



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0101868
(43) 공개일자 2023년07월06일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) G16H 10/60 (2018.01)
G16H 40/67 (2018.01) H04L 67/568 (2022.01)
H04L 67/63 (2022.01)
(52) CPC특허분류
H04L 63/102 (2013.01)
G16H 10/60 (2021.08)
(21) 출원번호 10-2023-7018742
(22) 출원일자(국제) 2021년11월08일
심사청구일자 없음
(85) 번역문제출일자 2023년06월02일
(86) 국제출원번호 PCT/US2021/058402
(87) 국제공개번호 WO 2022/103681
국제공개일자 2022년05월19일
(30) 우선권주장
63/111,997 2020년11월10일 미국(US)

(71) 출원인
제넨테크, 인크.
미합중국 캘리포니아 (우편번호 94080-4990) 사우
쓰샌프란시스코 디엔에이 웨이 1
(72) 발명자
잘랄, 니아즈 아산
미국 94080-4990 캘리포니아 사우쓰샌프란시스코
디엔에이 웨이 1 제넨테크, 인크. 내
드리디, 압데슬렘
미국 94080-4990 캘리포니아 사우쓰샌프란시스코
디엔에이 웨이 1 제넨테크, 인크. 내
(74) 대리인
장덕순, 이귀동

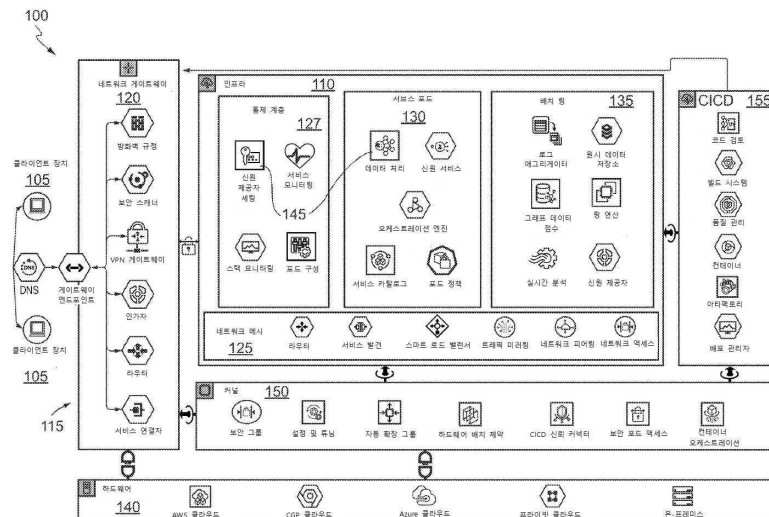
전체 청구항 수 : 총 33 항

(54) 발명의 명칭 중앙 네트워크 메시지를 통한 서비스 간 통신 및 인증

(57) 요약

본 개시는 네트워크 메시지를 통한 서비스 간 통신 및 인증을 위한 기술에 관한 것이다. 특히, 양태는 네트워크 메시지에서, 제1 서비스에 대한 서비스 요청을 수신하는 것과, 제1 서비스와 연관된 정보를 획득하는 것에 관한 것이다. 상기 정보는 제1 서비스를 캡슐화하는 제1 포드의 위치를 포함한다. 네트워크 메시지는 제1 포드의 위치를 사용하여 제1 포드에 특정한 보안 규칙을 불러온다. 네트워크 메시지는 제1 포드의 보안 규칙에 따라 서비스 요청을 제1 서비스로 전달하고, 제1 서비스로부터 서비스 요청의 결과를 획득한다. 이 결과는 제1 서비스를 캡슐화하는 제1 포드에 대한 보안 규칙 및 제2 서비스를 캡슐화하는 제2 포드에 대한 보안 규칙에 따라 제2 서비스로부터 획득된 하위 결과를 포함한다.

대표도 - 도1



(52) CPC특허분류

G16H 40/67 (2021.08)

H04L 63/105 (2013.01)

H04L 63/205 (2013.01)

H04L 67/568 (2022.05)

H04L 67/63 (2022.05)

명세서

청구범위

청구항 1

컴퓨터-구현 방법으로서:

네트워크 메시에서, 제1 서비스에 대한 서비스 요청을 수신하는 단계;

캐시 또는 서비스 레지스트리로부터 상기 제1 서비스와 연관된 정보를 네트워크 메시가 획득하는 단계 - 상기 정보는 상기 제1 서비스를 포함하는 제1 포드(pod)의 신원 및 제1 분산 컴퓨팅 환경 내의 상기 제1 포드의 위치를 포함함;

상기 네트워크 메시가 상기 제1 포드의 위치를 사용하여 상기 제1 포드에 대한 보안 규칙을 불러오는 단계 - 상기 보안 규칙은 (i) 상기 제1 서비스에 대한 고유 주소 식별자, 및 (ii) 상기 제1 서비스가 통신 및 액세스하도록 인가받은 서비스를 정의함;

상기 네트워크 메시가 상기 제1 서비스에 대한 상기 고유 주소 식별자를 사용하여 상기 서비스 요청을 상기 제1 서비스에 전달하는 단계;

상기 네트워크 메시가 제2 서비스와 통신하고 액세스하기 위한 액세스 요청을 상기 제1 서비스로부터 수신하는 단계 - 상기 액세스 요청은 상기 제2 서비스에 특정한 보안 키를 포함함;

상기 네트워크 메시가 상기 캐시 또는 상기 서비스 레지스트리로부터 상기 제2 서비스와 연관된 정보를 획득하는 단계 - 상기 정보는 상기 제2 서비스를 포함하는 제2 포드의 신원 및 상기 제1 분산 컴퓨팅 환경 또는 제2 분산 컴퓨팅 환경 내의 상기 제2 포드의 위치를 포함함; 그리고

상기 네트워크 메시가 상기 제2 포드의 위치를 사용하여 상기 제2 포드에 대한 보안 규칙을 불러오는 단계 - 상기 보안 규칙은 (i) 상기 제2 서비스에 대한 고유 주소 식별자, 및 (ii) 상기 제2 서비스가 통신 및 액세스하도록 인가받은 서비스를 정의함;

상기 네트워크 메시가 상기 제2 서비스에 대한 상기 고유 주소 식별자를 사용하여, 상기 제1 포드에 대한 보안 규칙 및 상기 제2 포드에 대한 보안 규칙에 기초하여 상기 제1 서비스로부터의 액세스 요청을 상기 제2 서비스로 전달하는 단계;

상기 네트워크 메시가 상기 제1 서비스로부터 상기 서비스 요청의 최종 결과를 수신하는 단계 - 상기 최종 결과는 상기 제2 서비스로부터 획득한 하위 결과를 포함함; 그리고

상기 네트워크 메시가 상기 서비스 요청의 최종 결과를 출력하는 단계

를 포함하는, 컴퓨터-구현 방법.

청구항 2

제1항에 있어서, 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 획득하는 단계는:

상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보가 상기 캐시로부터 이용 가능한지 여부를 결정하는 단계;

상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보가 상기 캐시로부터 이용 가능할 때, 상기 캐시로부터 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 획득하는 단계;

상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보가 상기 캐시로부터 이용가능하지 않은 경우, 상기 레지스트리로부터 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 획득하는 단계; 그리고

상기 레지스트리로부터 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 획득하는 것에 응답하여, 후속 요청을 위해 상기 캐시에 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 저장하는 단계

를 포함하는, 컴퓨터-구현 방법.

청구항 3

제1항 또는 제2항에 있어서, 상기 보안 키는 금고로부터 상기 제1 서비스에 의해 획득되고, 상기 제1 서비스는 상기 액세스 요청에 상기 보안 키를 내장하는, 컴퓨터-구현 방법.

청구항 4

제3항에 있어서, 상기 제1 서비스로부터의 액세스 요청은 상기 제1 서비스를 대신하여 하나 이상의 동작을 수행하고/거나 서비스를 획득하기 위한 상기 제2 서비스의 요청을 더 포함하는, 컴퓨터-구현 방법.

청구항 5

제4항에 있어서, 상기 제2 서비스는 상기 제1 서비스를 대신하여 상기 하나 이상의 동작을 수행하고/거나 상기 서비스를 획득하고; 상기 하나 이상의 동작의 수행 및/또는 상기 서비스의 획득을 기반으로 하위 결과를 생성하는, 컴퓨터-구현 방법.

청구항 6

제5항에 있어서, 상기 제2 서비스는 상기 제1 서비스를 대신하여 상기 하나 이상의 동작을 수행하기 전에 및/또는 상기 서비스를 획득하기 전에 상기 보안 키를 검증하는, 컴퓨터-구현 방법.

청구항 7

제1항 내지 제6항 중 어느 한 항에 있어서, 상기 제2 포드는 상기 제1 분산 컴퓨팅 환경과 다른 상기 제2 분산 컴퓨팅 환경 내에 위치하는, 컴퓨터-구현 방법.

청구항 8

제1항 내지 제7항 중 어느 한 항에 있어서, 상기 제1 포드에 대한 상기 보안 규칙은: (i) 상기 제1 서비스에 이용 가능한 인스턴스의 수, 및 (ii) 상기 서비스 요청의 처리에 이용 가능한 인스턴스를 더 정의하며, 상기 서비스 요청을 상기 제1 서비스로 전달하는 단계는:

상기 제1 포드에 대한 상기 보안 규칙에 기초하여 상기 서비스 요청을 처리하기 위해 이용 가능한 인스턴스를 결정하는 단계; 그리고

상기 제1 서비스의 인스턴스 중 적어도 하나에 상기 서비스 요청을 전달하는 단계

를 포함하는, 컴퓨터-구현 방법.

청구항 9

제1항 내지 제8항 중 어느 한 항에 있어서, 상기 제1 서비스로부터 상기 제2 서비스로 액세스 요청을 전달하는 단계는,

상기 제1 포드에 대한 상기 보안 규칙이 상기 제2 서비스를, 상기 제1 서비스가 통신 및 액세스하도록 인가받은 서비스로 정의하는지 여부를 결정하는 단계;

상기 제2 포드에 대한 상기 보안 규칙이 상기 제1 서비스를, 상기 제2 서비스가 상기 제1 서비스로부터 통신을 수신 및 액세스할 수 있도록 인가받은 서비스로 정의하는지 여부를 결정하는 단계;

그리고 상기 제2 서비스는, 상기 제1 서비스가 통신 및 액세스하도록 인가받은 서비스이고 상기 제1 서비스는, 상기 제2 서비스가 상기 제1 서비스로부터 통신을 수신 및 액세스할 수 있도록 인가받은 서비스인 경우, 상기 제1 서비스로부터 상기 제2 서비스로 상기 액세스 요청을 전달하는 단계

를 포함하는, 컴퓨터-구현 방법.

청구항 10

제9항에 있어서, 상기 제2 포드에 대한 상기 보안 규칙은: (i) 상기 제2 서비스에 이용 가능한 인스턴스의 수; 및 (ii) 상기 액세스 요청을 처리하기 위해 이용 가능한 인스턴스를 더 정의하고, 상기 제1 서비스로부터 상기 제2 서비스로 상기 액세스 요청을 전달하는 단계는:

상기 제2 포트에 대한 상기 보안 규칙에 기초하여 상기 액세스 요청을 처리하기 위해 이용 가능한 인스턴스를 결정하는 단계; 그리고

상기 액세스 요청을 상기 제2 서비스의 인스턴스 중 적어도 하나에 전달하는 단계를 더 포함하는, 컴퓨터-구현 방법.

청구항 11

제1항 내지 제10항 중 어느 한 항에 있어서,

상기 제1 서비스는 상기 제1 분산 컴퓨팅 환경에서 제1 컨테이너 또는 제1 컨테이너 세트로서 패키징된 하나 이상의 클러스터에 배치된 하나 이상의 프로그램을 포함하고, 상기 제1 컨테이너 또는 상기 제1 컨테이너 세트는 제1 포트로서 패키징되며, 이는 상기 하나 이상의 클러스터에서 실행되는 상기 하나 이상의 프로그램을 나타내는 상위 레벨 구조이고, 그리고

상기 제2 서비스는 상기 제1 분산 컴퓨팅 환경 또는 제2 분산 컴퓨팅 환경에서 제2 컨테이너 또는 제2 컨테이너 세트로서 패키징된 하나 이상의 클러스터에 배치된 하나 이상의 프로그램을 포함하고, 상기 제2 컨테이너 또는 상기 제2 컨테이너 세트는 제2 포트로서 패키징되며, 이는 상기 하나 이상의 클러스터에서 실행되는 상기 하나 이상의 프로그램을 나타내는 상위 레벨 구조인, 컴퓨터-구현 방법.

청구항 12

시스템으로서:

네트워크 메시지의 하나 이상의 데이터 프로세서; 그리고

상기 하나 이상의 데이터 프로세서에서 실행될 때 상기 하나 이상의 데이터 프로세서로 하여금 액션들을 수행하게 하는 명령어를 포함하는 비일시적 컴퓨터 판독가능 저장 매체

를 포함하며, 상기 액션들은:

제1 서비스에 대한 서비스 요청을 수신하는 것;

캐시 또는 서비스 레지스트리로부터 상기 제1 서비스와 연관된 정보를 획득하는 것 - 상기 정보는 상기 제1 서비스를 포함하는 제1 포트(pod)의 신원 및 제1 분산 컴퓨팅 환경 내의 상기 제1 포트의 위치를 포함함;

상기 제1 포트의 위치를 사용하여, 상기 제1 포트에 대한 보안 규칙을 불러오는 것 - 상기 보안 규칙은 (i) 상기 제1 서비스에 대한 고유 주소 식별자, 및 (ii) 상기 제1 서비스가 통신 및 액세스하도록 인가받은 서비스를 정의함;

상기 제1 서비스에 대한 상기 고유 주소 식별자를 사용하여 상기 서비스 요청을 상기 제1 서비스에 전달하는 것;

제2 서비스와 통신 및 액세스하기 위한 액세스 요청을 상기 제1 서비스로부터 수신하는 것 - 상기 액세스 요청은 상기 제2 서비스에 특정한 보안 키를 포함함;

상기 캐시 또는 상기 서비스 레지스트리로부터 상기 제2 서비스와 연관된 정보를 획득하는 것 - 상기 정보는 상기 제2 서비스를 포함하는 제2 포트의 신원 및 상기 제1 분산 컴퓨팅 환경 또는 제2 분산 컴퓨팅 환경 내의 상기 제2 포트의 위치를 포함함; 그리고

상기 제2 포트의 위치를 사용하여, 상기 제2 포트에 대한 보안 규칙을 불러오는 것 - 상기 보안 규칙은 (i) 상기 제2 서비스에 대한 고유 주소 식별자, 및 (ii) 상기 제2 서비스가 통신 및 액세스하도록 인가받은 서비스를 정의함;

상기 제2 서비스에 대한 상기 고유 주소 식별자를 사용하여, 상기 제1 포트에 대한 보안 규칙 및 상기 제2 포트에 대한 보안 규칙에 기초하여 상기 제1 서비스로부터의 액세스 요청을 상기 제2 서비스로 전달하는 것;

상기 제1 서비스로부터 상기 서비스 요청의 최종 결과를 수신하는 것 - 상기 최종 결과는 상기 제2 서비스로부터 획득한 하위 결과를 포함함; 그리고

상기 서비스 요청의 최종 결과를 출력하는 것

을 포함하는, 시스템.

청구항 13

제12항에 있어서, 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 획득하는 것은:

상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보가 상기 캐시로부터 이용 가능한지 여부를 결정하는 것;

상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보가 상기 캐시로부터 이용 가능할 때, 상기 캐시로부터 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 획득하는 것;

상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보가 상기 캐시로부터 이용가능하지 않은 경우, 상기 레지스트리로부터 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 획득하는 것; 그리고

상기 레지스트리로부터 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 획득하는 것에 응답하여, 후속 요청을 위해 상기 캐시에 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 저장하는 것

을 포함하는, 시스템.

청구항 14

제12항 또는 제13항에 있어서, 상기 보안 키는 금고로부터 상기 제1 서비스에 의해 획득되고, 상기 제1 서비스는 상기 액세스 요청에 상기 보안 키를 내장하는, 시스템.

청구항 15

제14항에 있어서, 상기 제1 서비스로부터의 액세스 요청은 상기 제1 서비스를 대신하여 하나 이상의 동작을 수행하고/거나 서비스를 획득하기 위한 상기 제2 서비스의 요청을 더 포함하는, 시스템.

청구항 16

제15항에 있어서, 상기 제2 서비스는 상기 제1 서비스를 대신하여 상기 하나 이상의 동작을 수행하고/거나 상기 서비스를 획득하고; 상기 하나 이상의 동작의 수행 및/또는 상기 서비스의 획득을 기반으로 하위 결과를 생성하는, 시스템.

청구항 17

제16항에 있어서, 상기 제2 서비스는 상기 제1 서비스를 대신하여 상기 하나 이상의 동작을 수행하기 전에 및/또는 상기 서비스를 획득하기 전에 상기 보안 키를 검증하는, 시스템.

청구항 18

제12항 내지 제17항 중 어느 한 항에 있어서, 상기 제2 포드는 상기 제1 분산 컴퓨팅 환경과 다른 상기 제2 분산 컴퓨팅 환경 내에 위치하는, 시스템.

청구항 19

제12항 내지 제18항 중 어느 한 항에 있어서, 상기 제1 포드에 대한 상기 보안 규칙은: (i) 상기 제1 서비스에 이용 가능한 인스턴스의 수, 및 (ii) 상기 서비스 요청의 처리에 이용 가능한 인스턴스를 더 정의하며, 상기 서비스 요청을 상기 제1 서비스로 전달하는 것은:

상기 제1 포드에 대한 상기 보안 규칙에 기초하여 상기 서비스 요청을 처리하기 위해 이용 가능한 인스턴스를 결정하는 것; 그리고

상기 제1 서비스의 인스턴스 중 적어도 하나에 상기 서비스 요청을 전달하는 것

을 포함하는, 시스템.

청구항 20

제12항 내지 제19항 중 어느 한 항에 있어서, 상기 제1 서비스로부터 상기 제2 서비스로 액세스 요청을 전달하는 것은,

상기 제1 포트에 대한 상기 보안 규칙이 상기 제2 서비스를, 상기 제1 서비스가 통신 및 액세스하도록 인가받은 서비스로 정의하는지 여부를 결정하는 것;

상기 제2 포트에 대한 상기 보안 규칙이 상기 제1 서비스를, 상기 제2 서비스가 상기 제1 서비스로부터 통신을 수신 및 액세스할 수 있도록 인가받은 서비스로 정의하는지 여부를 결정하는 것;

그리고 상기 제2 서비스는, 상기 제1 서비스가 통신 및 액세스하도록 인가받은 서비스이고 상기 제1 서비스는, 상기 제2 서비스가 상기 제1 서비스로부터 통신을 수신 및 액세스할 수 있도록 인가받은 서비스인 경우, 상기 제1 서비스로부터 상기 제2 서비스로 상기 액세스 요청을 전달하는 것

을 포함하는, 시스템.

청구항 21

제20항에 있어서, 상기 제2 포트에 대한 상기 보안 규칙은: (i) 상기 제2 서비스에 이용 가능한 인스턴스의 수; 및 (ii) 상기 액세스 요청을 처리하기 위해 이용 가능한 인스턴스를 더 정의하고, 상기 제1 서비스로부터 상기 제2 서비스로 상기 액세스 요청을 전달하는 것은:

상기 제2 포트에 대한 상기 보안 규칙에 기초하여 상기 액세스 요청을 처리하기 위해 이용 가능한 인스턴스를 결정하는 것; 그리고

상기 액세스 요청을 상기 제2 서비스의 인스턴스 중 적어도 하나에 전달하는 것

을 더 포함하는, 시스템.

청구항 22

제12항 내지 제21항 중 어느 한 항에 있어서,

상기 제1 서비스는 상기 제1 분산 컴퓨팅 환경에서 제1 컨테이너 또는 제1 컨테이너 세트로서 패키징된 하나 이상의 클러스터에 배치된 하나 이상의 프로그램을 포함하고, 상기 제1 컨테이너 또는 상기 제1 컨테이너 세트는 제1 포트로서 패키징되며, 이는 상기 하나 이상의 클러스터에서 실행되는 상기 하나 이상의 프로그램을 나타내는 상위 레벨 구조이고, 그리고

상기 제2 서비스는 상기 제1 분산 컴퓨팅 환경 또는 제2 분산 컴퓨팅 환경에서 제2 컨테이너 또는 제2 컨테이너 세트로 패키징된 하나 이상의 클러스터에 배치된 하나 이상의 프로그램을 포함하고, 상기 제2 컨테이너 또는 상기 제2 컨테이너 세트는 상기 제2 포트로서 패키징되며, 이는 상기 하나 이상의 클러스터에서 실행되는 상기 하나 이상의 프로그램을 나타내는 상위 레벨 구조인, 시스템.

청구항 23

네트워크 메시지의 하나 이상의 데이터 프로세서가 액션들을 수행하게 하도록 구성된 명령어를 포함하는, 비밀시적 기계 판독 가능 저장 매체에 유형적으로 구현된 컴퓨터-프로그램 제품으로서, 상기 액션들은:

제1 서비스에 대한 서비스 요청을 수신하는 것;

캐시 또는 서비스 레지스트리로부터 상기 제1 서비스와 연관된 정보를 획득하는 것 - 상기 정보는 상기 제1 서비스를 포함하는 제1 포트(pod)의 신원 및 제1 분산 컴퓨팅 환경 내의 상기 제1 포트의 위치를 포함함;

상기 제1 포트의 위치를 사용하여, 상기 제1 포트에 대한 보안 규칙을 불러오는 것 - 상기 보안 규칙은 (i) 상기 제1 서비스에 대한 고유 주소 식별자, 및 (ii) 상기 제1 서비스가 통신 및 액세스하도록 인가받은 서비스를 정의함;

상기 제1 서비스에 대한 상기 고유 주소 식별자를 사용하여 상기 서비스 요청을 상기 제1 서비스에 전달하는 것;

제2 서비스와 통신 및 액세스하기 위한 액세스 요청을 상기 제1 서비스로부터 수신하는 것 - 상기 액세스 요청은 상기 제2 서비스에 특정한 보안 키를 포함함;

상기 캐시 또는 상기 서비스 레지스트리로부터 상기 제2 서비스와 연관된 정보를 획득하는 것 - 상기 정보는 상기 제2 서비스를 포함하는 제2 포트의 신원 및 상기 제1 분산 컴퓨팅 환경 또는 제2 분산 컴퓨팅 환경 내의 상

기 제2 포트의 위치를 포함함; 그리고

상기 제2 포트의 위치를 사용하여, 상기 제2 포트에 대한 보안 규칙을 불러오는 것 - 상기 보안 규칙은 (i) 상기 제2 서비스에 대한 고유 주소 식별자, 및 (ii) 상기 제2 서비스가 통신 및 액세스하도록 인가받은 서비스를 정의함;

상기 제2 서비스에 대한 상기 고유 주소 식별자를 사용하여, 상기 제1 포트에 대한 보안 규칙 및 상기 제2 포트에 대한 보안 규칙에 기초하여 상기 제1 서비스로부터의 액세스 요청을 상기 제2 서비스로 전달하는 것;

상기 제1 서비스로부터 상기 서비스 요청의 최종 결과를 수신하는 것 - 상기 최종 결과는 상기 제2 서비스로부터 획득한 하위 결과를 포함함; 그리고

상기 서비스 요청의 최종 결과를 출력하는 것

을 포함하는, 컴퓨터-프로그램 제품.

청구항 24

제23항에 있어서, 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 획득하는 것은:

상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보가 상기 캐시로부터 이용 가능한지 여부를 결정하는 것;

상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보가 상기 캐시로부터 이용 가능할 때, 상기 캐시로부터 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 획득하는 것;

상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보가 상기 캐시로부터 이용가능하지 않은 경우, 상기 레지스트리로부터 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 획득하는 것; 그리고

상기 레지스트리로부터 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 획득하는 것에 응답하여, 후속 요청을 위해 상기 캐시에 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 저장하는 것

을 포함하는, 컴퓨터-프로그램 제품.

청구항 25

제23항 또는 제24항에 있어서, 상기 보안 키는 금고로부터 상기 제1 서비스에 의해 획득되고, 상기 제1 서비스는 상기 액세스 요청에 상기 보안 키를 내장하는, 컴퓨터-프로그램 제품.

청구항 26

제25항에 있어서, 상기 제1 서비스로부터의 액세스 요청은 상기 제1 서비스를 대신하여 하나 이상의 동작을 수행하고/거나 서비스를 획득하기 위한 상기 제2 서비스의 요청을 더 포함하는, 컴퓨터-프로그램 제품.

청구항 27

제26항에 있어서, 상기 제2 서비스는 상기 제1 서비스를 대신하여 상기 하나 이상의 동작을 수행하고/거나 상기 서비스를 획득하고; 상기 하나 이상의 동작의 수행 및/또는 상기 서비스의 획득을 기반으로 하위 결과를 생성하는, 컴퓨터-프로그램 제품.

청구항 28

제27항에 있어서, 상기 제2 서비스는 상기 제1 서비스를 대신하여 상기 하나 이상의 동작을 수행하기 전에 및/또는 상기 서비스를 획득하기 전에 상기 보안 키를 검증하는, 컴퓨터-프로그램 제품.

청구항 29

제23항 내지 제28항 중 어느 한 항에 있어서, 상기 제2 포트는 상기 제1 분산 컴퓨팅 환경과 다른 상기 제2 분산 컴퓨팅 환경 내에 위치하는, 컴퓨터-프로그램 제품.

청구항 30

제23항 내지 제29항 중 어느 한 항에 있어서, 상기 제1 포트에 대한 상기 보안 규칙은: (i) 상기 제1 서비스에 이용 가능한 인스턴스의 수, 및 (ii) 상기 서비스 요청의 처리에 이용 가능한 인스턴스를 더 정의하며, 상기 서

비스 요청을 상기 제1 서비스로 전달하는 것은:

상기 제1 포트에 대한 상기 보안 규칙에 기초하여 상기 서비스 요청을 처리하기 위해 이용 가능한 인스턴스를 결정하는 것; 그리고

상기 제1 서비스의 인스턴스 중 적어도 하나에 상기 서비스 요청을 전달하는 것

을 포함하는, 컴퓨터-프로그램 제품.

청구항 31

제23항 내지 제30항 중 어느 한 항에 있어서, 상기 제1 서비스로부터 상기 제2 서비스로 액세스 요청을 전달하는 것은,

상기 제1 포트에 대한 상기 보안 규칙이 상기 제2 서비스를, 상기 제1 서비스가 통신 및 액세스하도록 인가받은 서비스로 정의하는지 여부를 결정하는 것;

상기 제2 포트에 대한 상기 보안 규칙이 상기 제1 서비스를, 상기 제2 서비스가 상기 제1 서비스로부터 통신을 수신 및 액세스할 수 있도록 인가받은 서비스로 정의하는지 여부를 결정하는 것;

그리고 상기 제2 서비스는, 상기 제1 서비스가 통신 및 액세스하도록 인가받은 서비스이고 상기 제1 서비스는, 상기 제2 서비스가 상기 제1 서비스로부터 통신을 수신 및 액세스할 수 있도록 인가받은 서비스인 경우, 상기 제1 서비스로부터 상기 제2 서비스로 상기 액세스 요청을 전달하는 것

을 포함하는, 컴퓨터-프로그램 제품.

청구항 32

제31항에 있어서, 상기 제2 포트에 대한 상기 보안 규칙은: (i) 상기 제2 서비스에 이용 가능한 인스턴스의 수; 및 (ii) 상기 액세스 요청을 처리하기 위해 이용 가능한 인스턴스를 더 정의하고, 상기 제1 서비스로부터 상기 제2 서비스로 상기 액세스 요청을 전달하는 것은:

상기 제2 포트에 대한 상기 보안 규칙에 기초하여 상기 액세스 요청을 처리하기 위해 이용 가능한 인스턴스를 결정하는 것; 그리고

상기 액세스 요청을 상기 제2 서비스의 인스턴스 중 적어도 하나에 전달하는 것

을 더 포함하는, 컴퓨터-프로그램 제품.

청구항 33

제23항 내지 제32항 중 어느 한 항에 있어서,

상기 제1 서비스는 상기 제1 분산 컴퓨팅 환경에서 제1 컨테이너 또는 제1 컨테이너 세트로서 패키징된 하나 이상의 클러스터에 배치된 하나 이상의 프로그램을 포함하고, 상기 제1 컨테이너 또는 상기 제1 컨테이너 세트는 제1 포트로서 패키징되며, 이는 상기 하나 이상의 클러스터에서 실행되는 상기 하나 이상의 프로그램을 나타내는 상위 레벨 구조이고, 그리고

상기 제2 서비스는 상기 제1 분산 컴퓨팅 환경 또는 제2 분산 컴퓨팅 환경에서 제2 컨테이너 또는 제2 컨테이너 세트로 패키징된 하나 이상의 클러스터에 배치된 하나 이상의 프로그램을 포함하고, 상기 제2 컨테이너 또는 상기 제2 컨테이너 세트는 제2 포트로서 패키징되며, 이는 상기 하나 이상의 클러스터에서 실행되는 상기 하나 이상의 프로그램을 나타내는 상위 레벨 구조인, 컴퓨터-프로그램 제품.

발명의 설명

기술 분야

[0001]

우선권 주장

[0002]

본 출원은 2020년 11월 10일에 출원된 미국 가출원 제63/111,997호의 이익 및 우선권을 주장하며, 모든 목적을 위해 그 전문이 참조로 포함된다.

[0003] 기술분야

[0004] 본 발명은 디지털 및 개인화된 건강 관리에 관한 것으로, 특히 분산 컴퓨팅 환경에서 중앙 집중식 네트워크 메시지를 통한 서비스 간 통신 및 인증 기술에 관한 것이다.

배경 기술

[0005] 의료 분야에서, 데이터 기반 기술 솔루션은 비용을 절감하면서 더욱 개인화된 의료 서비스를 위해 개발되고 있다. 의료 환경이 맞춤형 의료 서비스 및 솔루션의 온-디맨드 배포 시스템으로 이동함에 따라, 의료 서비스 제공자는 소프트웨어 배포 및 서비스 관리 프로세스를 자동화하고 합리화하여 솔루션을 더 빠르게 혁신하는 데 도움이 되는 개발자를 찾고 있다. 의료 서비스 제공자와 서비스를 지원하기 위해 개발자는 분산 컴퓨팅 환경(예: 클라우드 컴퓨팅)을 의료 정보 기술 인프라 표준으로 고려했다. 클라우드 컴퓨팅에는 유연성, 비용 및 에너지 절약, 리소스 공유 및 빠른 배포와 같은 많은 이점이 있다. 예를 들어, 클라우드 컴퓨팅은 다양한 서비스 모델(예: AaaS(Analytics-as-a-Service)) 내에서 소프트웨어 배포 및 서비스 관리 프로세스를 지원하는 데 필요한 복잡한 인프라를 제공할 수 있어, 상이한 의료 제공자 간의 커뮤니케이션, 협업 및 조정을 촉진할 수 있다. 클라우드 컴퓨팅은 또한 의료 산업이 비용 대비 더 많은 가치를 제공하도록 도울 수 있다. 예를 들어, 클라우드 컴퓨팅은 빠르고 유연하며 확장 가능하고 비용 효율적인 인프라와 애플리케이션을 제공할 수 있다. 클라우드 컴퓨팅은 또한 전자 건강 기록(EHR), 실험실 정보 시스템, 제약 정보 시스템 및 의료 이미지를 저장, 관리, 보호, 공유 및 보관하는 데 도움이 될 수 있다.

[0006] 클라우드 컴퓨팅과 같은 분산 컴퓨팅 환경은 의료 서비스 제공자에게 많은 이점을 제공하지만 레거시 스토리지 또는 정보 공유 솔루션과는 다르게 기능하므로 고유한 프라이버시 및 보안 문제가 발생한다. 클라우드에서 데이터를 중앙 집중화하면 개인과 의료 서비스 제공자에게 많은 보안 및 프라이버시 문제가 발생한다. 이러한 데이터 중앙 집중화는 공격자에게 원스톱 쇼핑을 제공하여, 데이터를 훔치고 이동 중인 데이터를 가로채고 데이터 소유권을 클라우드 서비스 공급자에게 이전하여, 개인과 의료 제공자는 민감한 데이터에 대한 일부 통제력을 상실한다. 결과적으로 보안, 프라이버시, 효율성 및 확장성에 대한 우려가 클라우드 기술의 광범위한 채택을 방해하고 있다. 예를 들어 사용자가 인터넷 연결을 통해 데이터에 액세스하기 때문에, 정부 규정(예: HIPAA(Health Insurance Portability and Accountability Act), GxP("모범 사례"(good practice) 품질 지침 및 규정), GDPR(General Data Protection Regulation: 일반 데이터 보호 규정) 준수는 소프트웨어 배포 및 서비스 관리 프로세스를 지원하기 위해 클라우드 솔루션을 찾는 의료 제공자에게 고유한 과제이다. 따라서 보호되는 의료 정보의 기밀성, 가용성 및 무결성을 보장하도록 구축된 규정 준수 소프트웨어 배포 플랫폼의 발전이 필요하다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0007] 일부 실시예에서, 컴퓨터-구현 방법이 제공되며, 상기 방법은: 네트워크 메시에서, 제1 서비스에 대한 서비스 요청을 수신하는 단계; 캐시 또는 서비스 레지스트리로부터 상기 제1 서비스와 연관된 정보를 네트워크 메시가 획득하는 단계 - 상기 정보는 상기 제1 서비스를 포함하는 제1 포트(port)의 신원 및 제1 분산 컴퓨팅 환경 내의 상기 제1 포트의 위치를 포함함; 상기 네트워크 메시가 상기 제1 포트의 위치를 사용하여 상기 제1 포트에 대한 보안 규칙을 불러오는 단계 - 상기 보안 규칙은 (i) 상기 제1 서비스에 대한 고유 주소 식별자, 및 (ii) 상기 제1 서비스가 통신 및 액세스하도록 인가받은 서비스를 정의함; 상기 네트워크 메시가 상기 제1 서비스에 대한 상기 고유 주소 식별자를 사용하여 상기 서비스 요청을 상기 제1 서비스에 전달하는 단계; 상기 네트워크 메시가 제2 서비스와 통신하고 액세스하기 위한 액세스 요청을 상기 제1 서비스로부터 수신하는 단계 - 상기 액세스 요청은 상기 제2 서비스에 특정한 보안 키를 포함함; 상기 네트워크 메시가 상기 캐시 또는 상기 서비스 레지스트리로부터 상기 제2 서비스와 연관된 정보를 획득하는 단계 - 상기 정보는 상기 제2 서비스를 포함하는 제2 포트의 신원 및 상기 제1 분산 컴퓨팅 환경 또는 제2 분산 컴퓨팅 환경 내의 상기 제2 포트의 위치를 포함함; 그리고 상기 네트워크 메시가 상기 제2 포트의 위치를 사용하여 상기 제2 포트에 대한 보안 규칙을 불러오는 단계 - 상기 보안 규칙은 (i) 상기 제2 서비스에 대한 고유 주소 식별자, 및 (ii) 상기 제2 서비스가 통신 및 액세스하도록 인가받은 서비스를 정의함; 상기 네트워크 메시가 상기 제2 서비스에 대한 상기 고유 주소 식별자를 사

용하여, 상기 제1 포트에 대한 보안 규칙 및 상기 제2 포트에 대한 보안 규칙에 기초하여 상기 제1 서비스로부터의 액세스 요청을 상기 제2 서비스로 전달하는 단계; 상기 네트워크 메시가 상기 제1 서비스로부터 상기 서비스 요청의 최종 결과를 수신하는 단계 - 상기 최종 결과는 상기 제2 서비스로부터 획득한 하위 결과를 포함함; 그리고 상기 네트워크 메시가 상기 서비스 요청의 최종 결과를 출력하는 단계를 포함한다.

[0008] 일부 실시예에서, 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 획득하는 단계는: 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보가 상기 캐시로부터 이용 가능한지 여부를 결정하는 단계; 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보가 상기 캐시로부터 이용 가능할 때, 상기 캐시로부터 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 획득하는 단계; 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보가 상기 캐시로부터 이용가능하지 않은 경우, 상기 레지스트리로부터 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 획득하는 단계; 그리고 상기 레지스트리로부터 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 획득하는 것에 응답하여, 후속 요청을 위해 상기 캐시에 상기 제1 서비스 또는 상기 제2 서비스와 연관된 정보를 저장하는 단계를 포함한다.

[0009] 일부 실시예에서, 상기 보안 키는 금고(vault)로부터 상기 제1 서비스에 의해 획득되고, 상기 제1 서비스는 상기 액세스 요청에 상기 보안 키를 내장한다.

[0010] 일부 실시예에서, 상기 제1 서비스로부터의 액세스 요청은 상기 제1 서비스를 대신하여 하나 이상의 동작을 수행 및/또는 서비스를 획득하기 위한 상기 제2 서비스의 요청을 더 포함한다.

[0011] 일부 실시예에서, 상기 제2 서비스는 상기 제1 서비스를 대신하여 상기 하나 이상의 동작을 수행 및/또는 상기 서비스를 획득하고; 상기 하나 이상의 동작의 수행 및/또는 상기 서비스의 획득을 기반으로 하위 결과를 생성한다.

[0012] 일부 실시예에서, 상기 제2 서비스는 상기 제1 서비스를 대신하여 상기 하나 이상의 동작을 수행하기 전에 및/또는 상기 서비스를 획득하기 전에 상기 보안 키를 검증한다.

[0013] 일부 실시예에서, 상기 제2 포트는 상기 제1 분산 컴퓨팅 환경과 다른 상기 제2 분산 컴퓨팅 환경 내에 위치한다.

[0014] 일부 실시예에서, 상기 제1 포트에 대한 상기 보안 규칙은: (i) 상기 제1 서비스에 이용 가능한 인스턴스의 수, 및 (ii) 상기 서비스 요청의 처리에 이용 가능한 인스턴스를 더 정의하며, 상기 서비스 요청을 상기 제1 서비스로 전달하는 단계는: 상기 제1 포트에 대한 상기 보안 규칙에 기초하여 상기 서비스 요청을 처리하기 위해 이용 가능한 인스턴스를 결정하는 단계; 그리고 상기 제1 서비스의 인스턴스 중 적어도 하나에 상기 서비스 요청을 전달하는 단계를 포함한다.

[0015] 일부 실시예에서, 상기 제1 서비스로부터 상기 제2 서비스로 액세스 요청을 전달하는 단계는, 상기 제1 포트에 대한 상기 보안 규칙이 상기 제2 서비스를, 상기 제1 서비스가 통신 및 액세스하도록 인가받은 서비스로 정의하는지 여부를 결정하는 단계; 상기 제2 포트에 대한 상기 보안 규칙이 상기 제1 서비스를, 상기 제2 서비스가 상기 제1 서비스로부터 통신을 수신 및 액세스할 수 있도록 인가받은 서비스로 정의하는지 여부를 결정하는 단계; 그리고 상기 제2 서비스는, 상기 제1 서비스가 통신 및 액세스하도록 인가받은 서비스이고 상기 제1 서비스는, 상기 제2 서비스가 상기 제1 서비스로부터 통신을 수신 및 액세스할 수 있도록 인가받은 서비스인 경우, 상기 제1 서비스로부터 상기 제2 서비스로 상기 액세스 요청을 전달하는 단계를 포함한다.

[0016] 일부 실시예에서, 상기 제2 포트에 대한 상기 보안 규칙은: (i) 상기 제2 서비스에 이용 가능한 인스턴스의 수; 및 (ii) 상기 액세스 요청을 처리하기 위해 이용 가능한 인스턴스를 더 정의하고, 상기 제1 서비스로부터 상기 제2 서비스로 상기 액세스 요청을 전달하는 단계는: 상기 제2 포트에 대한 상기 보안 규칙에 기초하여 상기 액세스 요청을 처리하기 위해 이용 가능한 인스턴스를 결정하는 단계; 그리고 상기 액세스 요청을 상기 제2 서비스의 인스턴스 중 적어도 하나에 전달하는 단계를 더 포함한다.

[0017] 일부 실시예에서, 상기 제1 서비스는 상기 제1 분산 컴퓨팅 환경에서 제1 컨테이너 또는 제1 컨테이너 세트로서 패키징된 하나 이상의 클러스터에 배치된 하나 이상의 프로그램을 포함하고, 상기 제1 컨테이너 또는 상기 제1 컨테이너 세트는 제1 포트로서 패키징되며, 이는 상기 하나 이상의 클러스터에서 실행되는 상기 하나 이상의 프로그램을 나타내는 상위 레벨 구조이고, 그리고 상기 제2 서비스는 상기 제1 분산 컴퓨팅 환경 또는 상기 제2 분산 컴퓨팅 환경에서 제2 컨테이너 또는 제2 컨테이너 세트로서 패키징된 하나 이상의 클러스터에 배치된 하나 이상의 프로그램을 포함하고, 상기 제2 컨테이너 또는 상기 제2 컨테이너 세트는 제2 포트로서 패키징되며, 이는

상기 하나 이상의 클러스터에서 실행되는 상기 하나 이상의 프로그램을 나타내는 상위 레벨 구조이다.

[0018] 일부 실시예에서, 본 개시는 하나 이상의 데이터 프로세서를 포함하는 시스템을 포함한다. 일부 실시예에서, 상기 시스템은 상기 하나 이상의 데이터 프로세서에서 실행될 때, 여기서 개시되는 하나 이상의 방법의 방법의 일부 또는 전부 및/또는 하나 이상의 프로세스의 방법의 일부 또는 전부를 상기 하나 이상의 데이터 프로세서로 하여금 수행하게 하는 명령어를 포함하는 비일시적 컴퓨터 판독가능 저장 매체를 포함한다. 본 개시의 일부 실시예는 여기서 개시되는 하나 이상의 방법의 일부 또는 전부 및/또는 하나 이상의 프로세스의 방법의 일부 또는 전부를 상기 하나 이상의 데이터 프로세서로 하여금 수행하게 하도록 구성된 명령어를 포함하는, 비일시적 기계 판독가능 저장 매체에 유형적으로 구현된 컴퓨터 프로그램 제품을 포함한다.

[0019] 사용된 용어 및 표현은 제한이 아닌 설명의 용어로 사용되었으며, 그러한 용어 및 표현의 사용에 있어서 도시되고 설명된 특징 또는 그 일부의 등가물을 배제하려는 의도는 없다. 청구된 발명의 범위 내에서 다양한 수정이 가능하다는 것이 인정된다. 따라서, 청구된 본 발명이 실시예 및 선택적인 특징에 의해 구체적으로 개시되었지만, 본 명세서에 개시된 개념의 수정 및 변형이 당업자에 의해 이루어질 수 있고, 그러한 수정 및 변형이 첨부된 청구범위에 의해 정의된 바와 같이 본 발명의 범위 내에 있도록 고려됨을 이해해야 한다.

발명의 효과

도면의 간단한 설명

[0020] 본 개시는 첨부된 도면과 함께 설명된다:

도 1은 다양한 실시예에 따른 데이터 기반 기술 솔루션을 제공하기 위한 디지털 건강 플랫폼의 다이어그램을 도시한다.

도 2는 다양한 실시예에 따른 보안 시스템의 다이어그램을 도시한다.

도 3은 다양한 실시예에 따른 디지털 건강 플랫폼에서 서비스 간 통신 및 인증을 위한 프로세스를 예시하는 스웸 라인 다이어그램을 도시한다. 그리고

도 4는 다양한 실시예에 따른 중앙집중식 네트워크 메시 환경을 통한 서비스 간 통신 및 인증을 위한 프로세스를 예시하는 흐름도를 도시한다.

첨부된 도면에서, 유사한 구성요소 및/또는 특징은 동일한 참조 라벨을 가질 수 있다. 또한 동일한 유형의 다양한 구성 요소는 참조 레이블 뒤에 대시(-) 및 유사한 구성 요소를 구분하는 제2 레이블을 사용하여 구분할 수 있다. 본 명세서에서 제1 참조 표지만을 사용하는 경우에는 제2 참조 표지와 상관없이 동일한 제1 참조 표지를 갖는 유사한 구성요소 중 어느 하나에 대하여도 그 기재를 적용할 수 있다.

발명을 실시하기 위한 구체적인 내용

[0021] I. 개요

[0022] 본 개시는 분산 컴퓨팅 환경에서 중앙 집중식 네트워크 메시지를 통한 서비스 간 통신 및 인증을 위한 기술을 설명한다. 보다 구체적으로, 본 개시의 실시예는 서비스가 안전한 방식으로 여러 유형의 분산 컴퓨팅 환경에 걸쳐 서로 통신할 수 있도록 포트-레벨 네트워킹을 제공하는 네트워크 메시지를 제공한다. 네트워크 메시 및 포트-레벨 네트워킹은 서비스와 리소스 간의 격리를 유지하므로 데이터가 저장되는 위치, 누가 어떤 데이터에 액세스할 수 있는지, 서비스 또는 사용자가 지정된 시간에 사용할 수 있는 리소스에 대한 통제를 유지관리하는 것이 용이하며, 서비스 또는 리소스가 실행되거나 저장되는 위치에 관계없이 항상 올바른 서비스 및 리소스에 올바른 액세스 권한이 있는지 보장하는 것이 용이하다.

[0023] 클라우드 컴퓨팅은 기회와 과제를 제공한다. 다른 많은 정보 기술 솔루션과 마찬가지로, 클라우드에도 다양한 보안 문제와 우려 사항이 있다. 클라우드 컴퓨팅은 일반적으로 개방형 공유 환경에서 작동하기 때문에 데이터 손실, 도난 및 악의적인 공격에 취약한 경우가 많다. 약한 클라우드 보안은 의료 산업에서 클라우드 컴퓨팅의 완전한 확산을 방해하는 중요한 문제 중 하나이다. 의료 전문가들은 클라우드 컴퓨팅을 신뢰하지 않는 많은 이유가 있다. 예를 들어 의료 기록에 대한 통제권을 넘길 수 없다. 조직 및 클라우드 제공자는 일반적으로 서로 다른 지리적 위치에 있는 서로 다른 데이터 센터에 데이터를 저장한다. 이는 클라우드의 데이터 스토리지가 중

복되고 불가항력의 경우 서로 다른 데이터 센터가 재해 복구에 도움이 되기 때문에 고유한 이점을 나타낸다. 다른 한편으로, 상이한 위치에 저장된 데이터는 도난 및 손실되기 쉽기 때문에 동일한 이점으로 인해 보안 문제가 발생할 수 있다. 또한, 서로 다른 위치에 저장된 데이터와 그 보안은 다양한 국제, 지역 및 현지 규정의 적용을 받는다. 일반적으로 클라우드 컴퓨팅 사용과 관련된 많은 보안 위험이 있다. 예를 들어 가상 사용자 분리 실패, 신원 도용, 권한 남용 및 부실한 암호화가 이러한 보안 위험 중 일부이다.

[0024] 이러한 제한 및 문제를 해결하기 위해, 본 개시의 서비스간 통신 및 인증을 위한 기술은 통신 규칙 및 보안 키에 의해 관리되는 포트-레벨 네트워킹을 이용한다. 디지털 및 개인화된 의료 환경에는 일반적으로 서로 상호 작용하는 여러 파트너가 있으며 이러한 상호 작용은 서비스와 리소스 간의 격리 및 추적 가능성을 유지하기 위해 안전한 방식으로 제어되어야 한다. 서비스는 하나 이상의 파트너가 제공할 수 있는 임의의 서비스(예: 데이터 분석 또는 의료 기기로서의 소프트웨어와 같은 의료 관련 서비스)이다. 리소스는 일반적으로 서비스를 지원하는 하드웨어 및 소프트웨어 리소스(예: 메모리 및 처리 장치)이다. 그러나 어떤 경우에는 리소스가 데이터, 알고리즘, 모델 등(예: 데이터 저장소에 저장된 건강 관리 관련 데이터)을 포함할 수도 있음을 이해해야 한다. 이러한 상호 작용을 안전한 방식으로 제어하기 위해, 서로 통신할 수 있는 서비스들과, 해당 서비스가 액세스할 수 있는 리소스들을 정의하는 포트-레벨 보안 규칙이 제공된다. 또한, 서비스가 다른 서비스나 리소스에 액세스할 수 있도록 하는 보안 키(예: 공개/개인 키 쌍)가 제공된다. 이 2-계층 접근 방식은 서비스와 리소스 간의 격리 및 추적 가능성을 유지하기 위해, 하나 이상의 분산 컴퓨팅 환경에서 각 서비스의 포트-레벨 보안 규칙 및 위치에 액세스할 수 있는 중앙 집중식 네트워크 메시에 의해 촉진된다. 예를 들어, 서비스에 대한 호출(call)이 네트워크 메시에 의해 수신되면, 네트워크 메시는 포트-레벨 보안 규칙 및 서비스 위치에 관한 정보를 기반으로 호출을 적절한 서비스로 라우팅하고, 서비스를 제공하기 위한 다양한 작업을 수행할 수 있도록 네트워크 메시지를 통해 하나 이상의 보안 키 및 프록시 호출을 이용하여 서비스가 다른 서비스 및 리소스에 액세스할 수 있다.

[0025] 본 발명의 예시적인 일 실시예는 네트워크 메시에서 사용자로부터 제1 서비스에 대한 서비스 요청을 수신하는 단계; 및 네트워크 메시가 캐시 또는 서비스 레지스트리로부터 제1 서비스와 연관된 정보를 획득하는 단계를 포함한다. 정보는 제1 서비스를 포함하는 제1 포트의 신원 및 제1 분산 컴퓨팅 환경 내의 제1 포트의 위치를 포함한다. 방법은 네트워크 메시가 제1 포트의 위치를 사용하여 제1 포트에 대한 보안 규칙을 불러오는 단계를 더 포함한다. 보안 규칙은: (i) 제1 서비스에 대한 고유 주소 식별자 및 (ii) 제1 서비스가 통신하고 액세스할 수 있는 권한이 부여된 서비스를 정의한다. 이 방법은 네트워크 메시가, 제1 서비스에 대한 고유 주소 식별자를 사용하여 서비스 요청을 제1 서비스에 전달하는 단계; 및 상기 네트워크 메시가 상기 제1 서비스로부터 제2 서비스와 통신 및 액세스하기 위한 액세스 요청을 수신하는 단계를 더 포함한다. 액세스 요청에는 제2 서비스에 특정한 보안 키가 포함된다. 방법은 네트워크 메시가, 캐시 또는 서비스 레지스트리로부터 제2 서비스와 연관된 정보를 획득하는 단계를 더 포함한다. 정보는 제2 서비스를 포함하는 제2 포트의 신원 및 제1 분산 컴퓨팅 환경 또는 제2 분산 컴퓨팅 환경 내의 제2 포트의 위치를 포함한다. 방법은 제2 포트의 위치를 사용하여 네트워크 메시가, 제2 포트에 대한 보안 규칙을 불러오는 단계를 더 포함한다. 보안 규칙은: (i) 제2 서비스에 대한 고유 주소 식별자; 및 (ii) 제2 서비스가 통신하고 액세스할 수 있는 서비스를 정의한다. 이 방법은 제2 서비스에 대한 고유 주소 식별자를 사용하여 네트워크 메시가, 제1 포트에 대한 보안 규칙 및 제2 포트에 대한 보안 규칙에 기초하여 제1 서비스로부터 제2 서비스로 상기 액세스 요청을 전달하는 단계; 및 상기 네트워크 메시가 상기 제1 서비스로부터 서비스 요청의 최종 결과를 수신하는 단계를 더 포함한다. 최종 결과에는 제2 서비스에서 얻은 하위 결과가 포함된다. 이 방법은 네트워크 메시가 서비스 요청의 최종 결과를 사용자에게 전달하는 단계를 더 포함한다.

[0026] II. 디지털 건강 플랫폼

[0027] 도 1은 다양한 실시예에 따라 데이터 기반 기술 솔루션을 제공하기 위한 디지털 건강 플랫폼(100)의 단순화된 도면을 도시한다. 예시된 실시예에서, 디지털 건강 플랫폼(100)은 네트워크 게이트웨이(120) 및 네트워크 메시(125)를 포함하는 네트워크(115)를 통해 클라우드 기반 인프라(110)에 연결된 클라이언트 컴퓨팅 장치(105)를 포함한다. 인프라(110)는 다양한 하드웨어 및 클라우드 인프라(예를 들어, 프라이빗 클라우드 또는 온-프레미스 클라우드 인프라 및 퍼블릭 클라우드 인프라)를 사용하여 클라우드 서비스 제공자(140)(예를 들어, 분산 컴퓨팅 환경)에 의해 배치 링(135) 내에 프로비저닝된 리소스를 사용하여 서비스 포트(130) 내에서 서비스 또는 소프트웨어 애플리케이션을 실행하도록 적응된다. 이러한 서비스 또는 소프트웨어 애플리케이션은 클라이언트 컴퓨팅 장치(105)의 사용자에게 AaaS 또는 SaaS 모델과 같은 웹 기반 또는 클라우드 서비스로 제공될 수 있다. 여러 제공자는 Amazon, Google 및 Oracle과 같은 클라우드 서비스를 제공한다. 클라우드 서비스라는 용어는 일반적으로 의료 제공자 또는 정부 규제 대상과 같은 서비스 제공자의 시스템(예: 인프라(110))에 의해 인터넷과 같은 통신

네트워크를 통해 주문형으로 사용자에게 제공되는 서비스를 지칭하는 데 사용된다. 따라서 소비자는 이러한 서비스를 지원하는 별도의 라이선스, 지원 또는 서비스를 지원하는 하드웨어 및 소프트웨어 리소스를 구매하지 않고도 서비스 공급자가 제공하는 클라우드 서비스를 이용할 수 있다. 예를 들어, 클라우드 서비스 제공자의 시스템은 하나 이상의 프로그램을 호스팅할 수 있으며, 사용자는 하나 이상의 프로그램을 호스팅할 수 있고, 사용자는 인터넷을 통해 주문형으로 하나 이상의 프로그램을 사용할 수 있으며, 하나 이상의 프로그램을 실행하기 위해 인프라 리소스를 구매할 필요가 없다. 클라우드 서비스는 애플리케이션, 리소스 및 서비스에 대한 쉽고 확장 가능한 액세스를 제공하도록 설계되었다.

[0028] 일부 경우에, 클라이언트 컴퓨팅 장치(105)를 작동하는 사용자(예를 들어, 소프트웨어 또는 서비스 소비자)는 인프라(110)의 다양한 구성요소(145)에 의해 제공되는 소프트웨어 제품, 서비스 또는 시스템을 소비하기 위해 하나 이상의 클라이언트 애플리케이션을 활용한다. 다른 예에서, 클라이언트 컴퓨팅 장치(105)를 작동하는 사용자(예를 들어, 개발자)는 인프라(110)의 다양한 구성요소(145)에 의해 제공될 소프트웨어 제품, 서비스 또는 시스템에 대한 소스 코드를 업로드하기 위해 하나 이상의 클라이언트 애플리케이션을 활용한다. 구성요소(145)는 하나 이상의 프로세서, 하드웨어 구성 요소 또는 이들의 조합에 의해 실행될 수 있는, 소프트웨어 구성요소를 포함한다. 디지털 건강 플랫폼(100)에 대해 예시된 것과 상이할 수 있는 다양한 상이한 시스템 구성이 가능하다는 것을 이해해야 한다. 따라서 도 1에 도시된 실시예는 디지털 건강 플랫폼을 구현하기 위한 분산 컴퓨팅 환경의 한 예이며 제한하려는 의도가 아니다.

[0029] 클라이언트 컴퓨팅 장치(105)는 휴대용 핸드헬드 장치, 개인용 컴퓨터 및 랩탑과 같은 범용 컴퓨터, 워크스테이션 컴퓨터, 웨어러블 장치, 게임 시스템, 씰 클라이언트, 다양한 메시징 장치, 센서 또는 기타 감지 장치, 등과 같은 다양한 유형의 컴퓨팅 시스템을 포함한다. 이러한 컴퓨팅 장치는 다양한 모바일 운영 체제(예: Microsoft Windows Mobile®, iOS®, Windows Phone®, Android™, BlackBerry®, Palm OS®)를 포함한, 다양한 유형 및 버전의 소프트웨어 애플리케이션 및 운영 체제(예: Microsoft Windows®, Apple Macintosh®, UNIX® 또는 UNIX 유사 운영 체제, Linux 또는 Google Chrome™ OS와 같은 Linux 유사 운영 체제)를 실행할 수 있다. 휴대용 핸드헬드 장치는 휴대폰, 스마트폰(예: iPhone®), 태블릿(예: iPad®), PDA(Personal Digital Assistants) 등을 포함할 수 있다. 웨어러블 장치에는 Fitbit Versa™ 스마트 워치, magic leap 1®, HTC Vive® 및 Oculus®와 같은 가상 현실(VR) 또는 증강 현실(AR) 시스템, 및 기타 장치가 포함될 수 있다. 게임 시스템에는 다양한 핸드헬드 게임 장치, 인터넷 지원 게임 장치(예: Kinect® 제스처 입력 장치가 있거나 없는 Microsoft Xbox® 게임 콘솔, Sony PlayStation® 시스템, Nintendo®에서 제공하는 다양한 게임 시스템, 등), 등이 포함될 수 있다. 클라이언트 장치(105)는 다양한 인터넷 관련 앱, 통신 애플리케이션(예를 들어, 이메일 애플리케이션, 단문 메시지 서비스(SMS) 애플리케이션)과 같은 다양한 상이한 애플리케이션을 실행할 수 있고 다양한 통신 프로토콜을 사용할 수 있다.

[0030] 네트워크(115)는 제한 없이 TCP/IP(전송 제어 프로토콜/인터넷 프로토콜), SNA(시스템 네트워크 아키텍처), IPX(인터넷 패킷 교환), AppleTalk® 등을 포함한, 임의의 다양한 이용 가능한 프로토콜을 사용하여 데이터 통신을 지원할 수 있는 당업자에게 친숙한 임의 유형의 네트워크이다. 단지 예로서, 네트워크(115)는 근거리 통신망(LAN), 이더넷 기반 네트워크, 토큰링, 광역 통신망(WAN), 인터넷, 가상 네트워크, 가상 사설망(VPN), 인트라넷, 엑스트라넷, PSTN(Public Switched Telephone Network), 적외선 네트워크, 무선 네트워크(예: IEEE(Institute of Electrical and Electronics) 802.11 프로토콜 제품군에서 작동하는 네트워크, Bluetooth® 및/또는 기타 무선 프로토콜) 및/또는 이들 및/또는 기타 네트워크의 조합일 수 있다.

[0031] 네트워크 게이트웨이(120)는 동일하거나 상이한 프로토콜에서 동작하는 둘 이상의 네트워크(115) 사이에 안전한 통로를 형성하는 네트워크 노드이다. 네트워크 게이트웨이(120)는 다음 기술 중 하나 이상을 사용하여 네트워크 보안을 제공할 수 있다: 유입 및 유출 네트워크 트래픽을 모니터링하기 위한 방화벽, 사설 보안 통신 채널을 제공하기 위한 가상 사설망, 네트워크 내의 보안 결함을 식별하기 위한 보안 스캐닝, 인증 및 권한 부여 서비스 등을 위한 액세스 관리자, 등. 네트워크 게이트웨이(120)는 다양한 소프트웨어 제품, 서비스 또는 시스템에 대한 액세스를 관리하는 서비스 커넥터 및 라우터를 사용하여(예를 들어, 서비스 가입 비즈니스 모델을 사용하여) 네트워크 트래픽을 라우팅한다. 네트워크 메시(125)는 인프라(110)(예를 들어, 브리지, 스위치 및 기타 인프라 장치)가 가능한 한 많은 다른 노드에 직접, 동적으로 및 비계층적으로 연결하고, 장치와 노드 사이에서 데이터를 효율적으로 라우팅하기 위해 서로 협력하는 로컬 네트워크 토폴로지이다. 네트워크 메시(125)는 로드 밸런싱, 제품, 서비스 또는 시스템 발견, 네트워크 액세스, 라우팅 및 피어링, 트래픽 미러링 등의 기술 중 하나 이상을 사용하여 연결을 관리한다. 네트워크(115), 네트워크 게이트웨이(120) 및 네트워크 메시(125)는 결합

하여 인프라(110)로부터 유입 또는 유출되는 모든 데이터를 관리한다.

[0032] 구성요소(145)는 하나 이상의 범용 컴퓨터, 전문 서버 컴퓨터(예를 들어, PC(개인용 컴퓨터) 서버, 애플리케이션 특정 서버, 중급 서버, 메인프레임 컴퓨터, 랙 장착형 서버 등을 포함함), 서버 팜, 서버 클러스터, 또는 네트워크(115)를 통해 클라이언트 컴퓨팅 장치(105)에 리소스, 데이터, 서비스 또는 프로그램을 제공하기 위해 개별적으로 또는 조합하여 작동하는 임의의 다른 적절한 배열 및/또는 조합 컴퓨터 또는 시스템을 포함한다. 구성요소(145)는 가상 운영 체제, 또는 가상 저장 장치를 유지하기 위해 가상화될 수 있는 논리적 저장 장치의 하나 이상의 유연한 풀과 같은 가상화를 포함하는 다른 컴퓨팅 아키텍처를 실행하는 하나 이상의 가상 머신을 더 포함할 수 있다. 다양한 실시예에서, 구성요소(145)는 본 개시에 설명된 기능을 제공하는 하나 이상의 서비스 또는 소프트웨어 애플리케이션을 실행하도록 적응된다.

[0033] 구성요소(145)는 또한 하나 이상의 데이터 리포지토리(data repositories)를 포함한다. 이러한 데이터 리포지토리는 다양한 실시예에서 데이터 및 기타 정보를 저장하는 데 사용될 수 있다. 예를 들어, 하나 이상의 데이터 리포지토리는 SAMD(Software as a Medical Device)와 같은 데이터 기반 기술 솔루션을 제공하기 위한 정보를 저장하고, 데이터 기반 기술 솔루션을 구현하기 위한 소스 코드의 검증 및 배포를 위한 정보를 저장하는 데 사용될 수 있다. 데이터 리포지토리는 다양한 위치에 상주할 수 있다. 예를 들어, 구성 요소에 의해 사용되는 데이터 리포지토리는 구성 요소에 로컬이거나 구성 요소로부터 멀리 떨어져 있고 네트워크 기반 또는 전용 연결을 통해 구성 요소와 통신할 수 있다. 데이터 리포지토리는 상이한 유형의 것일 수 있다. 특정 실시예에서, 구성 요소에 의해 사용되는 데이터 리포지토리는 데이터베이스, 예를 들어 중앙집중형 데이터베이스, 분산 데이터베이스, NoSQL 데이터베이스, 관계형 데이터베이스 등일 수 있다. 이러한 데이터베이스 중 하나 이상은 SQL-형식 명령에 대한 응답으로 데이터베이스에서 데이터를 저장, 업데이트 및 불러오기할 수 있도록 조정될 수 있다. 특정 실시예에서, 하나 이상의 데이터 리포지토리는 또한 애플리케이션 데이터를 저장하기 위해 애플리케이션에 의해 사용될 수 있다. 애플리케이션에 의해 사용되는 데이터 리포지토리는 예를 들어 키-값 저장 리포지토리, 개체 저장 리포지토리 또는 파일 시스템에서 지원하는 일반 저장 리포지토리나 같은, 상이한 유형의 것일 수 있다.

[0034] 구성요소(145)는 또한 본 개시에 기술된 기능을 제공하는 서비스 또는 소프트웨어 애플리케이션(예를 들어, 웹 기반 또는 클라우드 서비스로 제공되는 서비스 또는 소프트웨어 애플리케이션 또는 지속적인 통합 및 지속적인 배포(CI/CD) 시스템을 구현하기 위한 애플리케이션)와 같은 하나 이상의 프로그램을 실행하도록 구성된 컴퓨팅 노드를 포함한다. 각 노드는 노드 클러스터 내에서 선택적으로 구현되는 단일 머신을 나타낸다. 단일 머신은 물리적 머신(예: 데이터 센터의 서버)이거나, 사용할 수 있는 일련의 CPU 및 RAM 리소스들의 세트를 구비한 Amazon Web Services™(AWS)와 같은 클라우드 제공자에서 호스팅되는 가상 머신일 수 있다. 클러스터에서, 노드는 리소스를 함께 풀링하여 보다 강력한 머신을 형성한다. 하나 이상의 프로그램이 클러스터에 배포되면 클러스터는 개별 노드에 대한 분산 작업을 지능적으로 처리한다. 노드가 추가되거나 제거되면 클러스터는 필요에 따라 작업을 이동할 수 있다. 어떤 개별 머신이 실제로 코드를 실행하고 있는지는 하나 이상의 프로그램 또는 인프라(110)에 중요하지 않다.

[0035] 하나 이상의 클러스터에 배포되는 하나 이상의 프로그램은 컨테이너로 패키징된다. 컨테이너는 널리 받아들여지는 표준이며 인프라(110)에 하나 이상의 프로그램을 배치하기 위해 다양한 이미지가 정의될 수 있다. 컨테이너화는 인프라(110)가 자체 포함 실행 환경을 생성할 수 있도록 한다. 모든 프로그램과 모든 종속성을 단일 파일로 묶은 다음, 인프라에서 공유할 수 있다. 컨테이너 생성은 프로그램 방식으로 이루어져서, 강력한 완전 자동화 CI/CD 파이프라인을 인프라(110) 상에서 코드 검증 및 코드 배포를 위해 사용할 수 있게 된다. 컨테이너는 포드(pod)(130)로 알려진 상위 레벨 구조로 래핑(wrapping)된다. 동일한 포드(130)의 컨테이너는 동일한 리소스 및 로컬 네트워크를 공유할 수 있다. 일부 경우에, 컨테이너는 다른 컨테이너로부터 어느 정도의 격리를 유지하면서 동일한 머신에 있는 것처럼 동일한 포드(130)의 다른 컨테이너와 통신할 수 있다. 포드(130)는 인프라(110)에서 복제 단위로 사용된다. 프로그램 또는 리소스가 처리로 압도되고 단일 포드(130) 인스턴스가 로드를 수행할 수 없는 경우, 인프라(110)는 필요에 따라 포드(130)의 새로운 복제본을 클러스터에 배포하도록 구성될 수 있다. 과부하 상태가 아닐 때에도, 로드 밸런싱 및 장애 허용을 허용하기 위해 생산 시스템에서 언제든지 실행 중인 포드(130)의 여러 복사본을 갖는 것이 유리할 수 있다. 포드(130)의 하나 이상의 인스턴스는 하나 이상의 클라우드 서비스 제공자(140)에 의해 제공되는 클라우드 인프라 시스템 상에 프로비저닝된다.

[0036] 하나 이상의 클라우드 서비스 제공자(140)에 의해 제공되는 클라우드 인프라 시스템은 인프라(110)에 의해 제공되는 다양한 클라우드 서비스를 지원하는 포드(130)의 하나 이상의 인스턴스의 제공을 용이하게 하기 위해 활용

되는 인프라 리소스를 포함한다. 포트(130)의 하나 이상의 인스턴스를 프로비저닝하기 위한 리소스의 효율적 활용을 용이하게 하기 위해, 리소스는 리소스 세트 또는 리소스 모듈 세트("배치 링(135)" 또는 "스테이트풀 링(stateful rings)(135)"이라고도 함)로 묶일 수 있다. 각각의 리소스 모듈 또는 배치 링(135)은 하나 이상의 유형의 리소스의 미리 통합되고 최적화된 조합을 포함할 수 있다. 특정 예에서, 상이한 배치 링(135)들이 상이한 유형의 클라우드 서비스에 대해 미리 프로비저닝될 수 있다. 예를 들어, 배치 링(135)의 제1 세트가 SAMD 서비스를 위해 프로비저닝될 수 있고, 배치 링(135)의 제1 세트의 배치 링(135)과 상이한 리소스 조합을 포함할 수 있는 배치 링(135)의 제2 세트가 데이터 분석 서비스, 등을 위해 프로비저닝될 수 있다. 일부 클라우드 서비스의 경우, 서비스 프로비저닝을 위해 할당된 리소스를 서비스 간에 공유할 수 있다.

[0037] 디지털 건강 플랫폼(100)은 하나 이상의 커널(150)을 더 포함한다. 커널(150)은 하나 이상의 클라우드 서비스 제공자(140)가 제공하는 각각의 클라우드 인프라 시스템에서 실행되도록 적응된다. 커널(150)은 전체 디지털 건강 플랫폼(100)에 걸쳐 분산된 애플리케이션 또는 프레임워크에 걸친 리소스 할당 및 격리를 제공하는 클러스터 관리자이다. 커널(150)은 리소스 관리 및 스케줄링을 포함하는 서비스 및 소프트웨어의 오케스트레이션을 위한 애플리케이션 프로그래밍 인터페이스(API)를 하나 이상의 프로그램에 제공한다. 커널(150)의 아키텍처는 작업을 실행하기 위한 에이전트 노드, 작업을 에이전트 노드로 전송하기 위한 마스터 노드, 마스터 노드의 선출 및 주소 조회를 위한 주키퍼, 마스터 노드와 협력하여 에이전트 노드에 작업을 예약하기 위한 프레임워크를 포함한다.

[0038] 디지털 건강 플랫폼(100)은 CI/CD 시스템(155)을 더 포함한다. CI/CD 시스템(155)은 클라우드 인프라 시스템 내에서 구현되며 디지털 건강 플랫폼(100)이 소프트웨어 제품, 서비스 또는 시스템에 대한 소스 코드 내의 변경 사항을 자주 업데이트, 테스트 및 전달할 수 있게 한다. 여기에서 자세히 논의한 바와 같이, 의료 분야에는 소프트웨어가 준수해야 하는 데이터 보안(예: 데이터 무결성 및 데이터 프라이버시)에 관한 정부 규정이 있다. CI/CD 시스템(155)에서, 이러한 정책 규정은 코드에 포함될 수 있어 준수가 자동으로 추적, 검증 및 재구성될 수 있다. SAMD의 예에서, 데이터 저장 위치, 서버 액세스 제어 및 활동 로깅이 소스 코드에 포함될 수 있으므로, 소프트웨어를 사용하는 동안 사용자 데이터를 보호하고 관리할 수 있다. 지속적인 통합 중에 암호화 및 암호 보호 작업을 추가로 포함할 수 있다. 지속적 전달 중에 보안 및 모니터링 도구를 사용하여 사용자 활동을 추적하고 보안 위협으로 이어질 수 있는 오류를 감지할 수 있다.

[0039] CI/CD 시스템(155)은 또한 머신 러닝 모델을 프로비저닝하기 위해 사용될 수 있다. 머신 러닝 모델은 처음에는 데이터 세트를 사용하여 훈련되지만 시간이 지남에 따라 모델이 드리프트되거나 데이터가 변경될 수 있으므로, 업데이트된 머신 러닝 모델이 필요하다. 머신 러닝 모델이 소프트웨어 애플리케이션 내에서 실행되는 경우 소프트웨어 애플리케이션과 연결된 코드에는 머신 러닝 모델을 재교육해야 하는 시기에 대한 트리거가 포함될 수 있다. 예를 들어, 코드는 새로운 훈련 데이터가 이용 가능하거나 머신 러닝 모델의 성능이 임계값 아래로 떨어지는 것으로 결정될 때, 미리 정의된 시간 간격으로 머신 러닝 모델을 재훈련하기 위한 명령어를 포함할 수 있다. 또한 소프트웨어 개발자는 생산 환경에서 머신 러닝 모델의 성능의 모니터링에 기초하여 또는 모델 최적화를 위한 예상 개선 사항을 기반으로, 테스트 환경에서 모델 아키텍처 및 하이퍼파라미터의 변형을 탐색할 수 있다. CI/CD 시스템(155)은 머신 러닝 모델이 성능 요구 사항을 충족하는 것으로 결정될 때 용이한 구축, 테스트 및 생산 환경으로의 배포를 허용한다.

[0040] III. 보안 시스템

[0041] 도 2는 다양한 실시예에 따라 분산 컴퓨팅 환경(205)에서 중앙 집중식 네트워크 메시지를 통한 서비스 간 통신 및 인증을 위한 보안 시스템(200)(도 1과 관련하여 설명된 네트워크 게이트웨이(120), 네트워크 메시(125) 및 포트(130) 포함)의 단순화된 도면을 도시한다. 단일 분산 컴퓨팅 환경만이 도시되어 있지만, 다중 분산 컴퓨팅 환경이 디지털 건강 플랫폼 내에서 구현될 수 있고 각각의 분산 컴퓨팅 환경이 도 2에 도시된 자체 구성요소 세트를 가질 것이라는 점을 이해해야 한다. 예시된 실시예에서, 보안 시스템(200)은 하나 이상의 클라이언트 애플리케이션(210)(예를 들어, 환자 및/또는 서비스 소비자)과 같은 인간 활동가에 의해 자체적으로 조작되는 장치의 애플리케이션/소프트웨어 모듈), 도메인 이름 시스템(DNS)(215), 게이트웨이(220), 네트워크 메시(225), 퍼블릭 에이전트(230) 및 프라이빗 에이전트(235)를 포함한다. 퍼블릭 에이전트(230)는 사용자(210)에게 퍼블릭 서비스를 제공한다. 프라이빗 에이전트(235)는 서비스 포트(240), 금고(vault)(245) 및 금고 게이트웨이(vault gateway)(250)를 포함하며, 이들은 함께 작업하여, 개인 서비스를 제공할 수 있다.

[0042] 클라이언트 애플리케이션(210)은 디지털 건강 플랫폼에 의해 제공되는 소프트웨어 제품, 서비스 또는 시스템을 소비하기 위해 사용자에게 의해 작동된다. 클라이언트 애플리케이션(210)은 분산 컴퓨팅 환경 커넥터 및 DNS(21

5)를 통해 디지털 건강 플랫폼과의 통신(예를 들어, 요청 전송)에 의해 소프트웨어 제품, 서비스 또는 시스템을 소비할 수 있다. DNS(215)는 IP 주소 및 기타 데이터를 저장하는 계층적 분산 데이터베이스이며, IP 주소로 호출(call)을 전달하기 위해 IP 주소를 이름으로 조회할 수 있게 한다. 예를 들어, 디지털 건강 플랫폼이 사용자의 요청을 수신하면, 분산 컴퓨팅 환경 커넥터는 요청을 만족시킬 수 있는 분산 컴퓨팅 환경을 식별하고, 요청 및 요청을 만족시킬 수 있는 분산 컴퓨팅 환경을 DNS(215)로 전달하며, - DNS(215)는 분산 컴퓨팅 환경과 연관된 IP 주소 및 기타 데이터를 조회함 - 연관된 분산 컴퓨팅 환경(예를 들어, 분산 컴퓨팅 환경(205))의 게이트웨이(예를 들어, 게이트웨이(220))의 게이트웨이 엔드포인트로 요청을 전달한다.

[0043]

일단 게이트웨이 엔드포인트에 연결되면, 클라이언트 애플리케이션(210)은 세션에서 하나 이상의 서비스에 액세스하기 위해 인가자(예를 들어, 액세스 관리 시스템)와 통신에 참여할 수 있다. 예시를 위해, 본 명세서에 기술된 바와 같은 "세션"은 사용자에게 하나 이상의 서비스에 대한 액세스를 제공하는 세션 또는 액세스 세션을 포함한다. 본 명세서에 개시된 세션은 예를 들어 SSO 세션, 인증 세션, 또는 사용자에게 액세스를 제공하는 임의의 다른 유형의 세션으로 지칭될 수 있다. 서비스에는 파일, 웹 페이지, 전자 콘텐츠, 문서, 웹 콘텐츠, 컴퓨팅 리소스 또는 애플리케이션에 의해 제공되는 액세스 및 기능이 제한 없이 포함될 수 있다. 예를 들어 디지털 건강 플랫폼에는 소프트웨어 제품, 클라우드 서비스 또는 시스템과 같은 액세스 가능한 서비스가 포함될 수 있다. 애플리케이션을 사용하여 서비스를 요청하고 액세스할 수 있다. 예를 들어, 애플리케이션은 요청된 서비스를 식별하는 URL을 기반으로 서비스 서버로부터 서비스에 대한 액세스를 요청할 수 있다. 본 명세서에서 사용되는 바와 같이, 동작이 무언가에 의해 "트리거된" 또는 "기반"인 경우, 이는 동작이 트리거되거나 무언가의 적어도 일부에 적어도 부분적으로 기초한다는 것을 의미한다. 서비스는 분산 컴퓨팅 시스템과 같은 하나 이상의 컴퓨터 시스템에 의해 저장 및/또는 관리될 수 있다. 분산 컴퓨팅 시스템은 클라이언트 애플리케이션(210)을 통한 사용자 인증 시 하나 이상의 서비스에 대한 액세스를 용이하게 하거나 제어할 수 있다.

[0044]

서비스 중 하나가 클라이언트 컴퓨팅 장치에서 클라이언트 애플리케이션(210)에 의해 액세스될 수 있도록 하기 위해, 클라이언트 애플리케이션(210)을 통해 사용자에게 서비스에 대한 액세스를 제공하는 세션(예를 들어, SSO 세션)을 설정하기 위해 사용자에게 인증이 요청된다. 클라이언트 컴퓨팅 장치는 인가자로부터 액세스를 요청하여 인증 프로세스를 시작한다. 인증 프로세스는 클라이언트 컴퓨팅 장치가 사용자의 자격 증명 정보를 수신하기 위해 하나 이상의 GUI를 디스플레이하고, 인가자에게 인증 요청을 제출하는 것을 포함할 수 있다. 액세스를 요청한 서비스에 대해 정의된 인증을 위해 사용자의 자격 증명 정보를 확인함에 기초하여 인증을 설정한다. 서비스에 접근을 시도할 때 사용자는 인가자를 통해 사용자 계정에 대한 접근을 관리하는 애플리케이션(예: 클라이언트 애플리케이션(210)의 일부 또는 별도의 애플리케이션)을 작동시킨다. 예를 들어, 애플리케이션은 GUI를 제공할 수 있는 액세스 관리 애플리케이션일 수 있다. 애플리케이션 및/또는 클라이언트 애플리케이션(210)을 사용하여 사용자는 하나 이상의 서비스에 대한 액세스를 요청하고, 인증에 참여하고, 인증 레벨의 수정을 요청한다.

[0045]

사용자의 클라이언트 컴퓨팅 장치와 인가자 사이의 통신은 게이트웨이(220)를 통해 수신된다. 게이트웨이(220)는 액세스 관리 서비스를 지원한다. 예를 들어, SSO 게이트웨이는 클라이언트 애플리케이션(210) 및 인가자로부터의 요청의 균형 및/또는 처리를 위해 하나 이상의 액세스 에이전트를 구현할 수 있다. 클라이언트 컴퓨팅 장치는 하나 이상의 서비스에 대한 클라이언트 컴퓨팅 장치의 액세스를 용이하게 하기 위해 에이전트에서 하나 이상의 통신을 송/수신할 수 있다. 인가자는 하나 이상의 서비스에 대한 클라이언트 컴퓨팅 장치의 액세스를 용이하게 하기 위해 에이전트에서 하나 이상의 통신을 송/수신할 수 있다. 자격 증명 정보의 성공적인 인증에 기초하여 클라이언트 애플리케이션(210)에 서비스가 액세스될 수 있다. 자격 증명 정보를 수신하면 인가자는 요청된 서비스가 액세스를 위해 자격 증명이 필요한 보호된 서비스인지 확인한다. 인가자는 서비스에 대한 액세스가 보호되는지 여부를 결정한다. 서비스가 보호되지 않는다고 판단되면, 인가자는 서비스(예: 공공 서비스)에 대한 액세스 권한을 부여한다. 서비스에 대한 액세스가 보호된다고 결정하면, 인가자는 자격 증명 정보에 기초하여 클라이언트 애플리케이션(210)을 통한 사용자의 인증을 결정한다. 구체적으로, 인가자는 하나 이상의 레벨 및/또는 하나 이상의 인증 요인에 대한 자격 정보를 수집하고, 인가자는 자격 증명 정보가 클라이언트 애플리케이션(210)을 통해 사용자가 서비스에 액세스할 수 있도록 등록된 자격 증명 정보와 일치하는지 확인할 수 있다. 인가자는 사용자의 인증을 판단할 때, 사용자에게 허용된 액세스를 기반으로 사용자가 서비스에 액세스할 수 있는 권한이 있는지 판단할 수 있다. 인가자는 사용자가 서비스에 액세스하도록 허용되는지 여부에 대한 사용자의 권한 부여를 나타내기 위해 클라이언트 컴퓨팅 장치에 통신을 보낼 수 있다. 그 후, 서비스는, 사용자가 서비스에 액세스할 수 있도록 인증되고 선택적으로 권한을 부여받았다고 결정하면, 클라이언트 애플리케이션(210)을 통해 사용자가 액세스할 수 있는 서비스로 활성화된다.

- [0046] 서비스가 클라이언트 애플리케이션(210)에 액세스 가능한 서비스로 활성화되면, 게이트웨이(220)는 요청을 네트워크 메시(225)로 전달한다. 네트워크 메시(225)는 서비스 레벨(예: 다양한 서비스가 서로 데이터를 공유하는 방식)에서 통신 및 네트워킹 문제를 관리하는 분산 컴퓨팅 환경에 구축된 전용 계층이다. 이상적으로는 서비스 간의 통신이 적을수록 좋다. 그러나 서비스가 종종 작업을 완료하기 위해 서로 의존하므로 회피가 항상 가능한 것은 아니다. 그러한 경우에, 네트워크 메시(225)는 (i) 인가자를 사용하여 사용자와 다양한 서비스 사이의 후속 요청 또는 상호 작용을 인증하고, (ii) 선택적으로 서비스 사이의 통신을 암호화하고, (iii) 보안 규칙 또는 정책(예: 동일한 포트 내의 서비스 간 통신 및 서로 다른 포트 내의 서비스 간 통신을 위한 포트-레벨 보안 규칙)을 시행함으로써, 서비스 사이의 통신을 관리하고 보호한다. 이러한 동작을 용이하게 하기 위해, 네트워크 메시(225)는 서비스에 대한 호출 및 서비스 간의 호출을 가로채도록 적응된 라우터 및 하나 이상의 프록시를 포함하고, 서비스에 대한 및 서비스 간의 호출을 제어 및 라우팅하기 위한 보안 규칙 또는 정책으로 구성된다. 서비스 간의 통신을 관리하고 보호하는 것 외에도, 네트워크 메시(225)는 서비스 발견 및 로드 밸런싱에 대한 지원도 제공할 수 있다. 예를 들어, 네트워크 메시(225)는 포트 엔드포인트로부터 대응하는 서비스 인스턴스 풀을 불러올 수 있다. 그런 다음 네트워크 메시(225)는 특정 서비스 인스턴스로 요청을 보내거나 라우팅하여, 대기 시간 및 결과의 응답 유형을 기록한다. 네트워크 메시(225)는 최근 요청에 대해 관찰된 대기 시간을 포함한, 다양한 요인에 기초하여 빠른 응답을 반환할 가능성이 가장 높은 인스턴스를 선택할 수 있다.
- [0047] 퍼블릭 에이전트(230)는 하나 이상의 퍼블릭 서비스를 제공하도록 적응된다. 이러한 서비스는 공용으로 지정되지만 이것이 반드시 공용 서비스에 액세스하는 데 인증/권한이 필요하지 않음을 의미하지는 않는다. 경우에 따라 퍼블릭 서비스에 액세스하려면 하나 이상의 레벨 또는 요소의 인증 및/또는 인가가 필요할 수 있다. 네트워크 메시(225)는 클라이언트 애플리케이션(210)과 퍼블릭 에이전트(230) 사이의 통신을 관리하고 보호한다. 어떤 경우에는, 인가자를 사용하여 사용자와 다양한 공용 서비스 사이의 요청 또는 상호 작용을 인증하고, 보안 규칙 또는 정책을 집행하면서 퍼블릭 에이전트(230)에 의해 제공되는 서비스에 대한 그리고 서비스 간의 호출을 라우팅하는 것을 포함한다.
- [0048] 프라이빗 에이전트(235)는 서비스 포트(240) 내에 포함된 하나 이상의 프라이빗 서비스(예를 들어, 제1 포트 내의 제1 서비스 및 제2 포트 내의 제2 서비스)를 제공하도록 적응된다. 네트워크 메시(225)는 클라이언트 애플리케이션(210)과 프라이빗 에이전트(235) 사이의 통신을 관리하고 보호한다. 어떤 경우에는, 이것은 보안 규칙 또는 정책을 시행하면서 프라이빗 에이전트(235)에 의해 제공되는 서비스에 대한 그리고 서비스 간의 호출을 라우팅하는 것을 포함한다. 프라이빗 에이전트(235)는 다른 서비스와 통신하고 액세스하기 위해 각 서비스에 의해 사용되는 보안 키 또는 액세스 키를 관리 및 저장하기 위해 금고(245) 및 금고 게이트웨이(250)를 활용한다. 금고 게이트웨이(250)는 서비스와 금고(245) 사이에 안전한 통로를 형성하는 네트워크 노드이다. 금고 게이트웨이(250)는 다음 기술 중 하나 이상을 사용하여 금고 네트워크 보안을 제공할 수 있다: 유입 및 유출 네트워크 트래픽의 모니터링을 위한 방화벽; 사설 보안 통신 채널 제공을 위한 가상 사설망; 네트워크 내의 보안 결함을 식별하기 위한 보안 스캐닝; 인증 및 인가 서비스를 위한 액세스 관리자, 등. 금고 게이트웨이(250)는 금고 및 다양한 비밀, 즉, 보안 또는 액세스 키에 대한 액세스를 관리하는 서비스 커넥터 및 라우터를 사용하여 금고 트래픽을 라우팅한다.
- [0049] 금고(245)는 보안 키 또는 액세스 키를 관리하고 저장한다. 보안 키는 서비스가 다른 서비스와 통신하고 액세스 권한을 얻기 위한 단기 자격 증명이다. 보안 키는 다른 서비스(예: 다른 서비스의 애플리케이션 프로그래밍 인터페이스)에 대한 프로그래밍 요청에 서명하는 데 사용될 수 있다. 보안 키는 액세스 식별자와 비밀 액세스 키로 구성된다. 사용자 이름 및 패스워드와 마찬가지로, 서비스는 액세스 요청을 인증하기 위해 액세스 식별자와 보안 액세스 키를 함께 사용해야 한다. 보안 키는 서비스에 대한 액세스를 제어하기 위해 데이터 저장소에 저장된 하나 이상의 규칙 또는 정책("정책")을 사용하여 관리될 수 있다. 정책은 각 서비스에서 액세스할 수 있는 다른 서비스를 정의한다. 예를 들어, 관리자는 서비스 및/또는 데이터 프라이버시 간의 격리를 유지하기 위해 특정 서비스가 특정 서비스에 액세스하도록 허용할 수 있다. 금고(245)는 하나 이상의 정책에 기초하여 어떤 서비스가 다른 서비스에 액세스하기 위해 어떤 보안 키를 받는지 결정한다.
- [0050] IV. 디지털 건강 플랫폼에 서비스를 배포하는 기술
- [0051] 도 3 및 4는 중앙 집중식 네트워크 메시지를 통한 서비스 간 통신 및 인증을 위한 프로세스 및 동작을 도시한다. 개별 실시예는 순서도, 흐름도, 데이터 흐름도, 구조도 또는 블록도로서 묘사되는 프로세스로서 기술될 수 있다. 순서도는 작업을 순차적 프로세스로 설명할 수 있지만 많은 작업이 병렬로 또는 동시에 수행될 수 있다. 또한 작업 순서를 다시 정렬할 수 있다. 작업이 완료되면 프로세스가 종료되지만 도면에 포함되지 않은 추가 단계가 있을 수 있다. 프로세스는 방법, 함수, 절차, 서브루틴, 서브프로그램 등에 해당할 수 있다. 프로세스가

함수에 해당하는 경우, 프로세스 종료는 호출 함수 또는 메인 함수로의 함수 복귀에 해당할 수 있다.

- [0052] 도 3 및 도 4에 도시된 프로세스 및/또는 동작은 하나 이상의 처리 장치(예: 프로세서 코어), 하드웨어 또는 이들의 조합에 의해 실행되는 소프트웨어(예: 코드, 명령어, 프로그램)로 구현될 수 있다. 소프트웨어는 메모리(예를 들어, 메모리 장치, 비일시적 컴퓨터 판독 가능 저장 매체)에 저장될 수 있다. 도 3 및 도 4의 특정한 일련의 처리 단계들은 제한하려는 의도가 아니다. 대안적인 실시예에 따라 다른 일련의 단계들이 또한 수행될 수 있다. 예를 들어, 대안적인 실시예에서, 위에서 설명한 단계들이 다른 순서로 수행될 수 있다. 또한, 도 3 및 도 4에 도시된 개별 단계는 개별 단계에 적합하다면 다양한 순서로 수행될 수 있는 다수의 하위 단계를 포함할 수 있다. 또한 특정 애플리케이션에 따라 추가 단계가 추가되거나 제거될 수 있다. 당업자는 많은 변형, 수정 및 대안을 인식할 것이다.
- [0053] 도 3은 디지털 건강 플랫폼에서 서비스 간 통신 및 인증을 위한 프로세스(300)를 예시한다. 순서도(300)에 도시된 프로세스는 도 1 및 도 2에 도시된 아키텍처, 시스템 및 기술에 의해 구현된다.
- [0054] 단계 305에서, 네트워크 메시는 서비스 요청(예를 들어, 사용자로부터 서비스 A와 같은 서비스에 대한 액세스 요청)을 수신한다. 네트워크 메시는 네트워크 메시가 해당 서비스에 익숙한지 판단하여 요청을 해결(resolving)한다. 이 결정은 네트워크 메시가 캐시의 서비스에 대한 데이터를 가지고 있는지 여부를 결정함으로써 이루어질 수 있다. 캐시는 해당 데이터에 대한 향후 요청을 더 빨리 처리할 수 있도록 데이터(예: 다양한 서비스에 대한 정보)를 저장하는 하드웨어 또는 소프트웨어 구성 요소이다. 캐시에 저장된 데이터는 서비스에 대한 이전 요청의 결과이거나 다른 곳에 저장된 데이터 사본일 수 있다. 네트워크 메시가 캐시에 서비스에 대한 데이터를 가지고 있는 경우 네트워크 메시는 캐시로부터 데이터를 획득한다. 데이터는 서비스(예: 서비스 A)를 포함하는 하나 이상의 포트(예: 포트 A)의 신원 및 분산 컴퓨팅 환경 내의 하나 이상의 포트의 위치를 포함한다. 위치는 특정 분산 컴퓨팅 환경, 노드, 노드의 클러스터, 노드 또는 클러스터의 인스턴스 또는 하나 이상의 포트를 실행하는 이들의 조합을 포함할 수 있다. 데이터는 서비스를 캡슐화(예: 서비스 관리)하는 포트와, 서비스를 캡슐화하는 포트에 연결하는 방법(예: 분산 컴퓨팅 환경 내 포트의 IP 주소)을 네트워크 메시에 알려준다.
- [0055] 단계 310에서, 네트워크 메시가 캐시에 서비스에 대한 데이터를 가지고 있지 않을 때, 네트워크 메시는 서비스에 대한 데이터를 얻기 위해 데이터 레지스트리에 접속한다. 데이터 레지스트리는 디지털 건강 플랫폼(예: 다중 분산 컴퓨팅 환경)에서 실행되는 모든 서비스에 관한 데이터를 저장하는 단일 진실 지점(single point of truth)이다. 캐시와 마찬가지로, 데이터는 서비스를 캡슐화(예: 서비스 관리)하는 포트와, 서비스를 캡슐화하는 포트에 연결하는 방법(예: 분산 컴퓨팅 환경 내 포트의 IP 주소)을 네트워크 메시에 알려준다. 레지스트리로부터 네트워크 메시에 의해 불러진 데이터는 다운로드 처리 및 향후 요청을 위해 캐시 내에 저장될 수 있다.
- [0056] 단계 315에서, 네트워크 메시는 캐시 또는 레지스트리로부터 획득된 데이터에 기초하여 서비스를 캡슐화하는 하나 이상의 포트(예를 들어, 포트 A)와 통신한다. 통신에는 하나 이상의 포트에 대한 보안 규칙에 대한 네트워크 메시로부터의 요청이 포함된다. 보안 규칙은 (i) 서비스에 대한 고유 주소 식별자 및 (ii) 서비스가 통신하고 액세스할 수 있는 서비스를 정의한다. 예를 들어 포트 A에 대한 보안 규칙은 서비스 A와, 서비스 A가 통신하고 액세스할 수 있는 서비스에 대한 고유 주소 식별자를 정의한다. 각 포트가 생성되면 각 포트에는 각 포트에 의해 캡슐화된 서비스와 통신하고 이에 의해 액세스할 수 있는 다른 포트 또는 서비스를 관리하는 규칙 또는 정책이 할당된다. 규칙 또는 정책은 디지털 건강 플랫폼의 관리자와 같은 관리자가 작성될 수 있다. 또한 생성 시 각 서비스에는 고유 주소 식별자 주소가 할당된다. 이 주소는 서비스 수명과 연결되어 있으며 서비스가 활성화되어 있는 동안에는 변경되지 않는다. 네트워크 메시와 포트는 고유 주소 식별자를 통해 서비스와 통신하며, 서비스에 대한 통신은 규칙 또는 정책에 의해 관리되고, 서비스를 캡슐화하는 포트의 인스턴스로 자동으로 로드 밸런싱된다.
- [0057] 단계(320)에서, 하나 이상의 포트에 대한 보안 규칙이 하나 이상의 포트(예를 들어, 포트 A)로부터 불러들여진다. 하나 이상의 포트(Pod)는 네트워크 메시로부터 보안 규칙에 대한 요청을 수신하고, 데이터 저장 장치로부터 보안 규칙을 획득하고, 보안 규칙을 네트워크 메시로 전달한다.
- [0058] 단계 325에서, 보안 규칙에 기초하여 서비스 요청이 서비스(예를 들어, 서비스 A)로 전달된다. 예를 들어, 네트워크 메시는 서비스에 대한 고유 주소 식별자를 사용하여 리소스와 통신하고, 리소스에 리소스 요청을 전달한다. 어떤 경우에는 네트워크 메시가 이러한 고유 주소 식별자 및 서비스와 관련된 프록시를 이용하여, 서비스와 통신하고 서비스 요청을 해당 서비스에 전달한다. 그런 다음 프록시는 서비스 요청과 관련하여 서비스와 의 모든 후속 통신에 사용될 수 있다.

- [0059] 단계 330에서, 서비스는 서비스 요청을 수신하고 처리한다. 처리에는 서비스 요청을 충족시키기 위해 서비스가 하나 이상의 프로그램 작업을 실행하는 것이 포함된다. 예를 들어, 서비스 요청에 대해, 서비스는 의료 데이터의 수집, 의료 데이터의 변환, 의료 데이터의 통신 등과 같이 서비스를 제공하기 위한 하나 이상의 동작을 실행할 수 있다. 경우에 따라, 서비스 요청을 충족하는 과정의 일부로, 서비스는 다른 포트(예: 포트 B)의 다른 서비스와 통신하고 액세스해야 할 수 있다(예: 서비스 B와 같은 별도의 데이터 저장 장치로부터 데이터 불러오기). 그러한 경우에, 단계 335에서, 서비스는 금고와 연결되어, 다른 포트의 다른 서비스와 통신 및 액세스하기 위한 비밀 키를 얻을 수 있다.
- [0060] 단계 335에서, 금고는 서비스와 연결하고, 데이터 저장소에 저장된 하나 이상의 규칙 또는 정책을 사용하여 다른 서비스에 대한 액세스를 제어한다. 예를 들어, 서비스와 연결되면, 금고는 서비스가 하나 이상의 정책을 기반으로 다른 서비스와 통신 및 액세스할 수 있는 권한이 있는지 여부를 결정한다. 서비스가 하나 이상의 정책을 기반으로 다른 서비스와 통신 및 액세스하도록 승인되면, 금고는 다른 서비스에 대한 보안 키를 불러와서, 단계 340에서 보안 키를 서비스에 전달한다. 서비스가 하나 이상의 정책에 따라 다른 서비스와 통신 및 액세스 권한이 없는 경우, 금고는 다른 서비스와 통신 및 액세스 권한이 없음을 서비스에 알린다.
- [0061] 단계 345에서, 서비스가 다른 서비스와 통신 및 액세스하도록 인가되면, 서비스는 다른 서비스에 대한 보안 키를 수신하고 다른 서비스에 대한 액세스 요청에 보안 키를 내장한다. 예를 들어, 서비스는 서비스 요청 충족을 돕기 위해 하나 이상의 프로그램 동작을 수행하도록 다른 서비스에 요청하는 액세스 요청을 생성할 수 있다. 액세스 요청은 보안 키를 사용하여 서명될 수 있다.
- [0062] 단계 350에서, 서비스는 액세스 요청을 네트워크 메시와 통신한다. 경우에 따라 서비스는 서비스와 연결된 프록시를 통해 네트워크 메시와 액세스 요청을 통신한다. 서비스는 (i) 서비스에 서비스에 대한 고유한 주소 식별자가 없고 (ii) 네트워크 메시가 모든 서비스간 통신에 대한 제어 및 보안을 유지하도록 허용하기 때문에, 액세스 요청을 네트워크 메시에 전달한다.
- [0063] 단계 355에서, 네트워크 메시는 서비스로부터 액세스 요청을 수신하고 처리한다. 액세스 요청을 처리하는 것은 단계 305-325(도 3에 도시되지 않음)에 대해 설명된 서비스 요청의 처리와 유사하다.
- [0064] 단계 360에서, 네트워크 메시는 서비스와 연관된 포트(예를 들어, 포트 A)에 대한 보안 규칙, 및 다른 서비스와 관련된 포트(가령, 포트 B)의 보안 규칙에 기초하여 서비스로부터 다른 서비스로 액세스 요청을 전달한다. 경우에 따라 네트워크 메시는 서비스와 연결된 프록시를 통해 액세스 요청을 서비스로부터 다른 서비스로 전달한다. 이러한 전달은 포트(예: 포트 A)에 대한 보안 규칙이 다른 서비스(가령, 서비스 B)를, 서비스(가령, 서비스 A)가 통신 및 액세스하도록 인가받은 서비스로 정의하는지 여부를 네트워크 메시가 결정하는 것과, 다른 포트(가령, 포트 B)에 대한 보안 규칙이 서비스(가령, 서비스 A)를, 다른 서비스(가령, 서비스 B)가 서비스로부터 통신을 수신 및 액세스하도록 인가받은 서비스로 정의하는지 여부를 네트워크 메시가 결정하는 것을 포함한다. 다른 서비스(가령, 서비스 B)가, 서비스(가령, 서비스 A)가 통신 및 액세스하도록 인가받은 서비스이고, 서비스(가령, 서비스 A)가, 다른 서비스(가령, 서비스 B)가 서비스로부터 통신을 수신 및 액세스하도록 인가받은 서비스일 때, 상기 액세스 요청을 서비스로부터 다른 서비스로 전달한다.
- [0065] 단계 365에서, 다른 서비스는 네트워크 메시로부터 액세스 요청을 수신하고 보안 키를 검증한다. 보안 키가 유효하지 않은 경우, 다른 서비스는 유효하지 않은 보안 키를 서비스에 직접 알린다. 보안 키가 유효하면 다른 서비스는 액세스 요청을 처리한다. 처리는 다른 서비스가 서비스 요청을 만족시키는 것을 돕기 위해 하나 이상의 프로그램 동작을 실행하는 것을 포함한다. 예를 들어, 서비스 요청에 대해, 서비스는 의료 데이터의 수집, 의료 데이터의 변환, 의료 데이터의 통신 등과 같이 서비스를 제공하기 위한 하나 이상의 동작을 실행할 수 있다.
- [0066] 단계 370에서, 다른 서비스는 액세스 요청을 처리한 결과를 직접 서비스로 다시 전달한다. 경우에 따라 다른 서비스는 서비스와 연결된 프록시를 통해 액세스 요청 결과를 서비스와 통신한다.
- [0067] 단계 375에서, 서비스는 액세스 요청의 결과를 수신하고, 액세스 요청의 결과를 서비스 요청을 처리하는 서비스의 결과와 통합하여 서비스 요청에 대한 최종 결과를 생성한다. 그런 다음 서비스는 서비스 요청의 최종 결과를 네트워킹 메시에 출력할 수 있으며, 이는 차례로 예를 들어 네트워크 게이트웨이를 통해 사용자에게 서비스 요청의 최종 결과를 전달한다.
- [0068] 도 4는 중앙 집중식 네트워크 메시지를 통한 서비스 간 통신 및 인증을 위한 프로세스(400)를 도시한다. 단계 405에서, 네트워크 메시는 예를 들어 사용자로부터 제1 서비스에 대한 서비스 요청을 수신한다. 경우에 따라 상기 서비스 요청은 서비스에 대한 요청이고 상기 제1 서비스는 제1 서비스이다. 제1 서비스는 제1 분산 컴퓨팅 환경

에서 제1 컨테이너 또는 제1 컨테이너 세트로서 패키징된 하나 이상의 클러스터에 배포된 하나 이상의 프로그램을 포함할 수 있고, 제1 컨테이너 또는 제1 컨테이너 세트는 제1 포드로서 패키징될 수 있고, 이는 하나 이상의 클러스터에서 실행되는 하나 이상의 프로그램을 나타내는 상위 레벨 구조이다.

[0069] 단계(410)에서, 네트워크 메시지는 캐시 또는 서비스 레지스트리로부터 제1 서비스와 연관된 정보를 획득한다. 정보는 제1 서비스를 포함하는 제1 포드의 신원과, 제1 분산 컴퓨팅 환경 내의 제1 포드의 위치를 포함한다. 정보를 획득하는 단계는 (i) 제1 서비스와 연관된 정보가 캐시로부터 이용 가능한지 여부를 결정하는 단계; (ii) 제1 서비스와 연관된 정보가 캐시로부터 이용 가능할 때, 캐시로부터 제1 서비스와 연관된 정보를 획득하는 단계; (iii) 캐시에서 제1 서비스와 연관된 정보를 사용할 수 없는 경우 레지스트리로부터 제1 서비스와 연관된 정보를 획득하는 단계; 및 (iv) 레지스트리로부터 제1 서비스와 연관된 정보를 획득한 것에 응답하여, 후속 요청을 위해 캐시에 제1 서비스와 연관된 정보를 저장하는 단계를 포함한다.

[0070] 단계 415에서, 네트워크 메시지는 제1 포드의 위치를 사용하여 제1 포드에 대한 보안 규칙을 불러온다. 보안 규칙은: (i) 제1 서비스에 대한 고유 주소 식별자 및 (ii) 제1 서비스가 통신 및 액세스할 수 있는 권한이 부여된 서비스를 정의한다. 경우에 따라 보안 규칙은 (iii) 제1 서비스에 사용할 수 있는 여러 인스턴스 및 (iv) 서비스 요청 처리에 사용할 수 있는 인스턴스를 추가로 정의한다.

[0071] 단계 420에서, 네트워크 메시지는 제1 포드에 대한 보안 규칙에 기초하여 제1 서비스에 서비스 요청을 전달한다. 전달은 (i) 제1 포드에 대한 보안 규칙에 기초하여 서비스 요청을 처리하기 위해 이용 가능한 인스턴스를 결정하는 것, 및 (ii) 제1 서비스에 대한 고유 주소 식별자를 사용하여 제1 서비스의 인스턴스들 중 적어도 하나에 서비스 요청을 전달하는 것을 포함한다.

[0072] 단계 425에서, 네트워크 메시지는 제2 서비스와 통신 및 액세스하기 위해 제1 서비스로부터 액세스 요청을 수신한다. 제2 서비스는 제1 분산 컴퓨팅 환경 또는 제2 분산 컴퓨팅 환경에서 제2 컨테이너 또는 제2 컨테이너 세트 로 패키징된 하나 이상의 클러스터에 배치된 하나 이상의 프로그램을 포함할 수 있고, 제2 컨테이너 또는 제2 컨테이너 세트는 하나 이상의 클러스터에서 실행되는 하나 이상의 프로그램을 나타내는 상위 레벨 구조인 제2 포드로 패키징된다. 액세스 요청에는 제2 서비스에 특정한 보안 키가 포함된다. 보안 키는 금고로부터 제1 서비스에 의해 획득되며, 제1 서비스는 액세스 요청에 보안 키를 내장한다. 액세스 요청은 또한 하나 이상의 동작을 수행하고/하거나 제1 서비스를 대신하여 서비스를 획득하기 위한 제2 서비스의 요청을 포함할 수 있다. 경우에 따라 상기 액세스 요청은 서비스에 대한 요청이고 상기 제2 서비스는 제2 서비스이다.

[0073] 단계 430에서, 네트워크 메시지는 캐시 또는 서비스 레지스트리로부터 제2 서비스와 연관된 정보를 획득한다. 정보는 제2 서비스를 포함하는 제2 포드의 신원과, 제1 분산 컴퓨팅 환경 또는 제2 분산 컴퓨팅 환경 내의 제2 포드의 위치를 포함한다. 일부 경우에, 제2 포드는 제1 분산 컴퓨팅 환경과 다른 제2 분산 컴퓨팅 환경 내에 위치한다. 정보를 획득하는 단계는 (i) 제2 서비스와 연관된 정보가 캐시로부터 이용 가능한지 여부를 결정하는 단계; (ii) 제2 서비스와 연관된 정보가 캐시로부터 이용 가능할 때, 캐시로부터 제2 서비스와 연관된 정보를 획득하는 단계; (iii) 캐시에서 제2 서비스와 연관된 정보를 사용할 수 없는 경우 레지스트리로부터 제2 서비스와 연관된 정보를 획득하는 단계; 및 (iv) 레지스트리로부터 제2 서비스와 연관된 정보를 획득한 것에 응답하여, 후속 요청을 위해 캐시에 제2 서비스와 연관된 정보를 저장하는 단계를 포함한다.

[0074] 단계 435에서, 네트워크 메시지는 제2 포드의 위치를 사용하여 제2 포드에 대한 보안 규칙을 불러온다. 보안 규칙은: (i) 제2 서비스에 대한 고유 주소 식별자 및 (ii) 제2 서비스가 통신 및 액세스할 수 있는 권한이 부여된 서비스를 정의한다. 경우에 따라 보안 규칙은: (iii) 제2 서비스에 사용할 수 있는 다수의 인스턴스; 및 (iv) 액세스 요청을 처리하는 데 사용할 수 있는 인스턴스를 더 정의한다.

[0075] 단계(440)에서, 네트워크 메시지는 제1 포드에 대한 보안 규칙 및 제2 포드에 대한 보안 규칙에 기초하여 액세스 요청을 제2 서비스로 전달한다. 이러한 전달은 (i) 제2 포드에 대한 보안 규칙이 제2 서비스를, 제1 서비스가 통신 및 액세스하도록 인가된 서비스로 정의하는지 여부를 결정하는 단계; (ii) 제2 포드에 대한 보안 규칙이 제1 서비스를, 제2 서비스가 제1 서비스로부터 통신을 수신하고 액세스를 허용하는 서비스로서 정의하는지 여부를 결정하는 단계; (iii) 제2 서비스가 제1 서비스가 통신 및 액세스 권한이 있는 서비스이고 제1 서비스가 제2 서비스가 제1 서비스로부터 통신 수신 및 액세스를 허용하는 서비스인 경우, 제2 서비스에 대한 고유 주소 식별자를 사용하여 제1 서비스로부터 제2 서비스로 액세스 요청을 전달하는 단계를 포함한다. 일부 경우에, 전달하는 단계는 (iv) 제2 포드에 대한 보안 규칙에 기초하여 액세스 요청을 처리하기 위해 이용 가능한 인스턴스를 결정하고, 제2 서비스에 대한 고유 주소 식별자를 이용하여 제2 서비스의 인스턴스 중 적어도 하나에 액세스 요청을 전달하는 단계를 더 포함한다. 제2 서비스는 제1 서비스를 대신하여 하나 이상의 동작을 수행 및/또는 서

비스를 획득할 수 있고, 하나 이상의 동작의 수행 및/또는 서비스의 획득에 기초하여 하위 결과를 생성할 수 있다. 제2 서비스는 제1 서비스를 대신하여 하나 이상의 작업을 수행 및/또는 서비스를 획득하기 전에 보안 키를 검증할 수 있다.

[0076] 단계 445에서, 네트워크 메시는 제1 서비스로부터 서비스 요청의 최종 결과를 수신한다. 최종 결과에는 제2 서비스에서 얻은 하위 결과가 포함된다.

[0077] 단계 450에서, 네트워크 메시는 서비스 요청의 최종 결과를 출력하고, 어떤 경우에는 예를 들어 사용자에게 최종 결과를 전달한다.

[0078] V. 추가 고려 사항

[0079] 본 개시의 일부 실시예는 하나 이상의 데이터 프로세서를 포함하는 시스템을 포함한다. 일부 실시예에서, 시스템은 하나 이상의 데이터 프로세서에서 실행될 때 하나 이상의 데이터 프로세서로 하여금 본 명세서에 개시된 하나 이상의 방법의 일부의 일부 또는 전부 및/또는 하나 이상의 프로세스의 일부 또는 전부를 수행하게 하는 명령어를 포함하는 비일시적 컴퓨터 판독 가능 저장 매체를 포함한다. 본 개시의 일부 실시예는 하나 이상의 데이터 프로세서로 하여금 본 명세서에 개시된 하나 이상의 방법의 일부의 일부 또는 전부 및/또는 하나 이상의 프로세스의 일부 또는 전부를 수행하게 하도록 구성된 명령어를 포함하는, 비일시적 컴퓨터 판독 가능 저장 매체에 유형적으로 구현된 컴퓨터 프로그램 제품을 포함한다.

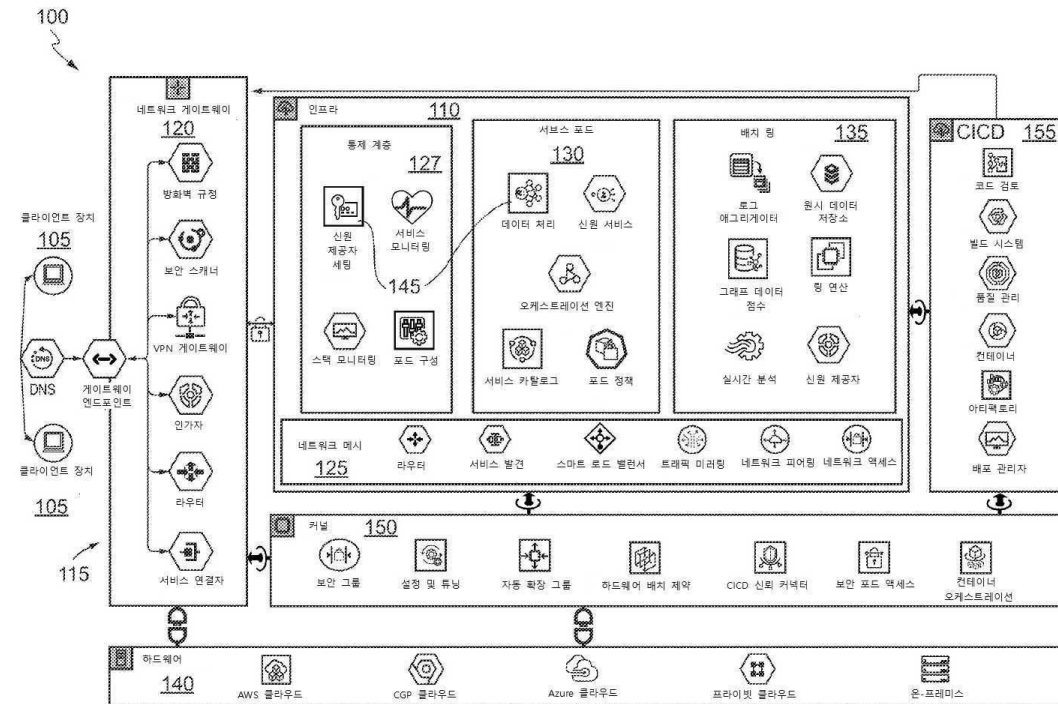
[0080] 사용된 용어 및 표현은 제한이 아닌 설명의 용어로 사용되었으며, 그러한 용어 및 표현의 사용에서 도시되고 설명된 특징 또는 그 일부의 등가물을 배제하려는 의도가 없다. 청구된 발명의 범위 내에서 다양한 수정이 가능하다는 것이 인정된다. 따라서, 청구된 본 발명이 실시예 및 선택적인 특징에 의해 구체적으로 개시되었지만, 본 명세서에 개시된 개념의 수정 및 변형이 당업자에 의해 이루어질 수 있고, 그러한 수정 및 변형이 첨부된 청구 범위에 의해 정의된 바와 같이 본 발명의 범위 내에 있다고 고려됨을 이해해야 한다.

[0081] 이어지는 설명은 단지 바람직한 예시적인 실시예를 제공할 뿐이며 본 발명의 범위, 적용 가능성 또는 구성을 제한하려는 의도가 아니다. 오히려, 바람직한 예시적인 실시예의 이어지는 설명은 당업자에게 다양한 실시예를 구현하기 위한 가능한 설명을 제공할 것이다. 첨부된 특허청구범위에 기재된 정신 및 범위를 벗어나지 않고 구성 요소의 기능 및 배열에 다양한 변경이 이루어질 수 있음을 이해해야 한다.

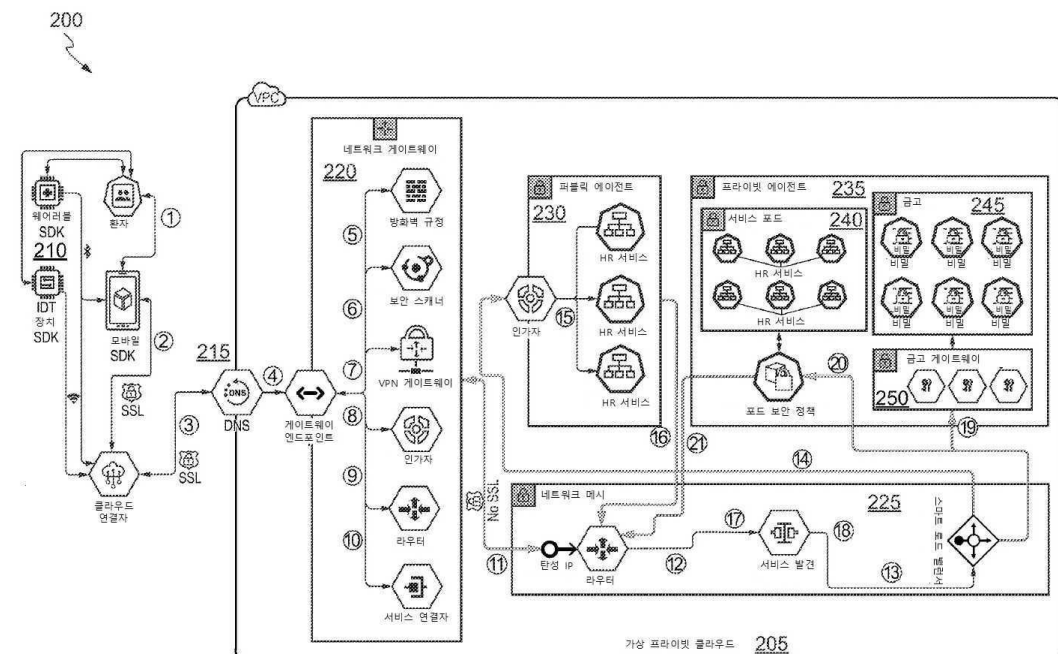
[0082] 구체적인 세부사항은 실시예의 완전한 이해를 제공하기 위해 다음 설명에서 제공된다. 그러나, 실시예는 이러한 특정 세부 사항 없이 실시될 수 있음을 이해할 것이다. 예를 들어, 회로, 시스템, 네트워크, 프로세스 및 기타 구성 요소는 불필요한 세부 사항으로 실시예를 모호하게 하지 않기 위해 블록 다이어그램 형식의 구성 요소로 표시될 수 있다. 다른 경우에, 잘 알려진 회로, 프로세스, 알고리즘, 구조 및 기술은 실시예를 모호하게 하는 것을 피하기 위해 불필요한 세부 사항 없이 표시될 수 있다.

도면

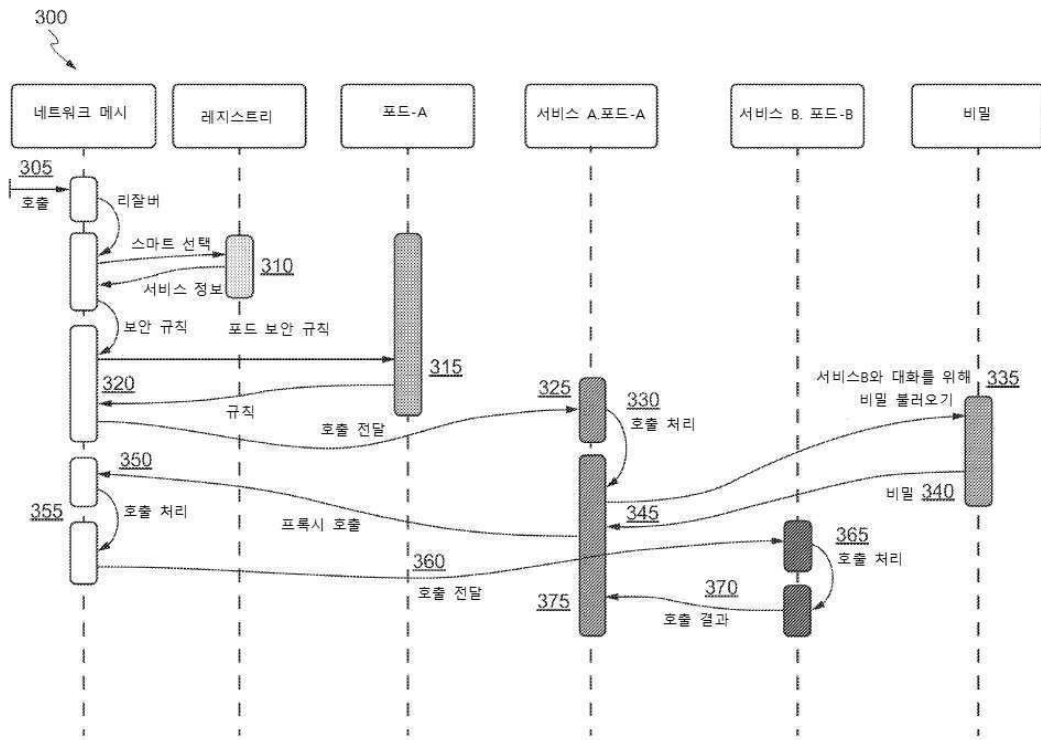
도면1



도면2



도면3



도면4

