(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년05월08일
(11) 등록번호 10-2107560
(24) 등록일자 2020년04월28일

(51) 국제특허분류(Int. Cl.)
G06F 21/57 (2013.01)
(52) CPC특허분류
G06F 21/577 (2013.01)
G06F 2221/034 (2013.01)
(21) 출원번호 10-2017-7012991
(22) 출원일자(국제) 2015년10월12일
심사청구일자 2018년10월29일
(85) 번역문제출일자 2017년05월12일
(65) 공개번호 10-2017-0069271
(43) 공개일자 2017년06월20일
(86) 국제출원번호 PCT/US2015/055120
(87) 국제공개번호 WO 2016/093945
국제공개일자 2016년06월16일
(30) 우선권주장
201410539483.2 2014년10월13일 중국(CN)
(56) 선행기술조사문헌
US20090199264 A1
US8856894 B1
US20130097659 A1

(73) 특허권자
알리바바 그룹 홀딩 리미티드
케이만군도, 그랜드 케이만, 피오박스 847, 원 캐피탈 플레이스 4층
(72) 발명자
루, 쿤
중국 311121 항저우시 위항 디스트릭트 웨스트 엔이 로드 넘버 969 빌딩 3 5층 알리바바 그룹 리갈 디파트먼트
(74) 대리인
특허법인 광장리앤고

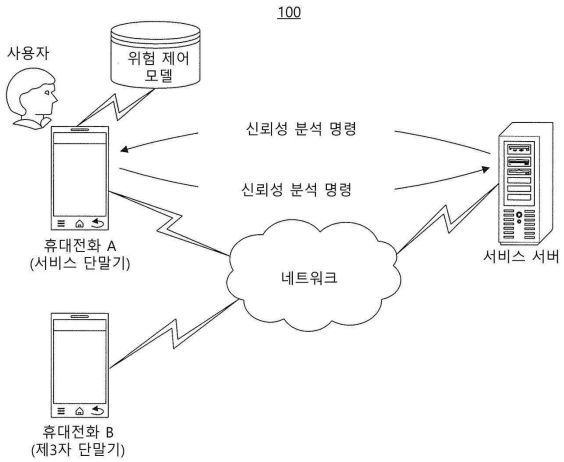
전체 청구항 수 : 총 26 항 심사관 : 구대성

(54) 발명의 명칭 **서비스 동작의 보안을 검증하는 방법, 장치, 단말기 및 서버**

(57) 요 약

서비스 동작의 보안을 검증하는 방법이 제공된다. 방법은, 서비스 단말기에 의한, 서비스 동작의 신뢰성 분석 명령 수신을 포함하고, 여기에서 신뢰성 분석 명령은 서비스 서버에 의해 송신된다. 방법은, 서비스 단말기에 의한, 신뢰성 분석 명령 및 서비스 단말기에 사전 저장된 하나 이상의 위험 제어 모델에 기반하여 서비스 동작의 신뢰성 분석 결과 획득, 및 서비스 동작의 보안을 판단하기 위하여 서비스 서버로 신뢰성 분석 결과 송신을 더 포함할 수 있다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

서비스 단말기의 사용자와 연관된 사용자 데이터에 기반하여 하나 이상의 위험 제어 모델을 생성하는 것;

상기 서비스 단말기에 의해, 서비스 동작(service operation)의 신뢰성 분석 명령을 수신하는 것 -- 상기 신뢰성 분석 명령은 상기 서비스 단말기와 연관된 동작 요청에 응답하여 서비스 서버에 의해 송신됨 --;

상기 서비스 단말기에 의해, 상기 신뢰성 분석 명령 및 상기 서비스 단말기에 사전 저장된 상기 하나 이상의 위험 제어 모델에 기반하여 상기 서비스 동작의 신뢰성 분석 결과를 획득하기 위해 신뢰성 분석을 수행하는 것; 및

상기 서비스 단말기에 의해, 상기 서비스 동작의 보안을 판단하기 위하여 상기 신뢰성 분석 결과를 상기 서비스 서버로 송신하는 것을 포함하는 서비스 동작의 보안 검증 방법.

청구항 2

제1항에 있어서,

상기 서비스 단말기의 사용자의 권한 허가에 기반하여 상기 서비스 단말기로부터 상기 사용자 데이터를 획득하는 것;

상기 사용자 데이터를 분석하여 상기 하나 이상의 위험 제어 모델을 생성하는 것; 및

상기 하나 이상의 위험 제어 모델을 상기 서비스 단말기의 데이터베이스에 저장하는 것을 더 포함하는 서비스 동작의 보안 검증 방법.

청구항 3

제2항에 있어서,

상기 하나 이상의 위험 제어 모델을 상기 서비스 단말기의 로컬 보안 제어 데이터베이스 내에 저장하기 전에 상기 하나 이상의 위험 제어 모델을 암호화하는 것; 및

상기 서비스 단말기의 상기 데이터베이스 내에 상기 암호화된 하나 이상의 위험 제어 모델을 저장하는 것을 더 포함하는 서비스 동작의 보안 검증 방법.

청구항 4

제2항에 있어서, 상기 사용자 데이터는 사용자 사회적 데이터, 관심 데이터 및 습관 데이터 중 적어도 하나를 포함하고, 상기 하나 이상의 위험 제어 모델은 상기 사용자 사회적 데이터에 기반하여 생성된 사회적 관계 제어 모델, 상기 관심 데이터에 기반하여 생성된 관심 제어 모델, 및 상기 습관 데이터에 기반하여 생성된 습관 제어 모델 중 적어도 하나를 포함하는 서비스 동작의 보안 검증 방법.

청구항 5

제1항에 있어서, 상기 서비스 동작의 상기 신뢰성 분석 결과를 획득하는 것은:

상기 신뢰성 분석 명령에 기반하여 상기 서비스 동작의 서비스 정보를 획득하는 것;

상기 서비스 동작의 유형에 기반하여 상기 하나 이상의 위험 제어 모델로부터 목표 위험 제어 모델을 획득하는 것 -- 상기 하나 이상의 위험 제어 모델은 상기 서비스 정보와 서비스 신뢰성 분석 값 사이의 대응하는 관계를 포함함 --; 및

상기 서비스 정보에 대응하는 서비스 신뢰성 분석 값을 획득하기 위하여 상기 서비스 정보를 키워드로 사용하여 상기 목표 위험 제어 모델을 검색하는 것을 포함하는 서비스 동작의 보안 검증 방법.

청구항 6

제5항에 있어서, 상기 신뢰성 분석 명령에 기반하여 상기 서비스 동작의 상기 서비스 정보를 획득하는 것은:

상기 서비스 동작의 상기 신뢰성 분석 명령으로부터 상기 서비스 정보를 획득하는 것을 포함하며, 상기 서비스 정보는 다른 단말기에 의해 송신된 상기 서비스 동작의 동작 요청에 기반하여 상기 서비스 서버에 의해 획득된 정보를 포함하는 서비스 동작의 보안 검증 방법.

청구항 7

제5항에 있어서,

상기 서비스 단말기의 사용자가 상기 서비스 동작을 개시할 때, 상기 신뢰성 분석 명령을 수신하기 전에 상기 서비스 서버로 상기 서비스 동작의 동작 요청을 송신하는 것; 및

상기 신뢰성 분석 명령을 수신할 때, 상기 서비스 동작의 상기 동작 요청에 기반하여 상기 서비스 동작의 상기 서비스 정보를 획득하는 것을 더 포함하는 서비스 동작의 보안 검증 방법.

청구항 8

서비스 단말기와 연관된 동작 요청에 응답하여, 상기 서비스 단말기로 서비스 동작의 신뢰성 분석 명령을 송신하는 것;

상기 서비스 단말기에 의해 송신된 신뢰성 분석 결과를 수신하는 것 -- 상기 신뢰성 분석 결과는 상기 서비스 단말기가 상기 서비스 동작의 신뢰성 분석 및 상기 서비스 단말기에 사전 저장된 하나 이상의 위험 제어 모델을 수행하는 것에 기반하여 상기 서비스 단말기에 의해 획득됨 --; 및

상기 신뢰성 분석 결과에 기반하여 상기 서비스 동작의 보안을 판단하는 것을 포함하는 서비스 동작의 보안 검증 방법.

청구항 9

제8항에 있어서,

상기 서비스 단말기로 상기 서비스 동작의 상기 신뢰성 분석 명령을 송신하기 전에, 다른 단말기에 의해 송신된 상기 서비스 동작의 상기 동작 요청을 수신하는 것; 및

상기 동작 요청에 기반하여 상기 서비스 동작의 서비스 정보를 획득하는 것을 더 포함하며, 상기 서비스 동작의 상기 신뢰성 분석 명령은 상기 서비스 동작의 상기 서비스 정보를 포함하는 서비스 동작의 보안 검증 방법.

청구항 10

제8항에 있어서,

상기 서비스 단말기로 상기 서비스 동작의 상기 신뢰성 분석 명령을 송신하기 전에, 상기 서비스 단말기에 의해 송신된 상기 서비스 동작의 상기 동작 요청을 수신하는 것을 더 포함하며, 상기 동작 요청은 상기 서비스 단말기로 상기 서비스 동작의 상기 신뢰성 분석 명령을 송신하기 위한 트리거 명령으로 사용되는 서비스 동작의 보안 검증 방법.

청구항 11

제8항에 있어서, 상기 신뢰성 분석 결과에 기반하여 상기 서비스 동작의 상기 보안을 판단하는 것은:

로컬 위험 제어 모델에 기반하여 상기 서비스 동작의 제1 신뢰성 분석 값을 획득하는 것;

상기 서비스 단말기에 의해 송신된 상기 신뢰성 분석 결과에 기반하여 제2 신뢰성 분석 값을 획득하는 것;

상기 제1 신뢰성 분석 값 및 제2 신뢰성 분석 값의 가중치를 획득하는 것;

상기 가중치에 기반하여 상기 제1 신뢰성 분석 값 및 상기 제2 신뢰성 분석 값의 결합된 신뢰성 분석 값을 계산하는 것;

상기 결합된 신뢰성 분석 값을 사전 설정된 신뢰성 임계치와 비교하는 것; 및

상기 결합된 신뢰성 분석 값이 상기 신뢰성 임계치보다 크면, 상기 서비스 동작이 안전한 것으로 판단하고, 상기 결합된 신뢰성 분석 값이 상기 신뢰성 임계치보다 크지 않으면, 상기 서비스 동작이 불안전한 것으로 판단하는 것을 포함하는 서비스 동작의 보안 검증 방법.

청구항 12

서비스 단말기의 사용자와 연관된 사용자 데이터에 기반하여 하나 이상의 위험 제어 모델을 생성하도록 구성되는 생성 유닛;

서비스 서버에 의해 송신된 서비스 동작의 신뢰성 분석 명령을 수신하도록 구성되는 수신 유닛;

상기 서비스 단말기가 신뢰성 분석 및 상기 서비스 단말기에 사전 저장된 하나 이상의 위험 제어 모델을 수행하는 것에 기반하여 상기 서비스 동작의 신뢰성 분석 결과를 획득하도록 구성되는 분석 유닛; 및

상기 서비스 동작의 보안을 판단하기 위하여 상기 서비스 서버로 상기 신뢰성 분석 결과를 송신하도록 구성되는 송신 유닛을 포함하는 서비스 동작의 보안 검증 장치.

청구항 13

서비스 단말기와 연관된 동작 요청에 응답하여 서비스 동작의 신뢰성 분석 명령을 상기 서비스 단말기에 송신하도록 구성되는 송신 유닛;

상기 서비스 단말기에 의해 송신된 신뢰성 분석 결과를 수신하도록 구성되는 수신 유닛 -- 상기 신뢰성 분석 결과는 상기 서비스 단말기가 상기 서비스 동작의 신뢰성 분석 및 상기 서비스 단말기에 사전 저장된 하나 이상의 위험 제어 모델을 수행하는 것에 기반하여 상기 서비스 단말기에 의해 획득됨 --; 및

상기 신뢰성 분석 결과에 기반하여 상기 서비스 동작의 보안을 판단하도록 구성되는 검증 유닛을 포함하는 서비스 동작의 보안 검증 장치.

청구항 14

단말기로서, 상기 단말기는:

명령의 세트를 저장하도록 구성되는 메모리; 및

프로세서를 포함하고,

상기 프로세서는 상기 명령의 세트를 실행하여 상기 단말기가:

상기 단말기의 사용자와 연관된 사용자 데이터에 기반하여 하나 이상의 위험 제어 모델을 생성하고;

상기 단말기와 연관된 동작 요청에 응답하여 서비스 서버에 의해 송신되는 서비스 동작의 신뢰성 분석 명령을 수신하고;

상기 단말기가 신뢰성 분석 및 상기 단말기에 사전 저장된 상기 하나 이상의 위험 제어 모델을 수행하는 것에 기반하여 상기 서비스 동작의 신뢰성 분석 결과를 획득하며;

상기 서비스 동작의 보안을 판단하기 위하여 상기 서비스 서버에 상기 신뢰성 분석 결과를 송신하게 하는, 단말기.

청구항 15

서비스 서버로서, 상기 서비스 서버는:

명령의 세트를 저장하도록 구성되는 메모리; 및

프로세서를 포함하고,

상기 프로세서는 상기 명령의 세트를 실행하여 상기 서비스 서버가:

서비스 단말기와 연관된 동작 요청에 응답하여 서비스 동작의 신뢰성 분석 명령을 상기 서비스 단말기에 송신하고;

상기 서비스 단말기에 의해 송신된 신뢰성 분석 결과를 수신하며 -- 상기 신뢰성 분석 결과는 상기 서비스 단말

기가 상기 서비스 동작의 신뢰성 분석 및 상기 서비스 단말기에 사전 저장된 하나 이상의 위험 제어 모델을 수행하는 것에 기반하여 상기 서비스 단말기에 의해 획득됨 --;

상기 신뢰성 분석 결과에 기반하여 상기 서비스 동작의 보안을 판단하게 하는, 서비스 서버.

청구항 16

서비스 단말기의 적어도 하나의 프로세서에 의해 실행 가능하고, 상기 서비스 단말기가 서비스 동작의 보안 검증 방법을 수행하게 하는 명령의 세트를 저장하는 비일시적 컴퓨터 판독가능 매체로서, 상기 방법은:

서비스 단말기의 사용자와 연관된 사용자 데이터에 기반하여, 하나 이상의 위험 제어 모델을 생성하는 것;

상기 서비스 동작의 신뢰성 분석 명령을 수신하는 것 -- 상기 신뢰성 분석 명령은 상기 서비스 단말기와 연관된 동작 요청에 응답하여 서비스 서버에 의해 송신됨 --;

상기 서비스 단말기가 신뢰성 분석 및 상기 서비스 단말기에 사전 저장된 상기 하나 이상의 위험 제어 모델을 수행하는 것에 기반하여 상기 서비스 동작의 신뢰성 분석 결과를 획득하는 것; 및

상기 서비스 동작의 보안을 판단하기 위하여 상기 서비스 서버로 상기 신뢰성 분석 결과를 송신하는 것을 포함하는 비일시적 컴퓨터 판독가능 매체.

청구항 17

제16항에 있어서, 상기 적어도 하나의 프로세서는 상기 명령의 세트를 실행하여 상기 서비스 단말기가:

상기 서비스 단말기의 상기 사용자의 권한 허가에 기반하여 상기 서비스 단말기로부터 상기 사용자 데이터를 획득하는 것;

상기 사용자 데이터를 분석하여 상기 하나 이상의 위험 제어 모델을 생성하는 것; 및

상기 하나 이상의 위험 제어 모델을 상기 서비스 단말기의 데이터베이스에 저장하는 것을 더 수행하게 하는 비일시적 컴퓨터 판독가능 매체.

청구항 18

제17항에 있어서, 상기 적어도 하나의 프로세서는 상기 명령의 세트를 실행하여 상기 서비스 단말기가:

상기 하나 이상의 위험 제어 모델을 상기 서비스 단말기의 로컬 보안 제어 데이터베이스 내에 저장하기 전에, 상기 하나 이상의 위험 제어 모델을 암호화하는 것; 및

상기 서비스 단말기의 상기 데이터베이스 내에 상기 암호화된 하나 이상의 위험 제어 모델을 저장하는 것을 더 수행하게 하는 비일시적 컴퓨터 판독가능 매체.

청구항 19

제17항에 있어서, 상기 사용자 데이터는 사용자 사회적 데이터, 관심 데이터 및 습관 데이터 중 적어도 하나를 포함하고, 상기 하나 이상의 위험 제어 모델은 상기 사용자 사회적 데이터에 기반하여 생성된 사회적 관계 제어 모델, 상기 관심 데이터에 기반하여 생성된 관심 제어 모델, 및 상기 습관 데이터에 기반하여 생성된 습관 제어 모델 중 적어도 하나를 포함하는 비일시적 컴퓨터 판독가능 매체.

청구항 20

제16항에 있어서, 상기 서비스 동작의 상기 신뢰성 분석 결과를 획득하는 것은:

상기 신뢰성 분석 명령에 기반하여 상기 서비스 동작의 서비스 정보를 획득하는 것;

상기 서비스 동작의 유형에 기반하여 상기 하나 이상의 위험 제어 모델로부터 목표 위험 제어 모델을 획득하는 것 -- 상기 하나 이상의 위험 제어 모델은 상기 서비스 정보와 서비스 신뢰성 분석 값 사이의 대응하는 관계를 포함함 --; 및

상기 서비스 정보에 대응하는 서비스 신뢰성 분석 값을 획득하기 위하여 상기 서비스 정보를 키워드로 사용하여 상기 목표 위험 제어 모델을 검색하는 것을 포함하는 비일시적 컴퓨터 판독가능 매체.

청구항 21

제20항에 있어서, 상기 신뢰성 분석 명령에 기반하여 상기 서비스 동작의 상기 서비스 정보를 획득하는 것은:

상기 서비스 동작의 상기 신뢰성 분석 명령으로부터 상기 서비스 정보를 획득하는 것을 포함하며, 상기 서비스 정보는 다른 단말기에 의해 송신된 상기 서비스 동작의 상기 동작 요청에 기반하여 상기 서비스 서버에 의해 획득된 정보를 포함하는 비일시적 컴퓨터 판독가능 매체.

청구항 22

제20항에 있어서, 상기 적어도 하나의 프로세서는 상기 명령의 세트를 실행하여 상기 서비스 단말기가:

상기 서비스 단말기의 사용자가 상기 서비스 동작을 개시할 때, 상기 신뢰성 분석 명령을 수신하기 전에 상기 서비스 서버로 상기 서비스 동작의 상기 동작 요청을 송신하는 것; 및

상기 신뢰성 분석 명령을 수신할 때, 상기 서비스 동작의 상기 동작 요청에 기반하여 상기 서비스 동작의 상기 서비스 정보를 획득하는 것을 더 수행하게 하는 비일시적 컴퓨터 판독가능 매체.

청구항 23

서비스 서버의 적어도 하나의 프로세서에 의해 실행 가능하고, 상기 서비스 서버가 서비스 동작의 보안 검증 방법을 수행하게 하는 명령의 세트를 저장하는 비일시적 컴퓨터 판독가능 매체로서, 상기 방법은:

서비스 단말기와 연관된 동작 요청에 응답하여, 상기 서비스 단말기로 상기 서비스 동작의 신뢰성 분석 명령을 송신하는 것;

상기 서비스 단말기에 의해 송신된 신뢰성 분석 결과를 수신하는 것 -- 상기 신뢰성 분석 결과는 상기 서비스 단말기가 상기 서비스 동작의 신뢰성 분석 및 상기 서비스 단말기에 사전 저장된 하나 이상의 위험 제어 모델을 수행하는 것에 기반하여 상기 서비스 단말기에 의해 획득됨 --; 및

상기 신뢰성 분석 결과에 기반하여 상기 서비스 동작의 보안을 판단하는 것을 포함하는 비일시적 컴퓨터 판독가능 매체.

청구항 24

제23항에 있어서, 상기 적어도 하나의 프로세서는 상기 명령의 세트를 실행하여 상기 서비스 서버가:

상기 서비스 동작의 신뢰성을 분석하기 위해 상기 서비스 단말기로 상기 신뢰성 분석 명령을 송신하기 전에, 다른 단말기에 의해 송신된 상기 서비스 동작의 상기 동작 요청을 수신하는 것; 및

상기 동작 요청에 기반하여 상기 서비스 동작의 서비스 정보를 획득하는 것을 더 수행하게 하며, 상기 서비스 동작의 상기 신뢰성 분석 명령은 상기 서비스 동작의 상기 서비스 정보를 포함하는 비일시적 컴퓨터 판독가능 매체.

청구항 25

제23항에 있어서, 상기 적어도 하나의 프로세서는 상기 명령의 세트를 실행하여 상기 서비스 서버가:

상기 서비스 단말기로 상기 서비스 동작의 상기 신뢰성 분석 명령을 송신하기 전에, 상기 서비스 단말기에 의해 송신된 상기 서비스 동작의 상기 동작 요청을 수신하는 것을 더 수행하게 하며, 상기 동작 요청은 상기 서비스 단말기로 상기 서비스 동작의 상기 신뢰성 분석 명령을 송신하기 위한 트리거 명령으로 사용되는 비일시적 컴퓨터 판독가능 매체.

청구항 26

제23항에 있어서, 상기 신뢰성 분석 결과에 기반하여 상기 서비스 동작의 상기 보안을 판단하는 것은:

로컬 위험 제어 모델에 기반하여 상기 서비스 동작의 제1 신뢰성 분석 값을 획득하는 것;

상기 서비스 단말기에 의해 송신된 상기 신뢰성 분석 결과에 기반하여 제2 신뢰성 분석 값을 획득하는 것;

상기 제1 신뢰성 분석 값 및 제2 신뢰성 분석 값의 가중치를 획득하는 것;

상기 가중치에 기반하여 상기 제1 신뢰성 분석 값 및 상기 제2 신뢰성 분석 값의 결합된 신뢰성 분석 값을 계산하는 것;

상기 결합된 신뢰성 분석 값을 사전 설정된 신뢰성 임계치와 비교하는 것; 및

상기 결합된 신뢰성 분석 값이 상기 신뢰성 임계치보다 크면, 상기 서비스 동작이 안전한 것으로 판단하고, 상기 결합된 신뢰성 분석 값이 상기 신뢰성 임계치보다 크지 않으면, 상기 서비스 동작이 불안전한 것으로 판단하는 것을 포함하는 비일시적 컴퓨터 판독가능 매체.

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

발명의 설명

기 술 분 야

[0001] 연관된 출원에 대한 상호참조

[0002] 이 출원은 2014년 10월 13일에 출원된 중국 특허 출원 제201410539483.2호에 기반하고 그 우선권을 주장하며, 그 전체 내용은 여기에서 참조로 포함된다.

[0003] 기술분야

[0004] 본 출원은 통신 기술 분야에 관한 것이며, 더 구체적으로는 서비스 동작의 보안을 검증하는 방법, 장치, 단말기 및 서버에 관한 것이다.

배 경 기 술

[0005] 스마트 단말기의 발전 및 네트워크 애플리케이션의 보급에 따라, 사용자는 인스턴트 메시징 서비스, 지불 서비스 등과 같은 단말기에 설치된 다양한 애플리케이션 클라이언트를 이용하여 다양한 서비스 동작을 수행할 수 있다. 상기 서비스를 사용하기 위해, 단말기의 사용자는 종종 서버에 서비스 계정을 등록하고, 이 서비스 계정에 기반하여 특정 서비스 동작을 수행해야 한다.

[0006] 통상적으로, 사용자의 네트워크 행동 패턴이 데이터 마이닝(mining) 기술에 기반하여 획득될 수 있다. 예를 들

면, 서비스 동작이 서비스 계정과 관련하여 수행될 때, 서비스 서버는 사용자의 네트워크 행동 패턴에 따라 서비스 보안을 검증하여 서비스 위험을 방지할 수 있다. 그러나, 사용자의 네트워크 행동 패턴의 마이닝은 일반적으로 사용자의 서비스 이력 데이터, 사용자의 탐색 이력 데이터 등에 제한되며, 여기에서 데이터 내용은 비교적 유사하여, 서비스 동작 보안의 부정확한 검증을 가져온다.

발명의 내용

[0007] 본 개시는 서비스 동작의 보안을 검증하는 방법을 제공한다. 일부 실시예에 부합하여, 방법은, 서비스 단말기에 의해, 서비스 동작의 신뢰성 분석 명령을 수신하는 것을 포함하며, 신뢰성 분석 명령은 서비스 서버에 의해 송신된다. 방법은, 서비스 단말기에 의해, 신뢰성 분석 명령 및 서비스 단말기에 사전 저장된 하나 이상의 위험 제어 모델에 기반하여 서비스 동작의 신뢰성 분석 결과를 획득하는 것과, 서비스 동작의 보안을 판단하기 위하여, 서비스 단말기에 의해, 신뢰성 분석 결과를 서비스 서버로 송신하는 것을 더 포함할 수 있다.

[0008] 일부 실시예에 부합하여, 이 개시는 서비스 동작의 보안을 검증하는 다른 방법을 제공한다. 방법은 서비스 동작의 신뢰성 분석 명령을 서비스 단말기로 송신하는 것과 서비스 단말기에 의해 송신된 신뢰성 분석 결과를 수신하는 것을 포함한다. 신뢰성 분석 결과는 서비스 동작의 신뢰성 분석 명령 및 서비스 단말기에 사전 저장된 하나 이상의 위험 제어 모델에 기반하여 서비스 단말기에 의해 획득될 수 있다. 방법은 신뢰성 분석 결과에 기반한 서비스 동작의 보안 판단을 더 포함할 수 있다.

[0009] 일부 실시예에 부합하여, 이 개시는 서비스 동작의 보안을 검증하는 장치를 제공한다. 장치는 서비스 서버에 의해 송신된 서비스 동작의 신뢰성 분석 명령을 수신하도록 구성되는 수신 유닛, 신뢰성 분석 명령 및 서비스 단말기에 사전 저장된 하나 이상의 위험 제어 모델에 기반하여 서비스 동작의 신뢰성 분석 결과를 획득하도록 구성되는 분석 유닛 및 서비스 동작의 보안을 판단하기 위하여 서비스 서버로 신뢰성 분석 결과를 송신하도록 구성되는 송신 유닛을 포함한다.

[0010] 일부 실시예에 부합하여, 이 개시는 서비스 동작의 보안을 검증하는 다른 장치를 제공한다. 장치는 서비스 단말기로 서비스 동작의 신뢰성 분석 명령을 송신하도록 구성되는 송신 유닛 및 서비스 단말기에 의해 송신된 신뢰성 분석 결과를 수신하도록 구성되는 수신 유닛을 포함한다. 신뢰성 분석 결과는 서비스 동작의 신뢰성 분석 명령 및 서비스 단말기에 사전 저장된 하나 이상의 위험 제어 모델에 기반하여 서비스 단말기에 의해 획득될 수 있다. 장치는 신뢰성 분석 결과에 기반하여 서비스 동작의 보안을 판단하도록 구성되는 검증 유닛을 더 포함할 수 있다.

[0011] 일부 실시예에 부합하여, 이 개시는 단말기를 제공한다. 단말기는 프로세서 및 프로세서에 의해 실행 가능한 명령을 저장하도록 구성되는 메모리를 포함한다. 프로세서는 서비스 서버에 의해 송신되는 서비스 동작의 신뢰성 분석 명령을 수신하고, 신뢰성 분석 명령 및 단말기에 사전 저장된 하나 이상의 위험 제어 모델에 기반하여 서비스 동작의 신뢰성 분석 결과를 획득하고, 서비스 동작의 보안을 판단하기 위하여 서비스 서버로 신뢰성 분석 결과를 송신하도록 구성될 수 있다.

[0012] 일부 실시예에 부합하여, 이 개시는 서비스 서버를 제공한다. 서비스 서버는 프로세서 및 프로세서에 의해 실행 가능한 명령을 저장하도록 구성되는 메모리를 포함한다. 프로세서는 서비스 동작의 신뢰성 분석 명령을 서비스 단말기로 송신하고 서비스 단말기에 의해 송신된 신뢰성 분석 결과를 수신하도록 구성될 수 있다. 신뢰성 분석 결과는 서비스 동작의 신뢰성 분석 명령 및 서비스 단말기에 사전 저장된 하나 이상의 위험 제어 모델에 기반하여 서비스 단말기에 의해 획득될 수 있다. 프로세서는 신뢰성 분석 결과에 기반하여 서비스 동작의 보안을 판단하도록 더 구성될 수 있다.

[0013] 개시된 실시예의 추가적인 목적과 이점은 다음의 설명에 의해 부분적으로 제시되고, 부분적으로는 설명으로부터 명백하거나 실시예의 실행으로부터 습득될 수 있을 것이다. 개시된 실시예의 목적 및 이점은 청구범위에 제시된 요소 및 조합에 의해 실현되고 달성될 수 있다.

[0014] 전술한 일반적인 설명 및 다음의 상세한 설명은 모두 예시적이고 설명적인 것일 뿐 청구된 바에 따르는 개시된 실시예를 제한하지 않는다는 것을 이해하여야 한다.

도면의 간단한 설명

[0015] 첨부된 도면은 본 명세서에 통합되어 본 명세서의 일부를 구성하고, 본 발명에 부합하는 실시예를 도시하며, 설명과 함께 본 발명의 원리를 설명하는 역할을 한다.

도 1은 본 개시에 부합하는 방법 및 장치를 구현하는 예시적인 시스템 환경을 도시한다.

도 2는 이 개시의 일부 실시예에 부합하는 서비스 동작의 보안 검증을 위한 예시적인 방법의 흐름도이다.

도 3은 이 개시의 일부 실시예에 부합하는 서비스 동작의 보안 검증을 위한 다른 예시적인 방법의 흐름도이다.

도 4는 이 개시의 일부 실시예에 부합하는 서비스 동작의 보안 검증을 위한 예시적인 방법의 흐름도이다.

도 5는 이 개시의 일부 실시예에 부합하는 서비스 동작의 보안 검증을 위한 예시적인 서비스 서버의 블록도이다.

도 6은 이 개시의 일부 실시예에 부합하는 서비스 동작의 보안 검증을 위한 예시적인 장치의 블록도이다.

도 7은 이 개시의 일부 실시예에 부합하는 서비스 동작의 보안 검증을 위한 다른 예시적인 장치의 블록도이다.

도 8은 이 개시의 일부 실시예에 부합하는 서비스 동작의 보안 검증을 위한 다른 예시적인 장치의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0016] 이제 첨부된 도면에 예시가 설명된 예시적인 실시예를 상세히 참조한다. 달리 나타내지 않는 한 다음의 설명은 상이한 도면에서 동일한 도면 부호가 동일하거나 유사한 요소를 나타내는 첨부된 도면을 참조한다. 예시적인 실시예의 다음 설명에 기재된 구현들은 본 발명에 부합하는 모든 구현을 나타내지는 않는다. 대신, 이들은 첨부된 청구 범위에 기재된 본 발명과 관련된 양상들에 부합하는 장치 및 방법의 예에 불과하다.

[0017] 도 1은 본 개시에 부합하는 방법 및 장치를 구현하는 예시적인 시스템 환경(100)을 도시한다. 도 1에 나타난 바와 같이, 시스템 환경(100)은 서비스 서버와 서비스 서버에 서비스 계정을 등록한 사용자의 휴대전화를 포함한다. 도 1에 나타난 휴대전화는 서비스 단말기의 역할을 하는 휴대전화 "A"와 제3자 단말기의 역할을 하는 휴대전화 "B"를 포함한다.

[0018] 일부 실시예에서, 휴대전화 A에는 로컬로 보안 제어 데이터베이스가 제공되며, 이는 휴대전화 A 내의 사용자 데이터에 따라 수립된 복수의 위험 제어 모델을 포함한다. 서비스 서버가 서비스 동작 요청을 수신한 후에, 서비스 동작의 신뢰성 분석 명령이 휴대전화 A로 송신될 수 있다. 휴대전화 A는 이어서 위험 제어 모델을 호출하여 신뢰성 분석 결과를 획득하고 신뢰성 분석 결과를 서비스 서버로 리턴할 수 있다. 서비스 서버는 신뢰성 분석 결과에 따라 서비스 동작의 보안을 판단할 수 있다. 사용자 데이터가 휴대전화에 저장된 사용자의 개인적인 데이터를 포함하므로, 사용자 데이터는 사용자의 사회적 관계, 일상 등을 반영할 수 있다. 따라서, 위험 제어 모델을 이용하여 사용자의 서비스 동작의 신뢰성을 검증함으로써, 서비스 동작의 보안 검증의 정확성이 개선될 수 있다.

[0019] 도 2는 이 개시의 일부 실시예에 부합하는 서비스 동작의 보안 검증을 위한 예시적인 방법(200)의 흐름도이다. 예시적인 방법(200)은 스마트폰, 태블릿, 개인용 컴퓨터(PC) 등과 같은 서비스 단말기에 의해 수행될 수 있다. 도 2를 참조하면, 방법(200)은 다음의 단계를 포함한다.

[0020] 단계 201에서, 서비스 단말기는 서비스 서버에 의해 송신된 서비스 동작의 신뢰성 분석 명령을 수신한다. 예를 들면, 서비스 단말기의 사용자는 미리 서비스 서버에 서비스 계정을 등록하여 사용자가 서비스 계정에 따라 서비스 서버로 로그인한 후에 서비스 서버에 기반하여 다양한 서비스 동작을 완료할 수 있다. 일부 구현에서, 서비스 서버는 상품 구매 거래를 용이하게 하기 위한 제3자 지불 시스템 서버와 같이 특정한 서비스의 구현을 지원하는 제3자에 의해 유지되는 서버일 수 있다.

[0021] 일부 실시예에서, 서비스 단말기의 사용자는 서비스 단말기를 통해 서비스 서버로 서비스 동작의 동작 요청을 송신할 수 있다. 예를 들면, 사용자는 서비스 단말기를 통해 이체 동작을 수행할 수 있으며, 서비스 단말기는 이 이체 동작의 동작 요청을 서비스 서버로 송신할 수 있다. 다른 실시예에서, 제3자 단말기와 같은 다른 단말기가 서비스 단말기의 사용자에 대하여 서비스 동작의 동작 요청을 서비스 서버로 송신할 수 있다. 예를 들면, 다른 단말기의 사용자는 어떤 상품을 구매한 후에, 서비스 단말기의 사용자가 지불 동작을 수행하도록 요청하는 동작 요청을 서비스 서버로 송신할 수 있다. 서비스 서버는 다른 단말기로부터 서비스 동작의 동작 요청을 수신한 후에 서비스 단말기로 이 서비스 동작의 신뢰성 분석 명령을 송신할 수 있다.

[0022] 단계 202에서, 서비스 단말기가 신뢰성 분석 명령 및 하나 이상의 사전 저장된 위험 제어 모델에 기반하여 서비스 동작의 신뢰성 분석 결과를 획득한다. 예를 들면, 서비스 단말기는 서비스 서버로부터 신뢰성 분석 명령을 수신할 때 사전 저장된 위험 제어 모델을 호출하여 신뢰성 분석 결과를 획득할 수 있다. 일부 실시예에서, 사용

자의 권한(authorization) 허가 획득 후에, 서비스 단말기는 권한 허가에 기반하여 서비스 단말기로부터 사용자 데이터를 획득할 수 있다. 사용자 데이터는 사용자의 사회적 데이터, 관심 데이터, 습관 데이터 등을 포함할 수 있다. 서비스 단말기는 상기 사용자 데이터를 분석하여 복수의 위험 제어 모델을 생성할 수 있으며, 여기에서 각 위험 제어 모델은 서비스 정보와 서비스 신뢰성 분석 값 사이의 대응하는 관계를 포함할 수 있다. 예를 들면, 위험 제어 모델은 사용자 사회적 데이터에 따라 생성된 사회적 관계 제어 모델, 관심 데이터에 따라 생성된 관심 제어 모델, 습관 데이터에 따라 생성된 습관 제어 모델 등을 포함할 수 있다. 그리고 나서, 서비스 단말기는 위험 제어 모델을 암호화한 후에 이들 위험 제어 모델을 로컬 보안 제어 데이터베이스에 저장할 수 있다.

[0023] 일부 실시예에서, 서비스 단말기는 신뢰성 분석 명령에 따라 서비스 동작의 서비스 정보를 획득할 수 있다. 예를 들면, 서비스 단말기가 서비스 서버로 동작 요청을 송신하는 경우, 서비스 단말기는 신뢰성 분석 명령을 수신할 때 서비스 단말기에 의해 송신된 동작 요청에 따른 서비스 동작의 서비스 정보를 획득할 수 있다. 서비스 정보는 서비스 수령인의 정보, 서비스 동작의 유형, 서비스 동작의 내용 등을 포함할 수 있다. 예를 들면, 서비스 동작이 이체 동작일 때, 서비스 수령인의 정보는 이체 동작의 당사자의 이름을 포함할 수 있으며, 서비스 동작의 유형은 이체 거래일 수 있고, 서비스 동작의 내용 정보는 이체 금액을 포함할 수 있다.

[0024] 다른 단말기가 서비스 서버로 동작 요청을 송신하는 경우, 서비스 서버는 이 동작 요청으로부터 서비스 정보를 획득하고, 이 서비스 정보를 신뢰성 분석 명령 내에 포함하며, 서비스 정보를 서비스 단말기로 송신할 수 있어 서비스 단말기가 신뢰성 분석 명령으로부터 서비스 정보를 획득할 수 있다. 서비스 정보는 서비스 수령인의 정보, 서비스 동작의 유형, 서비스 동작의 내용 등을 포함할 수 있다. 예를 들면, 서비스 동작이 지불 동작일 때, 서비스 수령인의 정보는 지불 거래의 신청자(initiator)의 이름을 포함할 수 있으며, 서비스 동작의 유형은 지불 거래일 수 있고, 서비스 동작의 내용 정보는 지불 금액을 포함할 수 있다.

[0025] 서비스 동작의 서비스 정보를 획득한 후에, 서비스 단말기는 서비스 동작의 유형에 기반하여 사전 저장된 위험 제어 모델로부터 목표 위험 제어 모델을 호출할 수 있다. 예를 들면, 서비스 단말기는 서비스 정보를 키워드로 사용하여 목표 위험 제어 모델을 검색하여 신뢰성 분석 결과로서 서비스 신뢰성 분석 값을 얻을 수 있다.

[0026] 단계 203에서, 서비스 단말기는 서비스 서버로 신뢰성 분석 결과를 송신한다. 서비스 서버는 신뢰성 분석 결과에 따라 서비스 동작의 보안을 판단할 수 있다.

[0027] 방법(200)에서, 서비스 동작의 보안을 검증할 때, 서비스 동작의 신뢰성 분석 결과는 서비스 단말기의 위험 제어 모델을 사용하여 획득될 수 있다. 위험 제어 모델이 서비스 단말기에 저장된, 사용자의 사회적 관계, 습관 등을 반영할 수 있는 사용자 데이터에 따라 생성되므로, 서비스 동작의 보안 검증의 정확도가 개선될 수 있다.

[0028] 도 3은 이 개시의 일부 실시예에 부합하는 서비스 동작의 보안 검증을 위한 예시적인 방법(300)의 흐름도이다. 예시적인 방법(300)은 서비스 서버에 의해 수행될 수 있다. 도 3을 참조하면, 방법(300)은 다음의 단계를 포함한다.

[0029] 단계 301에서, 서비스 서버는 서비스 동작의 신뢰성 분석 명령을 서비스 단말기로 송신한다. 신뢰성 분석 명령을 서비스 단말기로 송신하는 과정은 도 2와 연관된 방법(200)의 설명에 부합하는 방식으로 구현될 수 있으며, 여기에서는 생략한다.

[0030] 단계 302에서, 서비스 서버는 서비스 단말기에 의해 송신된 신뢰성 분석 결과를 수신하며, 신뢰성 분석 결과는 서비스 동작의 신뢰성 분석 명령 및 서비스 단말기에 사전 저장된 하나 이상의 위험 제어 모델에 기반하여 서비스 단말기에 의해 획득된다. 서비스 서버에 의한 신뢰성 분석 결과 수신 과정은 도 2와 연관된 방법(200)의 설명에 부합하는 방식으로 구현될 수 있으며, 여기에서는 생략한다.

[0031] 단계 303에서, 서비스 서버는 신뢰성 분석 결과에 따라 서비스 동작의 보안을 판단한다.

[0032] 일부 실시예에서, 로컬 위험 제어 모델이 서비스 서버 내에 저장될 수 있으며, 로컬 위험 제어 모델은 단말기 사용자의 네트워크 행동 데이터에 따라 생성될 수 있다. 서비스 동작의 보안이 검증될 때, 서비스 서버는 로컬 위험 제어 모델에 따라 서비스 동작의 제1 신뢰성 분석 값을 획득할 수 있으며, 서비스 단말기에 의해 송신된 신뢰성 분석 결과를 제2 신뢰성 분석 값으로 사용할 수 있다. 서비스 서버는 제1 신뢰성 분석 값 및 제2 신뢰성 분석 값에 대한 가중치를 각각 획득할 수 있으며, 제1 신뢰성 분석 값 및 제2 신뢰성 분석 값에 각 가중치를 곱하고, 가중된 제1 신뢰성 분석 값 및 가중된 제2 신뢰성 분석 값을 합계하여 결합된 신뢰성 분석 값을 획득한다. 그 다음 서비스 서버는 결합된 신뢰성 분석 값을 사전 설정된 신뢰성 임계치와 비교할 수 있다. 서비스 서버는 결합된 신뢰성 분석 값이 신뢰성 임계치보다 크면 서비스 동작이 안전한 것으로 판단할 수 있으며,

결합된 신뢰성 분석 값이 신뢰성 임계치보다 크지 않으면 서비스 동작이 불안전한 것으로 판단할 수 있다.

[0033] 방법(300)에서, 서비스 동작의 보안이 검증될 때, 서비스 동작의 신뢰성 분석 결과는 서비스 단말기 내의 위험 제어 모델을 사용하여 획득될 수 있다. 위험 제어 모델이 서비스 단말기에 저장된, 사용자의 사회적 관계, 습관 등을 반영할 수 있는 사용자 데이터에 따라 생성되므로, 서비스 동작의 보안 검증의 정확도가 개선될 수 있다.

[0034] 도 4는 이 개시의 일부 실시예에 부합하는 서비스 동작의 보안 검증을 위한 예시적인 방법의 흐름도이다. 예시적인 방법(400)은 서비스 동작의 보안 검증을 위하여 서비스 단말기와 서비스 서버 사이에서 구현될 수 있다. 도 4를 참조하면, 방법(400)은 다음의 단계를 포함한다.

[0035] 단계 401에서, 서비스 단말기는 서비스 단말기의 사용자의 권한 허가에 따라 서비스 단말기로부터 사용자 데이터를 획득한다. 서비스 단말기 내의 사용자 데이터는 사용자의 개인적인 정보를 포함할 수 있다.

[0036] 일부 구현에서, 사용자의 권한 허가는 미리 획득될 수 있다. 예를 들면, 사용자 데이터를 획득하기 위하여 서비스 단말기에 애플리케이션("앱(APP)")이 설치될 수 있다. 사용자는 이 앱을 설치함으로써 권한 허가를 부여할 수 있으며, 그 결과로 서비스 단말기가 사용자 데이터에 액세스할 수 있다.

[0037] 사용자 데이터는 사용자 사회적 데이터, 관심 데이터, 습관 데이터 등을 포함할 수 있다. 예를 들면, 사용자 사회적 데이터는 서비스 단말기 내의 통상적인 통신 정보, 예컨대 주소록 내의 그룹, 연락처 및 메모, 통화 기록 내의 과거 통화 참여자, 통화 시간 및 통화횟수 정보, 문자 메시지 기록 내의 과거 문자 메시지의 송신인과 수령인 및 문자 메시지 양 등을 포함할 수 있다. 사용자 데이터는 서비스 단말기에 설치된 인스턴트 메시지 애플리케이션과 연관된 통신 정보, 예컨대 인스턴트 메시지 연락처, 각 연락처의 연결 시간 등을 더 포함할 수 있다. 관심 데이터는 서비스 단말기 내의 브라우저에 의해 획득된 사용자의 탐색 이력, 예컨대 사용자에 의해 검색된 상품, 이벤트 등을 포함할 수 있다. 관심 데이터는 서비스 단말기 내의 위치결정 장치에 의해 획득된 사용자의 지리적 위치 정보, 예컨대 사용자가 자주 방문하는 식당, 쇼핑몰 등을 더 포함할 수 있다. 습관 데이터는 서비스 단말기 내의 메모장(notebook)에 기록된 정보, 예컨대 사용자 일정, 리마인더 등을 포함할 수 있다. 습관 데이터는 서비스 단말기 내의 애플리케이션의 설정, 예컨대 알람 설정, 달력 리마인더 등을 더 포함할 수 있다. 서비스 단말기의 사용자는 본 개시의 범위를 벗어나지 않고 서비스 단말기가 상술한 사용자 데이터의 일부 또는 전부를 획득하도록 권한을 부여할 수 있다.

[0038] 단계 402에서, 서비스 단말기는 사용자 데이터를 분석하여 하나 이상의 위험 제어 모델을 생성한다. 단계 401에서 사용자 데이터를 획득한 후에, 상이한 유형의 사용자 데이터가 분석되어 사회적 관계 제어 모델, 관심 제어 모델, 및/또는 습관 제어 모델이 획득될 수 있으며, 각 위험 제어 모델은 서비스 정보와 서비스 신뢰성 분석 값 사이의 대응하는 관계를 포함한다.

[0039] 사용자 사회적 데이터에 기반하여 사회적 관계 제어 모델이 생성될 수 있으며 사용자의 연락처와 이들 연락처의 신뢰성 분석 값 사이의 대응하는 관계를 포함할 수 있다. 예를 들면, 연락처 멤버 "A" 가 단말기 사용자의 친척이면, 연락처 멤버 A는 높은 신뢰성 분석 값을 획득할 수 있다. 다른 예로서, 연락처 멤버 "B" 가 사용자 주소록에 추가된 지 오래되었으며 연락처 멤버 B가 사용자와 통신하는 빈도가 높으면, 연락처 멤버 B는 사용자의 동료 또는 친구일 수 있으며, 따라서, 높은 신뢰성 분석 값을 획득할 수 있다. 다른 예로서, 연락처 멤버 "C" 가 사용자 주소록에 최근에 추가되었으며 연락처 멤버 C는 사용자와 몇몇 문자 메시지만을 주고받았으면, 연락처 멤버 C는 모르는 사람일 수 있으며, 따라서, 낮은 신뢰성 분석 값을 획득할 수 있다.

[0040] 관심 데이터에 따라 관심 제어 모델이 생성될 수 있으며 사용자의 관심 대상과 관심 대상의 신뢰성 분석 값 사이의 대응하는 관계를 나타낼 수 있다. 예를 들면, 사용자의 관심 대상이 랩톱이며 사용자의 탐색 이력이 특정 시간 주기 내에 랩톱 관련 정보를 자주 탐색하였음을 나타내면, 랩톱에 대해 높은 신뢰성 분석 값이 설정될 수 있다. 다른 예로서, 사용자의 관심 대상이 쇼핑몰이지만 지리적 위치 정보가 사용자가 그 쇼핑몰을 거의 방문하지 않는 것을 나타낸다면, 그 쇼핑몰에 대해서는 낮은 신뢰성 분석 값이 설정될 수 있다.

[0041] 습관 데이터에 따라 습관 제어 모델이 생성될 수 있으며 사용자의 통상적 활동과 통상적 활동의 신뢰성 분석 값 사이의 대응하는 관계를 나타낼 수 있다. 예를 들면, 사용자의 통상적 활동이 매일 밤 8 PM에 한 시간 동안 공원을 달리는 것이면, 매일 밤 8 PM부터 9 PM까지 공원을 달리는 것에 대해 높은 신뢰성 분석 값이 설정될 수 있다.

[0042] 일부 실시예에서, 서비스 정보는 상기 위험 제어 모델로부터 제외될 수 있으며, 서비스 정보에 대응하는 신뢰성 분석 값이 디폴트로 0으로 설정될 수 있다.

[0043] 단계 403에서, 서비스 단말기는 위험 제어 모델을 서비스 단말기의 로컬 보안 제어 데이터베이스 내에 저장한다.

[0044] 일부 실시예에서, 단계 402에서 획득된 위험 제어 모델은 서비스 단말기 내의 위험 제어 모델의 보안을 보장하기 위하여 암호화될 수 있으며, 암호화된 위험 제어 모델이 로컬 보안 제어 데이터베이스 내에 저장될 수 있다. 위험 제어 모델이 서비스 단말기에 의해 사용될 때, 암호화된 제어 모델은 암호화 알고리즘에 대응하는 해독 알고리즘을 수행하여 해독될 수 있다.

[0045] 단계 404에서, 서비스 단말기의 사용자가 서비스 동작을 개시할 때, 서비스 단말기가 서비스 동작의 동작 요청을 서비스 서버로 송신한다. 예를 들면, 사용자는 미리 서비스 서버에 서비스 계정을 등록하여, 단말기 사용자가 서비스 계정에 따라 서비스 서버로 로그인할 때 다양한 서비스 동작을 완료할 수 있다. 사용자가 특정 서비스 동작을 개시할 때, 서비스 단말기가 서비스 동작의 동작 요청을 서비스 서버로 송신할 수 있다. 동작 요청은 서비스 수령인의 정보, 서비스 동작의 유형, 서비스 동작의 내용 등을 포함할 수 있다. 예를 들면, 서비스 동작이 사용자가 RMB 10,000을 친구에게 이체하는 것일 때, 서비스 수령인의 정보는 친구의 사용자명, 이름, 휴대전화 번호, 이메일 주소 등을 포함할 수 있으며, 서비스 동작 유형은 이체 거래일 수 있고, 서비스 동작의 내용 정보는 이체 금액 RMB 10,000을 포함할 수 있다.

[0046] 단계 405에서, 서비스 서버는 동작 요청에 따라 서비스 동작의 신뢰성 분석 명령을 서비스 단말기로 송신한다. 예를 들면, 서비스 동작의 동작 요청을 수신한 후에, 서비스 서버는 서비스 단말기로 서비스 동작의 신뢰성 분석 명령을 송신하여 서비스 단말기가 서비스 동작의 신뢰성을 분석하도록 요청할 수 있다.

[0047] 단계 406에서, 서비스 단말기는 단계 404에서 사전 송신된 동작 요청에 따라 서비스 동작의 서비스 정보를 획득한다. 단계 404에서 상술된 바와 같이, 서비스 동작의 동작 요청은 서비스 수령인의 정보, 서비스 동작의 유형, 서비스 동작의 내용 등을 포함할 수 있다. 서비스 단말기는 상술한 정보를 서비스 동작의 서비스 정보로 사용할 수 있다.

[0048] 단계 407에서, 서비스 단말기는 서비스 동작의 유형에 따라 위험 제어 모델로부터 목표 위험 제어 모델을 호출한다. 위험 제어 모델이 서비스 단말기의 로컬 보안 제어 데이터베이스 내에 저장되고 각 위험 제어 모델이 상이한 서비스 동작 유형에 대응할 수 있으므로, 서비스 단말기는 서비스 동작 유형에 대응하는 목표 위험 제어 모델을 위험 제어 모델로부터 호출할 수 있다. 예를 들면, 서비스 동작의 유형이 이체 또는 지불일 때, 서비스 동작은 이체 당사자(party) 또는 지불을 개시하는 서비스 사용자를 포함하며, 사용자와 이체 상대방 또는 서비스 사용자 사이에 특정한 사회적 관계가 존재할 수 있고, 따라서, 사회적 관계 제어 모델이 위험 제어 모델로부터 호출될 수 있다.

[0049] 단계 408에서, 서비스 단말기는 서비스 정보에 대응하는 서비스 신뢰성 분석 값을 획득하기 위하여 서비스 정보를 키워드로 사용하여 목표 위험 제어 모델을 검색하며, 서비스 신뢰성 분석 값은 제2 신뢰성 분석 값에 대응한다. 계속해서 서비스 동작이 사용자가 친구에게 RMB 10,000를 이체하는 것인 예에서, 대응하여 단계 406에서 획득된 서비스 정보는 서비스 수령인의 정보로서 친구의 사용자명, 이름, 휴대전화 번호, 이메일 주소 등을 포함할 수 있으며, 서비스 동작의 유형은 이체 거래일 수 있고, 단계 407에서 서비스 유형 "이체"에 대응하여 서비스 유형에 따라 호출된 목표 위험 제어 모델은 사회적 관계 제어 모델이다. 서비스 단말기는 친구의 이름 및 휴대전화 번호를 키워드로 사용하여 사회적 관계 제어 모델을 검색하여 대응하는 서비스 신뢰성 분석 값을 얻을 수 있다. 친구와 사용자 사이에 친밀한 관계가 존재한다고 가정하면, 사회적 관계 제어 모델이 생성될 때, 서비스 신뢰성 분석 값이 상대적으로 높을 것이다.

[0050] 단계 409에서, 서비스 단말기는 제2 신뢰성 분석 값을 서비스 서버로 송신한다.

[0051] 단계 410에서, 서비스 서버는 로컬 위험 제어 모델에 따라 서비스 동작의 제1 신뢰성 분석 값을 획득한다.

[0052] 이 실시예에서, 로컬 위험 제어 모델은 서비스 서버 내에 저장되며, 로컬 위험 제어 모델은 단말기 사용자의 네트워크 행동 데이터에 따라 생성될 수 있다. 일부 구현에서, 서비스 동작의 보안이 검증될 때, 서비스 서버는 로컬 위험 제어 모델에 따라 서비스 동작의 제1 신뢰성 분석 값을 획득할 수 있다.

[0053] 단계 411에서, 서비스 서버는 제1 신뢰성 분석 값 및 제2 신뢰성 분석 값의 가중치를 획득한다.

[0054] 예를 들면, 서비스 서버는 제1 신뢰성 분석 값 및 제2 신뢰성 분석 값에 대해 가중치를 설정할 수 있으며, 가중치를 로컬로 저장할 수 있다. 상기 가중치는 실질적인 애플리케이션의 요구에 따라 조정될 수 있으며, 본 개시에서 제한되지 않음을 유의하여야 한다.

[0055] 단계 412에서, 서비스 서버는 가중치에 따른 제1 신뢰성 분석 값 및 제2 신뢰성 분석 값에 기반하여 결합된 신뢰성 분석 값을 계산한다.

[0056] 이 단계에서, 서비스 서버는 제1 신뢰성 분석 값에 그 가중치를 곱하고, 제2 신뢰성 분석 값에 그 가중치를 곱하고, 상기 두 곱을 합하여 결합된 신뢰성 분석 값을 획득하도록 구성될 수 있다.

[0057] 단계 413에서, 서비스 서버는 결합된 신뢰성 분석 값을 사전 설정된 신뢰성 임계치와 비교한다. 일부 실시예에서, 서비스 서버는 서비스 동작의 보안을 판단하기 위하여 미리 신뢰성 임계치를 설정할 수 있다.

[0058] 계속해서 서비스 동작이 사용자가 친구에게 RMB 10,000를 이체하는 것인 예에서, 서비스 서버에서 미리 설정된 신뢰성 임계치가 60이고, 제1 신뢰성 분석 값 및 제2 신뢰성 분석 값에 대해 설정된 가중치가 각각 80% 및 20%, 서비스 서버 자체에 의해 획득된 제1 신뢰성 분석 값이 55, 서비스 서버에 의해 서비스 단말기로부터 획득된 제2 신뢰성 분석 값이 90이라고 가정하면, 단계 412를 수행하여 획득된 결합된 신뢰성 분석 값은 (80%×55)+(20%×90)=62이다.

[0059] 단계 414에서, 서비스 서버는 비교 결과에 따라 서비스 동작의 보안을 판단한다.

[0060] 단계 413의 비교 결과에 따라, 종합적인 신뢰성 분석 값이 신뢰성 임계치보다 크면, 서비스 서버는 서비스 동작이 안전하다고 판단할 수 있다. 종합적인 신뢰성 분석 값이 신뢰성 임계치보다 크지 않으면, 서비스 서버는 서비스 동작이 불안전하다고 판단할 수 있다. 예를 들면, 단말기 사용자가 친구에게 RMB 10,000을 이체하고자 할 때, 이체 금액이 크기 때문에, 서비스 서버는 계산에 따라 획득된 제1 신뢰성 분석 값 55(신뢰성 임계치 60보다 낮음)에 따라 이 이체 서비스가 신뢰할 만하지 않다고 판단할 수 있으며, 이에 따라 부정확한 검증 결과를 나타낼 수 있다. 그러나, 서비스 단말기에 의해 획득된 제2 신뢰성 분석 값을 결합함으로써, 획득된 결합된 신뢰성 분석 값은 62이며, 이체 서비스가 안전하다고 판단될 수 있다. 따라서, 서비스 단말기에 의해 획득된 제2 신뢰성 분석 값을 결합하여, 서비스 동작의 보안 검증의 정확도가 개선될 수 있다.

[0061] 도 5는 이 개시의 일부 실시예에 부합하는 서비스 동작의 보안 검증을 위한 예시적인 서비스 서버(500)의 블록도이다. 도 5에 나타난 바와 같이, 예시적인 서버(500)는 CPU, 메모리, 네트워크 인터페이스 및 비휘발성 저장 장치를 포함한다. CPU는 메모리에 저장된 프로그램 및 모듈을 동작시켜, 다양한 기능과 데이터 처리를 수행하도록 구성될 수 있다. 예를 들면, CPU는 명령을 실행하여 상술된 방법의 모든 또는 일부 단계를 수행하도록 구성될 수 있다. 예시적인 실시예에서, 서비스 서버(500) 내의 CPU에 의해 실행 가능한, 서비스 동작의 보안 검증을 위한 명령과 같은 명령은 비휘발성 저장장치로부터 메모리로 읽혀져, 상술한 방법을 수행한다. 유사한 구조가 서비스 단말기 내에 구현되어 상술한 서비스 동작의 보안을 검증하기 위한 방법을 수행할 수 있다. 서비스 서버 및 서비스 단말기는 도 5에 나타나지 않은 다른 구성요소를 또한 포함할 수 있다.

[0062] 도 6은 이 개시의 일부 실시예에 부합하는 서비스 동작의 보안 검증을 위한 예시적인 장치(600)의 블록도이다. 예시적인 장치(600)는 서비스 단말기 내에 구현될 수 있다. 도 6을 참조하면, 장치(600)는 수신 유닛(610), 분석 유닛(620) 및 송신 유닛(630)을 포함한다.

[0063] 수신 유닛(610)은, 서비스 서버에 의해 송신된, 서비스 동작의 신뢰성 분석 명령을 수신하도록 구성된다.

[0064] 분석 유닛(620)은 신뢰성 분석 명령 및 하나 이상의 사전 저장된 위험 제어 모델에 기반하여 서비스 동작의 신뢰성 분석 결과를 획득하도록 구성된다.

[0065] 송신 유닛(630)은 서비스 서버가 신뢰성 분석 결과를 기반으로 서비스 동작의 보안을 판단할 수 있도록 신뢰성 분석 결과를 서비스 서버로 송신하도록 구성된다. 일부 구현에서, 송신 유닛(630)은 서비스 단말기의 사용자가 서비스 동작을 개시할 때 서비스 서버로 서비스 동작의 동작 요청을 송신하도록 더 구성될 수 있다.

[0066] 도 7은 이 개시의 일부 실시예에 부합하는 서비스 동작의 보안 검증을 위한 다른 예시적인 장치(700)의 블록도이다. 예시적인 장치(700)는 서비스 단말기 내에 구현될 수 있다. 도 7을 참조하면, 장치(700)는 수신 유닛(610), 분석 유닛(620) 및 송신 유닛(630)에 더하여, 획득 유닛(640), 생성 유닛(650), 암호화 유닛(660) 및 저장 유닛(670)을 더 포함한다.

[0067] 획득 유닛(640)은 단말기 사용자의 권한 허가에 따라 서비스 단말기로부터 사용자 데이터를 획득하도록 구성된다.

[0068] 생성 유닛(650)은 사용자 데이터를 분석하여 하나 이상의 위험 제어 모델을 생성하도록 구성된다.

[0069] 암호화 유닛(660)은 생성 유닛에 의해 생성된 위험 제어 모델을 암호화하도록 구성된다.

[0070] 저장 유닛(670)은 암호화된 위험 제어 모델을 서비스 단말기의 로컬 보안 제어 데이터베이스 내에 저장하도록 구성된다.

[0071] 일부 실시예에서, 분석 유닛(620)은 서비스 정보 획득 서브유닛, 목표 위험 제어 모델 호출 서브유닛, 및 서비스 신뢰성 분석 값 획득 서브유닛을 포함할 수 있다.

[0072] 서비스 정보 획득 서브유닛은 신뢰성 분석 명령에 따라 서비스 동작의 서비스 정보를 획득하도록 구성된다. 일부 구현에서, 서비스 정보 획득 서브유닛은 신뢰성 분석 명령으로부터 서비스 동작의 서비스 정보를 획득하도록 구성될 수 있으며, 서비스 동작의 서비스 정보는 다른 단말기, 예컨대 제3자 단말기에 의해 송신된 동작 요청에 따라 서비스 서버에 의해 획득된다. 일부 구현에서, 서비스 정보 획득 서브유닛은 신뢰성 분석 명령을 수신할 때, 서비스 서버로 송신된 동작 요청에 따라 서비스 동작의 서비스 정보를 획득하도록 구성될 수도 있다.

[0073] 목표 위험 제어 모델 호출 서브유닛은 서비스 동작의 유형에 따라 사전 저장된 위험 제어 모델로부터 목표 위험 제어 모델을 호출하도록 구성되며, 목표 위험 제어 모델은 서비스 정보와 서비스 신뢰성 분석 값 사이의 대응하는 관계를 나타낸다.

[0074] 서비스 신뢰성 분석 값 획득 서브유닛은 서비스 신뢰성 분석 값을 획득하기 위하여 서비스 정보를 키워드로 사용하여 목표 위험 제어 모델을 검색하도록 구성된다.

[0075] 도 8은 이 개시의 일부 실시예에 부합하는 서비스 동작의 보안 검증을 위한 다른 예시적인 장치(800)의 블록도이다. 예시적인 장치(800)는 서비스 서버 내에 구현될 수 있다. 도 8을 참조하면, 장치(800)는 송신 유닛(810), 수신 유닛(820) 및 검증 유닛(830)을 포함한다.

[0076] 송신 유닛(810)은 서비스 동작의 신뢰성 분석 명령을 서비스 단말기로 송신하도록 구성된다.

[0077] 수신 유닛(820)은 서비스 단말기에 의해 송신된 신뢰성 분석 결과를 수신하도록 구성되며, 신뢰성 분석 결과는 서비스 동작의 신뢰성 분석 명령 및 서비스 단말기에 사전 저장된 하나 이상의 위험 제어 모델에 기반하여 서비스 단말기에 의해 획득된다.

[0078] 검증 유닛(830)은 신뢰성 분석 결과에 따라 서비스 동작의 보안을 판단하도록 구성된다.

[0079] 일부 구현에서, 수신 유닛(820)은 제3자 단말기와 같은 다른 단말기에 의해 송신된 서비스 동작의 동작 요청을 수신하도록 더 구성될 수 있다. 일부 실시예에서, 장치(800)는 다른 단말기에 의해 송신된 동작 요청에 따라 서비스 동작의 서비스 정보를 획득하도록 구성되는 획득 유닛(도 8에서는 도시되지 않음)을 더 포함할 수 있다. 송신 유닛(810)은 서비스 동작의 서비스 정보를 포함하는 동작 요청을 서비스 단말기로 송신하도록 구성될 수 있다.

[0080] 일부 구현에서, 수신 유닛(820)은 서비스 단말기의 사용자가 서비스 동작을 개시할 때, 서비스 단말기에 의해 송신된 서비스 동작의 동작 요청을 수신하도록 더 구성될 수 있다. 송신 유닛(810)은, 동작 요청을 트리거 명령으로 사용하여, 서비스 동작의 신뢰성 분석 명령을 서비스 단말기로 송신하도록 구성될 수 있다.

[0081] 일부 실시예에서, 검증 유닛(830)은 신뢰성 분석 값 획득 서브유닛, 가중치 획득 서브유닛, 결합된 신뢰성 분석 값 계산 서브유닛, 신뢰성 분석 값 비교 서브유닛, 및 서비스 보안 판단 서브유닛(도 8에서는 도시되지 않음)을 포함할 수 있다.

[0082] 신뢰성 분석 값 획득 서브유닛은 로컬 위험 제어 모델에 따라 서비스 동작의 제1 신뢰성 분석 값을 획득하도록 구성된다.

[0083] 가중치 획득 서브유닛은, 서비스 단말기에 의해 송신된 신뢰성 분석 결과를 제2 신뢰성 분석 값으로 사용하여, 제1 신뢰성 분석 값 및 제2 신뢰성 분석 값의 가중치를 획득하도록 구성된다.

[0084] 결합된 신뢰성 분석 값 계산 서브유닛은 가중치에 따라 제1 신뢰성 분석 값 및 제2 신뢰성 분석 값의 결합된 신뢰성 분석 값을 계산하도록 구성된다.

[0085] 신뢰성 분석 값 비교 서브유닛은 결합된 신뢰성 분석 값을 사전 설정된 신뢰성 임계치와 비교하도록 구성된다.

[0086] 서비스 보안 판단 서브유닛은, 결합된 신뢰성 분석 값이 신뢰성 임계치보다 크면, 서비스 동작이 안전한 것으로 판단하고, 결합된 신뢰성 분석 값이 신뢰성 임계치보다 크지 않으면, 서비스 동작이 불안전한 것으로 판단하도

록 구성된다.

[0087] 예시적인 실시예에서, 명령을 포함하는 비일시적 컴퓨터-판독 가능 저장 매체가 또한 제공되며, 명령은 상술한 방법을 수행하기 위하여 장치(예컨대 단말 장치, 서버, 개인용 컴퓨터 등)에 의해 실행될 수 있다. 장치는 하나 이상의 처리장치(CPUs), 입/출력 인터페이스, 네트워크 인터페이스 및/또는 메모리를 포함할 수 있다.

[0088] 여기에서 "제1" 및 "제2"와 같은 관계형 용어는 하나의 대상 또는 동작을 다른 대상 또는 동작과 구분하기 위해서만 사용되며 이들 대상 또는 동작 사이의 임의의 실제 관계 또는 순서를 요구하거나 암시하지 않는 점을 유의하여야 한다. 또한, "포함하는(comprising)", "갖는(having)", "함유하는(containing)" 및 "포함하는(including)"의 용어 및 다른 유사한 형태는 의미가 동일한 것으로 의도되며 이들 용어 중 임의의 것을 따르는 항목 또는 항목들이 이러한 항목 또는 항목들의 철저한 목록이 되거나 열거된 항목 또는 항목들로만 제한되도록 의도되지 않는다는 점에서 열려 있다(open ended).

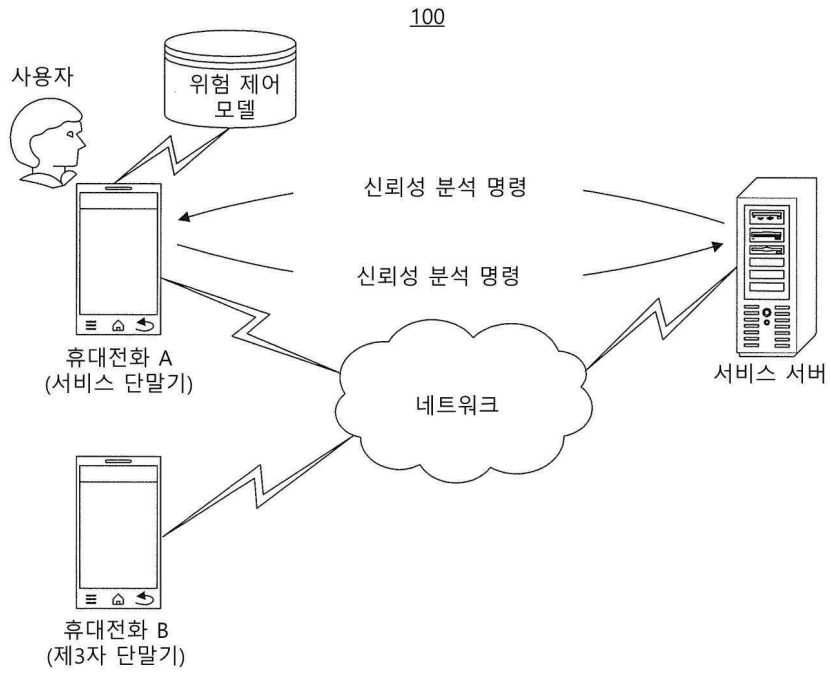
[0089] 이 분야의 기술자는 상술한 실시예가 하드웨어, 또는 소프트웨어(프로그램 코드), 또는 하드웨어 및 소프트웨어의 조합으로 구현될 수 있음을 이해할 것이다. 소프트웨어에 의해 구현되면, 이는 상술한 컴퓨터-판독 가능 매체에 저장될 수 있다. 처리장치에 의해 실행될 때, 소프트웨어는 개시된 방법을 수행할 수 있다. 이 개시에서 설명된 컴퓨팅 유닛 및 다른 기능적 유닛은 하드웨어, 또는 소프트웨어, 또는 하드웨어 및 소프트웨어의 조합으로 구현될 수 있다. 이 분야의 기술자는 또한 상술한 모듈/유닛의 다수가 하나의 모듈/유닛으로 결합될 수 있으며, 상술한 모듈/유닛 각각이 다수의 서브-모듈/서브-유닛으로 더 나뉠 수 있음을 이해할 것이다.

[0090] 발명의 다른 실시예가 여기에서 개시된 발명의 실행 및 명세서의 고려로부터 이 분야의 기술자에게 명백할 것이다. 이 출원은 그 일반적인 원리를 따르며 이 분야에서 공지되거나 통상적인 관행에 따르는 것과 같은 본 개시로부터의 이탈을 포함하는 발명의 임의의 변형, 용도, 또는 적용을 커버하는 것으로 의도된다. 본 명세서 및 예들은 단지 예시적인 것으로 의도되며, 본 발명의 진정한 범위 및 사상은 다음의 청구범위에 의해 나타난다.

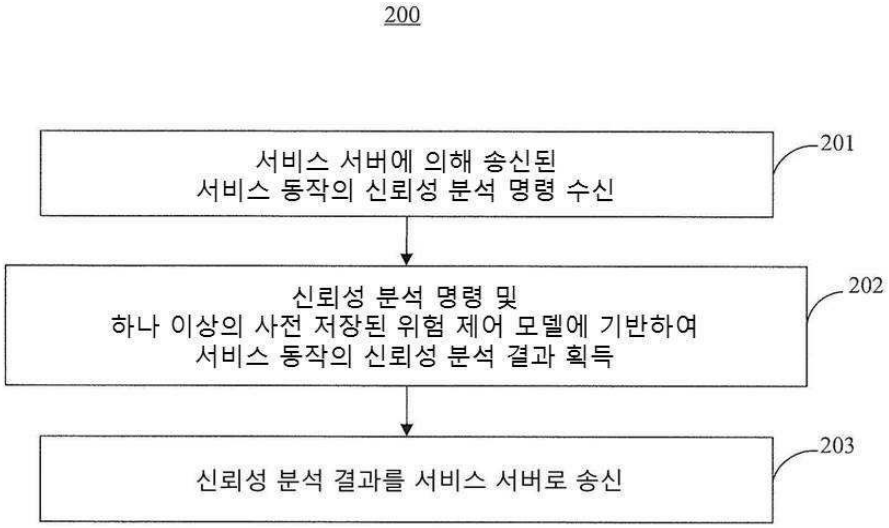
[0091] 본 발명이 위에서 설명되고 첨부된 도면에서 도시된 정확한 구성에 제한되지 않으며, 그 범위로부터 벗어나지 않고 다양한 변경 및 변화가 이루어질 수 있음을 이해할 것이다. 본 발명의 범위는 첨부된 청구범위에 의해서만 제한되는 것으로 의도된다.

도면

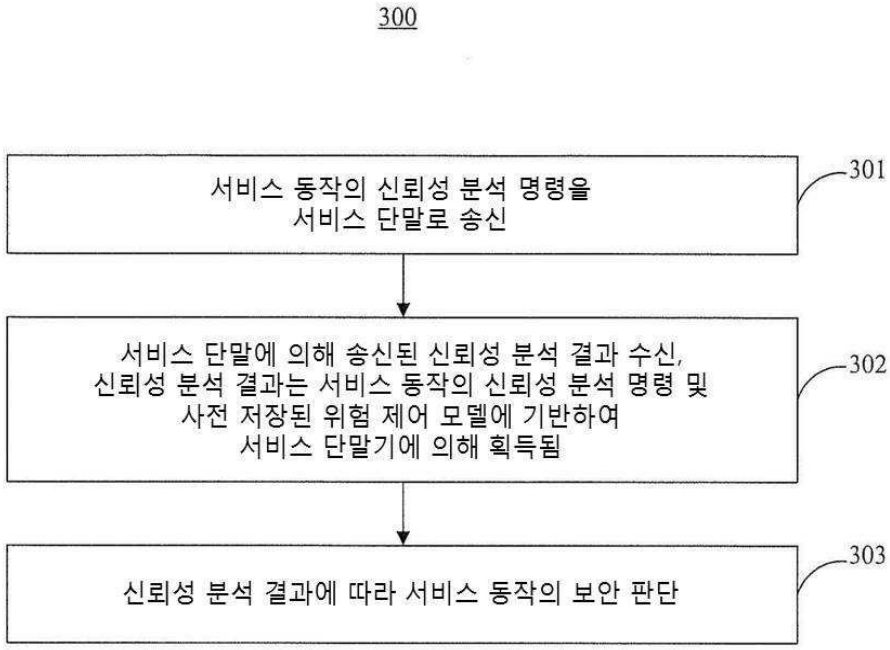
도면1



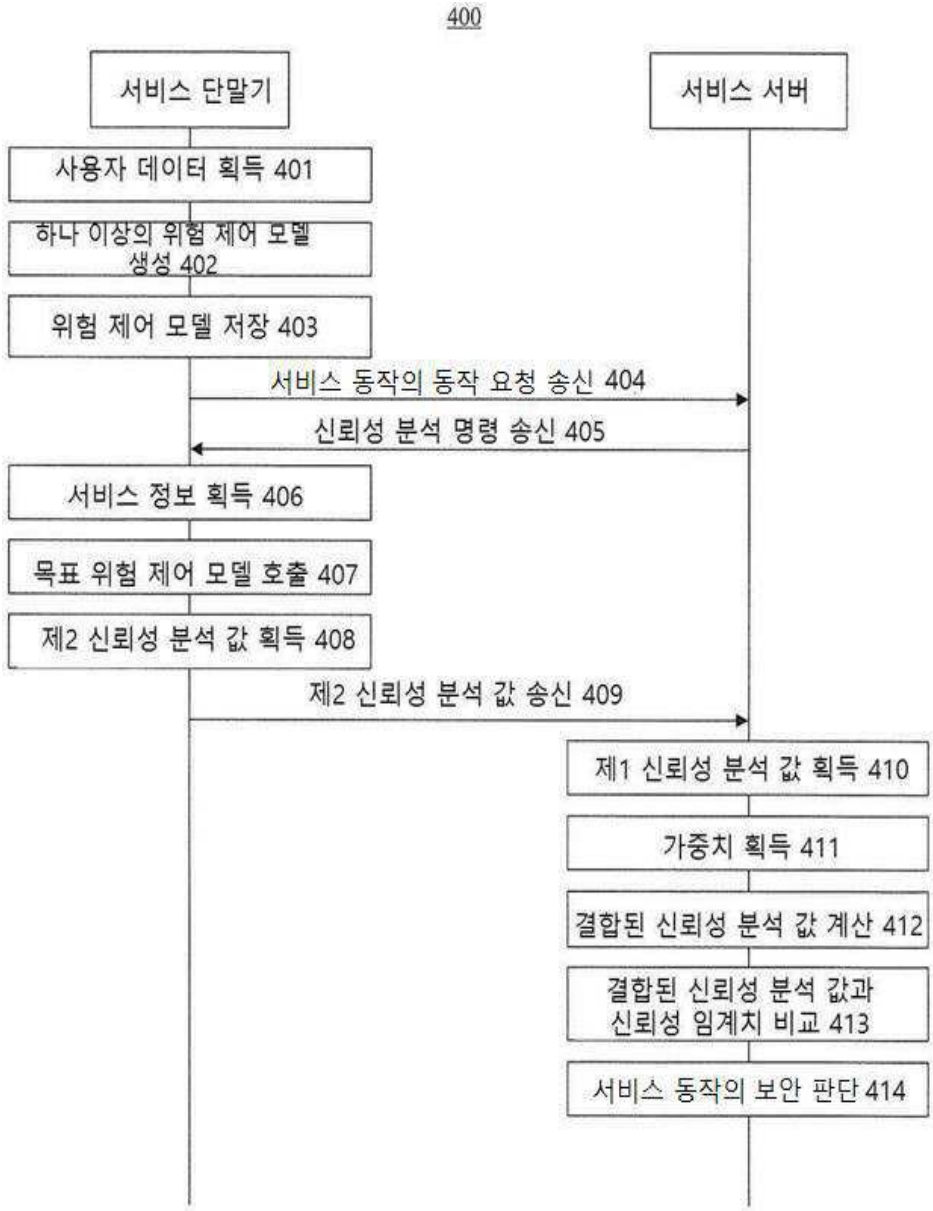
도면2


200
서비스 서버에 의해 송신된
서비스 동작의 신뢰성 분석 명령 수신
201
신뢰성 분석 명령 및
하나 이상의 사전 저장된 위험 제어 모델에 기반하여
서비스 동작의 신뢰성 분석 결과 획득
202
신뢰성 분석 결과를 서비스 서버로 송신
203

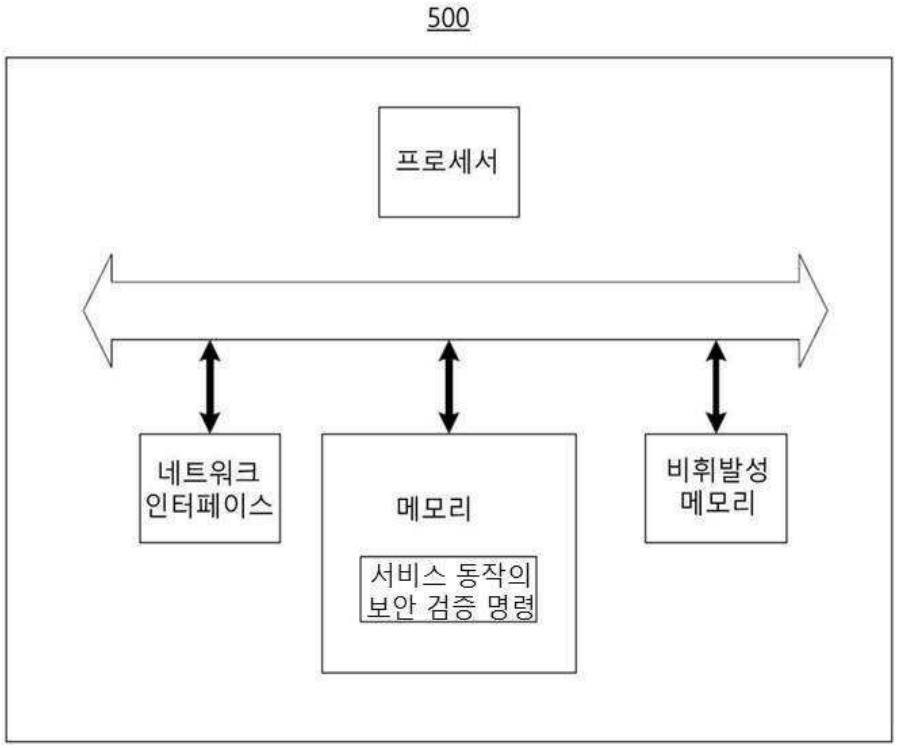
도면3


300
서비스 동작의 신뢰성 분석 명령을
서비스 단말로 송신
301
서비스 단말에 의해 송신된 신뢰성 분석 결과 수신,
신뢰성 분석 결과는 서비스 동작의 신뢰성 분석 명령 및
사전 저장된 위험 제어 모델에 기반하여
서비스 단말기에 의해 획득됨
302
신뢰성 분석 결과에 따라 서비스 동작의 보안 판단
303

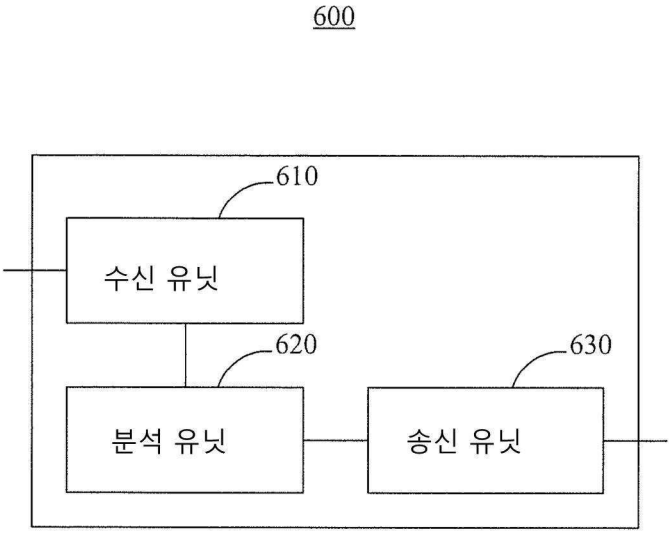
도면4


400
서비스 단말기
서비스 서버
사용자 데이터 획득 401
하나 이상의 위험 제어 모델 생성 402
위험 제어 모델 저장 403
서비스 동작의 동작 요청 송신 404
신뢰성 분석 명령 송신 405
서비스 정보 획득 406
목표 위험 제어 모델 호출 407
제2 신뢰성 분석 값 획득 408
제2 신뢰성 분석 값 송신 409
제1 신뢰성 분석 값 획득 410
가중치 획득 411
결합된 신뢰성 분석 값 계산 412
결합된 신뢰성 분석 값과 신뢰성 임계치 비교 413
서비스 동작의 보안 판단 414

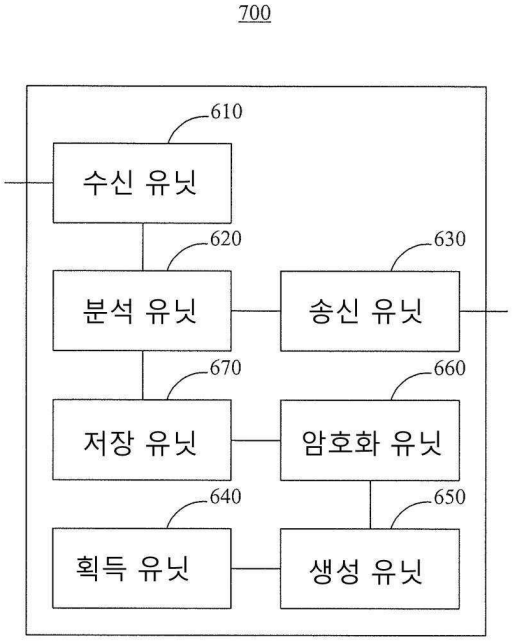
도면5


500
프로세서
네트워크
인터페이스
메모리
서비스 동작의
보안 검증 명령
비휘발성
메모리

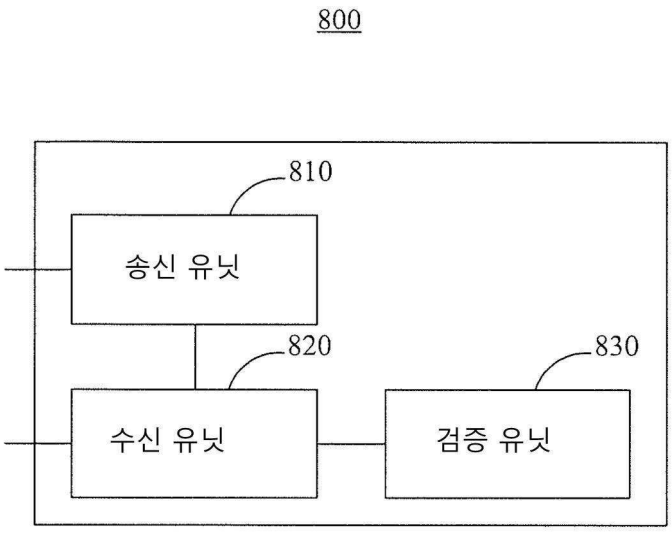
도면6


600
610
수신 유닛
620
분석 유닛
630
송신 유닛

도면7


700
610
수신 유닛
620
분석 유닛
630
송신 유닛
670
저장 유닛
660
암호화 유닛
640
획득 유닛
650
생성 유닛

도면8


800
810
송신 유닛
820
수신 유닛
830
검증 유닛