 상기 사용자를 검증하고, 상기 전자서명을 이용하여 상기 분석코드를 검증하는 단계, 및 상기 사용자 및 상기 분석코드에 대한 검증에 성공 시, 상기 서비스 서버가 상기 분석코드를 실행하여, 상기 병원의 CDM 데이터를 분석하는 단계를 포함한다.

발명의 효과

[0014] 다양한 실시예들에 따르면, 플랫폼에 연결된 병원들의 의료 데이터가 CDM으로 통일화되기 때문에, 외부 연구자가 동일한 방법론을 통해 여러 병원의 데이터를 분석할 수 있다. 그리고, CDM 데이터가 병원의 로컬 네트워크 밖으로 전송되지 않고, 내부, 즉 서비스 서버에서만 분석되기 때문에, 환자들은 개인정보를 병원 외부로의 유출을 염려하지 않아도 된다.

[0015] 다양한 실시예들에 따르면, 사용자들은 병원의 로컬 네트워크 외부에 위치한 플랫폼의 보안 서버 그룹을 통해 (여러 단계의) 인증을 수행한다. 인증에 통과한 사용자는 데이터 분석을 요청할 각 병원에서 추가로 인증을 수행하지 않는다. 따라서, 각 병원은 사용자의 신원을 확인하기 위한 계정 데이터베이스를 운영하지 않아도 된다.

[0016] 사용자가 작성한 CDM 데이터 분석코드는 사용자로부터 병원의 서비스 서버까지 전달되는 동안 제3자에 의해 변조되어서는 안된다. 다양한 실시예들은 이 과정에서 분석코드의 무결성을 보장할 수 있다.

도면의 간단한 설명

[0017] 도 1은 다양한 실시예들에 따른 다기관 분산 환경에서 안전한 다기관 CDM 데이터를 분석하기 위한 플랫폼 시스템 및 그의 방법을 개략적으로 도시하는 도면이다.

도 2는 도 1의 사용자가 인증 서버를 통해 플랫폼의 인증을 수행하는 과정를 세부적으로 도시하는 도면이다.

도 3은 도 1의 사용자가 CDM 데이터를 분석하기 위한 분석코드에 대한 전자서명을 코드 사이너로부터 발급받는 과정을 세부적으로 도시하는 도면이다.

도 4는 도 1의 사용자가 티켓 발행 서버를 통해 플랫폼의 모든 병원의 CDM 데이터 접근하기 위한 티켓을 발급받는 과정을 세부적으로 도시하는 도면이다.

도 5 및 도 6은 도 1의 사용자가 중계 서버를 통해 티켓과 전자서명이 포함된 분석코드를 플랫폼에 연결된 모든 병원에 분배하고, 분석 결과를 회신받는 과정를 세부적으로 도시하는 도면들이다.

도 7은 다양한 실시예들에 따른 플랫폼 시스템의 서비스 서버의 내부 구성을 도시하는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0018] 이하, 본 문서의 다양한 실시예들이 첨부된 도면을 참조하여 설명된다.

[0020] 도 1은 다양한 실시예들에 따른 다기관 분산 환경에서 안전한 다기관 CDM 데이터를 분석하기 위한 플랫폼 시스템(100) 및 그의 방법을 개략적으로 도시하는 도면이다.

[0021] 도 1을 참조하면, 다양한 실시예들에 따른 플랫폼 시스템(100)은, 병원들의 각각이 CDM 데이터를 자체 서버에 보관하면서, 네트워크로 연결되는 분산 네트워크 위에서 구축된다. 구체적으로, 플랫폼 시스템(100)은 보안 서버 그룹(110), 인증 기관(certificate authority; CA) (120), 및 각 병원의 병원 네트워크(130)를 포함한다. 보안 서버 그룹(110)은 인증 서버(authentication server; AS)(111), 코드 사이너(code signer; CS)(113), 티켓 발행 서버(ticket-granting server; TGS)(115), 및 중계 서버(relaying server; RS)(117)로 구성된다. 보안 서버 그룹(110)의 각 서버(111, 113, 115, 117)들은 하나의 컴퓨터 내의 각 응용 프로그램 형태로 구현되거나, 네트워크에 연결되어 있는 복수의 컴퓨터들의 각각에 독립적으로 구현될 수 있다. 독립적으로 동작하는 인증 기관(120)은 인터넷을 통해 보안 서버 그룹(110)에 연결된다. 병원 네트워크(130)는 서비스 서버(service server; SS)(131) 및 CDM 데이터를 위한 데이터베이스(133)로 구성된다. 이 플랫폼 시스템(100)은 의료 CDM으로써 OMOP-CDM을 사용한다. 따라서, 플랫폼 시스템(100)은 OMOP-CDM으로 변환된 의료 데이터를 분석하기 위해 R 언어로 작성된 분석코드(analysis codes; AC)를 이용한다. 병원 네트워크(130)는 인터넷을 통해 보안 서버 그룹(110)에 연결된다.

[0022] 이 플랫폼 시스템(100)을 구성하는 각 컴포넌트와 사용자(140)가 플랫폼 시스템(100)에 연결된 병원의 데이터를 분석하는 방법은 다음과 같다. 먼저, 151 단계에서, 사용자(140)가 보안 서버 그룹(110)에 자신의 신원을 증명한다. 인증 서버(111)가 사용자 인증을 책임지고, 인증된 사용자(140)에게 토큰을 발행한다. 이어서, 153 단계에서, 사용자(140)는 분석코드를 코드 사이너(113)에 보내어, 코드 사이너(113)를 통해 병원들이 보유한 의료 CDM 데이터를 분석하기 위해 작성한 분석코드에 대한 전자서명을 획득한다. 계속해서, 155 단계에서, 사용자(140)는 티켓 발행 서버(115)로부터 각 병원의 서비스 서버(131)를 이용하기 위한 티켓을 발급받는다. 마지막으로, 157 단계에서, 사용자(140)는 중계 서버(117)를 통해 티켓과 전자서명이 포함된 분석코드를 플랫폼에 연결된 모든 병원에 분배하고, 분석 결과를 회신받는다. 이 모든 과정이 안전하게 운영되기 위한 사전 작업으로써 사용자(140)와 플랫폼을 구성하는 모든 컴포넌트는 각자 개인키와 공개키를 생성하고, 인증 기관(120)으로부터 공개키 인증서를 발급받는다. 이 인증서는 현시점에서 가장 널리 보편적으로 사용되고 있는 X.509 version 3 표준을 따른다. 플랫폼 참여자들은 일반적인 전자 금융 거래와 유사하게 인증서를 발급받을 수 있다.

[0024] 도 2는 도 1의 사용자(140)가 인증 서버(111)를 통해 플랫폼의 인증을 수행하는 과정(151 단계)를 세부적으로 도시하는 도면이다.

[0025] 도 2를 참조하면, 플랫폼을 이용하려는 사용자(140)는 211 단계에서, 인증 서버(111)에 신원을 증명을 요청하기 위해 아이디(ID)와 패스워드(password), 또는 생체 정보(biometric)와 같은 사용자(140)의 식별 정보(ID_C)를 포함하는 메시지(M_{C-AS})와 이에 대한 서명($sig_{M_{C-AS}}$)을 전달한다. 메시지와 함께 서명이 전달되는 이유는 메시지가 네트워크를 통해 전달되는 동안 공격자에 의해 변조되는 것을 방지하고, 송신자를 확인하기 위함이다. 플랫폼의 모든 컴포넌트는 항상 이와 같이 메시지와 서명 쌍을 전달하기 때문에 특별한 경우를 제외하고 앞으로 편의상 서명에 대한 설명은 생략한다.

[0026] 만약 적법한 사용자(140)라면, 인증 서버(111)는 213 단계에서, 암호학적으로 생성된 토큰(token)을 포함한 메시지(M_{AS-C})와 이에 대한 서명($sig_{M_{AS-C}}$)를 사용자(140)에게 반환한다. 이 토큰(token)은 사용자(140)의 신원과 유효기간을 DES(data encryption standard)나 AES(advanced encryption standard)와 같은 대칭키 암호 알고리즘으로 암호화하여 생성된다. 따라서, 토큰(token) 생성에 사용된 키를 알고 있는 참여자만 토큰(token)의 유효성을 검증할 수 있다. 인증 서버(111)는 제3자가 임의로 토큰(token)을 생성하는 것을 방지하기 위해 토큰(token) 생성에 사용된 키를 누구와도 공유하지 않는다. 반대로, 플랫폼에 등록되지 않은 사용자(140)나 불법적인 요청이라면, 인증 서버(111)는 인증 실패 응답을 사용자(140)에게 전달하고, 사용자(140)는 플랫폼의 어떠한 서비스도 이용할 수 없다.

[0028] 도 3은 도 1의 사용자(140)가 CDM 데이터를 분석하기 위한 분석코드(AC)에 대한 전자서명을 코드 사이너(113)로부터 발급받는 과정(153 단계)을 세부적으로 도시하는 도면이다.

[0029] 도 3을 참조하면, 코드 사이너(113)에 접근하기 전에, 사용자(140)는 플랫폼을 통해 병원들의 CDM 데이터를 분석하기 위한 분석코드(AC)를 작성한다. 분석코드(AC)는 다양한 방식으로 작성될 수 있다. 플랫폼이 OMOP-CDM에 기반해 구현되었기 때문에, 사용자(140)는 OHDSI에서 제공하는 소프트웨어를 이용한다. 따라서, 분석코드(AC)는 일반적으로 R 언어로 작성된다. 분석코드(AC)는 코호트 정의와 SQL 질의문 같이 CDM 데이터를 분석하기 위한 모든 정보를 포함한다. 분석코드(AC)는 의료 데이터를 분석에 사용하기 때문에 네트워크를 통해 각 병원에 전달되기까지 어떠한 방식으로든 변조되어서는 안된다. 전자서명은 데이터의 무결성과 전송에서의 부인방지를 위해 사용된다. 이 요구사항을 만족하기 위해 사용자(140)는 코드 사이너(113)에게 분석코드(AC)에 대한 전자서명 생성을 요청한다. 이를 위해, 사용자(140)는, 311 단계에서, 이전 단계(213 단계)에서 인증 서버(111)로부터 발급받은 토큰(token)과 분석코드(AC)를 포함한 메시지(M_{C-CS})와 이에 대한 서명($sig_{M_{C-CS}}$)을 코드 사이너(113)에 전달한다.

[0030] 메시지에 이상이 없다면, 코드 사이너(113)는 313 단계에서, 자신의 개인키를 이용해 분석코드(AC)에 대한 전자서명(sig^{AC})을 생성하고, 이를 포함하는 메시지(M_{CS-C})와 이에 대한 서명($sig_{M_{CS-C}}$)을 사용자(140)에게 응답으로 전달한다. 이 전자서명은 코드 사이너(113)의 개인키로 생성되었기 때문에 코드 사이너(113)를 제외한 누구도 동일한 전자서명을 생성할 수 없다. 반면, 코드 사이너(113)의 공개키를 획득할 수 있다면 누구나 전자서명을 검증할 수 있다. 만약 사용자(140)가 분석코드(AC)의 일부를 수정하거나, 완전히 새로운 분석코드(AC)를 작성할 경우, 코드 사이너(113)에 새로운 전자서명 생성을 요청해야 한다.

[0032] 도 4는 도 1의 사용자(140)가 티켓 발행 서버(115)를 통해 플랫폼의 모든 병원의 CDM 데이터 접근하기 위한 티켓을 발급받는 과정(155 단계)을 세부적으로 도시하는 도면이다.

[0033] 도 4를 참조하면, 사용자(140)는 티켓 발행 서버(115)에 플랫폼에 연결된 병원에 접근하기 위한 티켓 발급을 요청한다. 이를 위해, 사용자(140)는 411 단계에서, 인증 서버(111)의 토큰(token)과 코드 사이너(113)의 전자서명(sig^{AC})을 포함하는 메시지(M_{C-TGS})와 이에 대한 서명($sig_{M_{C-TGS}}$)를 전달한다.

[0034] 티켓 발행 서버(115)는 413 단계에서, 플랫폼의 사용자(140)에게 암호학적으로 생성된 티켓(ticket)을 포함하는 메시지(M_{TGS-C})와 이에 대한 서명($sig_{M_{TGS-C}}$)을 전달한다. 이 티켓(ticket)은 인증 서버(111)의 토큰(token)과 유사하게 사용자의 ID와 유효기간 같은 정보를 DES나 AES와 같은 대칭키 암호 알고리즘을 이용해 생성된다. 하지만, 티켓 발행 서버(115)는, 인증 서버(111)와는 달리, 티켓(ticket)을 암호화하는 데 사용한 키를 티켓(ticket)을 수신할 각 서비스 서버(131)의 공개키로 암호화하여 티켓(ticket)과 함께 사용자(140)에게 전달한다. 사용자(140)는 티켓(ticket)과 함께 전달받은 티켓 검증을 위한 키를 복호화할 수 없다. 즉, 서비스 서버(131)를 제외하고, 사용자(140)를 포함하여 어떠한 방식으로든 티켓(ticket)을 획득한 제3자는 티켓(ticket)을 생성하거나 복호화할 수 없다. 티켓 발행 서버(115)는 분산 네트워크 위에서 운영되는 플랫폼에 있어 가장 중요한 컴포넌트이다. 플랫폼의 도움 없이, 사용자(140)가 여러 의료 기관의 CDM 데이터를 분석하려 한다면 사용자(140)는 각 기관의 관리자에게 일일이 신원을 증명하고, 분석코드(AC) 실행을 요청해야 한다. 심지어, 이런 환경에서는, 각 기관이 데이터를 이용하려는 모든 사용자(140)의 신원 정보를 저장하는 데이터베이스를 운영해야 한다. 티켓 발행 서버(115)는 이러한 번거로움을 해소하기 위해 모든 의료 기관에서 데이터를 분석하려는 사용자(140)의 신원을 인증할 수 있게 하는 티켓을 생성한다. 각 병원은 이 티켓을 검증함으로써, 별도의 사용자 계정 데이터베이스 없이 사용자(140)를 인증할 수 있게 된다.

[0036] 도 5 및 도 6은 도 1의 사용자(140)가 중계 서버(117)를 통해 티켓과 전자서명이 포함된 분석코드를 플랫폼에

연결된 모든 병원에 분배하고, 분석 결과를 회신받는 과정(157 단계)를 세부적으로 도시하는 도면들이다.

[0037] 도 5는 일 실시예에 따라 완전 자동화 모델에서 사용자(140), 중계 서버(117), 그리고 병원들의 서비스 서버(131)들이 통신하는 과정을 보여준다. 이 모델에서는 분석코드(AC) 분배에서 CDM 데이터 분석 결과의 회신까지 전체 과정이 완전하게 자동으로 진행된다.

[0038] 도 5를 참조하면, 사용자(140)는 사전에 인증 서버(111)의 토큰(token), 분석코드(AC), 코드 사이너(113)의 전자서명(sig^{AC}), 및 티켓 발행 서버(115)의 티켓(ticket)을 소유하고 있다고 가정한다. 먼저 사용자(140)는 511 단계에서, 이 4개의 정보를 포함한 메시지(M_{C-RS})와 이에 대한 서명($sig_{M_{C-RS}}$)을 보안 서버 그룹(110)의 중계 서버(117)에 전달한다. 중계 서버(117)는 토큰(token)을 검증하여 송신자의 인증 서버(111)에 의해 인증된 사용자(140)인지 확인한다. 사용자(140)의 신원이 확인되면, 중계 서버(117)는 513 단계에서, 토큰(token)을 제외한 나머지 정보를 메시지(M_{RS-SS})로 다시 포장하고, 이 메시지와 이에 대한 서명($sig_{M_{RS-SS}}$)을 플랫폼에 등록된 모든 병원의 서비스 서버(131)들(SS1-SSn)에 전달한다.

[0039] 이들을 전달받은 서비스 서버(131)들의 각각은 티켓(ticket)과 전자서명(sig^{AC})을 이용해 사용자(140)와 분석코드(AC)의 진위를 확인한다. 사용자(140)와 분석코드(AC)에 대한 검증에 성공하면, 서비스 서버(131)들의 각각은 515 단계에서, 분석코드(AC)를 실행하여 해당 병원의 CDM 데이터를 분석한다. 그런 다음, 서비스 서버(131)들의 각각은 517 단계에서, 분석 결과(analysis results; AR)를 다시 중계 서버(117)로 회신한다. 마지막으로, 사용자(140)는 519 단계에서, 병원들로부터 수집된 분석 결과(AR)들을 다운로드한다. 완전 자동화 모델에서, 사용자(140)는 어느 누구의 개입 없이 병원들의 데이터를 분석할 수 있다.

[0040] 도 6은 다른 실시예에 따라 승인 우선 모델에서 사용자(140), 중계 서버(117), 및 병원들의 서비스 서버(131)들이 통신하는 과정을 보여준다.

[0041] 도 6을 참조하면, 사용자(140)는 611 단계에서, 인증 서버(111)의 토큰(token), 분석코드(AC), 코드 사이너(113)의 전자서명(sig^{AC}), 및 티켓 발행 서버(115)의 티켓(ticket)을 중계 서버(117)에 전달한다. 중계 서버(117)는 인증 서버(111)의 토큰(token)을 검증하여 사용자의 신원을 확인한다. 중계 서버(117)는 613 단계에서, 인증된 사용자(140)가 전달한 분석코드(AC), 전자서명(sig^{AC}), 및 티켓(ticket)을 병원들의 서비스 서버(131)들에 분배한다.

[0042] 서비스 서버(131)들의 각각은 전달받은 티켓(ticket)을 검증하여 사용자를 인증하고, 전자서명(sig^{AC})을 검증하여 분석코드(AC)의 무결성을 확인한다. 서비스 서버(131)들의 각각은 검증을 통과한 분석코드(AC)를 곧바로 실행하지 않고, 병원의 데이터 관리자(custodian)(135)의 승인을 대기한다. 관리자(135)는 615 단계에서, 해당 병원으로 전달된 분석코드(AC)를 확인하고, 실행을 승인한다. 승인 즉시, 서비스 서버(131)들의 각각은 617 단계에서, 분석코드(AC)를 실행하여 병원의 CDM 데이터를 분석한다. 만약 관리자(135)가 분석코드(AC)의 실행을 보류하거나, 거부할 경우, 분석코드(AC)는 실행되지 않는다. 서비스 서버(131)들의 각각은 CDM 데이터에 대한 분석 결과(AR)를 곧바로 사용자(140)에게 회신하지 않고, 관리자(135)의 반출 승인을 대기한다. 관리자(135)가 619 단계에서, 분석 결과(AR)의 반출을 승인하면, 사용자(140)는 621 단계에서, 분석 결과(AR)를 다운로드할 수 있다. 반면, 관리자(135)가 분석 결과(AR)의 반출을 보류하거나, 거부할 경우, 사용자(140)는 데이터 분석이 완료되었음에도 분석 결과(AR)에 접근할 수 없다.

[0043] 한편, 어떤 실시예들에서는, 완전 자동화 모델과 승인 우선 모델을 결합한 하이브리드 모델이 가능하다. 하이브리드 모델에서는 병원별로 설치된 서비스 서버(131)들이 신뢰 연구자에 대한 화이트리스트를 보유한다. 만약 CDM 데이터 분석을 요청한 사용자(140)가 화이트리스트에 등록되었다면, 해당 요청은 완전 자동화 모델로 처리되고, 그렇지 않은 경우, 승인 우선 모델로 처리된다.

[0045] 도 7은 다양한 실시예들에 따른 플랫폼 시스템(100)의 서비스 서버(131)의 내부 구성을 도시하는 도면이다. 이때, 도 7의 서비스 서버(131)는 완전 자동화 모델, 승인 우선 모델, 및 하이브리드 모델을 지원하기 위한 구조를 갖는다.

[0046] 도 7을 참조하면, 서비스 서버(131)는 플랫폼 시스템(100)의 다른 컴포넌트와 달리, 의료 데이터를 분석하기 위해 다양한 기능들을 제공한다. 이를 위해, 서비스 서버(131)는 검증 모듈(710), 대기 큐(720), 실행 관리자(730), 분석코드 풀(740), R 엔진(750), 및 분석 결과 관리자(760)를 포함한다.

[0047] 서비스 서버(131)는 분석코드(AC), 분석코드(AC)의 전자서명(sig^{AC}), 및 티켓(ticket)을 검증 모듈(710)에 전달한다. 검증 모듈(710)은 도 5및 6을 참조하여 설명한 바와 같이 분석코드(AC)에 대한 검증을 수행한다. 서비스 서버(131)는 분석코드(AC)를 실행 대기 큐(720)에 넣는다.

[0048] 일반적으로 분석코드(AC)의 실행은 많은 컴퓨팅 자원을 요구하기 때문에 사용자(140)의 모든 분석 요청을 병렬로 실행할 수 없다. 따라서, 서비스 서버(131)는 실행 관리자(730)를 두어, 분석코드(AC)에 대한 분석코드 풀(740)을 이용해 한 번에 실행 가능한 분석코드(AC)를 제한한다. 실행 관리자(730)는 관리자의 승인을 얻어 분석코드(AC)를 실행하여 해당 기관의 데이터베이스(133)의 CDM 데이터를 분석할 수 있다. 앞서 모든 유효성 검증에 성공하면, 서비스 서버(131)는 R 엔진(750)을 이용해 분석코드(AC)를 실행한다. 혹은 R 언어 이외의 다른 프로그래밍 언어로 분석코드(AC)가 작성되었을 경우, 적절한 실행 엔진이 호출된다.

[0049] 데이터 분석이 완료되면, 서비스 서버(131)는 분석 결과(AR)을 분석 결과 관리자(760)에 보관한다. 이 때, 분석결과(AR)는 zip과 같은 압축 파일 유형으로 보관될 수 있다. 서비스 서버(131)는 사용자(140)에게 CDM 데이터 분석 상태를 알릴 수 있다. 데이터 분석 과정은 많은 시간이 소요된다. 또한 기관 별로 분석코드(AC)의 실행 시간에 차이가 있을 수 있다. 사용자(140)는 모든 병원의 데이터 분석이 완료되는 것을 대기할 수 없기 때문에 주기적으로 각 병원의 분석 상태를 확인할 수 있다. 서비스 서버(131)는 사용자(140)가 분석 상태를 요청하면, "실행 대기", "실행 중", 또는 "분석 완료" 중 하나로 응답한다. 만약, 서비스 서버(131)가 완전 자동화 모델인 경우, 분석코드(AC)는 실행 대기 상태를 거치지 않고, 곧바로 실행된다. 서비스 서버(131)는 분석 결과 관리자(760)를 통해 분석결과(AR) 반출 상태를 사용자(140)에게 알릴 수 있다. 실행 관리자(730)와 마찬가지로, 분석결과 관리자(760)는 CDM 데이터 분석 결과(AR)에 대한 사용자(140)의 회신 여부를 관리자(135)로부터 입력받는다. 사용자(140)가 서비스 서버(131)에게 분석 결과(AR) 회신 가능 여부를 요청하면, 서비스 서버(131)는 "다운로드 가능" 혹은 "반출 대기" 상태 중 하나를 회신한다. 사용자(140)는 "다운로드 가능"인 경우에만 분석 결과(AR)를 다운로드할 수 있다. 마찬가지로, 서비스 서버(131)가 완전 자동화 모델인 경우, "반출 대기" 상태는 사용되지 않는다.

[0051] 전술된 바와 같이, 분석코드(AC)는 사용자(140)에 의해 작성되되, 각 병원, 즉 서비스 서버(131)에 의해 실행된다. 따라서, 플랫폼 시스템(100)에서, 분석코드(AC)에 대한 사용자(140)와 서비스 서버(131)의 역할 분담 및 협력적 분석이 이루어질 수 있다. 아울러, 분석코드(AC)는 공통 데이터 모델(CDM)에 기반한 코드이기 때문에, 표준화된 환경에서 실행될 수 있으며, 복수의 병원들, 즉 서비스 서버(131)들에서 일괄적으로 인증될 수 있다. 따라서, 복수의 병원들, 즉 서비스 서버(131)들의 각각이 독립적으로 분석 코드(AC)를 실행하여, 각각의 CDM 데이터를 분석할 수 있다.

[0052] 다양한 실시예들에 따르면, 플랫폼에 연결된 병원들의 의료 데이터가 CDM으로 통일화되기 때문에, 외부 연구자가 동일한 방법론을 통해 여러 병원의 데이터를 분석할 수 있다. 그리고, CDM 데이터가 병원의 로컬 네트워크 밖으로 전송되지 않고, 내부, 즉 서비스 서버(131)에서만 분석되기 때문에, 환자들은 개인정보를 병원 외부로의 유출을 염려하지 않아도 된다.

[0053] 다양한 실시예들에 따르면, 사용자(140)들은 병원의 로컬 네트워크 외부에 위치한 플랫폼의 보안 서버 그룹을 통해 (여러 단계의) 인증을 수행한다. 인증에 통과한 사용자(140)는 데이터 분석을 요청할 각 병원에서 추가로 인증을 수행하지 않는다. 따라서, 각 병원은 사용자(140)의 신원을 확인하기 위한 계정 데이터베이스를 운영하지 않아도 된다.

[0054] 사용자(140)가 작성한 CDM 데이터에 대한 분석코드(AC)는 사용자(140)로부터 병원의 서비스 서버(131)까지 전달되는 동안 제3자에 의해 변조되어서는 안된다. 다양한 실시예들은 이 과정에서 분석코드(AC)의 무결성을 보장할 수 있다.

[0056] 다양한 실시예들은 다기관 분산 환경에서 안전한 다기관 CDM 데이터를 분석하기 위한 플랫폼 시스템(100) 및 그의 방법을 제공한다.

[0057] 다양한 실시예들에 따른 플랫폼 시스템(100)은, 사용자(140)를 위한 토큰을 생성하도록 구성되는 인증 서버(111), 사용자(140)의 분석코드에 대한 전자서명을 생성하도록 구성되는 코드 사이너(113), 사용자(140)를 위한 티켓을 발행하도록 구성되는 티켓 발행 서버(115), 및 각 병원에서, 티켓을 이용하여 사용자(140)를 검증하고, 전자서명을 이용하여 분석코드를 검증하며, 사용자(140) 및 분석코드에 대한 검증에 성공 시, 분석코드를 실행하여, 병원의 CDM 데이터를 분석하도록 구성되는 서비스 서버(131)를 포함한다.

[0058] 다양한 실시예들에 따르면, 인증 서버(111)는, 사용자(140)로부터 사용자(140)의 식별 정보가 수신되면, 식별 정보를 기반으로 사용자(140)를 인증하여, 토큰을 생성하고, 사용자(140)에게 토큰을 제공하도록 구성된다.

[0059] 다양한 실시예들에 따르면, 코드 사이너(113)는, 사용자(140)로부터 토큰 및 분석코드가 수신되면, 개인키를 이용하여, 분석코드에 대한 전자서명을 생성하고, 사용자(140)에게 전자서명을 제공하도록 구성된다.

[0060] 다양한 실시예들에 따르면, 분석코드는, 사용자(140)에 의해 작성되고, 각 병원의 CDM 데이터를 분석하기 위한 정보를 포함한다.

[0061] 다양한 실시예들에 따르면, 티켓 발행 서버(115)는, 사용자(140)로부터 토큰 및 전자서명이 수신되면, 암호화 키를 이용하여, 티켓을 생성하고, 서비스 서버(131)의 공개키를 이용하여, 암호화 키를 암호화하고, 사용자(140)에게 티켓을 암호화 키와 함께 제공하도록 구성된다.

[0062] 다양한 실시예들에 따르면, 서비스 서버(131)는, 사용자(140)에게 CDM 데이터에 대한 분석 결과를 회신하도록 구성된다.

[0063] 다양한 실시예들에 따르면, 플랫폼 시스템(100)은, 사용자(140)와 서비스 서버(131) 간 통신을 중계하도록 구성되는 중계 서버를 더 포함한다.

[0064] 다양한 실시예들에 따르면, 중계 서버는, 사용자(140)로부터 토큰, 전자서명, 및 티켓이 수신되면, 토큰을 이용하여, 사용자(140)를 확인하고, 서비스 서버(131)에 전자서명 및 티켓을 전달하도록 구성된다.

[0065] 일 실시예에 따르면, 서비스 서버(131)는, 분석 결과를 중계 서버에 회신하도록 구성되고, 사용자(140)는, 중계 서버로부터 분석 결과를 다운로드한다.

[0066] 다른 실시예에 따르면, 서비스 서버(131)는, 관리자의 승인을 기반으로, 분석코드를 실행하여, CDM 데이터를 분석하고, 관리자의 승인을 기반으로, 분석 결과를 사용자(140)에게 회신하도록 구성된다.

[0067] 또 다른 실시예에 따르면, 서비스 서버(131)는, 사용자(140)가 화이트리스트에 등록되어 있으면, 분석 결과를 사용자(140)에게 회신하고, 사용자(140)가 화이트리스트에 등록되어 있지 않으면, 관리자의 승인을 기반으로, 분석 결과를 사용자(140)에게 회신하도록 구성된다.

[0068] 다양한 실시예들에 따른 플랫폼 시스템(100)의 방법은, 인증 서버(111)가 사용자(140)를 위한 토큰을 생성하는 단계(151 단계), 코드 사이너(113)가 사용자(140)의 분석코드에 대한 전자서명을 생성하는 단계(153 단계), 티켓 발행 서버(115)가 사용자(140)를 위한 티켓을 발행하는 단계(155 단계), 각 병원의 서비스 서버(131)가 티켓을 이용하여 사용자(140)를 검증하고, 전자서명을 이용하여 분석코드를 검증하는 단계(157 단계), 및 사용자(140) 및 분석코드에 대한 검증에 성공 시, 서비스 서버(131)가 분석코드를 실행하여, 병원의 CDM 데이터를 분석하는 단계(157 단계)를 포함한다.

[0069] 다양한 실시예들에 따르면, 토큰을 생성하는 단계(151 단계)는, 사용자(140)가 인증 서버(111)에 사용자(140)의 식별 정보를 전송하는 단계, 인증 서버(111)가 식별 정보를 기반으로 사용자(140)를 인증하여, 토큰을 생성하는 단계, 및 인증 서버(111)가 사용자(140)에게 토큰을 제공하는 단계를 포함한다.

[0070] 다양한 실시예들에 따르면, 전자서명을 생성하는 단계(153 단계)는, 사용자(140)가 코드 사이너(113)에 코드 사이너(113)에 토큰 및 분석코드를 전송하는 단계, 코드 사이너(113)가 개인키를 이용하여, 분석코드에 대한 전자서명을 생성하는 단계, 및 코드 사이너(113)가 사용자(140)에게 전자서명을 제공하는 단계를 포함한다.

[0071] 다양한 실시예들에 따르면, 분석코드는, 사용자(140)에 의해 작성되고, 각 병원의 CDM 데이터를 분석하기 위한 정보를 포함한다.

[0072] 다양한 실시예들에 따르면, 티켓을 발행하는 단계(155 단계)는, 사용자(140)가 티켓 발행 서버(115)에 토큰 및 전자서명을 전송하는 단계, 티켓 발행 서버(115)가 암호화 키를 이용하여, 티켓을 생성하는 단계, 티켓 발행 서버(115)가 서비스 서버(131)의 공개키를 이용하여, 암호화 키를 암호화하는 단계, 및 티켓 발행 서버(115)가 사

용자(140)에게 티켓을 암호화 키와 함께 제공하는 단계를 포함한다.

[0073] 다양한 실시예들에 따르면, 플랫폼 시스템(100)의 방법은, 서비스 서버(131)가 사용자(140)에게 CDM 데이터에 대한 분석 결과를 회신하는 단계(157 단계)를 더 포함한다.

[0074] 다양한 실시예들에 따르면, 사용자(140) 및 분석 코드를 검증하는 단계(157 단계)는, 사용자(140)가 중계 서버에 토큰, 전자서명, 및 티켓을 전송하는 단계, 중계 서버가 토큰을 이용하여, 사용자(140)를 확인하는 단계, 중계 서버가 서비스 서버(131)에 전자서명 및 티켓을 전달하는 단계, 및 서비스 서버(131)가 티켓을 이용하여 사용자(140)를 검증하고, 전자서명을 이용하여 분석코드를 검증하는 단계를 포함한다.

[0075] 일 실시예에 따르면, 분석 결과를 회신하는 단계(157 단계)는, 서비스 서버(131)가 분석 결과를 중계 서버에 회신하는 단계, 및 사용자(140)가 중계 서버로부터 분석 결과를 다운로드하는 단계를 포함한다.

[0076] 다른 실시예에 따르면, CDM 데이터를 분석하는 단계(157 단계)는, 서비스 서버(131)가 관리자의 승인을 기반으로, 분석코드를 실행하여, CDM 데이터를 분석하는 단계를 포함하고, 분석 결과를 회신하는 단계는, 관리자의 승인을 기반으로, 분석 결과를 사용자(140)에게 회신하는 단계를 포함한다.

[0077] 또 다른 실시예에 따르면, 분석 결과를 회신하는 단계(157 단계)는, 사용자(140)가 화이트리스트에 등록되어 있으면, 서비스 서버(131)가 분석 결과를 사용자(140)에게 회신하는 단계, 및 사용자(140)가 화이트리스트에 등록되어 있지 않으면, 서비스 서버(131)가 관리자의 승인을 기반으로, 분석 결과를 사용자(140)에게 회신하는 단계를 포함한다.

[0079] 이상에서 설명된 장치는 하드웨어 구성 요소, 소프트웨어 구성 요소, 및/또는 하드웨어 구성 요소 및 소프트웨어 구성 요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성 요소는, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 어플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0080] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성 요소(component), 물리적 장치, 컴퓨터 저장 매체 또는 장치에 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0081] 다양한 실시예들에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 이 때 매체는 컴퓨터로 실행 가능한 프로그램을 계속 저장하거나, 실행 또는 다운로드를 위해 임시 저장하는 것일 수도 있다. 그리고, 매체는 단일 또는 수 개의 하드웨어가 결합된 형태의 다양한 기록수단 또는 저장수단일 수 있는데, 어떤 컴퓨터 시스템에 직접 접속되는 매체에 한정되지 않고, 네트워크 상에 분산 존재하는 것일 수도 있다. 매체의 예시로는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM 및 DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical medium), 및 ROM, RAM, 플래시 메모리 등을 포함하여 프로그램 명령어가 저장되도록 구성된 것이 있을 수 있다. 또한, 다른 매체의 예시로, 어플리케이션을 유통하는 앱 스토어나 기타 다양한 소프트웨어를 공급 내지 유통하는 사이트, 서버 등에서 관리하는 기록매체 내지 저장매체도 들 수 있다.

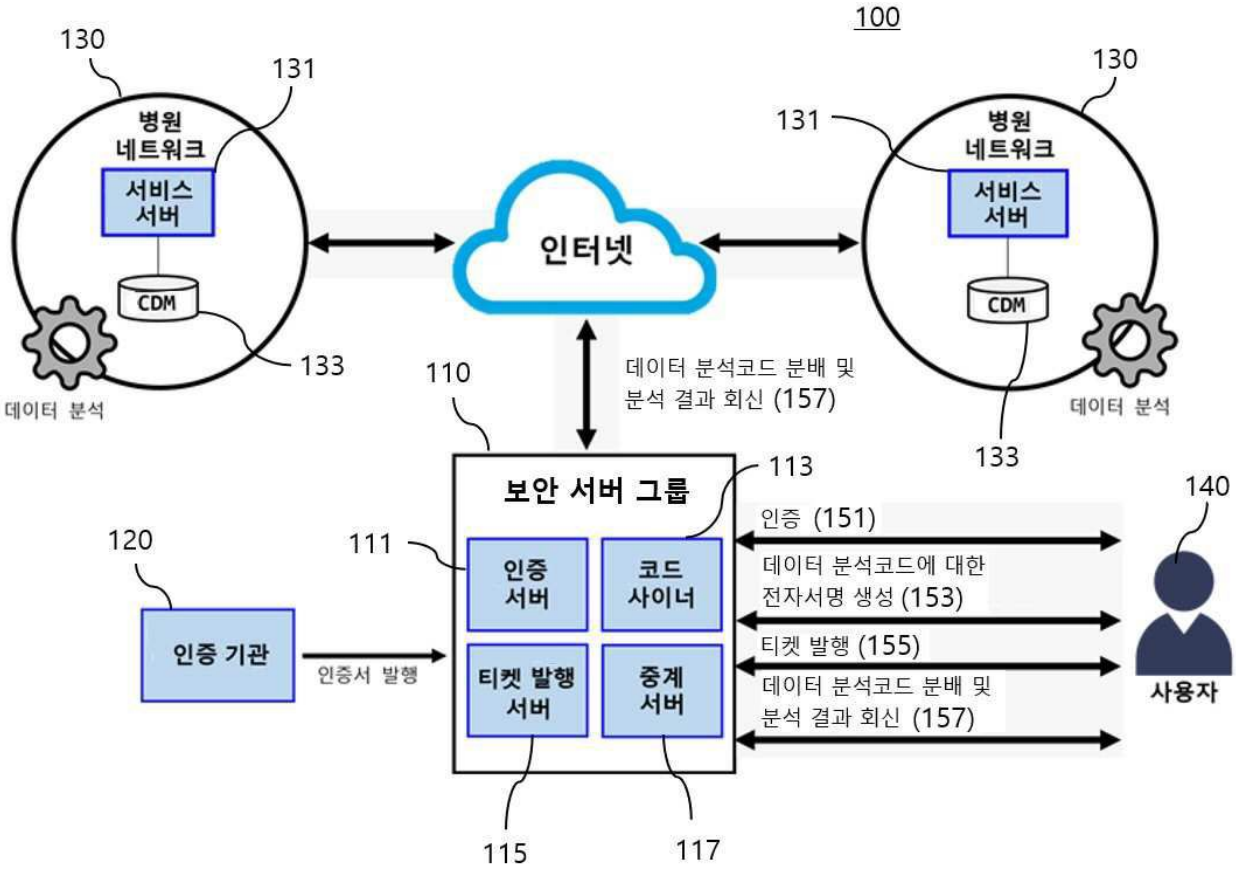
[0083] 본 문서의 다양한 실시예들 및 이에 사용된 용어들은 본 문서에 기재된 기술을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 해당 실시 예의 다양한 변경, 균등물, 및/또는 대체물을 포함하는 것으로 이해되어야 한다. 도면의 설명과 관련하여, 유사한 구성 요소에 대해서는 유사한 참조 부호가 사용될 수 있다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함할 수 있다. 본 문서에서, "A 또는 B", "A 및/또는 B 중 적어도 하나", "A, B 또는 C" 또는 "A, B 및/또는 C 중 적어도 하나" 등의 표현은 함께 나열된 항목들의 모든 가능한 조합을 포함할 수 있다. "제 1", "제 2", "첫째" 또는 "둘째" 등의 표현들은 해당 구성 요소들을, 순서 또는 중요도에 상관없이 수식할 수 있고, 한 구성 요소를 다른 구성 요소와 구분하기 위해 사용될 뿐 해당 구성 요소들을 한정하지 않는다. 어떤(예: 제 1) 구성 요소가 다른(예: 제 2) 구성 요소에 "(기능적으로 또는 통신적으로) 연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 상기 어떤 구성 요소가 상기 다른 구성 요소에 직접적으로 연결되거나, 다른 구성 요소(예: 제 3 구성 요소)를 통하여 연결될 수 있다.

[0084] 본 문서에서 사용된 용어 "모듈"은 하드웨어, 소프트웨어 또는 펌웨어로 구성된 유닛을 포함하며, 예를 들면, 로직, 논리 블록, 부품, 또는 회로 등의 용어와 상호 호환적으로 사용될 수 있다. 모듈은, 일체로 구성된 부품 또는 하나 또는 그 이상의 기능을 수행하는 최소 단위 또는 그 일부가 될 수 있다. 예를 들면, 모듈은 ASIC(application-specific integrated circuit)으로 구성될 수 있다.

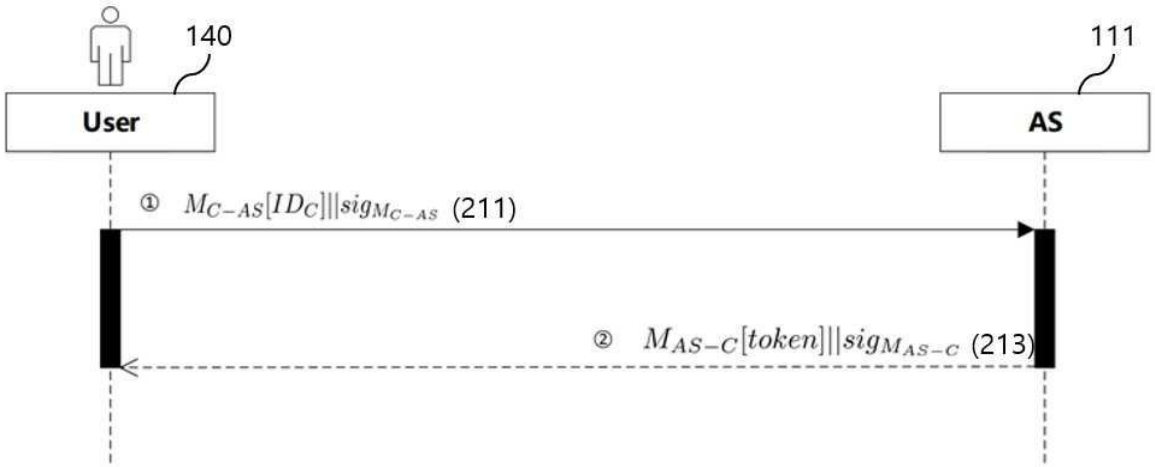
[0085] 다양한 실시예들에 따르면, 기술한 구성 요소들의 각각의 구성 요소(예: 모듈 또는 프로그램)는 단수 또는 복수의 개체를 포함할 수 있다. 다양한 실시예들에 따르면, 전술한 해당 구성 요소들 중 하나 이상의 구성 요소들 또는 단계들이 생략되거나, 또는 하나 이상의 다른 구성 요소들 또는 단계들이 추가될 수 있다. 대체적으로 또는 추가적으로, 복수의 구성 요소들(예: 모듈 또는 프로그램)은 하나의 구성 요소로 통합될 수 있다. 이런 경우, 통합된 구성 요소는 복수의 구성 요소들 각각의 구성 요소의 하나 이상의 기능들을 통합 이전에 복수의 구성 요소들 중 해당 구성 요소에 의해 수행되는 것과 동일 또는 유사하게 수행할 수 있다. 다양한 실시예들에 따르면, 모듈, 프로그램 또는 다른 구성 요소에 의해 수행되는 단계들은 순차적으로, 병렬적으로, 반복적으로, 또는 휴리스틱하게 실행되거나, 단계들 중 하나 이상이 다른 순서로 실행되거나, 생략되거나, 또는 하나 이상의 다른 단계들이 추가될 수 있다.

도면

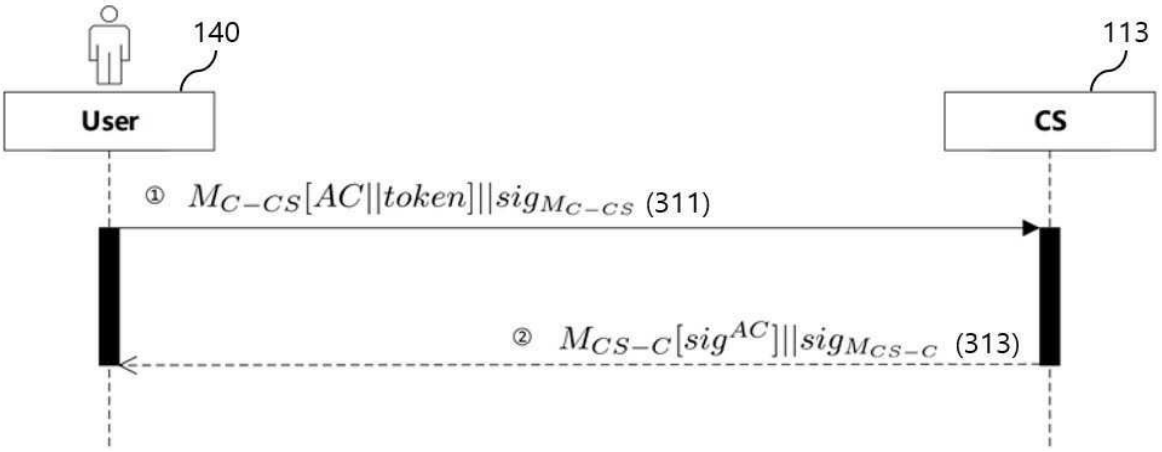
도면1


100
130
131
병원
네트워크
서비스
서버
CDM
133
데이터 분석
인터넷
데이터 분석코드 분배 및
분석 결과 회신 (157)
110
보안 서버 그룹
113
111
인증
서버
코드
사이너
티켓 발행
서버
중계
서버
115
117
120
인증 기관
인증서 발행
인증 (151)
데이터 분석코드에 대한
전자서명 생성 (153)
티켓 발행 (155)
데이터 분석코드 분배 및
분석 결과 회신 (157)
140
사용자

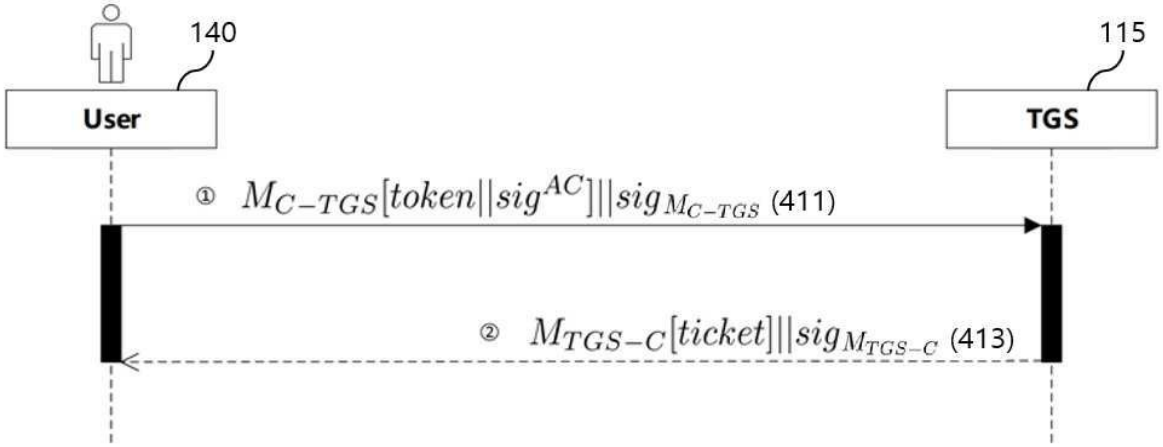
도면2


140
User
111
AS
① $M_{C-AS}[ID_C]||sig_{M_{C-AS}}$ (211)
② $M_{AS-C}[token]||sig_{M_{AS-C}}$ (213)

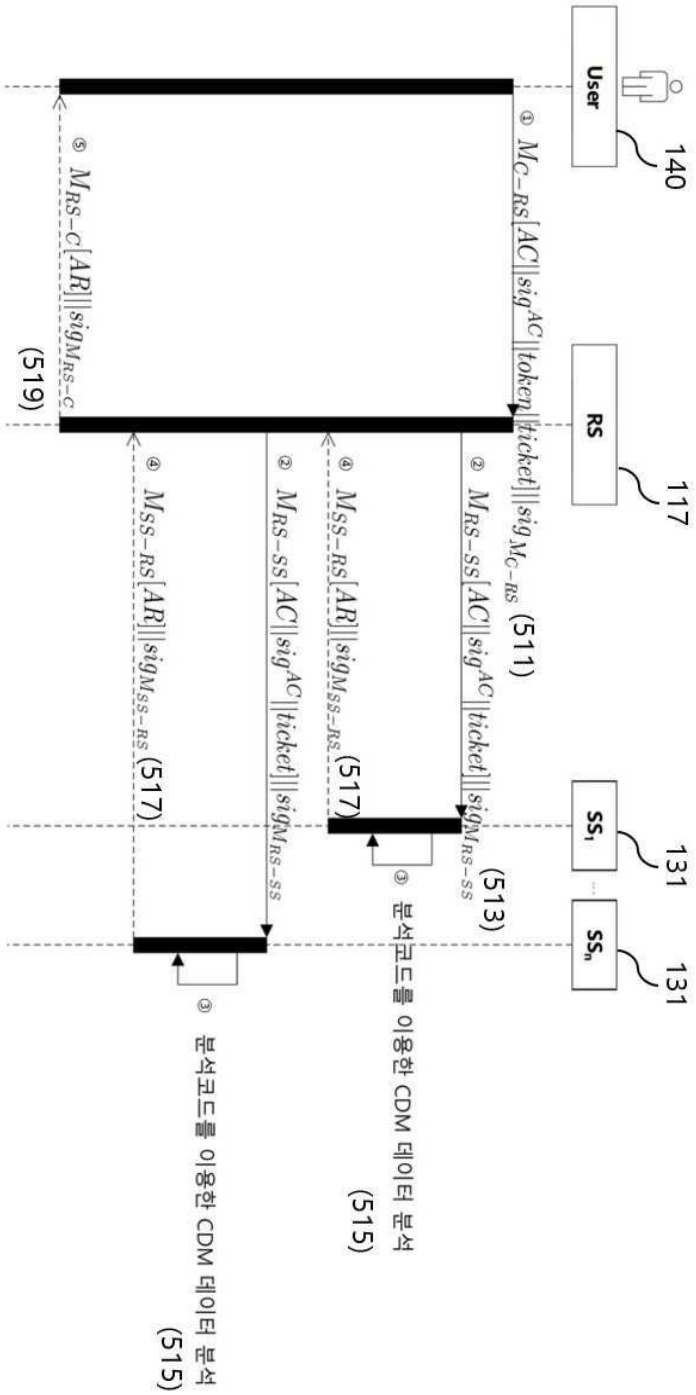
도면3


140
113
User
CS
① $M_{C-CS}[AC||token]||sig_{M_{C-CS}}$ (311)
② $M_{CS-C}[sig^{AC}]||sig_{M_{CS-C}}$ (313)

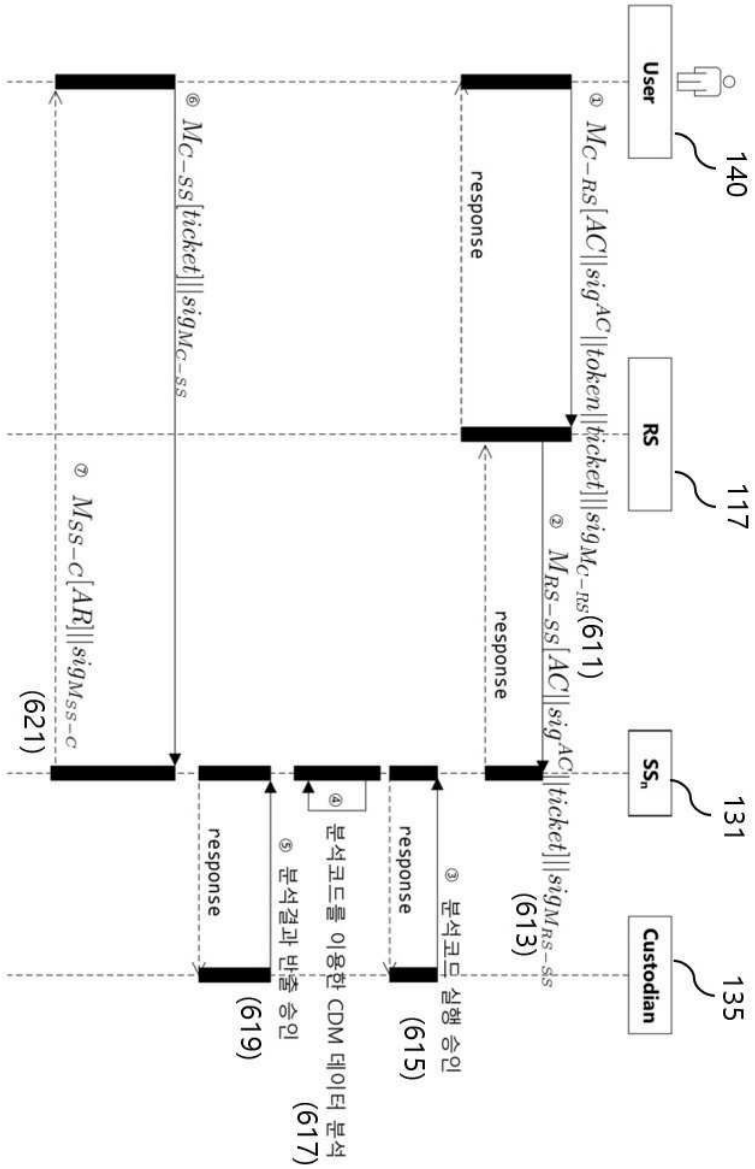
도면4


140
115
User
TGS
① $M_{C-TGS}[token||sig^{AC}]||sig_{M_{C-TGS}}$ (411)
② $M_{TGS-C}[ticket]||sig_{M_{TGS-C}}$ (413)

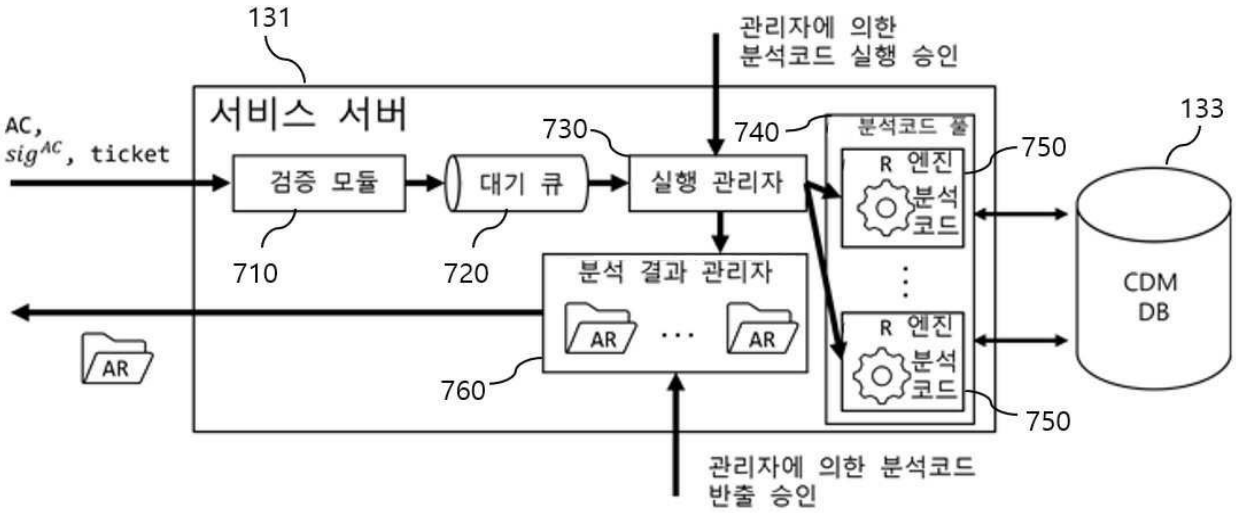
도면5


User
140
RS
117
SS1
131
SSn
131
① $M_{C-RS}[AC||sig^{AC}||token||ticket]||sig_{M_{C-RS}}$ (511)
② $M_{RS-SS}[AC||sig^{AC}||ticket]||sig_{M_{RS-SS}}$ (513)
③ 분석코드를 이용한 CDM 데이터 분석 (515)
④ $M_{SS-RS}[AR]||sig_{M_{SS-RS}}$ (517)
⑤ $M_{RS-C}[AR]||sig_{M_{RS-C}}$ (519)
② $M_{RS-SS}[AC||sig^{AC}||ticket]||sig_{M_{RS-SS}}$
④ $M_{SS-RS}[AR]||sig_{M_{SS-RS}}$ (517)
③ 분석코드를 이용한 CDM 데이터 분석 (515)

도면6


User
RS
SSn
Custodian
140
117
131
135
① $M_{C-RS}[AC||sig^{AC}||token||ticket]||sig_{M_{C-RS}}$
② $M_{RS-SS}[AC||sig^{AC}||ticket]||sig_{M_{RS-SS}}$
(611)
(613)
③ 분석코드 실행 승인
(615)
④ 분석코드를 이용한 CDM 데이터 분석
(617)
⑤ 분석결과 반출 승인
(619)
⑥ $M_{C-SS}[ticket]||sig_{M_{C-SS}}$
⑦ $M_{SS-C}[AR]||sig_{M_{SS-C}}$
(621)
response

도면7


131
서비스 서버
AC,
sig^{AC}, ticket
검증 모듈
710
대기 큐
720
730
실행 관리자
740
관리자에 의한
분석코드 실행 승인
분석코드 풀
R 엔진
분석
코드
750
133
CDM
DB
분석 결과 관리자
AR
760
관리자에 의한 분석코드
반출 승인