



등록특허 10-2125116



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년06월22일
(11) 등록번호 10-2125116
(24) 등록일자 2020년06월15일

- (51) 국제특허분류(Int. Cl.)
G06F 21/57 (2013.01) *G06F 21/55* (2013.01)
- (52) CPC특허분류
G06F 21/577 (2013.01)
G06F 21/55 (2013.01)
- (21) 출원번호 10-2017-7026844
- (22) 출원일자(국제) 2016년02월24일
심사청구일자 2019년09월23일
- (85) 번역문제출일자 2017년09월22일
- (65) 공개번호 10-2017-0125864
- (43) 공개일자 2017년11월15일
- (86) 국제출원번호 PCT/CN2016/074424
- (87) 국제공개번호 WO 2016/138830
국제공개일자 2016년09월09일
- (30) 우선권주장
201510093725.4 2015년03월02일 중국(CN)
- (56) 선행기술조사문헌
US20130117397 A1
WO2014088559 A1
CN104011731 A
CN103297267 A

(73) 특허권자
알리바바 그룹 홀딩 리미티드
케이만군도, 그랜드 케이만, 피오박스 847, 원 캐피탈 플레이스 4층

(72) 발명자
마오 런신
중국 저지양 311121 항저우 위항 디스트릭트 웨스트 원 이 로드 넘버 969 빌딩 3 5층 알리바바 그룹 법무팀
순 차오
중국 저지양 311121 항저우 위항 디스트릭트 웨스트 원 이 로드 넘버 969 빌딩 3 5층 알리바바 그룹 법무팀
(뒷면에 계속)

(74) 대리인
김태홍, 김진희

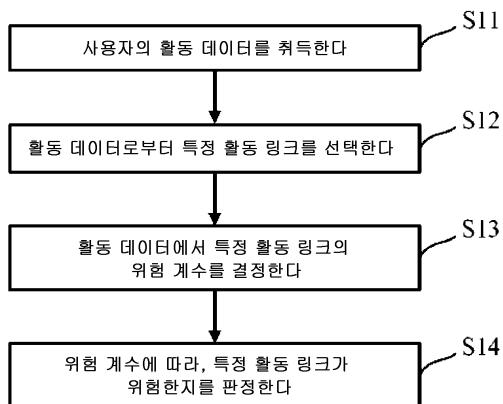
전체 청구항 수 : 총 20 항

심사관 : 구대성

(54) 발명의 명칭 위험성 있는 활동을 인식하기 위한 방법 및 장치

(57) 요약

종래 기술에서 네트워크 활동 위험성을 인식함에 있어 규칙 취약점을 교정함으로써 야기되는 낮은 효율성을 해결하기 위해 사용되는, 위험성 있는 활동을 인식하기 위한 방법 및 장치가 개시된다. 본 방법은: 사용자의 활동 데이터를 취득하는 단계; 활동 데이터로부터 특정 활동 링크를 선택하는 단계; 활동 데이터에서 특정 활동 링크의 위험 계수를 결정하는 단계; 및 위험 계수에 따라 특정 활동 링크에 위험성이 존재하는지를 결정하는 단계를 포함한다.

대 표 도 - 도1

(72) 발명자

리 신카이

중국 저지양 311121 항저우 위항 디스트릭트 웨스트 원 이 로드 넘버 969 빌딩 3 5층 알리바바 그룹
법무팀

허 디준

중국 저지양 311121 항저우 위항 디스트릭트 웨스트 원 이 로드 넘버 969 빌딩 3 5층 알리바바 그룹
법무팀

명세서

청구범위

청구항 1

컴퓨터 구현(computer-implemented) 방법에 있어서,

사용자의 활동 데이터를 결정하는 단계 - 상기 활동 데이터는 컴퓨터 네트워크를 사용한 상기 사용자의 사용자 행위들을 기술함 -;

상기 활동 데이터로부터 특정 이벤트 체인을 식별하는 단계 - 상기 특정 이벤트 체인은 상기 컴퓨터 네트워크 상에서 수행된 상기 사용자 행위들의 하나 이상의 이벤트를 포함함 -;

상기 특정 이벤트 체인의 위험 계수를 결정하는 단계 - 상기 위험 계수는 상기 특정 이벤트 체인의 희소성(rareness) 정도를 표현함 -; 및

상기 위험 계수에 기초하여, 상기 특정 이벤트 체인이 위험성 있는 네트워크 활동을 나타내는지를 결정하는 단계

를 포함하는, 컴퓨터 구현 방법.

청구항 2

제1항에 있어서,

상기 활동 데이터로부터 상기 특정 이벤트 체인을 식별하는 단계는,

기간을 식별하는 단계;

상기 기간에 대응하는 활동 데이터에 기초하여, 상기 기간 동안에 발생한 이벤트들을 결정하는 단계;
및

상기 결정된 이벤트들을 시간순으로 정렬함으로써 상기 특정 이벤트 체인을 결정하는 단계

를 포함한 것인, 컴퓨터 구현 방법.

청구항 3

제1항에 있어서,

상기 위험 계수는 단기 위험 계수, 장기 위험 계수, 또는 그룹 위험 계수 중 하나 이상을 포함한 것인, 컴퓨터 구현 방법.

청구항 4

제3항에 있어서,

상기 단기 위험 계수를 결정하는 단계는,

상기 단기 위험 계수와 연관된 단기 기간을 결정하는 단계;

상기 단기 기간에서 상기 사용자가 수행한 총 이벤트 체인 수를 결정하는 단계;

상기 단기 기간에서 상기 사용자가 상기 특정 이벤트 체인을 수행한 횟수를 결정하는 단계; 및

상기 총 이벤트 체인 수 및 상기 사용자가 상기 특정 이벤트 체인을 수행한 횟수에 기초하여 상기 단기 위험 계수를 결정하는 단계

를 포함한 것인, 컴퓨터 구현 방법.

청구항 5

제3항에 있어서,

상기 장기 위험 계수를 결정하는 단계는,

상기 장기 위험 계수와 연관된 장기 기간을 결정하는 단계;

상기 장기 기간 동안에 상기 사용자가 상기 특정 이벤트 체인을 수행한 시간 길이를 결정하는 단계; 및

상기 장기 기간 및 상기 특정 이벤트 체인을 수행하기 위한 시간 길이에 기초하여 상기 장기 위험 계수를 결정하는 단계

를 포함한 것인, 컴퓨터 구현 방법.

청구항 6

제3항에 있어서,

상기 그룹 위험 계수를 결정하는 단계는,

상기 사용자와 연관된 사용자 그룹 내의 총 사용자 수를 결정하는 단계;

상기 그룹 위험 계수와 연관된 그룹 기간을 결정하는 단계;

상기 그룹 기간에서 상기 특정 이벤트 체인을 수행한 상기 사용자 그룹 내의 사용자 수를 결정하는 단계; 및

상기 사용자 그룹 내의 상기 총 사용자 수 및 상기 특정 이벤트 체인을 수행한 상기 사용자 수에 기초하여 상기 그룹 위험 계수를 결정하는 단계

를 포함한 것인, 컴퓨터 구현 방법.

청구항 7

제1항에 있어서,

상기 특정 이벤트 체인이 위험성 있는 네트워크 활동을 나타내는지를 결정하는 단계는 상기 위험 계수가 문턱값 보다 높은지를 결정하는 단계를 포함한 것인, 컴퓨터 구현 방법.

청구항 8

동작들을 수행하도록 컴퓨터 시스템에 의해 실행 가능한 하나 이상의 명령어를 저장하는 컴퓨터 판독가능 비일시적 매체에 있어서, 상기 동작들은,

사용자의 활동 데이터를 결정하는 동작 - 상기 활동 데이터는 컴퓨터 네트워크를 사용한 상기 사용자의 사용자 행위들을 기술함 -;

상기 활동 데이터로부터 특정 이벤트 체인을 식별하는 동작 - 상기 특정 이벤트 체인은 상기 컴퓨터 네트워크 상에서 수행된 상기 사용자 행위들의 하나 이상의 이벤트를 포함함 -;

상기 특정 이벤트 체인의 위험 계수를 결정하는 동작 - 상기 위험 계수는 상기 특정 이벤트 체인의 희소성 정도를 표현함 -; 및

상기 위험 계수에 기초하여, 상기 특정 이벤트 체인이 위험성 있는 네트워크 활동을 나타내는지를 결정하는 동작

을 포함한 것인, 컴퓨터 판독가능 비일시적 매체.

청구항 9

제8항에 있어서,

상기 활동 데이터로부터 상기 특정 이벤트 체인을 식별하는 동작은,

기간을 식별하는 동작;

상기 기간에 대응하는 활동 데이터에 기초하여, 상기 기간 동안에 발생한 이벤트들을 결정하는 동작;

및

상기 결정된 이벤트들을 시간순으로 정렬함으로써 상기 특정 이벤트 체인을 결정하는 동작
을 포함한 것인, 컴퓨터 판독가능 비일시적 매체.

청구항 10

제8항에 있어서,

상기 위험 계수는 단기 위험 계수, 장기 위험 계수, 또는 그룹 위험 계수 중 하나 이상을 포함한 것인, 컴퓨터
판독가능 비일시적 매체.

청구항 11

제10항에 있어서,

상기 단기 위험 계수를 결정하는 동작은,

상기 단기 위험 계수와 연관된 단기 기간을 결정하는 동작;

상기 단기 기간에서 상기 사용자가 수행한 총 이벤트 체인 수를 결정하는 동작;

상기 단기 기간에서 상기 사용자가 상기 특정 이벤트 체인을 수행한 횟수를 결정하는 동작; 및

상기 총 이벤트 체인 수 및 상기 사용자가 상기 특정 이벤트 체인을 수행한 횟수에 기초하여 상기 단기
위험 계수를 결정하는 동작

을 포함한 것인, 컴퓨터 판독가능 비일시적 매체.

청구항 12

제10항에 있어서,

상기 장기 위험 계수를 결정하는 동작은,

상기 장기 위험 계수와 연관된 장기 기간을 결정하는 동작;

상기 장기 기간 동안에 상기 사용자가 상기 특정 이벤트 체인을 수행한 시간 길이를 결정하는 동작; 및

상기 장기 기간 및 상기 특정 이벤트 체인을 수행하기 위한 시간 길이에 기초하여 상기 장기 위험 계수
를 결정하는 동작

을 포함한 것인, 컴퓨터 판독가능 비일시적 매체.

청구항 13

제10항에 있어서,

상기 그룹 위험 계수를 결정하는 동작은,

상기 사용자와 연관된 사용자 그룹 내의 총 사용자 수를 결정하는 동작;

상기 그룹 위험 계수와 연관된 그룹 기간을 결정하는 동작;

상기 그룹 기간에서 상기 특정 이벤트 체인을 수행한 상기 사용자 그룹 내의 사용자 수를 결정하는 동
작; 및

상기 사용자 그룹 내의 상기 총 사용자 수 및 상기 특정 이벤트 체인을 수행한 상기 사용자 수에 기초
하여 상기 그룹 위험 계수를 결정하는 동작

을 포함한 것인, 컴퓨터 판독가능 비일시적 매체.

청구항 14

제8항에 있어서,

상기 특정 이벤트 체인이 위험성 있는 네트워크 활동을 나타내는지를 결정하는 동작은 상기 위험 계수가 문턱값 보다 높은지를 결정하는 동작을 포함한 것인, 컴퓨터 판독가능 비일시적 매체.

청구항 15

컴퓨터 구현 시스템에 있어서,

하나 이상의 컴퓨터; 및

상기 하나 이상의 컴퓨터와 상호 동작 가능하게 결합되고, 상기 하나 이상의 컴퓨터에 의해 실행될 때 동작들을 수행하는 명령어들을 저장하는 유형의(tangible) 머신 판독가능 비일시적 매체를 갖는 하나 이상의 컴퓨터 메모리 디바이스

를 포함하고,

상기 동작들은,

사용자의 활동 데이터를 결정하는 동작 - 상기 활동 데이터는 컴퓨터 네트워크를 사용한 상기 사용자의 사용자 행위들을 기술함 -;

상기 활동 데이터로부터 특정 이벤트 체인을 식별하는 동작 - 상기 특정 이벤트 체인은 상기 컴퓨터 네트워크 상에서 수행된 상기 사용자 행위들의 하나 이상의 이벤트를 포함함 -;

상기 특정 이벤트 체인의 위험 계수를 결정하는 동작 - 상기 위험 계수는 상기 특정 이벤트 체인의 희소성 정도를 표현함 -; 및

상기 위험 계수에 기초하여, 상기 특정 이벤트 체인이 위험성 있는 네트워크 활동을 나타내는지를 결정하는 동작

을 포함한 것인, 컴퓨터 구현 시스템.

청구항 16

제15항에 있어서,

상기 활동 데이터로부터 상기 특정 이벤트 체인을 식별하는 동작은,

기간을 식별하는 동작;

상기 기간에 대응하는 활동 데이터에 기초하여, 상기 기간 동안에 발생한 이벤트들을 결정하는 동작; 및

상기 결정된 이벤트들을 시간순으로 정렬함으로써 상기 특정 이벤트 체인을 결정하는 동작
을 포함한 것인, 컴퓨터 구현 시스템.

청구항 17

제15항에 있어서,

상기 위험 계수는 단기 위험 계수, 장기 위험 계수, 또는 그룹 위험 계수 중 하나 이상을 포함한 것인, 컴퓨터 구현 시스템.

청구항 18

제17항에 있어서,

상기 단기 위험 계수를 결정하는 동작은,

상기 단기 위험 계수와 연관된 단기 기간을 결정하는 동작;

상기 단기 기간에서 상기 사용자가 수행한 총 이벤트 체인 수를 결정하는 동작;

상기 단기 기간에서 상기 사용자가 상기 특정 이벤트 체인을 수행한 횟수를 결정하는 동작; 및

상기 총 이벤트 체인 수 및 상기 사용자가 상기 특정 이벤트 체인을 수행한 횟수에 기초하여 상기 단기

위험 계수를 결정하는 동작

을 포함한 것인, 컴퓨터 구현 시스템.

청구항 19

제17항에 있어서,

상기 장기 위험 계수를 결정하는 동작은,

상기 장기 위험 계수와 연관된 장기 기간을 결정하는 동작;

상기 장기 기간 동안에 상기 사용자가 상기 특정 이벤트 체인을 수행한 시간 길이를 결정하는 동작; 및

상기 장기 기간 및 상기 특정 이벤트 체인을 수행하기 위한 시간 길이에 기초하여 상기 장기 위험 계수를 결정하는 동작

을 포함한 것인, 컴퓨터 구현 시스템.

청구항 20

제17항에 있어서,

상기 그룹 위험 계수를 결정하는 동작은,

상기 사용자와 연관된 사용자 그룹 내의 총 사용자 수를 결정하는 동작;

상기 그룹 위험 계수와 연관된 그룹 기간을 결정하는 동작;

상기 그룹 기간에서 상기 특정 이벤트 체인을 수행한 상기 사용자 그룹 내의 사용자 수를 결정하는 동작; 및

상기 사용자 그룹 내의 상기 총 사용자 수 및 상기 특정 이벤트 체인을 수행한 상기 사용자 수에 기초하여 상기 그룹 위험 계수를 결정하는 동작

을 포함한 것인, 컴퓨터 구현 시스템.

발명의 설명

기술 분야

[0001]

본 출원은 컴퓨터 기술 분야에 관한 것으로, 특히 네트워크 위험 활동을 식별하는 방법 및 장치에 관한 것이다.

배경 기술

[0002]

인터넷의 발달과 함께, 사람들의 네트워크 활동들은 더 자주 뒤섞인다. 개념적으로, 네트워크 활동은 네트워크 내의 각각의 네트워크 개체가 네트워크 데이터를 획득, 전송, 또는 송신하는 프로세스를 지칭하며, 이는 일반적으로 정보 조회, 파일 다운로드, 메일 전송 등을 포함한다. 정상적인 네트워크 활동 이외에, 업무 중에 회사 직원이 업무와 관련 없는 정보를 검색하는 것 또는 네트워크 고객 서비스 직원이 비용 내역을 불법적으로 조회하는 것과 같이, 의도적으로 또는 본의 아니게 네트워크 개체들이 수행하는 비정상적인 네트워크 활동들은 손실을 초래할 수 있다. 상기 문제를 해결하기 위해, 네트워크 위험성 활동을 모니터링하기 위한 위험 모니터링 시스템이 등장한다.

[0003]

현재, 종래의 위험 모니터링 시스템은, 규칙 엔진을 구성함으로써, 규칙의 정의들에 부합하는 네트워크 활동들의 특성을 추출 및 분석하고, 이에 따라 네트워크 활동들의 위험성을 식별한다. 그러나 규칙 엔진이 이용하는 규칙들은 통상적으로 취약점이 있으며, 규칙들의 취약점을 교정하기 위해 규칙들을 계속적으로 추가할 필요가 있다. 이는 확실히 개발자의 작업 부하를 증가시킬 수 있으며, 효율성은 낮다. 또한, 규칙 엔진 자체가 여분의 컴퓨터 자원들을 소비할 필요가 있으므로, 컴퓨터 시스템에 부담을 초래한다.

발명의 내용

[0004]

본 출원의 실시예들은 네트워크 활동 위험성의 식별 동안 규칙 취약점을 교정함으로써 야기되는 종래 기술에서의 낮은 효율성의 문제, 및 규칙 엔진이 여분의 컴퓨터 자원들을 소비하는 문제를 해결하기 위해 위험성 있는

활동을 식별하기 위한 방법 및 장치를 제공한다.

[0005] 본 출원의 실시예들에서 제공되는 위험성 있는 활동을 식별하기 위한 방법은:

[0006] 사용자의 활동 데이터를 취득하는 단계;

[0007] 활동 데이터에서 특정 활동 링크의 위험 계수를 결정하는 단계; 및

[0008] 위험 계수에 따라, 특정 활동 링크가 위험한지를 판정하는 단계를 포함한다.

[0009] 본 출원의 실시예들에서 제공되는 위험성 있는 활동을 식별하기 위한 장치는:

[0010] 사용자의 활동 데이터를 취득하도록 구성된 취득 모듈;

[0011] 활동 데이터에서 특정 활동 링크의 위험 계수를 결정하도록 구성된 결정 모듈; 및

[0012] 위험 계수에 따라, 특정 활동 링크가 위험한지를 판정하도록 구성된 판정 모듈을 포함한다.

[0013] 본 출원의 실시예들에서 이용되는 상기 적어도 하나의 기술적 해결 방안은 다음의 유익한 효과들을 달성할 수 있다:

[0014] 본 출원의 실시예들에서는, 사용자의 활동 데이터가 취득되고, 활동 데이터로부터 특정 활동 링크가 선택되고; 활동 데이터에서 특정 활동 링크의 위험 계수가 계산에 의해 결정되고, 마지막으로, 위험 계수에 따라, 특정 활동 링크가 위험한지가 결정된다. 규칙 엔진 방식과 비교하여, 전술한 프로세스에서는, 규칙 취약점을 수동으로 교정할 필요가 없으므로, 활동 위험성 식별의 효율이 향상된다. 또한, 전술한 프로세스는 규칙 엔진이 여분의 컴퓨터 자원들을 소비하는 불리한 점을 회피하므로, 컴퓨터 시스템의 부담이 경감된다.

도면의 간단한 설명

[0015] 본 명세서에 설명된 첨부 도면들은 본 출원의 추가적인 이해를 제공하고 본 출원의 일부를 구성하는 데 사용된다. 본 출원의 개략적인 실시예들 및 그 설명은 본 출원을 예시하기 위해 사용되지만, 본 출원에 대한 부적절한 제한을 구성하지는 않는다. 도면들에서:

도 1은 본 출원의 실시예에 따른 위험성 있는 활동을 식별하기 위한 방법의 프로세스를 도시한다;

도 2는 본 출원의 실시예에 따른 위험성 있는 활동을 식별하기 위한 방법에서 활동 데이터로부터 특정 활동 링크를 선택하는 프로세스를 도시한다;

도 3은 본 출원의 실시예에 따른 위험성 있는 활동을 식별하기 위한 방법에서 단기 위험 계수를 결정하는 프로세스를 도시한다;

도 4는 본 출원의 실시예에 따른 위험성 있는 활동을 식별하기 위한 방법에서 이력 위험 계수를 결정하는 프로세스를 도시한다;

도 5는 본 출원의 실시예에 따른 위험성 있는 활동을 식별하기 위한 방법에서 팀 위험 계수를 결정하는 프로세스를 도시한다;

도 6은 본 출원의 실시예에 따른 위험성 있는 활동을 식별하기 위한 방법에서 특정 활동 링크가 위험한지를 판정하는 프로세스를 도시한다;

도 7은 본 출원의 실시예에 따른 위험성 있는 활동을 식별하기 위한 장치의 개략적인 구조도이다.

발명을 실시하기 위한 구체적인 내용

[0016] 본 출원의 목적들, 기술적 해결 방안들, 및 이점들을 더 명확하게 하기 위해, 본 출원의 기술적 해결 방안들이 본 출원의 구체적인 실시예들 및 상응하는 도면들을 참조하여 명확하고 완전하게 설명된다. 명백하게, 설명된 실시예들은 본 출원의 실시예들의 전부가 아니라 일부에 불과하다. 본 출원의 실시예들에 기초하여, 창의적인 노력을 기울이지 않고 이 기술분야의 통상의 기술자들에 의해 얻어지는 모든 다른 실시예들은 모두 본 출원의 보호 범위에 속한다.

[0017] 도 1은 본 출원의 실시예에 따른 위험성 있는 활동을 식별하기 위한 방법의 프로세스를 도시하며, 이는 다음의 단계들을 포함한다:

- [0018] S11: 사용자의 활동 데이터를 취득한다.
- [0019] 본 출원의 실시예에서, 활동 데이터는 네트워크 모니터링 시스템을 통해 획득된다. 네트워크 모니터링 시스템은 네트워크의 컴퓨터들을 모니터링하고 제어하여 시간 차원에서 네트워크의 사용자들이 수행하는 인터넷 행위들(네트워크 활동)을 기록한다. 네트워크 모니터링 시스템은 모니터링 하드웨어 또는 모니터링 소프트웨어를 포함하고, 네트워크는 LAN(local area network), MAN(metropolitan area network), 또는 WAN(wide area network)을 포함한다. 활동 데이터는 특정 저장 매체에 저장되고, 실제 분석 요건에 따라, 대응하는 활동 데이터가 분석을 위해 저장 매체로부터 추출된다.
- [0020] 이 명세서에서는, e-비즈니스 웹사이트가 본 출원의 기술적 해결 방안들을 소개하기 위한 예로 이용된다. 따라서, 위험성 있는 활동을 식별하기 위한 방법은 e-비즈니스 웹사이트의 고객 서비스 직원의 네트워크 활동이 위험한지를 모니터링하기 위해 사용된다.
- [0021] S12: 활동 데이터로부터 특정 활동 링크를 선택한다. 활동 링크는 다수의 활동을 발생 시간에 따라 순차적으로 배열함으로써 얹어지는 조합을 지칭한다. 활동 링크가 사용자의 실제 활동 의도에 더 가까울수록, 네트워크 활동 위험성 식별의 신뢰도가 향상된다.
- [0022] 도 2는 본 출원의 실시예에 따른 위험성 있는 활동을 식별하기 위한 방법에서 활동 데이터로부터 특정 활동 링크를 선택하는 프로세스를 도시한다. 본 출원의 실시예에서, 단계 S12는 구체적으로 다음의 단계들을 포함한다:
- [0023] S121: 활동 데이터로부터 특정 시구간에서의 단편 데이터를 선택한다.
- [0024] 계속 이 명세서의 예를 이용하여, 활동 위험성 분석을 필요로 하는 네트워크 개체가 사용자 M이라고 가정한다. 이 경우, 특정 일 D의 특정 시구간에서의 사용자 M의 단편 데이터가 저장 매체로부터 추출된다. 특정 시구간이 15분, 예를 들어 13:10 ~ 13:25인 경우, 단편 데이터는 해당 일의 13:10 ~ 13:25의 시구간에서 사용자 M이 수행한 활동들에 관한 데이터를 지칭한다.
- [0025] S122: 단편 데이터에 포함된 활동들을 취득한다.
- [0026] 전술한 예에서는, 해당 일의 13:10 ~ 13:25의 시구간에서, 사용자 M이 수행한 활동들이 활동 X, 활동 Y, 및 활동 Z를 포함한다고 가정한다.
- [0027] S123: 활동들을 발생 시간들에 따라 시간순(chronological order)으로 정렬하여 활동 링크를 획득한다.
- [0028] 전술한 예에서는, 활동 X, 활동 Y, 및 활동 Z의 발생 시간에 따라 시간순으로 정렬을 수행하며, 획득된 특정 활동 링크 G는: 활동 X → 활동 Y → 활동 Z이다.
- [0029] S13: 활동 데이터에서 특정 활동 링크의 위험 계수를 결정한다.
- [0030] 본 출원의 실시예에서, 위험 계수는 특정 활동 링크 G의 희소성 정도를 표현하기 위한 수치이다. 일반적으로, 네트워크 활동이 비교적 높은 발생 확률을 갖는 경우, 즉 네트워크 활동이 비교적 흔한 경우, 이는 네트워크 활동이 정상적인 활동, 예를 들어, 고객 서비스 직원이 상점 정보를 살펴보는 활동임을 나타낸다. 네트워크 활동이 비교적 낮은 발생 확률을 갖는 경우, 즉 네트워크 활동이 매우 드문 상황에서만 발생하는 경우, 이는 네트워크 활동이 위험성 있는 활동, 예를 들어, 고객 서비스 직원이 친척과 친구들의 지출 내역을 조회하는 활동임을 나타낸다. 본 출원은, 위험 계수에 따라, 네트워크 활동이 위험한지를 판정한다.
- [0031] 본 출원의 실시예에서, 전술한 위험 계수는 단기 위험 계수 a, 이력 위험 계수 b, 및 팀 위험 계수 c 중 하나 이상을 포함한다. 당연히, 본 출원의 다른 실시예들에서, 분석된 위험 계수는 전술한 3가지 유형으로 한정되지 않을 수 있다. 단기 위험 계수 a는 사용자 M이 제1 시구간 t_1 (예컨대, 하루)에 특정 활동 링크 G를 조작하는 것의 희소성 정도를 지칭한다. 이력 위험 계수 b는 사용자 M이 사용자의 등록의 총 시간 길이 t_2 (등록 시간에서 현재 시간까지의 간격)에 특정 활동 링크 G를 조작하는 것의 희소성 정도를 지칭한다. 사용자 M이 속하는 사용자 모집단이 사용자 그룹이고 사용자 그룹이 다수의 사용자를 포함하는 것으로 정의되는 경우, 팀 위험 계수 c는 사용자 M이 속하는 사용자 그룹이 특정 활동 링크 G를 조작하는 것의 희소성 정도를 지칭한다.
- [0032] 이하에서는 전술한 위험 계수들을 결정하는 프로세스들을 상세히 설명한다:
- [0033] 도 3은 본 출원의 실시예에 따른 위험성 있는 활동을 식별하기 위한 방법에서 단기 위험 계수를 결정하는 프로세스를 도시하며, 이는 구체적으로 다음의 단계들을 포함한다:

- [0034] S131: 사용자 M이 제1 시구간 t_1 에 모든 활동 링크를 조작하는 총 조작 횟수 s_1 을 취득한다.
- [0035] 계속 이 실시예의 예를 이용하여, 제1 시구간 t_1 이 하루라고 가정하면, 해당 일에 사용자 M이 수행한 모든 활동 링크의 수(즉, 총 조작 횟수 s_1)는 해당 일의 사용자 M의 활동 데이터에 기초하여 카운팅될 수 있다. 본 출원의 실시예에서, 해당 일의 사용자 M의 총 조작 횟수 s_1 은 단일의 특정 활동 링크 G가 지속되는 시간 간격 t_6 를 기준으로 사용하여 카운팅된다. 구체적으로, t_6 가 15분인 경우, 총 조작 횟수 $s_1=24*60/15=96$ 이다.
- [0036] S132: 사용자 M이 제1 시구간 t_1 에 특정 활동 링크 G를 조작하는 조작 횟수 s_2 를 취득한다.
- [0037] 전술한 예에서, 설정된 제1 시구간 t_1 은 하루이므로, 사용자 M이 해당 일에 특정 활동 링크 G를 조작하는 횟수 (즉, 조작 횟수 s_2)가 카운팅된다. 구체적으로, t_6 가 15분인 경우, 그 날은 몇 개의 15분 타임 슬라이스로 분할되고, 각각의 15분 타임 슬라이스에서 특정 활동 링크 G가 발생하는지가 순차적으로 판정되고; 특정 활동 링크 G가 발생하면, 조작 횟수 s_2 가 1 증가되고, 특정 활동 링크 G가 발생하지 않으면, 조작 횟수 s_2 가 0 증가되고, 해당 일의 조작 횟수 s_2 가 획득될 때까지 계속된다.
- [0038] S133: 조작 횟수 s_2 에 대한 총 활동 횟수 s_1 의 비를 결정하여 단기 위험 계수 a를 획득한다.
- [0039] 본 출원의 실시예에서, 단기 위험 계수 a를 계산하는 공식은 다음과 같다:
- [0040] $a=s_1/s_2$.
- [0041] 도 4는 본 출원의 실시예에 따른 위험성 있는 활동을 식별하기 위한 방법에서 이력 위험 계수를 결정하는 프로세스를 도시하며, 이는 구체적으로 다음의 단계들을 포함한다:
- [0042] S134: 등록 시간 t_0 에서 현재 시간 t_a 까지의 사용자 M의 총 시간 길이 t_2 를 취득한다.
- [0043] 계속 이 명세서의 예를 이용하여, e-비즈니스 웹사이트의 고객 서비스 시스템에서 사용자 M의 등록 시간 t_0 가 2014년 1월 1일이고, 현재 시간 t_a 가 2015년 1월 1일이라고 가정한다; 이 경우, 총 시간 길이 t_2 는 365일이다.
- [0044] S135: 사용자 M이 특정 활동 링크 G를 조작하는 실제 시간 길이 t_3 를 취득한다.
- [0045] 본 출원의 실시예에서, 사용자 M이 특정 활동 링크 G를 조작하는 실제 시간 길이 t_3 를 취득하는 단계에서는, 매 일 계산이 수행된다. 이 경우, 365일간의 사용자 M의 활동 데이터는 매일 365개의 단편 데이터로 분할되고, 매 일의 단편 데이터에서 특정 활동 링크 G가 발생하는지가 순차적으로 판단되고; 특정 활동 링크 G가 발생하면, 실제 시간 길이 t_3 가 1 증가되고; 특정 활동 링크 G가 발생하지 않으면, 실제 시간 길이 t_3 가 0 증가되고, 사용자 M이 특정 활동 링크 G를 조작하는 실제 일 수(즉, 실제 시간 길이 t_3)가 획득될 때까지 계속된다.
- [0046] S136: 총 시간 길이 t_2 및 실제 시간 길이 t_3 에 따라 이력 위험 계수 b를 결정한다.
- [0047] 본 출원의 실시예에서, 오래된 사용자의 경우, 그 사용자는 더 이른 시간에 등록하므로, 총 시간 길이 t_2 는 비교적 길다(예컨대, 3년). 오래된 사용자가 특정 활동 링크 G를 조작하는 실제 시간 길이 t_3 가 2일이라고 가정하면, 최종적으로 총 시간 길이 t_2 에서 오래된 사용자가 특정 활동 링크 G를 조작할 확률은 비교적 낮다는 결론이 내려진다. 그러나, 새로운 사용자의 경우, 그 사용자는 최근에 등록되었으므로, 총 시간 길이 t_2 는 비교적 짧다(예컨대, 5일). 새로운 사용자가 특정 활동 링크 G를 조작하는 실제 시간 길이 t_3 가 2일이라고 가정하면, 최종적으로 총 시간 길이 t_2 에서 새로운 사용자가 특정 활동 링크 G를 조작할 확률은 비교적 높다는 결론이 내려진다. 알 수 있는 바와 같이, 새로운 사용자와 오래된 사용자 간의 차이는 이력 위험 계수 b의 신뢰도에 영향을 줄 수 있고, 새로운 사용자와 오래된 사용자 간의 차이를 평활화하기 위하여, 단계 S136는 구체적으로 다음을 포함한다:
- [0048] 우선, 총 시간 길이 t_2 와 실제 시간 길이 t_3 를 평활화하여 평활화된 총 시간 길이 t_{2k} 및 평활화된 실제 시간 길이 t_{3k} 를 획득한다. 본 출원의 실시예에서, 평활화는 대수 처리(logarithmic processing), 모듈로 처리(modulo

processing), 근 추출 처리(root extraction processing), 또는 기타 등등일 수 있다. 대수 처리 방식을 예로 이용하여, $t_{2k} = \lg t_2$ 이고; $t_{3k} = \lg t_3$ 이다. 당연히, 대수 처리의 밑수는 한정되지 않는다.

[0049] 그 후, 평활화된 실제 시간 길이 t_{2k} 와 평활화된 총 시간 길이 t_{3k} 에 대해 계산을 수행하여 이력 위험 계수 b 를 획득한다. 본 출원의 실시예에서, 이력 위험 계수 b 를 계산하기 위한 공식은 다음과 같다:

$$b = (1+t_{3k})/(1+t_{2k}) = (1+\lg t_3)/(1+\lg t_2).$$

[0051] 도 5는 본 출원의 실시예에 따른 위험성 있는 활동을 식별하기 위한 방법에서 팀 위험 계수를 결정하는 프로세스를 도시하며, 이는 구체적으로 다음의 단계들을 포함한다:

[0052] S137: 사용자 M이 속하는 사용자 그룹에 포함된 총 사용자 수 n 을 결정한다.

[0053] 계속 이 명세서의 예를 이용하여, 사용자 M은 e-비즈니스 웹사이트의 고객 서비스 직원이라고 가정한다. 이 경우, 사용자 M이 속하는 부서가 사용자 그룹이다. 이 부서에 포함된 총 사용자 수 n 은 20명이라고 가정한다.

[0054] S138: 사용자 그룹에서 제2 시구간 t_4 에 특정 활동 링크 G를 조작한 실제 사용자 수 m 을 취득한다.

[0055] 전술한 예에서, 제2 시구간 t_4 가 하루인 경우, 단계 S138은 사용자 M이 속하는 부서 내의 20명의 사람 중 특정 일에 특정 활동 링크 G를 조작한 사람들의 수(즉, 실제 사용자 수 m)를 카운팅하는 데 사용된다. 구체적으로, 해당 일의 부서 내의 20명의 사람의 활동 데이터가 사전에 개별적으로 취득되고, 그 후 20명의 사용자가 해당 일에 특정 활동 링크 G를 조작했는지를 순차적으로 살펴본다; 특정 활동 링크 G를 조작했다면, 실제 사용자 수 m 이 1 증가되고; 특정 활동 링크 G를 조작하지 않았다면, 실제 사용자 수 m 이 0 증가되고, 해당 일에 특정 활동 링크 G를 조작한 실제 사용자 수 m 이 획득될 때까지 계속된다.

[0056] S139: 총 사용자 수 n 및 실제 사용자 수 m 에 따라 팀 위험 계수 c 를 결정한다.

[0057] 본 출원의 실시예에서, 분석될 필요가 있는 사용자 그룹이 다수의 사용자를 포함하는 경우(예를 들어, $n=1000$), 그리고 특정 일에 특정 활동 링크 G를 조작한 실제 사용자 수 m 이 이 시점에서 5명인 경우, 이는 사용자 그룹에서 특정 활동 링크 G가 조작될 확률이 비교적 낮다는 것을 나타낸다. 그러나, 분석될 필요가 있는 사용자 그룹이 소수의 사용자를 포함하는 경우(예를 들어, $n=10$), 그리고 특정 일에 특정 활동 링크 G를 조작한 실제 사용자 수 m 이 이 시점에서 5명인 경우, 이는 사용자 그룹에서 특정 활동 링크 G가 조작될 확률이 비교적 높다는 것을 나타낸다. 알 수 있는 바와 같이, 상이한 사용자 그룹 내의 상이한 사용자 수는 팀 위험 계수 c 의 신뢰도에 영향을 줄 수 있고, 상이한 사용자 그룹 내의 상이한 사용자 수를 평활화하기 위하여, 단계 S139는 구체적으로 다음을 포함한다:

[0058] 우선, 총 사용자 수 n 과 실제 사용자 수 m 을 평활화하여 평활화된 총 사용자 수 p 및 평활화된 실제 사용자 수 q 를 획득한다. 본 출원의 실시예에서, 평활화는 대수 처리(logarithmic processing), 모듈로 처리(modulo processing), 근 추출 처리(root extraction processing), 또는 기타 등등일 수 있다. 대수 처리 방식을 예로 이용하여, $p = \lg n$ 이고; $q = \lg m$ 이다. 당연히, 대수 처리의 밑수는 한정되지 않는다.

[0059] 그 후, 평활화된 총 사용자 수 p 와 평활화된 실제 사용자 수 q 에 대해 계산을 수행하여 팀 위험 계수 c 를 획득한다. 본 출원의 실시예에서, 팀 위험 계수 c 를 계산하기 위한 공식은 다음과 같다:

$$c = (1+p)/(1+q) = (1+\lg n)/(1+\lg m).$$

[0061] S14: 위험 계수 r 에 따라, 특정 활동 링크 G가 위험한지를 판정한다.

[0062] 본 출원의 실시예에서, 위험 계수 r 을 계산하기 위한 공식은 다음과 같다:

$$r = a \times b \times c.$$

[0064] 당연히, 본 출원의 다른 실시예들에서, 위험 계수 $r = a+b+c$ 이다.

[0065] 도 6은 본 출원의 실시예에 따른 위험성 있는 활동을 식별하기 위한 방법에서 특정 활동 링크가 위험한지를 판정하는 프로세스를 도시한다. 본 출원의 실시예에서, 단계 S14는 구체적으로 다음을 포함한다:

[0066] S141: 활동 링크들의 위험 계수 r 들을 내림차순으로 정렬한다.

[0067] 계속 이 명세서의 예를 이용하여, 추출된 활동 데이터는 특정 일 D의 사용자 M의 모든 활동 링크라고 가정한다.

활동 데이터에는, 100개의 모니터링된 활동 링크가 있다; 이 경우, 100개의 활동 링크의 위험 계수 r_1 내지 r_{100} 이 전술한 방법에 따라 개별적으로 결정되고, 그 후 위험 계수 r_1 내지 r_{100} 이 내림차순으로 정렬된다.

[0068] S142: 특정 활동 링크 G에 대응하는 위험 계수 r_G 가 위험 랭킹들 내에 있는지를 판정한다.

[0069] 본 출원의 실시예에서, 위험 계수의 랭킹이 높을수록 활동 링크의 회소성 정도가 더 높고 그 위험 계수가 더 높다는 것을 나타낸다. 사전 설정된 위험 랭킹이 상위 3개라고 가정하면, 특정 활동 링크 G에 대응하는 위험 계수 r_G 가 상위 3개에 랭킹되어 있는지가 판정된다.

[0070] S143: 위험 계수 r_G 가 상위 3개에 랭킹되어 있으면, 특정 활동 링크 G는 위험하다고 결정한다.

[0071] 특정 활동 링크 G에 대응하는 위험 계수 r_G 가 상위 3개에 랭킹되어 있는 경우, 이는 특정 활동 링크 G가 위험하다는 것을 나타내고, 그 후, 특정 활동 링크 G를 위험성 있는 활동으로 공표하여 e-비즈니스 웹사이트의 고객 서비스 직원에게 그 활동 링크를 조작하지 않도록 고지할 수 있다.

[0072] S144: 위험 계수 r_G 가 상위 3개에 랭킹되어 있지 않으면, 특정 활동 링크 G는 위험하지 않다고 판정한다.

[0073] 특정 활동 링크 G에 대응하는 위험 계수 r_G 가 상위 3개에 랭킹되어 있지 않는 경우, 이는 특정 활동 링크 G가 위험하지 않다는 것을 나타낸다.

[0074] 도 7은 본 출원의 실시예에 따른 위험성 있는 활동을 식별하기 위한 장치의 개략적인 구조도이다. 동일한 아이디어에 기초하여, 이 장치는 다음을 포함한다:

[0075] 사용자의 활동 데이터를 취득하도록 구성된 취득 모듈(10);

[0076] 활동 데이터로부터 특정 활동 링크를 선택하도록 구성된 선택 모듈(20);

[0077] 활동 데이터에서 특정 활동 링크의 위험 계수를 결정하도록 구성된 결정 모듈(30); 및

[0078] 위험 계수에 따라, 특정 활동 링크가 위험한지를 판정하도록 구성된 판정 모듈(40).

[0079] 본 출원의 실시예에서, 선택 모듈(20)은 구체적으로:

[0080] 활동 데이터로부터, 특정 시구간에서의 단편 데이터를 선택하고;

[0081] 단편 데이터에 포함된 활동들을 취득하고;

[0082] 활동들을 발생 시간들에 따라 시간순으로 정렬하여 특정 활동 링크를 획득하도록 구성된다.

[0083] 본 출원의 실시예에서, 위험 계수는 단기 위험 계수, 이력 위험 계수, 및 팀 위험 계수 중 하나 이상을 포함한다.

[0084] 본 출원의 실시예에서, 결정 모듈(30)은 단기 위험 결정 모듈(31)을 포함하고, 이 단기 위험 결정 모듈(31)은:

[0085] 사용자가 제1 시구간에서 모든 활동 링크를 조작하는 총 조작 횟수를 취득하고;

[0086] 사용자가 제1 시구간에서 특정 활동 링크를 조작하는 조작 횟수를 취득하고;

[0087] 총 조작 횟수와 조작 횟수의 비를 결정하여 단기 위험 계수를 획득하도록 구성된다.

[0088] 본 출원의 실시예에서, 결정 모듈(30)은 이력 위험 결정 모듈(32)을 포함하고, 이 이력 위험 결정 모듈(32)은:

[0089] 등록 시간에서 현재 시간까지의 사용자에 대한 총 시간 길이를 취득하고;

[0090] 사용자가 특정 활동 링크를 조작하는 실제 시간 길이를 취득하고;

[0091] 총 시간 길이 및 실제 시간 길이에 따라 이력 위험 계수를 결정하도록 구성된다.

[0092] 본 출원의 실시예에서, 결정 모듈(30)은 팀 위험 결정 모듈(33)을 포함하고, 이 팀 위험 결정 모듈(33)은:

[0093] 사용자가 속하는 사용자 그룹에 포함된 총 사용자 수를 결정하고;

[0094] 사용자 그룹 내에서, 제2 시구간에서 특정 활동 링크를 조작한 실제 사용자 수를 취득하고;

[0095] 총 사용자 수 및 실제 사용자 수에 따라 팀 위험 계수를 결정하도록 구성된다.

- [0096] 본 출원의 실시예에서, 이력 위험 결정 모듈(32)은 제1 평활화 유닛을 포함하고, 이 제1 평활화 유닛은:
- [0097] 총 시간 길이와 실제 시간 길이를 평활화하여 평활화된 총 시간 길이 및 평활화된 실제 시간 길이를 획득하고;
- [0098] 평활화된 실제 시간 길이와 평활화된 총 시간 길이에 대해 계산을 수행하여 이력 위험 계수를 획득하도록 구성된다.
- [0099] 본 출원의 실시예에서, 팀 위험 결정 모듈(33)은 제2 평활화 유닛을 포함하고, 이 제2 평활화 유닛은:
- [0100] 총 사용자 수와 실제 사용자 수를 평활화하여 평활화된 총 사용자 수 및 평활화된 실제 사용자 수를 획득하고;
- [0101] 평활화된 총 사용자 수와 평활화된 실제 사용자 수에 대해 계산을 수행하여 팀 위험 계수를 획득하도록 구성된다.
- [0102] 본 출원의 실시예에서, 결정 모듈(30)은 구체적으로: 단기 위험 계수, 이력 위험 계수, 및 팀 위험 계수를 승산 또는 합산하여 위험 계수를 획득하도록 구성된다.
- [0103] 본 출원의 실시예에서, 판정 모듈(40)은 구체적으로:
- [0104] 활동 링크들의 위험 계수들을 내림차순으로 정렬하고;
- [0105] 특정 활동 링크에 대응하는 위험 계수가 위험 랭킹들 내에 있는지를 판정하고;
- [0106] 위험 계수가 위험 랭킹들 내에 있으면, 특정 활동 링크는 위험하다고 판정하고; 위험 계수가 위험 랭킹들 내에 있지 않으면, 특정 활동 링크는 위험하지 않다고 판정하도록 구성된다.
- [0107] 본 출원의 실시예들에서 제공된 방법 및 장치는 사용자의 활동 데이터를 취득하고, 활동 데이터로부터 특정 활동 링크를 선택하고; 활동 데이터에서 특정 활동 링크의 위험 계수를 계산에 의해 결정하고, 마지막으로, 위험 계수에 따라, 특정 활동 링크가 위험한지를 결정한다. 규칙 엔진 방식과 비교하여, 전술한 프로세스에서는, 규칙 취약점을 수동으로 교정할 필요가 없으므로, 활동 위험성 식별의 효율이 향상된다. 또한, 전술한 프로세스는 규칙 엔진이 여분의 컴퓨터 자원들을 소비하는 불리한 점을 회피하므로, 컴퓨터 시스템의 부담이 경감된다.
- [0108] 본 출원의 실시예들에서는 단기(예컨대, 특정 일), 이력(등록 시간에서 현재 시간까지) 및 팀(사용자가 속하는 사용자 그룹)의 3가지 요인을 포괄적으로 고려하여 사용자의 활동이 위험한지를 분석하므로, 사용자의 활동 링크에 대한 일부 갑작스러운 요인 전환(예컨대, 팀의 서비스 방향 조정 또는 사용자의 근무 부서 이동)의 영향이 감소되고, 따라서 위험성 있는 활동 식별의 정확도와 신뢰도가 향상된다.
- [0109] 이 명세서에서 개시된 위험성 있는 활동을 식별하기 위한 장치는 위험성 있는 활동을 식별하기 위한 방법에 기초한 동일한 아이디어에 따라 생성된다는 것은 언급할 만하다. 그러므로, 위험성 있는 활동을 식별하기 위한 방법은 위험성 있는 활동을 식별하기 위한 상기 장치의 모든 기술적 특징을 계속 사용할 수 있다. 세부 사항들은 여기에서 다시 설명하지 않는다.
- [0110] 또한, 본 출원에서 위험 계수들을 계산하기 위한 공식들은 개시된 실시예들로 한정되지 않는다는 점에 주목해야 한다. 예를 들어, 다른 실시예들에서, 단기 위험 계수 $a=s_2/s_1$ 이고; 이력 위험 계수 $b=(1+lg t_2)/(1+lg t_3)$ 이고; 팀 위험 계수 $c=(1+lgm)/(1+lgm)$ 이다. 상응하여, 활동 링크가 위험한지를 후속 판정하는 동안, 활동 링크들의 위험 계수들을 오름차순으로 정렬하여 특정 활동 링크에 대응하는 위험 계수가 위험 랭킹들 내에 있는지를 판정한다.
- [0111] 이 기술분야의 기술자들은 본 발명의 실시예들이 방법, 시스템, 또는 컴퓨터 프로그램 제품으로서 제공될 수 있음을 이해해야 한다. 따라서, 본 발명은 완전한 하드웨어 실시예, 완전한 소프트웨어 실시예, 또는 소프트웨어와 하드웨어를 결합한 실시예의 형태로 구현될 수 있다. 또한, 본 발명은 컴퓨터 사용 가능한 프로그램 코드를 포함하는 하나 이상의 컴퓨터 사용 가능한 저장 매체(자기 디스크 메모리, CD-ROM, 광학 메모리 등을 포함하지만 이에 한정되지는 않음) 상에 구현된 컴퓨터 프로그램 제품의 형태를 이용할 수 있다.
- [0112] 본 발명은 본 발명의 실시예들에 따른 방법, 디바이스(시스템), 및 컴퓨터 프로그램 제품의 호름도들 및/또는 블록도들을 참조하여 설명된다. 호름도들 및/또는 블록도들에서의 각각의 프로세스 및/또는 블록 및 호름도들 및/또는 블록도들에서의 프로세스 및/또는 블록의 조합을 구현하기 위해 컴퓨터 프로그램 명령들이 사용될 수 있다는 것을 이해해야 한다. 이들 컴퓨터 프로그램 명령들은 머신을 생성하기 위한 범용 컴퓨터, 특수 목적 컴퓨터, 임베디드 프로세서, 또는 또 다른 프로그램 가능 데이터 처리 디바이스의 프로세서에 제공될 수 있으며, 이에 따라 컴퓨터 또는 또 다른 프로그램 가능 데이터 처리 디바이스의 프로세서에 의해 실행되는 명령들은 호

름도들에서의 하나 이상의 프로세스 및/또는 블록도들에서의 하나 이상의 블록에서 특정 기능을 구현하기 위한 장치를 생성하게 된다.

[0113] 컴퓨터 또는 또 다른 프로그램 가능 데이터 처리 디바이스에게 특정 방식으로 동작하도록 지시할 수 있는 이들 컴퓨터 프로그램 명령들은 또한 컴퓨터 판독 가능 메모리에 저장될 수 있으며, 이에 따라 컴퓨터 판독 가능 메모리에 저장된 명령들은 명령 장치를 포함하는 제조 물품을 생성하게 된다. 명령 장치는 흐름도들에서의 하나 이상의 프로세스 및/또는 블록도들에서의 하나 이상의 블록에서 특정 기능을 구현한다.

[0114] 이들 컴퓨터 프로그램 명령들은 또한 컴퓨터 또는 또 다른 프로그램 가능 데이터 처리 디바이스 상에 로딩될 수 있으며, 이에 따라 일련의 동작 단계들이 컴퓨터 또는 다른 프로그램 가능 디바이스 상에서 수행됨으로써, 컴퓨터 구현 처리를 생성하게 된다. 따라서, 컴퓨터 또는 또 다른 프로그램 가능 디바이스에서 실행되는 명령들은 흐름도들에서의 하나 이상의 프로세스 및/또는 블록도들에서의 하나 이상의 블록에서 특정 기능을 구현하기 위한 단계들을 제공한다.

[0115] 전형적인 구성에서, 컴퓨팅 디바이스는 하나 이상의 프로세서(CPU), 입력/출력 인터페이스, 네트워크 인터페이스, 및 메모리를 포함한다.

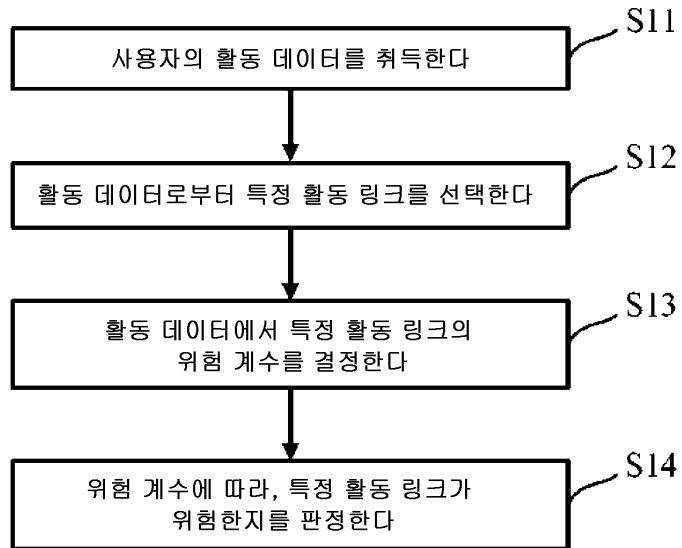
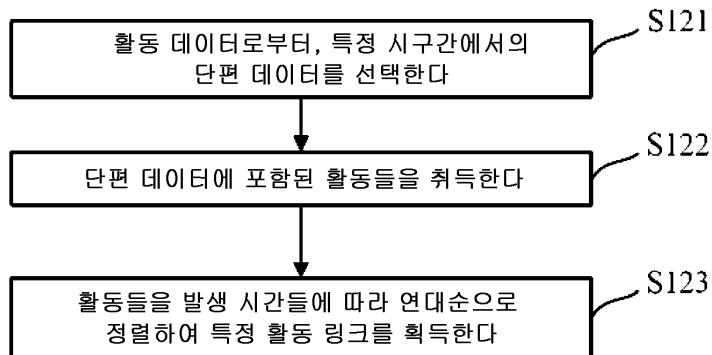
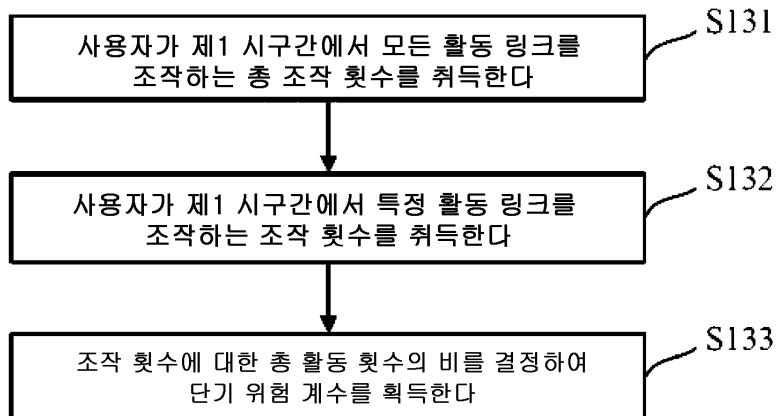
[0116] 메모리는 컴퓨터 판독 가능 매체, 예를 들어 판독 전용 메모리(ROM) 또는 플래시 RAM에서 회발성 메모리, 랜덤 액세스 메모리(RAM) 및/또는 비회발성 메모리 등을 포함할 수 있다. 메모리는 컴퓨터 판독 가능 매체의 예이다.

[0117] 컴퓨터 판독 가능 매체는 비회발성 또는 회발성, 이동식 또는 비이동식 매체를 포함하며, 임의의 방법 또는 기술에 의해 정보 저장을 구현할 수 있다. 정보는 컴퓨터 판독 가능 명령, 데이터 구조, 및 프로그램 또는 다른 데이터의 모듈일 수 있다. 컴퓨터의 저장 매체는, 예를 들어, 상변화 메모리(PRAM), 정적 랜덤 액세스 메모리(SRAM), 동적 랜덤 액세스 메모리(DRAM), 다른 유형의 랜덤 액세스 메모리(RAM), 판독 전용 메모리(ROM), 전기적으로 소거 가능한 프로그램 가능 판독 전용 메모리(EEPROM), 플래시 메모리 또는 다른 메모리 기술들, 컴팩트 디스크 판독 전용 메모리(CD-ROM), 디지털 다용도 디스크(DVD) 또는 다른 광학 저장 장치, 카세트 테이프, 자기 테이프/자기 디스크 저장 장치 또는 다른 자기 저장 장치, 또는 임의의 다른 비전송 매체를 포함하지만, 이들로 한정되지 않으며, 컴퓨팅 디바이스에 의해 액세스 가능한 정보를 저장하는 데 사용될 수 있다. 본 문서의 정의에 따르면, 컴퓨터 판독 가능 매체는 변조된 데이터 신호 및 반송파와 같은 같은 일시적인 매체를 포함하지 않는다.

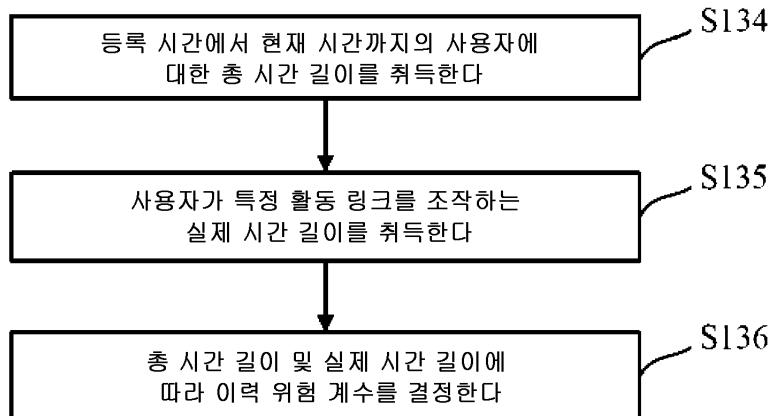
[0118] "포함한다", "구비한다"라는 용어들, 또는 임의의 그의 변형어들은 비배타적인 포함을 포괄하도록 의도된 것이며, 이에 따라 일련의 요소들을 포함하는 프로세스, 방법, 상품 또는 디바이스는 그러한 요소를 포함할 뿐만 아니라 명시적으로 특정되지 않은 다른 요소들도 포함하거나, 또는 프로세스, 방법, 상품 또는 디바이스의 고유 요소들을 더 포함할 수 있다. 더 많은 제한이 없다면, "...를 포함한다"라는 문구에 의해 한정되는 요소는 해당 요소를 포함하는 프로세스, 방법, 상품, 또는 디바이스에 존재하는 다른 동일한 요소들을 배제하지 않는다.

[0119] 이 기술분야의 기술자들은 본 출원의 실시예들이 방법, 시스템, 또는 컴퓨터 프로그램 제품으로서 제공될 수 있음을 이해해야 한다. 따라서, 본 출원은 완전한 하드웨어 실시예, 완전한 소프트웨어 실시예, 또는 소프트웨어와 하드웨어를 결합한 실시예의 형태로 구현될 수 있다. 또한, 본 출원은 컴퓨터 사용 가능한 프로그램 코드를 포함하는 하나 이상의 컴퓨터 사용 가능한 저장 매체(자기 디스크 메모리, CD-ROM, 광학 메모리 등을 포함하지만 이에 한정되지는 않음) 상에 구현된 컴퓨터 프로그램 제품의 형태를 이용할 수 있다.

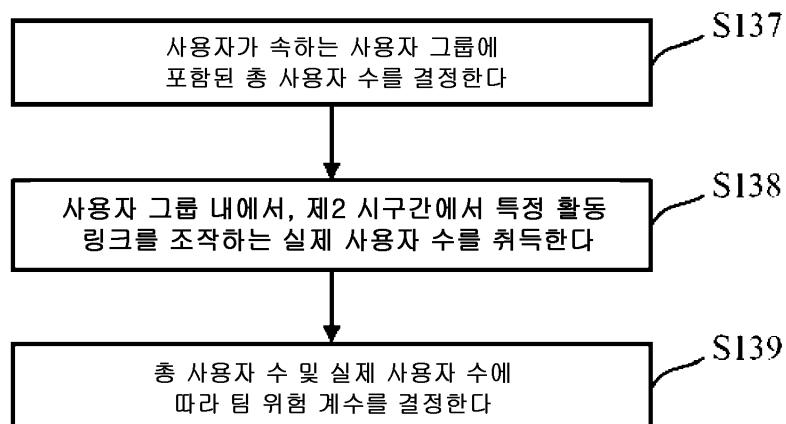
[0120] 상기 내용은 본 출원의 실시예들에 불과하며, 본 출원을 한정하기 위해 이용되지 않는다. 이 기술분야의 기술자들에게, 본 출원은 다양한 변화 및 변경을 가질 수 있다. 본 출원의 정신 및 원리에서 이루어지는 임의의 수정, 동등한 대체, 및 개선은 본 출원의 청구항들의 범위에 포함되어야 한다.

도면**도면1****도면2****도면3**

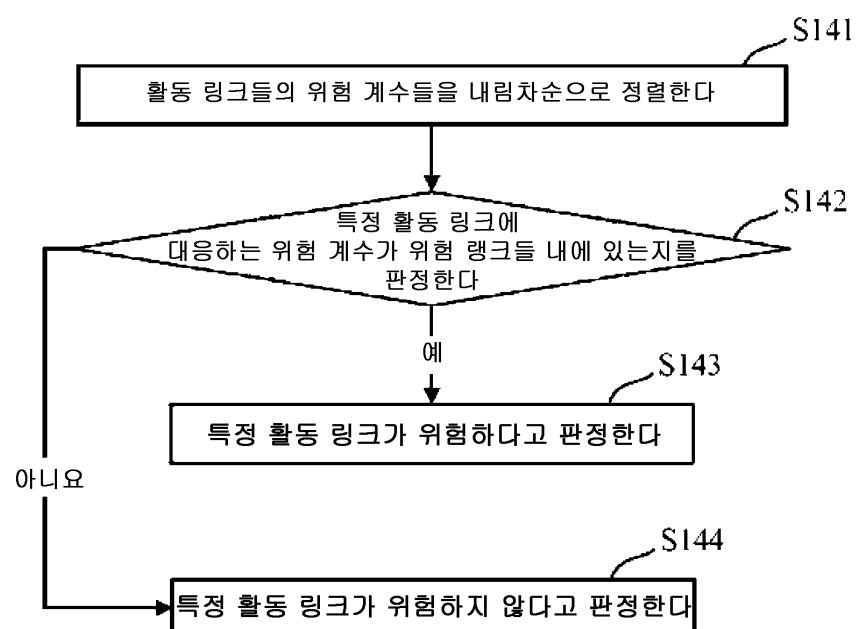
도면4



도면5



도면6



도면7

