(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년12월19일
(11) 등록번호 10-2057565
(24) 등록일자 2019년12월13일

(51) 국제특허분류(Int. Cl.)
G06F 21/56 (2013.01) *G06F 21/55* (2013.01)
(21) 출원번호 10-2014-7029226
(22) 출원일자(국제) 2013년03월14일
심사청구일자 2018년02월27일
(85) 번역문제출일자 2014년10월17일
(65) 공개번호 10-2014-0137003
(43) 공개일자 2014년12월01일
(86) 국제출원번호 PCT/US2013/031184
(87) 국제공개번호 WO 2013/142228
국제공개일자 2013년09월26일
(30) 우선권주장
13/424,251 2012년03월19일 미국(US)
(56) 선행기술조사문헌
JP2012008777 A*
KR1020090005934 A*
US20040187023 A1
US20070074289 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
흐시아오, 흐수-춘
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
덩, 수오
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(뒷면에 계속)
(74) 대리인
특허법인 남앤남

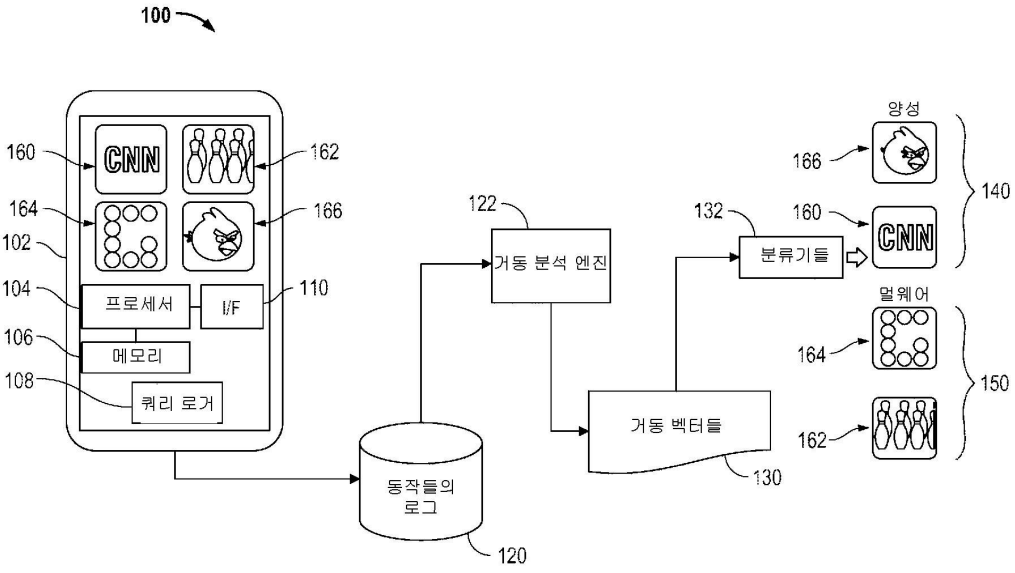
전체 청구항 수 : 총 32 항 심사관 : 윤혜숙

(54) 발명의 명칭 **멀웨어를 검출하기 위한 컴퓨팅 디바이스**

(57) 요 약

컴퓨팅 디바이스가 애플리케이션이 멀웨어인지를 결정하기 위한 장치 및 방법이 기재된다. 컴퓨팅 디바이스는, 로그를 생성하기 위해 컴퓨팅 디바이스 상의 애플리케이션의 거동을 로깅하기 위한 쿼리 로거; 애플리케이션의 거동을 특성화하는 거동 벡터를 생성하기 위해 쿼리 로거로부터의 로그를 분석하기 위한 거동 분석 엔진; 및 애플리케이션에 대한 거동 벡터를 양성 또는 멀웨어로서 분류하기 위한 분류기를 포함할 수도 있다.

대 표 도



(72) 발명자

사라마트, 바박

미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775

굽타, 라자쉬

미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775

명 세 서

청구범위

청구항 1

컴퓨팅 디바이스로서,

상기 컴퓨팅 디바이스 상의 복수의 애플리케이션들 각각에 대한 동작들을 동작들의 로그(log)에 로깅하는 것;

상기 동작들의 로그에 레코딩된 동작들에 기초하여 그리고 각각의 거동 벡터가 자신의 연관된 애플리케이션의 거동을 특성화하도록, 상기 복수의 애플리케이션들의 각각의 애플리케이션에 대한 거동 벡터를 생성하는 것; 및

각각의 거동 벡터에 의해 특성화된 거동이 양성(benign)인지를 결정하는 것

을 포함하는 동작들을 수행하도록 프로세서-실행가능 명령들을 이용하여 구성된 프로세서를 포함하고,

상기 프로세서는, 상기 각각의 애플리케이션에 대한 거동 벡터를 생성하는 것이, 상기 동작들의 로그의 쿼리들의 세트에 기초하여 각각의 거동 벡터를 생성하는 것을 포함하게 하기 위한 동작들을 수행하도록 프로세서-실행가능 명령들을 이용하여 구성되는, 컴퓨팅 디바이스.

청구항 2

제 1 항에 있어서,

상기 프로세서는, 상기 애플리케이션과 연관된 거동 벡터에 의해 특성화된 거동이 양성이 아니라고 결정하는 것에 응답하여, 애플리케이션을 삭제하거나 사용을 제한하는 것을 더 포함하는 동작들을 수행하도록 프로세서-실행가능 명령들을 이용하여 구성되는, 컴퓨팅 디바이스.

청구항 3

삭제

청구항 4

제 1 항에 있어서,

상기 프로세서는, 상기 동작들의 로그의 쿼리들의 세트에 기초하여 상기 거동 벡터를 생성하는 것이, 자신의 연관된 애플리케이션에 대한 동작들의 로그의 쿼리의 결과에 기초하여 수치값을 포함하도록 각각의 거동 벡터를 생성하는 것을 포함하게 하기 위한 동작들을 수행하도록 프로세서-실행가능 명령들을 이용하여 구성되는, 컴퓨팅 디바이스.

청구항 5

제 1 항에 있어서,

상기 프로세서는, 상기 동작들의 로그의 쿼리들의 세트에 기초하여 상기 거동 벡터를 생성하는 것이, 존재(existence) 쿼리, 양(amount) 쿼리, 순서 쿼리, 및 카테고리 쿼리 중 적어도 하나에 기초하여 각각의 거동 벡터를 생성하는 것을 포함하게 하기 위한 동작들을 수행하도록 프로세서-실행가능 명령들을 이용하여 구성되는, 컴퓨팅 디바이스.

청구항 6

제 5 항에 있어서,

상기 프로세서는, 상기 동작들의 로그의 쿼리들의 세트에 기초하여 각각의 거동 벡터를 생성하는 것이, 관측된 거동 또는 예상된 거동을 포함하는 쿼리에 기초하여 상기 거동 벡터들 중 적어도 하나를 생성하는 것을 더 포함하게 하기 위한 동작들을 수행하도록 프로세서-실행가능 명령들을 이용하여 구성되는, 컴퓨팅 디바이스.

청구항 7

제 1 항에 있어서,

상기 프로세서는, 상기 동작들의 로그의 쿼리들의 세트에 기초하여 상기 거동 벡터를 생성하는 것이, 디바이스-독립적인 동작들을 분석하는 것을 포함하게 하기 위한 동작들을 수행하도록 프로세서-실행가능 명령들을 이용하여 구성되는, 컴퓨팅 디바이스.

청구항 8

제 1 항에 있어서,

상기 프로세서는, 상기 동작들의 로그의 쿼리들의 세트에 기초하여 상기 거동 벡터를 생성하는 것이, 디바이스-종속적인 동작들을 분석하는 것을 포함하게 하기 위한 동작들을 수행하도록 프로세서-실행가능 명령들을 이용하여 구성되는, 컴퓨팅 디바이스.

청구항 9

제 8 항에 있어서,

상기 프로세서는, 상기 디바이스-종속적인 동작들을 분석하는 것이, 애플리케이션 인스톨레이션 정보, 디바이스 정보, 통신 정보, 및 사용자 상호작용 정보를 분석하는 것을 더 포함하게 하기 위한 동작들을 수행하도록 프로세서-실행가능 명령들을 이용하여 구성되는, 컴퓨팅 디바이스.

청구항 10

컴퓨팅 디바이스로서,

상기 컴퓨팅 디바이스 상의 복수의 애플리케이션들 각각에 대한 동작들을 동작들의 로그에 로깅하는 것;

상기 동작들의 로그에 레코딩된 동작들에 기초하여 그리고 각각의 거동 벡터가 자신의 연관된 애플리케이션의 거동을 특성화하도록, 상기 복수의 애플리케이션들의 각각의 애플리케이션에 대한 거동 벡터를 생성하는 것; 및

각각의 거동 벡터에 의해 특성화된 거동이 양성인지를 결정하는 것

을 포함하는 동작들을 수행하도록 프로세서-실행가능 명령들을 이용하여 구성된 프로세서를 포함하고,

상기 프로세서는, 상기 각각의 거동 벡터에 의해 특성화된 거동이 양성인지를 결정하는 것이, 알려진-양호한 애플리케이션들의 세트 및 알려진-불량한 애플리케이션들의 세트를 사용하는 것으로부터 획득된 정보에 대해 트레이닝된(trained) 분류기 모델을 적어도 하나의 거동 벡터에 적용하는 것을 포함하게 하기 위한 동작들을 수행하도록 프로세서-실행가능 명령들을 이용하여 구성되는, 컴퓨팅 디바이스.

청구항 11

제 1 항에 있어서,

상기 컴퓨팅 디바이스는 모바일 디바이스인, 컴퓨팅 디바이스.

청구항 12

컴퓨팅 디바이스에서 동작하는 애플리케이션이 양성인지를 결정하는 방법으로서,

복수의 애플리케이션들 각각에 대한 동작들을 동작들의 로그에 로깅하는 단계;

상기 동작들의 로그에 레코딩된 동작들에 기초하여 그리고 각각의 거동 벡터가 자신의 연관된 애플리케이션의 거동을 특성화하도록, 상기 복수의 애플리케이션들의 각각의 애플리케이션에 대한 거동 벡터를 생성하는 단계; 및

각각의 거동 벡터에 의해 특성화된 거동이 양성인지를 결정하는 단계를 포함하고,

상기 각각의 애플리케이션에 대한 거동 벡터를 생성하는 단계는, 상기 동작들의 로그의 쿼리들의 세트에 기초하

여 각각의 거동 벡터를 생성하는 단계를 포함하는, 컴퓨팅 디바이스에서 동작하는 애플리케이션이 양성인지를 결정하는 방법.

청구항 13

제 12 항에 있어서,

상기 애플리케이션과 연관된 거동 벡터에 의해 특성화된 거동이 양성이 아니라고 결정하는 것에 응답하여, 애플리케이션을 삭제하거나 사용을 제한하는 단계를 더 포함하는, 컴퓨팅 디바이스에서 동작하는 애플리케이션이 양성인지를 결정하는 방법.

청구항 14

삭제

청구항 15

제 12 항에 있어서,

상기 동작들의 로그의 쿼리들의 세트에 기초하여 상기 거동 벡터를 생성하는 단계는, 자신의 연관된 애플리케이션에 대한 동작들의 로그의 쿼리의 결과에 기초하여 수치값을 포함하도록 각각의 거동 벡터를 생성하는 단계를 포함하는, 컴퓨팅 디바이스에서 동작하는 애플리케이션이 양성인지를 결정하는 방법.

청구항 16

제 12 항에 있어서,

상기 동작들의 로그의 쿼리들의 세트에 기초하여 상기 거동 벡터를 생성하는 단계는, 존재 쿼리, 양 쿼리, 순서 쿼리, 및 카테고리 쿼리 중 적어도 하나에 기초하여 각각의 거동 벡터를 생성하는 단계를 포함하는, 컴퓨팅 디바이스에서 동작하는 애플리케이션이 양성인지를 결정하는 방법.

청구항 17

제 16 항에 있어서,

상기 동작들의 로그의 쿼리들의 세트에 기초하여 각각의 거동 벡터를 생성하는 단계는, 관측된 거동 또는 예상된 거동을 포함하는 쿼리에 기초하여 상기 거동 벡터들 중 적어도 하나를 생성하는 단계를 더 포함하는, 컴퓨팅 디바이스에서 동작하는 애플리케이션이 양성인지를 결정하는 방법.

청구항 18

제 12 항에 있어서,

상기 동작들의 로그의 쿼리들의 세트에 기초하여 상기 거동 벡터를 생성하는 단계는, 디바이스-독립적인 동작들을 분석하는 단계를 포함하는, 컴퓨팅 디바이스에서 동작하는 애플리케이션이 양성인지를 결정하는 방법.

청구항 19

제 12 항에 있어서,

상기 동작들의 로그의 쿼리들의 세트에 기초하여 상기 거동 벡터를 생성하는 단계는, 디바이스-종속적인 동작들을 분석하는 단계를 포함하는, 컴퓨팅 디바이스에서 동작하는 애플리케이션이 양성인지를 결정하는 방법.

청구항 20

제 19 항에 있어서,

상기 디바이스-종속적인 동작들을 분석하는 단계는, 애플리케이션 인스톨레이션, 디바이스 정보, 통신들, 및 사용자 상호작용을 분석하는 단계를 더 포함하는, 컴퓨팅 디바이스에서 동작하는 애플리케이션이 양성인지를 결정하는 방법.

청구항 21

프로세서-실행가능 소프트웨어 명령들이 저장된 비-일시적인 컴퓨터 판독가능 저장 매체로서,

상기 프로세서-실행가능 소프트웨어 명령들은 컴퓨팅 디바이스의 프로세서로 하여금,

복수의 애플리케이션들 각각에 대한 동작들을 동작들의 로그에 로깅하는 것;

상기 동작들의 로그에 레코딩된 동작들에 기초하여 그리고 각각의 거동 벡터가 자신의 연관된 애플리케이션의 거동을 특성화하도록, 상기 복수의 애플리케이션들의 각각의 애플리케이션에 대한 거동 벡터를 생성하는 것; 및

각각의 거동 벡터에 의해 특성화된 거동이 양성인지를 결정하는 것

을 포함하는 동작들을 수행하게 하도록 구성되고,

상기 저장된 프로세서-실행가능 소프트웨어 명령들은 프로세서로 하여금,

상기 각각의 애플리케이션에 대한 거동 벡터를 생성하는 것이, 상기 동작들의 로그의 쿼리들의 세트에 기초하여 각각의 거동 벡터를 생성하는 것을 포함하게 하기 위한 동작들을 수행하게 하도록 구성되는, 비-일시적인 컴퓨터 판독가능 저장 매체.

청구항 22

제 21 항에 있어서,

상기 저장된 프로세서-실행가능 소프트웨어 명령들은 프로세서로 하여금,

상기 애플리케이션과 연관된 거동 벡터에 의해 특성화된 거동이 양성이 아니라고 결정하는 것에 응답하여, 애플리케이션을 삭제하거나 사용을 제한하는 것을 더 포함하는 동작들을 수행하게 하도록 구성되는, 비-일시적인 컴퓨터 판독가능 저장 매체.

청구항 23

삭제

청구항 24

제 21 항에 있어서,

상기 저장된 프로세서-실행가능 소프트웨어 명령들은 프로세서로 하여금,

상기 동작들의 로그의 쿼리들의 세트에 기초하여 상기 거동 벡터를 생성하는 것이, 존재 쿼리, 양 쿼리, 순서 쿼리, 및 카테고리 쿼리 중 적어도 하나에 기초하여 각각의 거동 벡터를 생성하는 것을 포함하게 하기 위한 동작들을 수행하게 하도록 구성되는, 비-일시적인 컴퓨터 판독가능 저장 매체.

청구항 25

제 24 항에 있어서,

상기 저장된 프로세서-실행가능 소프트웨어 명령들은 프로세서로 하여금,

상기 동작들의 로그의 쿼리들의 세트에 기초하여 각각의 거동 벡터를 생성하는 것이, 관측된 거동 또는 예상된 거동을 포함하는 쿼리에 기초하여 상기 거동 벡터들 중 적어도 하나를 생성하는 것을 포함하게 하기 위한 동작들을 수행하게 하도록 구성되는, 비-일시적인 컴퓨터 판독가능 저장 매체.

청구항 26

제 21 항에 있어서,

상기 저장된 프로세서-실행가능 소프트웨어 명령들은 프로세서로 하여금,

상기 동작들의 로그의 쿼리들의 세트에 기초하여 상기 거동 벡터를 생성하는 것이, 디바이스-독립적인 동작들을 분석하는 것을 포함하게 하기 위한 동작들을 수행하게 하도록 구성되는, 비-일시적인 컴퓨터 판독가능 저장 매체.

청구항 27

제 21 항에 있어서,

상기 저장된 프로세서-실행가능 소프트웨어 명령들은 프로세서로 하여금,

상기 동작들의 로그의 쿼리들의 세트에 기초하여 상기 거동 벡터를 생성하는 것이, 디바이스-종속적인 동작들을 분석하는 것을 포함하게 하기 위한 동작들을 수행하게 하도록 구성되는, 비-일시적인 컴퓨터 판독가능 저장 매체.

청구항 28

제 27 항에 있어서,

상기 저장된 프로세서-실행가능 소프트웨어 명령들은 프로세서로 하여금,

상기 디바이스-종속적인 동작들을 분석하는 것이, 애플리케이션 인스톨레이션, 디바이스 정보, 통신들, 및 사용자 상호작용을 분석하는 것을 포함하게 하기 위한 동작들을 수행하게 하도록 구성되는, 비-일시적인 컴퓨터 판독가능 저장 매체.

청구항 29

컴퓨팅 디바이스로서,

복수의 애플리케이션들 각각에 대한 동작들을 동작들의 로그에 로깅하기 위한 수단;

상기 동작들의 로그에 레코딩된 동작들에 기초하여 그리고 각각의 거동 벡터가 자신의 연관된 애플리케이션의 거동을 특성화하도록, 상기 복수의 애플리케이션들의 각각의 애플리케이션에 대한 거동 벡터를 생성하기 위한 수단; 및

각각의 거동 벡터에 의해 특성화된 거동이 양성인지를 결정하기 위한 수단을 포함하고,

상기 각각의 애플리케이션에 대한 거동 벡터를 생성하기 위한 수단은, 상기 동작들의 로그의 쿼리들의 세트에 기초하여 각각의 거동 벡터를 생성하기 위한 수단을 포함하는, 컴퓨팅 디바이스.

청구항 30

제 29 항에 있어서,

상기 애플리케이션과 연관된 거동 벡터에 의해 특성화된 거동이 양성이 아니라고 결정하는 것에 응답하여, 애플리케이션을 삭제하거나 사용을 제한하기 위한 수단을 더 포함하는, 컴퓨팅 디바이스.

청구항 31

삭제

청구항 32

제 29 항에 있어서,

상기 동작들의 로그의 쿼리들의 세트에 기초하여 상기 거동 벡터를 생성하기 위한 수단은, 존재 쿼리, 양 쿼리, 순서 쿼리, 및 카테고리 쿼리 중 적어도 하나에 기초하여 각각의 거동 벡터를 생성하기 위한 수단을 포함하는, 컴퓨팅 디바이스.

청구항 33

제 32 항에 있어서,

상기 동작들의 로그의 쿼리들의 세트에 기초하여 각각의 거동 벡터를 생성하기 위한 수단은, 관측된 거동 또는 예상된 거동을 포함하는 쿼리에 기초하여 상기 거동 벡터들 중 적어도 하나를 생성하기 위한 수단을 더 포함하는, 컴퓨팅 디바이스.

청구항 34

제 29 항에 있어서,

상기 동작들의 로그의 쿼리들의 세트에 기초하여 상기 거동 벡터를 생성하기 위한 수단은, 디바이스-독립적인 동작들을 분석하기 위한 수단을 포함하는, 컴퓨팅 디바이스.

청구항 35

제 29 항에 있어서,

상기 동작들의 로그의 쿼리들의 세트에 기초하여 상기 거동 벡터를 생성하기 위한 수단은, 디바이스-종속적인 동작들을 분석하기 위한 수단을 포함하는, 컴퓨팅 디바이스.

청구항 36

제 35 항에 있어서,

상기 디바이스-종속적인 동작들을 분석하기 위한 수단은, 애플리케이션 인스톨레이션, 디바이스 정보, 통신들, 및 사용자 상호작용을 분석하기 위한 수단을 포함하는, 컴퓨팅 디바이스.

청구항 37

삭제

청구항 38

삭제

청구항 39

삭제

청구항 40

삭제

청구항 41

삭제

청구항 42

삭제

청구항 43

삭제

청구항 44

삭제

청구항 45

삭제

청구항 46

삭제

청구항 47

삭제

청구항 48

삭제

청구항 49

삭제

청구항 50

삭제

청구항 51

삭제

청구항 52

삭제

청구항 53

삭제

청구항 54

삭제

청구항 55

삭제

청구항 56

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 일반적으로, 애플리케이션이 멀웨어(malware)인지를 검출할 수 있는 컴퓨팅 디바이스에 관한 것이다.

배 경 기 술

[0002] 컴퓨팅 디바이스들은, 많은 소스들로부터 유래하는 다양한 애플리케이션들을 구동시키는데 종종 사용된다. 불운하게도, 악성 의도(malicious intent)(예를 들어, 멀웨어)를 갖는 애플리케이션들이 사용자의 컴퓨팅 디바이스 상으로 종종 인스톨된다. 악성 애플리케이션들이 잘 알려진 애플리케이션들로서 종종 가장(masquerade)하기 때문에, 통상적으로, 사용자들은 이것을 인식하지 못한다. 추가적으로, 이들 악성 애플리케이션들은, 그들의 기능들에 필요한 것보다 더 많은 승인들을 이용한다.

[0003] 멀웨어와 같은 보안 위협들로부터 컴퓨팅 디바이스들을 보호하는 것은, 현대의 컴퓨팅 디바이스들에 대한 관심사이다. 멀웨어는, 컴퓨팅 디바이스 또는 사용자에게 손상을 입히기를 시도하는 원치않는 애플리케이션들을 포함한다. 상이한 타입들의 멀웨어는, 트로잔(trojan)들, 웜(worm)들, 키로거(keylogger)들, 바이러스들, 백도어들 및 스파이웨어를 포함한다. 멀웨어 개발자들은, 신용카드 번호들 및 은행 계좌 번호들과 같은 개인 정보를 수집하거나 셀 전화기가 유료 서비스들에 접속하게 하려는 소망에 의해 동기를 부여받는다. 따라서, 검출을 피하기 위해 더 정교한 방법들을 개발하려는 금전적인 인센티브가 동기가 되는 멀웨어 개발자들이 존재한다.

[0004] 종래의 멀웨어 서명 검출 방법들은, 타겟 애플리케이션의 실제 실행가능한 부분의 불변(invariant) 부분으로부터 서명들을 추출한다. 서명-기반 멀웨어 검출은, 각각의 멀웨어 변형에 대해 서명(예를 들어, 멀웨어의 코드에서의 고유한 패턴)을 요구한다. 따라서, 서명-기반 멀웨어 검출을 이용하는 알려지지 않은 멀웨어를 검출하는 것은 불가능하다. 부가적으로, 알려진 멀웨어에 대해서도, 서명의 검출과 그 서명이 컴퓨팅 디바이스 상에서 실제로 업데이트되는 시간 사이에 지연이 있는 경향이 있다. 추가적으로, 서명들을 사용하는 멀웨어 체크는 종종 프로세서 및 메모리 집중적이다. 이것은 특히, 모바일 컴퓨팅 디바이스들에 더 어렵다. 또한, 서명 체크

가 셀 전화기들과 같은 모바일 디바이스들 상에서 고가이기 때문에, 많은 검출기들은 잘 알려진 도둑(rogue) 애플리케이션들에 대한 애플리케이션 파일명칭들을 간단히 체크한다.

[0005] 이들 이슈들 때문에, 애플리케이션들이 멀웨어인지를 결정하기 위해 컴퓨팅 디바이스 상에서 애플리케이션들을 특성화, 비교 및 분류하려는 목적을 위해 거동(behavior) 분석을 이용하는 것이 유익할 것이며, 이는 프로세서 및 메모리 덜 집중적이고, 훨씬 더 신속한 방식으로 발생할 수 있다.

발명의 내용

[0006] 본 발명의 양상들은, 컴퓨팅 디바이스 애플리케이션이 멀웨어인지를 결정하기 위한 장치 및 방법에 관한 것일 수도 있다. 컴퓨팅 디바이스는, 로그(log)를 생성하기 위해 컴퓨팅 디바이스 상의 애플리케이션의 거동을 로깅하기 위한 쿼리 로거; 애플리케이션의 거동을 특성화하는 거동 벡터를 생성하기 위해 쿼리 로거로부터의 로그를 분석하기 위한 거동 분석 엔진; 및 애플리케이션에 대한 거동 벡터를 양성(benign) 또는 멀웨어로서 분류하기 위한 분류기를 포함할 수도 있다.

[0007] 본 발명의 양상들은 또한, 서버가 애플리케이션이 컴퓨팅 디바이스에 대한 멀웨어인지를 결정하기 위한 장치 및 방법에 관한 것일 수도 있다. 서버는, 복수의 컴퓨팅 디바이스들로부터 복수의 거동 벡터 세트들을 수신하기 위한 프로세싱 회로 – 각각의 거동 벡터 세트는 애플리케이션의 거동을 특성화할 수도 있음 –; 및 거동 분석 엔진을 포함할 수도 있다. 거동 분석 엔진은, 양성 또는 멀웨어로서의 수신된 거동 벡터 세트들에 기초하여 글로벌 분류기를 업데이트할 수도 있다.

도면의 간단한 설명

[0008] 도 1은, 본 발명의 양상들이 실시될 수도 있는 시스템의 블록도이다.

도 2는, 거동 분석 엔진 및 로그의 쿼리들의 세트에 기초하여 생성될 수도 있는 거동 벡터들을 도시한 블록도이다.

도 3은 쿼리들, 동작들, 및 동작 속성들의 예들을 도시한 표이다.

도 4는, 애플리케이션 코드 및 네이티브(native) 코드를 이용하여 컴퓨팅 디바이스 상에서 동작하는 애플리케이션을 도시한 블록도이다.

도 5는, 애플리케이션들이 양성 또는 멀웨어로서 식별되도록 애플리케이션의 거동을 특성화하는 거동 벡터들을 생성하기 위해 쿼리 로거로부터의 로그를 분석하기 위한 거동 분석 엔진을 이용하는 결과들을 도시한 표이다.

도 6은, 다수의 컴퓨팅 디바이스들로부터의 거동 리포트들을 어그리게이팅(aggregate)하기 위해 이용될 수도 있는 서버를 도시한 다이어그램이다.

발명을 실시하기 위한 구체적인 내용

[0009] 단어 "예시적인" 또는 "예"는, "예, 예시, 또는 예증으로서 제공되는 것"을 의미하도록 본 명세서에서 사용된다. "예시적인" 것으로서 또는 "예"로서 본 명세서에 설명된 임의의 양상 또는 실시예는, 다른 양상들 또는 실시예들에 비해 반드시 바람직하거나 유리한 것으로서 해석될 필요는 없다.

[0010] 도 1을 참조하면, 도 1은, 본 발명의 양상들이 실시될 수도 있는 시스템(100)의 블록도이다. 특히, 시스템(100)은, 애플리케이션이 멀웨어인지를 결정하는데 사용될 수도 있는 컴퓨팅 디바이스(102)를 도시한다. 컴퓨팅 디바이스(102)는 쿼리 로거(108), 거동 분석 엔진(122), 및 분류기(132)를 포함할 수도 있다. 일 양상에서, 쿼리 로거(108)는, 로그(120)를 생성하기 위해 컴퓨팅 디바이스 상의 애플리케이션의 거동을 로깅할 수도 있다. 로그(120)는 애플리케이션으로 수행되거나 애플리케이션과 연관된 동작들의 로그일 수도 있다. 따라서, 동작들의 로그(120)는 애플리케이션의 거동을 나타낸다. 거동 분석 엔진(122)은, 애플리케이션의 거동을 특성화하는 거동 벡터들(130)을 생성하기 위해 쿼리 로거로부터의 로그(120)를 분석할 수도 있다. 분류기(132)는, 애플리케이션에 대한 거동 벡터들(130)을 양성(140) 또는 멀웨어(150)로서 분류할 수도 있다. 거동 벡터(130)가 멀웨어(150)로서 분류되면, 거동 벡터들(130)과 연관된 애플리케이션은 삭제되거나 사용이 제한될 수도 있다. 설명될 바와 같이, 많은 상이한 거동 벡터들(130)은 애플리케이션의 거동을 특성화하기 위해 생성될 수도 있으며, 이들에 기초하여, 분류기(132)는 양상(140) 또는 멀웨어(150)로서 애플리케이션을 분류할 수도 있다.

[0011] 컴퓨팅 디바이스(102)는, 프로세서(104), 메모리(106), 및 인터페이스(110)를 포함할 수도 있다. 컴퓨팅 디바

이스(102)가 디스플레이 디바이스, 사용자 인터페이스(예를 들어, 키보드, 터치-스크린 등), 전력 디바이스(예를 들어, 배터리) 뿐만 아니라 컴퓨팅 디바이스와 통상적으로 연관된 다른 컴포넌트들을 포함할 수도 있음을 인식해야 한다. 컴퓨팅 디바이스(102)는 모바일 디바이스 또는 비-모바일 디바이스일 수도 있다. 예를 들어, 인터페이스(110)는, 무선 네트워크로/로부터 무선 링크를 통해 호들 및 데이터를 송신 및 수신하기 위한 무선 트랜시버일 수도 있거나, 네트워크들(예를 들어, 인터넷)로의 직접 접속을 위한 유선 인터페이스일 수도 있다. 따라서, 컴퓨팅 디바이스(102)는, 모바일 디바이스, 무선 디바이스, 셀 전화기, 개인 휴대 정보 단말, 모바일 컴퓨터, 태블릿, 개인용 컴퓨터, 랩탑 컴퓨터, 서버 컴퓨터, 또는 임의의 타입의 컴퓨팅 디바이스일 수도 있다.

[0012] 컴퓨팅 디바이스(102)는, 쿼리 로거(108), 거동 분석 엔진(122), 및 분류기(132)를 구현하기 위한 명령들을 실행하도록 구성된 프로세서(104)를 포함할 수도 있다. 메모리(106)는, 프로세서(104)에 의한 실행을 위한 명령들을 저장하기 위해 프로세서(104)에 커플링될 수도 있다. 일 양상에서, 컴퓨팅 디바이스(102)는, 동작들의 로그(120)를 생성하기 위해 컴퓨팅 디바이스(102) 상의 애플리케이션의 거동을 로깅할 수도 있는 쿼리 로거(108); 애플리케이션의 거동을 특성화하는 거동 벡터들(130)을 생성하기 위해 쿼리 로거(108)로부터의 동작들의 로그(120)를 분석할 수도 있는 거동 분석 엔진(122); 및 양성(140) 또는 멀웨어(150)로서 애플리케이션에 대한 거동 벡터들(130)을 분류할 수도 있는 분류기(132)를 구현하기 위한 명령들을 실행하도록 구성된 프로세서(104)를 포함할 수도 있다. 거동 벡터(130)가 멀웨어(150)로서 분류되면, 거동 벡터들(130)과 연관된 애플리케이션은 컴퓨팅 디바이스(102)에 의해 삭제되거나 사용이 제한될 수도 있다.

[0013] 후술될 바와 같이, 본 발명이 양상들이, 컴퓨팅 디바이스(102)의 프로세서(104) 및/또는 컴퓨팅 디바이스(102)의 다른 회로 및/또는 다른 디바이스들에 의한 명령들의 실행과 함께 구현될 수도 있음을 인식해야 한다. 특히, 프로세서(104)를 포함하지만 이에 제한되지는 않는 컴퓨팅 디바이스(102)의 회로는 본 발명의 실시예들에 따라, 프로그램, 루틴, 또는 방법들 또는 프로세스들을 실행하기 위한 명령들의 실행의 제어 하에서 동작할 수도 있다. 예를 들어, 그러한 프로그램은 (예를 들어, 메모리(106) 및/또는 다른 위치들에 저장된) 펌웨어 또는 소프트웨어로 구현될 수도 있으며, 컴퓨팅 디바이스(102)의 프로세서(104)와 같은 프로세서들 및/또는 다른 회로에 의해 구현될 수도 있다. 추가적으로, 용어들 프로세서, 마이크로프로세서, 회로, 제어기 등이, 로직, 커맨드들, 명령들, 소프트웨어, 펌웨어, 기능 등을 실행할 수 있는 임의의 타입의 로직 또는 회로를 지칭함을 인식해야 한다.

[0014] 추가적으로, 쿼리 로거(108), 거동 분석 엔진(122), 및 분류기(132)의 기능들 중 몇몇 또는 전부가 컴퓨팅 디바이스(102) 그 자체에 의해 수행될 수도 있고 그리고/또는 기능들 중 몇몇 또는 전부가, 인터페이스(110)를 통해 (무선 또는 유선으로) 컴퓨팅 디바이스(102)에 접속된 다른 컴퓨팅 디바이스에 의해 수행될 수도 있음을 인식해야 한다. 따라서, 기능들 중 몇몇 및/또는 전부는, 다른 컴퓨팅 디바이스에 의해 수행될 수도 있으며, 결과들은 컴퓨팅 디바이스(102)로 다시 전달될 수도 있다. 또한, 특정한 양상들에 따르면, 분류기(132)는 머신 학습(learning) 분류기일 수도 있고, 컴퓨팅 디바이스(102)는 모바일 디바이스일 수도 있다.

[0015] 도 1에 도시된 바와 같이, 특정한 예를 참조하면, 4개의 애플리케이션들, 즉 뉴스 애플리케이션(160)(예를 들어, CNN), 게임(예를 들어, 볼링)(162), 게임(예를 들어, 스네이크)(164), 및 게임(예를 들어, 버드(bird))(166)이 (사용자의 동의로 또는 동의 없이) 컴퓨팅 디바이스(102)에 로딩될 수도 있다. 컴퓨팅 디바이스(102)는, 이들 애플리케이션들이 양성 또는 멀웨어인지를 자동적으로 결정할 수도 있다. 특히, 쿼리 로거(108)는, 동작들의 로그(120)를 생성하기 위해 컴퓨팅 디바이스 상의 애플리케이션들(160, 162, 164, 및 166)의 동작들 또는 거동을 로깅할 수도 있다. 거동 분석 엔진(122)은, 각각의 애플리케이션(160, 162, 164, 및 166)의 거동을 특성화하는 애플리케이션들 각각에 대한 거동 벡터들(130)을 생성하기 위하여 애플리케이션들 각각에 대한 동작들의 로그(120)를 분석할 수도 있다. 분류기(132)는, 양성(140) 또는 멀웨어(150)로서 애플리케이션들(160, 162, 164, 및 166) 각각에 대한 거동 벡터들(130)을 분류할 수도 있다. 이러한 예에서, 뉴스 애플리케이션(160) 및 게임 애플리케이션(166)은, 그들의 거동 벡터들(130)에 기초하여 양성(140)으로서 분류되며, 컴퓨팅 디바이스(102)에 의한 사용이 허용된다. 한편, 게임 애플리케이션들(162 및 164)은, 그들의 거동 벡터들(130)에 기초하여 멀웨어(150)로서 분류되며, 삭제되거나 컴퓨팅 디바이스(102)에 의한 사용이 제한된다. 쿼리 로거, 동작들의 로그, 거동 분석 엔진, 및 거동 벡터들의 양상들이 더 상세히 후술될 것이다.

[0016] 부가적으로 도 2를 참조하면, 거동 벡터들(130)은 동작들의 로그(120)의 쿼리들(210)의 세트에 기초하여 생성될 수도 있다. 거동 분석 엔진(122)은, 분류기가 애플리케이션에 대한 거동 벡터들(130)을 양성 또는 멀웨어로서 결정 및 분류할 수도 있도록 애플리케이션의 거동을 특성화하는 거동 벡터들(130)을 생성하기 위해, 쿼리들(210)에 기초하여 로그(120)에 의해 레코딩된 동작들을 분석할 수도 있다. 도 3을 또한 참조하면, 거동 분석 엔진(122)에 의해 이용될 수도 있는 쿼리들(310), 동작들(320), 및 동작 속성들(330)의 예들을 제공하는 챠트

(300)가 도시되어 있다.

[0017] 예를 들어, 쿼리들(310)의 세트는, 존재 쿼리, 양 쿼리, 순서 쿼리, 또는 카테고리 쿼리 중 적어도 하나 또는 그 초과를 포함할 수도 있다(블록(312)). 쿼리(310)는, 관측된 거동 또는 기대된 거동일 수도 있다. 추가적인 설명으로서, 거동 분석 엔진(122)은, 디바이스-의존적인 동작들(220) 및 디바이스-독립적인 동작들(222)을 분석할 수도 있다. 예들로서, 도 3에 도시된 바와 같이, 동작들(320)은, 애플리케이션 인스톨레이션(installation), 디바이스 정보, 통신들, 및 사용자 상호작용을 포함할 수도 있다. 추가적인 동작들(320)은, 액세스 디바이스 정보, 부트 시의 시작, 사용자 데이터, 패키지 인스톨레이션, 센서, 위치, 미디어, 카메라, SMS, 전화통화, 전화기 정보를 포함할 수도 있다(블록(322)). 또한, 시작 시간, 종료 시간, 이전, 이후, 존재와 같은 동작 속성들(330)이 거동 분석 엔진(122)에 의해 이용될 수도 있다(블록(332)). 이들이 거동 분석 엔진(122)에 의해 이용될 수도 있고, 많은 다른 타입들이 이용될 수도 있는 쿼리들, 동작들, 및 동작 속성들의 예들일 뿐임을 인식해야 한다.

[0018] 상술된 바와 같이, 3개의 컴포넌트들, 즉, 1) 동작들(120)의 로그를 생성하기 위해 컴퓨팅 디바이스(102) 상의 애플리케이션들의 거동을 로깅하기 위한 메커니즘들을 구현하는 쿼리 로거(108); 2) 동작들(120)의 로그를 분석하고, 컴퓨팅 디바이스(102) 상에서 구동하고 있는 애플리케이션들의 거동을 설명하는 거동 벡터들(130)을 생성하는 거동 분석 엔진(122); 및 3) 양성 또는 악성 카테고리 중 어느 하나로 거동 벡터들(130)을 분류하는 분류기(132)가 이용될 수도 있다.

[0019] 이러한 방식으로, 거동 벡터들(130)은, 컴퓨팅 디바이스들 상에서 멀웨어를 검출하기 위해 거동 분석 프레임워크에서 사용될 수도 있다. 결과적인 거동 벡터들(130)은, 로깅으로부터 추출된 객관적인 관측들을 포함한다. 일 예로서, 거동 분석 엔진(122)은 동작들(예를 들어, "사용자의 합의 없는 애플리케이션 인스톨레이션?", "애플리케이션이 게임과 같이 거동해야 하는가?", "웹사이트가 뉴스처럼 작동해야 하는가?", 애플리케이션이 SMS 메시지들을 프로세싱하고 있어야 하는가?", "애플리케이션이 전화통화들을 프로세싱하고 있어야 하는가?" 등)에 관해 쿼리들(210)에 대답(answer)한다. 이들 쿼리들(210)에 대한 대답들은 거동 벡터들(130)을 생성한다.

[0020] 예들로서, 각각의 작동은, 4개의 타입들의 쿼리들(310), 즉 존재 쿼리, 양 쿼리, 순서 쿼리, 및 카테고리 쿼리 중 하나 또는 그 초과와 연관될 수도 있다. 예를 들어, 존재 쿼리(310)는 동작 세트의 존재를 지칭할 수도 있다. 이러한 쿼리의 일 예로서, 쿼리는, 애플리케이션이 디바이스 정보에 액세스했는지(예를 들어, 액세스된 전화기 정보를 갖는지, 액세스된 위치 정보를 갖는지 등)를 결정할 것일 수도 있다. 거동 분석 엔진(122)은, 동작들(120)의 로그가 애플리케이션에 의한 디바이스 액세스 중 임의의 로그를 포함하는지를 결정할 수도 있으며, 거동 벡터(130)는 이에 기초하여 셋팅될 수도 있다. 예를 들어, 전화기 정보가 액세스되었다는 것을 표시하는 거동 벡터(130)가 셋팅될 수도 있다.

[0021] 추가적으로, 양 쿼리(310)는 동작들의 발생의 수를 지칭할 수도 있다. 이러한 쿼리의 일 예로서, 쿼리는, 애플리케이션에 의한 동작들의 발생의 수를 결정할 것일 수도 있다. 일 예로서, 이것은, 전송된 SMS(예를 들어, SMS를 통한 아웃고잉 통신)의 수일 수도 있다. 따라서, 거동 분석 엔진(122)은, 동작들(120)의 로그로부터 전송된 SMS의 수를 결정할 수도 있다. 이러한 쿼리는, 얼마나 많은 횟수들로 SMS가 전송되었는지를 표시하는 거동 벡터(130)를 생성하기 위해 사용될 수도 있다.

[0022] 다른 예로서, 순서 쿼리(310)는, 동작들의 시퀀스의 발생들의 수를 지칭할 수도 있다. 이러한 쿼리의 일 예로서, 쿼리는, 애플리케이션이 인스톨되었기 전에 (예를 들어, 인스톨레이션 전에 30초 내에서) 발생했던 사용자 상호작용들의 수를 결정할 것일 수도 있다. 따라서, 거동 분석 엔진(122)은, 애플리케이션이 동작들(120)의 로그로부터 인스톨되었기 전에 발생했던 사용자 상호작용들(예를 들어, UI 이벤트들)의 수를 결정할 수도 있다. 이러한 쿼리는, 애플리케이션 인스톨레이션 이전의 UI 이벤트들의 양을 표시하는 거동 벡터(130)를 생성하기 위해 사용될 수도 있다.

[0023] 다른 예로서, 카테고리 쿼리(310)는, 애플리케이션이 카테고리에 속하는지를 지칭할 수도 있다. 이러한 쿼리의 일 예로서, 쿼리는, 애플리케이션이 위치-기반 서비스인지를 결정할 것일 수도 있다. 따라서, 거동 분석 엔진(122)은, 애플리케이션이 동작들(120)의 로그로부터 위치-기반 서비스인지, 그리고 (로그에 기초하여) 위치 정보가 액세스되고 있는 카테고리에 그 애플리케이션이 속하는지를 결정할 수도 있다. 일 예로서, 이러한 쿼리는, 위치 정보가 리트리브(retrieve)되고 있는 횟수들에 관련된 거동 벡터(130)로서 사용될 수도 있다.

[0024] 추가적으로, 광범위하게 다양한 상이한 타입들의 동작들(320), 즉 애플리케이션 인스톨레이션, 디바이스 정보, 통신들, 사용자 상호작용, 액세스 디바이스 정보, 부트시의 시작, 사용자 데이터, 패키지 인스톨레이션, 센서,

위치, 미디어, 카메라, SMS, 전화통화, 및 전화기 정보(블록 322))가 거동 벡터들(130)을 생성하기 위하여 거동 분석 엔진(122)에 의해 이용될 수도 있다. 동작들(120)의 로그에 의해 레코딩된 바와 같은 이들 동작들 각각은, 애플리케이션의 거동을 특성화하는 거동 벡터(130)를 생성하기 위하여 거동 분석 엔진(122)에 의해 이용될 수도 있다. 또한, 광범위하게 다양한 상이한 타입들의 동작 속성들(330), 즉 시작 시간, 종료 시간, 이전, 이후, 및 존재(블록(332))는, 거동 벡터들(130)을 생성하기 위하여 거동 분석 엔진(122)에 의해 이용될 수도 있다. 동작들(120)의 로그에 의해 레코딩된 바와 같은 이들 동작 속성들 각각은, 애플리케이션의 거동을 특성화하는 거동 벡터(130)를 생성하는 것을 보조하기 위하여 거동 분석 엔진(122)에 의해 이용될 수도 있다.

[0025] 특히, 도 2에 도시된 바와 같이, 거동 벡터들(130)[1,0,0.207,0,2,5,...]은, 애플리케이션의 거동을 특성화하도록 동작들(120)의 로그에 의해 레코딩된 바와 같이, 쿼리들, 동작들, 동작 속성들 등에 기초하여 거동 분석 엔진(122)에 의해 생성될 수도 있다. 일 예로서, 상이한 타입들의 동작들에 대해, 약 5의 거동 벡터는 빈번한 사용을 지정할 수도 있고, 약 1-2의 거동 벡터는 드문(rare) 사용을 지정할 수도 있으며, 약 0의 거동 벡터는 사용없음을 지정할 수도 있다. 광범위하게 다양한 상이한 타입들의 애플리케이션들, 모니터링된 동작들, 및 거동 벡터들(130)을 생성하기 위한 거동 분석 엔진(122)에 의한 그들의 분석이 후술될 것이다.

[0026] 동작들(102)의 로그에 의해 레코딩된 바와 같이 그리고 거동 분석 엔진(122)에 의해 분석된 바와 같이, 관측된 동작들에 기초한 거동 벡터들(130)의 생성에 관해, 관측 또는 모니터링될 이들 동작들은, 그들이 멀웨어를 식별할 높은 가능성을 표현하기 때문에 모니터링되어야 하는 거동 또는 동작들의 타입들을 식별하는 것에 기초할 수도 있다. 예를 들어, 시스템 전문가들은, 멀웨어일 높은 가능성을 갖는 고레벨 거동들 또는 동작들에 어떤 세트의 시스템 이벤트들이 관련되는지를 식별할 수도 있다.

[0027] 도 4를 간단히 참조하면, 애플리케이션은 애플리케이션 코드(402) 및 네이티브 코드(404)를 이용하여 컴퓨팅 디바이스(102) 상에서 동작하고 있을 수도 있다. 애플리케이션 코드(402)는 애플리케이션 라이브러리들(412)과 상호작용하고, 네이티브 코드(404)는, 네이티브 라이브러리들(414) 및 컴퓨팅 디바이스(102)의 시스템 인터페이스의 커널(416)과 상호작용할 수도 있다. 네이티브 코드(404)는 애플리케이션 및 애플리케이션 코드(402)로 하여금, 네이티브 라이브러리들(414) 및 커널(416)의 하부(underlying) 기능들을 이용하게 할 수도 있다. 특히, 하부 기능들은 애플리케이션으로 하여금, 센서들(420)(예를 들어, 가속도계들, 압력 센서들 등), SMS 전화통화들(422), 연락처 리스트(424), 위치 센서(426), 네트워크 인터페이스(428) 등과 같은 컴퓨팅 디바이스(102)의 리소스들 중 몇몇 또는 전부와 상호작용하게 할 수도 있다. 라이브러리들(예를 들어, 애플리케이션 라이브러리(412) 및 네이티브 라이브러리(414)) 각각 및 커널(416)은 쿼리 로거(108)에 의해 모니터링될 수도 있다. 이러한 방식으로, 쿼리 로거(108)는, 동작들(120)의 로그를 생성하기 위해 컴퓨팅 디바이스 상의 애플리케이션들의 동작들을 모니터링 및 로깅할 수도 있다. 추가적으로, 그 후, 거동 분석 엔진(122)은, 애플리케이션의 거동을 특성화하는 애플리케이션에 대한 거동 벡터들(130)을 생성하기 위해, 쿼리 로거(108)로부터 애플리케이션에 대한 동작들(120)의 로그를 분석할 수도 있다.

[0028] 일 예로서, 게임 애플리케이션에 대해, 쿼리 로거(108)는, 네트워크(428) 사용(예를 들어, 웹사이트와의 네트워크 통신), 사용자 인터페이스 이벤트들 및 센서 사용(420)(예를 들어, 그들이 게임을 플레이하는 컴퓨팅 디바이스를 홀딩하는 사용자에 관한 터치 센서)에 관한 애플리케이션 라이브러리들(412) 및 네이티브 라이브러리들(414)의 실질적인 사용의 동작들 뿐만 아니라 실질적인 미디어 동작과 같은 다른 동작들의 로그를 생성할 수도 있다. 이러한 방식으로, 거동 분석 엔진(122)은, 빈번한 네트워크 사용, 센서 사용, 및 미디어 사용과 같이 애플리케이션의 거동을 특성화하는 애플리케이션에 대한 거동 벡터들(130)을 생성하기 위해, 쿼리 로거(108)로부터 애플리케이션에 대한 동작들(120)의 로그를 분석할 수도 있다. 광범위하게 다양한 상이한 타입들의 애플리케이션들, 모니터링된 동작들, 및 거동 벡터들(130)을 생성하기 위한 거동 분석 엔진(122)에 의한 그들의 분석이 후술될 것이다.

[0029] 도 5를 참조하면, 도 5는, 분류기(132)가 양성 또는 멀웨어로서 애플리케이션을 분류할 수 있도록 애플리케이션의 거동을 특성화하는 거동 벡터들(130)을 생성하기 위해, 쿼리 로거(108)로부터의 동작들(120)의 로그를 분석하기 위한 거동 분석 엔진(122)을 이용하는 결과들을 도시한 표(500)이다.

[0030] 표(500)에 도시된 바와 같이, 복수의 애플리케이션들은, 거동 분석 엔진을 이용하여 분석된다. 특히, 다음의 애플리케이션들, 즉 게임(502), 유투브(504), 노트패드(506), 피트니스(508), 뉴스(510), 페이크(fake) 유투브(520), 페이크 호텔탐색(522), 스파이웨어(524), 페이크 게임(526), 및 페이크 무비플레이어(528)는, 양성(538) 또는 멀웨어(536)로서 분류된다.

[0031] 이들 애플리케이션들 각각에 대해, 거동 벡터(529)는, 쿼리 로거로부터의 동작들의 로그를 분석하는 것에 기초

하여 거동 분석 엔진에 의해 생성된다. 거동 벡터들은, 빈번한 사용(530), 드문 사용(532), 및 사용없음(534)으로서 간략화된다. 수치적인 예로서, 약 5의 거동 벡터는 빈번한 사용을 지정할 수도 있고, 약 1-2의 거동 벡터는 드문 사용을 지정할 수도 있으며, 약 0의 거동 벡터는 사용없음을 지정할 수도 있다. 물론, 임의의 수치적인 지정이 이용될 수도 있다. 거동 벡터들은, 사용자 인터페이스(UI) 동작들(550), 통신 동작들(552), 센서 동작들(554), 위치(556), 미디어 동작들(558), 카메라 동작들(560), SMS 동작들(562), 전화통화 동작들(564), 및 전화기 정보(566)에 기초하여 생성된다. 이에 기초하여, 애플리케이션들은 멀웨어 애플리케이션들(536) 또는 양성 애플리케이션들(538)로서 지정된다.

[0032] 애플리케이션이 양성 또는 멀웨어로서 분류될 수 있도록 애플리케이션의 거동을 특성화하는 거동 벡터들을 생성하기 위해 쿼리 로거로부터의 동작들의 로그를 분석하기 위한 거동 분석 엔진을 이용하는 결과들을 도시하여 다양한 예들이 이제 설명될 것이다. 예를 들어, 빈번한(530) UI 동작들(550), 빈번한(530) 통신 동작들(552), 빈번한(530) 미디어 동작들(558), 및 없거나(534) 드문(532) 전화, SMS, 카메라, 위치 등의 동작들을 표시하는 거동 벡터들(529)을 갖는 게임 애플리케이션(502)은 양성(538)으로서 분류된다. 빈번한(530) UI 동작들(550), 빈번한(530) 통신 동작들(552), 및 빈번한(530) 미디어 동작들(558), 및 전화통화 없음(534), SMS, 카메라, 위치 등의 동작들을 표시하는 거동 벡터들(529)을 갖는 유투브 애플리케이션(504)은 양성(538)으로서 분류된다. 빈번한(530) UI 동작들(550), 및 전화통화 없음(534), SMS, 카메라, 위치 등의 동작들을 표시하는 거동 벡터들(529)을 갖는 노트패드 애플리케이션(506)은 양성(538)으로서 분류된다. 빈번한(530) UI 동작들(550), 빈번한(530) 통신 동작들(552), 빈번한(530) 센서 동작들(554), 및 없거나(534) 드문(532) 전화, SMS, 카메라, 위치 등의 동작들을 표시하는 거동 벡터들(529)을 갖는 피트니스 애플리케이션(508)은 양성(538)으로 분류된다. 빈번한(530) UI 동작들(550), 빈번한(530) 통신 동작들(552), 빈번한(530) 센서 동작들(554), 및 빈번한 미디어 동작(558), 및 없거나(534) 드문(532) 전화, SMS, 카메라, 위치 등의 동작들을 표시하는 거동 벡터들(529)을 갖는 뉴스 애플리케이션(510)은 양성(538)으로 분류된다.

[0033] 한편, 드문(532) UI 동작들(550) 및 드문 SMS 동작들(562)이지만 빈번한(530) 통신 동작들(552), 빈번한(530) 위치 동작들(556), 및 빈번한(530) 전화기 정보(566)를 표시하는 거동 벡터들(529)을 갖는 페이크 유투브 애플리케이션(520)은 멀웨어(536)로서 분류된다. 드문(532) UI 동작들(550) 및 드문 SMS 동작들(562)이지만 빈번한(530) 통신 동작들(552), 빈번한(530) 위치 동작들(556), 및 빈번한(530) 전화기 정보(566)를 표시하는 거동 벡터들(529)을 갖는 페이크 호텔탐색 애플리케이션(522)은 멀웨어(536)로서 분류된다. 드문(532) UI 동작들(550)이지만 빈번한(530) 통신 동작들(552), 빈번한(530) 위치 동작들(556), 및 빈번한(530) 전화통화들(564), 및 빈번한(530) 전화기 정보(566)를 표시하는 거동 벡터들(529)을 갖는 스파이웨어 애플리케이션(524)은 멀웨어(536)로서 분류된다. UI 동작들(550)은 없지만(534) 빈번한(530) 통신 동작들(552), 빈번한(530) SMS 동작들(562), 및 빈번한(530) 전화기 정보(566)를 표시하는 거동 벡터들(529)을 갖는 페이크 게임 애플리케이션(526)은 멀웨어(536)로서 분류된다. UI 동작들(550) 및 미디어 동작들(558)은 없지만(534) 빈번한(530) SMS 동작들(562)을 표시하는 거동 벡터들(529)을 갖는 페이크 무비플레이어 애플리케이션(528)은 멀웨어(536)로서 분류된다.

[0034] 넓은 세트의 거동 벡터들(130)을 생성하기 위하여 거동 분석 엔진(122)에 의해 쿼리 로거(120)로부터의 동작들(120)의 로그로부터 분석되는 넓은 세트의 동작들을 가짐으로써, 애플리케이션이 멀웨어 또는 양성으로서 분류되어야 하는지를 결정하도록 충분한 구별 특징들이 분석될 수 있다는 것이 발견되었다. 많은 악성 애플리케이션들이 사용자 정보를 훔치기를 시도하고 그리고/또는 금전을 생성하기 위한 허위(false) 과금들(예를 들어, 페이크 SMS 과금들)을 행하는 것이 관측된다. 또한, 애플리케이션들이 멀웨어 또는 양성인지를 결정하기 위해 컴퓨팅 디바이스(102) 상의 애플리케이션들을 특성화, 비교, 및 분류하려는 목적을 위해 거동 분석을 이용함으로써, (서명-기반 멀웨어 검출과는 대조적으로) 제한된 프로세서 및 메모리 기능을 이용하는 것이 새로운 멀웨어 또는 새로운 요구된 서명들에 관한 서버로부터의 업데이트들을 대기할 필요없이 즉시 발생할 수 있다.

[0035] 도 6을 부가적으로 참조하면, 본 발명의 다른 양상에 따르면, 서버(620)를 포함하는 시스템(600)은, 다수의 컴퓨팅 디바이스들(602)로부터의 거동 리포트들을 어그리게이팅하기 위해 이용될 수도 있다. 하나의 컴퓨팅 디바이스(602)만이 도시되어 있지만, 후술되는 양상들은 복수의 또는 다수의 컴퓨팅 디바이스들(602)에 관련된다. 컴퓨팅 디바이스(602)의 컴포넌트들 및 기능들은, 컴퓨팅 디바이스(102)를 참조하여 상술된 것과 동일한 방식으로 동작하므로, 이들 컴포넌트들 및 기능들은 간략화의 목적을 위해 상세히 반복되지는 않을 것이다. 일 양상에서, 서버(620)는, 프로세싱 회로(624), 거동 분석 엔진(626), 및 글로벌 분류기(628)를 적어도 포함하는 컴포넌트들(622)을 포함한다. 프로세싱 회로(624)는 송신기 및 수신기를 포함할 수도 있다. 거동 분석 엔진들, 쿼리 로거들, 거동 벡터들, 분류기들 등 뿐만 아니라 다른 컴포넌트들 및 기능들의 사용이 상세히 상술되었다.

프로세싱 회로(624)는, 프로세싱 회로(624) 또는 다른 컴포넌트들에 커플링된 메모리에 저장된 명령들에 기초하여, 수신기, 송신기, 거동 분석 엔진(626), 글로벌 분류기(628) 뿐만 아니라 다른 컴포넌트들을 구현하고 그들과 동작하기 위한 명령들을 실행하도록 구성될 수도 있다. 서버의 이용 프로세서들 및 메모리가 당업계에 잘 알려져 있음은 당업자들에 의해 인식되어야 한다.

[0036] 일 양상에서, 서버(620)의 프로세싱 회로(624)의 수신기는, (예를 들어, 컴퓨팅 디바이스(602)가, 애플리케이션의 거동이 의심스럽거나 가끔(occasional) 거동 벡터 세트가 업데이트한다고 자신의 거동 분석 엔진(608)을 통해 결정할 경우(결정 블록(612) 참조)) 복수의 상이한 컴퓨팅 디바이스들(602)로부터 복수의 거동 벡터 세트들(610)을 수신할 수도 있다. 상술된 바와 같이, 거동 벡터 세트(610)는, 애플리케이션의 거동을 특성화한다. 서버(620)의 거동 분석 엔진(626)은, 컴퓨팅 디바이스들(602)로부터의 수신된 거동 벡터 세트들(610)에 기초하여 글로벌 분류기(628)를 업데이트할 수도 있다. 추가적으로, 설명될 바와 같이, 글로벌 분류기(628)는, 의심스러운 거동을 갖는 것으로 애플리케이션을 식별했던 (예를 들어, 블록(612)) 컴퓨팅 디바이스(602)로부터의 애플리케이션에 대한 수신된 거동 벡터 세트를 양성 또는 멀웨어로서 분류할 수도 있다.

[0037] 일 특정한 양상에서, 컴퓨팅 디바이스(602)는, 애플리케이션의 거동이 의심스럽다고 결정할 수도 있으며, 서버(620)가 거동 벡터 세트(610)를 분석하게 하도록 애플리케이션에 대한 거동 벡터 세트(610)를 서버(620)에 송신할 수도 있다. 서버(620)의 글로벌 분류기(628)는, 송신된 거동 벡터 세트(610)를 양성 또는 멀웨어로서 분류할 수도 있다. 애플리케이션에 대한 거동 벡터 세트(610)가 멀웨어로서 분류되면, 멀웨어 표시자는, 복수의 컴퓨팅 디바이스들(602)로 송신될 수도 있으며, 컴퓨팅 디바이스들(602)은 애플리케이션을 삭제(632)할 수도 있다.

[0038] 추가적으로, 서버(620)는 프로세싱 회로(624)의 송신기를 통해, 복수의 컴퓨팅 디바이스들(602)에 업데이트를 송신할 수도 있으며, 여기서, 업데이트들은, 복수의 컴퓨팅 디바이스들(602)의 거동 분석 엔진들(608)을 업데이트하는데 사용된다. 이러한 방식으로, 다수의 컴퓨팅 디바이스들(602)로부터 수신된 거동 벡터 세트들 모두 및 다른 데이터에 기초하여, 서버(620)는, 컴퓨팅 디바이스들 그 자체에 의해 수행된 거동 분석을 주기적으로 업데이트할 수 있다.

[0039] 따라서, 서버(620)는, 다수의 컴퓨팅 디바이스들(602)로부터의 거동 리포트들을 어그리게이팅함으로써 다수의 소싱 서버로서 동작한다. 시간에 걸쳐 큰 입력 세트를 수집함으로써, 더 정확하고 업데이트된 거동 모델들이 촉진(expedited) 방식으로 생성되며, 모든 동작 컴퓨팅 디바이스들(602)로 전달될 수 있다. 또한, 애플리케이션이 멀웨어인 것으로 결정되는 경우, 컴퓨팅 디바이스들(602) 모두는 이를 통지받을 수 있다.

[0040] 동작의 일 예로서, 도 6에 도시된 바와 같이, 컴퓨팅 디바이스(602)의 쿼리 로거(604)는, 동작들의 로그(606)를 생성하기 위해 애플리케이션의 거동을 로깅할 수도 있다. 다음으로, 컴퓨팅 디바이스(602)의 거동 분석 엔진(608)은, 애플리케이션의 거동을 특성화하는 거동 벡터 세트(610)를 생성하도록 동작들의 로그(608)를 분석할 수도 있다. 일 예로서, 거동 벡터 세트(610)는 적어도 하나의 수치값을 포함할 수도 있다. 결정 블록(612)에서, 거동 벡터 세트가 애플리케이션에 관해 임의의 의심스러운 것을 표시한다는 것(예를 들어, 애플리케이션이 멀웨어일 낮은 가능성을 가짐)을 컴퓨팅 디바이스(602)의 분류기가 발견하지 못하면, 로그가 삭제되고(블록(616)), 프로세스는 종료된다(블록(618)). 이들 기능들의 대부분은 상세히 상술되었다.

[0041] 그러나, 거동이 컴퓨팅 디바이스(602)에 의해 의심스러운 것으로 결정되면(결정 블록(612)), 컴퓨팅 디바이스(602)는, 애플리케이션의 사용을 블록할 수도 있고(블록(614)), 거동 벡터 세트(610)를 서버(620)에 송신할 수도 있다. 서버(620)는, 프로세싱 회로(624)를 통해 거동 벡터 세트(610)를 수신할 수도 있으며, 애플리케이션이 양성 또는 멀웨어인지를 결정하기 위해 거동 벡터 세트(610)를 체크할 수도 있다. 또한, 컴퓨팅 디바이스(602)로부터 서버(620)로 송신된 거동 벡터 세트(610)는 또한, 애플리케이션이 블록되었다는 표시자를 포함할 수도 있다. 부가적으로, 컴퓨팅 디바이스(602)는, 로그 뿐만 아니라 다른 데이터를 서버(620)에 송신할 수도 있다. 이러한 단계가 실시간으로(즉, 거동이 분류되는 시간에) 발생할 수도 있거나 그것이 추후의 시간(예를 들어, 디바이스가 대역폭 또는 전력으로의 더 양호한 액세스를 갖는 경우)에 발생할 수도 있음을 유의해야 한다.

[0042] 수신된 거동 벡터 세트(610)에 기초하여, 서버(620)의 글로벌 분류기(628)는 애플리케이션을 양성 또는 멀웨어로서 분류할 수도 있다. 애플리케이션에 대한 거동 벡터 세트(610)가 멀웨어로서 분류되면, 멀웨어 표시자는 복수의 컴퓨팅 디바이스들(602)에 송신될 수도 있다. 이에 기초하여, 컴퓨팅 디바이스(602)가 멀웨어 표시를 수신하면(결정 블록(630)), 컴퓨팅 디바이스(602)는 애플리케이션을 삭제할 수도 있다(블록(632)). 그러나, 그것이 멀웨어가 아니면, 로그가 삭제될 수도 있으며(블록(616)), 컴퓨팅 디바이스(602)가 애플리케이션을 이용하

는 것을 포함하는 통상적인 동작들을 유지하도록 프로세스가 완료 또는 종료된다(블록(618)).

[0043] 다른 양상에서, 애플리케이션의 거동이 의심스럽지 않다고 컴퓨팅 디바이스들(602)이 결정할 경우(블록(612)), 서버(620)의 거동 분석 엔진(626) 및 글로벌 분류기(628)가 컴퓨팅 디바이스들(602)에 의해 이용되는 애플리케이션들에 관한 광범위한 범위의 정보를 수신하도록, 컴퓨팅 디바이스들(602)은 때때로, 애플리케이션들에 관련된 그들의 거동 벡터 세트들(610)(로그들, 쿼리들, 및 다른 정보)을 서버(620)에 송신한다. 이러한 방식으로, 컴퓨팅 디바이스들(602) 모두는, 서버(620)가 자신의 거동 모델링으로 업데이트되게 유지하도록 협력한다.

[0044] 유사하게, 서버(620)는 프로세싱 회로(624)를 통해 때때로, 복수의 컴퓨팅 디바이스들(602)에 업데이트들을 송신하며, 여기서, 업데이트들은 컴퓨팅 디바이스들(602)에 의해, 그들의 거동 분석 엔진들(608) 및 분류기들을 업데이트하고, 일반적으로는 그들의 거동 모델링 및 애플리케이션들의 분석을 업데이트하기 위해 사용될 수도 있다. 또한, 서버(620)는 프로세싱 회로(624)를 통해 때때로, 컴퓨팅 디바이스들이 그들의 동작들의 로그(606)를 쿼리하고, 그들의 쿼리 로거들(604)을 업데이트하기 위해 이용될 수도 있으며, 거동 모델링 및 애플리케이션들의 분석을 업데이트하기 위해 그들의 거동 분석 엔진들(608) 및 분류기들과 함께 이용될 수도 있는 업데이트된 쿼리들을 복수의 컴퓨팅 디바이스들(602)에 송신할 수도 있다. 이러한 방식으로, 거동 업데이트들, 거동 벡터 세트들, 쿼리들 뿐만 아니라 서버(620)로부터 수신된 다른 데이터에 기초하여, 서버(620)는 주기적으로, 컴퓨팅 디바이스들(602) 그 자체에 의해 수행된 거동 분석을 업데이트할 수 있다.

[0045] 따라서, 서버(620)는, 다수의 컴퓨팅 디바이스들(602)로부터의 거동 리포트들을 어그리게이팅함으로써 다수의 소싱 서버로서 동작한다. 본질적으로, 서버(620)는, 다수의 컴퓨팅 디바이스들(602)로부터의 협력적인 업로딩으로부터 획득된 양성 및 악성 거동의 모델에 대해 애플리케이션의 거동을 평가할 수도 있다. 시간에 걸쳐 큰 입력 세트를 수집함으로써, 더 정확하고 업데이트된 거동 모델들이 촉진 방식으로 생성되며, 모든 동작 컴퓨팅 디바이스들(602)로 전달될 수 있다. 개별 컴퓨팅 디바이스들에 의한 바이어스들이 고려될 수도 있다. 또한, 개별 컴퓨팅 디바이스들(602)은, 다른 컴퓨팅 디바이스들로부터의 다수의 리포트들에 기초하여 생성된 거동 모델들을 이용할 수 있다. 또한, 애플리케이션이 멀웨어인 것으로 결정되는 경우, 컴퓨팅 디바이스들(602) 모두는 이를 통지받을 수 있다. 추가적으로, 멀웨어 검출의 목적을 위한 개별 컴퓨팅 디바이스들(602) 상의 모니터링 및 계산 오버헤드는, 다수-기반 서버(620)를 이용함으로써 감소될 수 있다. 특히, 협력적인 분석을 이용함으로써, 많은 양의 거동 벡터들 및 로그들이 적시의 멀웨어 검출을 위하여 다수의 컴퓨팅 디바이스들(602)로부터 서버(620)에 의해 누산될 수도 있다. 따라서, 결과적인 거동 모델은 정확하고(낮은 거짓 포지티브 및 거짓 네거티브) 일반적(광범위하게 다양한 상이한 타입들의 멀웨어를 캡처할 수도 있음)인 둘 모두일 수도 있다. 각각의 컴퓨팅 디바이스(602)에서의 거동 분석 엔진(608)에 대한 거동 모델들이 고유함을 유의해야 한다. 추가적으로, 서버(620)로부터 수신된 전체 특징들은, 컴퓨팅 디바이스(602)에 대해 고유하게 변경된다.

[0046] 일 예로서, 3개의 상이한 단계들, 즉 초기화; 협력적인 거동 모델링 및 멀웨어 검출; 및 거동 모델링 업데이팅은, 다수의 컴퓨팅 디바이스들(602)을 서버(620)와 협력시킬 시에 이용될 수도 있다. 초기화에 관해, (예를 들어, 컴퓨팅 디바이스(602)에 대한) 거동 분석 엔진 및 분류기는, 알려진-불량한 애플리케이션들의 세트, 또는 멀웨어, 및 알려진-양호한 애플리케이션들의 세트에 의해 트레이닝(train)될 수도 있다. 트레이닝 프로세스는, 표준 관리 머신 학습 기술들을 사용하여 달성될 수도 있다. 컴퓨팅 디바이스(602)가 사용자에게 제공되기 전에, 컴퓨팅 디바이스(602)는, 자신의 거동 분석 엔진(608)에 대한 최신 거동 모델을 서버(620)로부터 획득하도록 요구될 수도 있다. 부가적으로, 서버(620)는, 로깅되어야 하는 API들의 리스트, 및 거동 분석 엔진을 이용하여 API 로그로부터 거동 벡터(예를 들어, 애플리케이션의 거동의 간결한 표현)를 어떻게 생성하는지에 관한 명령들을 컴퓨팅 디바이스(602)에 제공할 수도 있다.

[0047] 협력적인 거동 모니터링 및 멀웨어 검출에 관해, 상술된 바와 같이, 사용자가 자신의 컴퓨팅 디바이스(602)를 이용하고 있는 경우, 컴퓨팅 디바이스(602)는, 각각의 구동중인 애플리케이션에 대한 거동 분석 엔진(608)을 이용하여 거동 벡터(610)를 주기적으로 모니터링 및 컴퓨팅하며, 분류기를 이용함으로써, 이러한 애플리케이션이 멀웨어 또는 양성 애플리케이션들과 유사하게 거동하는지를 결정할 수도 있다. 컴퓨팅 디바이스(602)에 의해 악성인 것으로 분류된 애플리케이션들은, 서버(620)에 의해 확인될 수 있으며, 컴퓨팅 디바이스(602)로부터 제거(예를 들어, 블록(632))되거나 인스톨레이션이 거부되어야 한다. 양성으로서 분류된 애플리케이션들은 완전한 승인들을 이용하여 구동할 수 있다. 의심스러운 것으로서 결정된(결정 블록(612)), 예를 들어, 컴퓨팅 디바이스(602) 그 자체에 의해 로컬적으로 의심스러운 것으로 검출된 (하지만 그것은 추가적인 조사를 요구함) 애플리케이션들에 대해, 이들 경우들에서, 컴퓨팅 디바이스(602)는, 제약된 환경에 애플리케이션을 놓을 수 있으며, 제한된 액세스만이 허용될 수도 있다. 그 후, 상술된 바와 같이, 이러한 애플리케이션은 추가적인 조사를 위해

서버(620)에 리포팅될 수도 있다.

[0048] 거동 모델 업데이트들에 관해, 협력을 가능하게 하기 위해, 컴퓨팅 디바이스들(602)은 상술된 바와 같이, 자신의 거동 벡터들(610) 및 다른 데이터를 서버(620)에 주기적으로 업로딩한다. 서버(620)는 부가적으로, 컴퓨팅 디바이스들(602)로부터 본래의 로그들을 또한 요청할 수 있다. 리소스-풍부한 머신(또는 클러스터)일 수도 있는 서버(620)는, 심층(in-depth) 분석을 수행하고, 그 후, 거동 분석 엔진(626) 및 글로벌 분류기(628)를 통해 거동 모델을 업데이트할 수 있다. 모델이 업데이트 이후 현저하게 변하면, 서버(620)는, 컴퓨팅 디바이스(602)의 업데이트된 모델을 거동 분석 엔진(608) 및 분류기에 푸쉬(push)할 수도 있다. 더 많은 데이터가 수집되고 모델이 안정화될 때, 변경들이 덜 빈번할 수도 있다.

[0049] 따라서, 상술된 시스템은, 정적인 분석 및 서명-기반 바이러스방지 접근법들에 보충적인 보호의 부가적인 계층으로서 동작할 수도 있다. 하나의 특정한 이득에 관해, 바이러스방지의 데이터베이스에 부가되지 않은 멀웨어, 또는 인스톨레이션 시간에 양성인 것으로 가장하는 멀웨어가 검출될 수도 있다. 특히, 서버(620)는, 다수의 컴퓨팅 디바이스들(602)로부터의 거동 리포트들을 어그리게이팅함으로써 다수의 소싱 서버로서 동작한다. 본질적으로, 서버(620)는, 다수의 컴퓨팅 디바이스들(602)로부터의 협력적인 업로딩으로부터 획득된 양성 및 악성 거동의 모델에 대해 애플리케이션의 거동을 평가할 수도 있다. 시간에 걸쳐 큰 입력 세트를 수집함으로써, 더 정확하고 업데이트된 거동 모델들이 촉진 방식으로 생성되며, 모든 동작 컴퓨팅 디바이스들(602)로 전달될 수 있다.

[0050] 컴퓨팅 디바이스 또는 서버가 모바일 또는 무선 디바이스인 경우, 그것은, 임의의 적절한 무선 통신 기술에 기초하거나 그렇지 않으면 지원하는 무선 네트워크를 통한 하나 또는 그 초과의 무선 통신 링크들을 통해 통신할 수도 있음을 인식해야 한다. 예를 들어, 몇몇 양상들에서, 컴퓨팅 디바이스 또는 서버는 무선 네트워크를 포함하는 네트워크와 연관될 수도 있다. 몇몇 양상들에서, 네트워크는 보디(body) 영역 네트워크 또는 개인 영역 네트워크(예를 들어, 울트라-광대역 네트워크)를 포함할 수도 있다. 몇몇 양상들에서, 네트워크는 로컬 영역 네트워크 또는 광역 네트워크를 포함할 수도 있다. 무선 디바이스는, 예를 들어, CDMA, TDMA, OFDM, OFDMA, WiMAX, 및 Wi-Fi와 같은 다양한 무선 통신 기술들, 프로토콜들, 또는 표준들 중 하나 또는 그 초과를 지원하거나 그렇지 않으면 사용할 수도 있다. 유사하게, 무선 디바이스는 다양한 대응하는 변조 또는 멀티플렉싱 방식들 중 하나 또는 그 초과를 지원하거나 그렇지 않으면 사용할 수도 있다. 따라서, 무선 디바이스는 상기 또는 다른 무선 통신 기술들을 사용하여 하나 또는 그 초과의 무선 통신 링크들을 설정하고 그 통신 링크들을 통해 통신하기 위한 적절한 컴포넌트들(예를 들어, 에어 인터페이스들)을 포함할 수도 있다. 예를 들어, 디바이스는, 무선 매체를 통한 통신을 용이하게 하는 다양한 컴포넌트들(예를 들어, 신호 생성기들 및 신호 프로세서들)을 포함할 수도 있는 연관된 송신기 및 수신기 컴포넌트들(예를 들어, 송신기 및 수신기)을 갖는 무선 트랜시버를 포함할 수도 있다. 따라서, 잘 알려진 바와 같이, 모바일 무선 통신 디바이스는, 다른 모바일 디바이스들, 셀 전화기들, 다른 유선 및 무선 컴퓨터들, 인터넷 웹-사이트들 등과 무선으로 통신할 수도 있다.

[0051] 본 명세서에 설명된 기술들은, 코드 분할 다중 액세스(CDMA), 시분할 다중 액세스(TDMA), 주파수 분할 다중 액세스(FDMA), 직교 주파수-분할 다중 액세스(OFDMA), 단일 캐리어 FDMA(SC-FDMA), 및 다른 시스템들과 같은 다양한 무선 통신 네트워크들에 대해 사용될 수 있다. 용어들 "시스템" 및 "네트워크"는 종종 상호교환가능하게 사용된다. CDMA 시스템은 UTRA(Universal Terrestrial Radio Access), CDMA2000 등과 같은 라디오 기술을 구현할 수 있다. UTRA는 광대역-CDMA(W-CDMA) 및 CDMA의 다른 변형들을 포함한다. CDMA2000은 IS(Interim Standard)-2000, IS-95 및 IS-856 표준들을 커버한다. TDMA 시스템은 모바일 통신들을 위한 글로벌 시스템(GSM)과 같은 라디오 기술을 구현할 수 있다. OFDMA 시스템은 이벌브드 유니버셜 지상 라디오 액세스(이벌브드 UTRA 또는 E-UTRA), 울트라 모바일 브로드밴드(UMB), IEEE(Institute of Electrical and Electronics Engineers) 802.11(Wi-Fi), IEEE 802.16(WiMAX), IEEE 802.20, Flash-OFDM.RTM 등과 같은 라디오 기술을 구현할 수 있다. 유니버셜 지상 라디오 액세스(UTRA) 및 E-UTRA는 UMTS(Universal Mobile Telecommunication System)의 일부이다. 3GPP 롱텀 에볼루션(LTE)은, 다운링크 상에서는 OFDMA 그리고 업링크 상에서는 SC-FDMA를 이용하는 E-UTRA를 사용하는 UMTS의 도래하는 릴리즈이다. UTRA, E-UTRA, UMTS, LTE 및 GSM은 "3세대 파트너쉽 프로젝트" (3GPP)로 명칭된 조직으로부터의 문헌들에 설명되어 있다. CDMA2000 및 UMB는 "3세대 파트너쉽 프로젝트 2" (3GPP2)로 명칭된 조직으로부터의 문헌들에 설명되어 있다.

[0052] 본 명세서의 교시들은 다양한 장치들(예를 들어, 디바이스들)로 포함(예를 들어, 그들 내에 구현 또는 그들에 의해 수행)될 수도 있다. 예를 들어, 본 명세서에 교시된 하나 또는 그 초과의 양상들은, 전화기(예를 들어, 셀룰러 전화기), 개인 휴대 정보 단말("PDA"), 태블릿, 모바일 컴퓨터, 랩탑 컴퓨터, 태블릿, 엔터테인먼트 디바이스(예를 들어, 뮤직 또는 비디오 디바이스), 헤드셋(예를 들어, 헤드폰들, 이어피스 등), 의료 디바이스(예

를 들어, 생체 센서, 심박 모니터, 계보기, EKG 디바이스 등), 사용자 I/O 디바이스, 컴퓨터, 서버, 판매 시점 디바이스, 엔터테인먼트 디바이스, 셋톱 박스, 또는 임의의 다른 적절한 디바이스로 포함될 수도 있다. 이들 디바이스들은 상이한 전력 및 데이터 요건들을 가질 수도 있다.

[0053] 몇몇 양상들에서, 무선 디바이스는 통신 시스템에 대한 액세스 디바이스(예를 들어, Wi-Fi 액세스 포인트)를 포함할 수도 있다. 그러한 액세스 디바이스는, 예를 들어, 유선 또는 무선 통신 링크를 통해 다른 네트워크(예를 들어, 인터넷 또는 셀룰러 네트워크와 같은 광역 네트워크)로의 접속을 제공할 수도 있다. 따라서, 액세스 디바이스는, 다른 디바이스가(예를 들어, Wi-Fi 스테이션) 다른 네트워크 또는 몇몇 다른 기능에 액세스할 수 있게 할 수도 있다. 부가적으로, 디바이스들 중 하나 또는 둘 모두가 휴대가능하거나 몇몇 경우들에서는, 비교적 비-휴대가능할 수도 있음을 인식해야 한다.

[0054] 당업자들은, 정보 및 신호들이 다양한 상이한 기법들 및 기술들 중 임의의 기법 및 기술을 사용하여 표현될 수도 있음을 이해할 것이다. 예를 들어, 상기 설명 전반에 걸쳐 참조될 수도 있는 데이터, 명령들, 커맨드들, 정보, 신호들, 비트들, 심볼들, 및 칩들은 전압들, 전류들, 전자기파들, 자기장들 또는 자기 입자들, 광학 필드들 또는 광학 입자들, 또는 이들의 임의의 결합에 의해 표현될 수도 있다.

[0055] 당업자들은, 본 명세서에 기재된 실시예들과 관련하여 설명된 다양한 예시적인 로직 블록들, 모듈들, 회로들, 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 이 둘의 결합들로서 구현될 수도 있음을 추가적으로 인식할 것이다. 하드웨어와 소프트웨어의 이러한 상호교환가능성을 명확히 예시하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들, 및 단계들은 그들의 기능의 관점들에서 일반적으로 상술되었다. 그러한 기능이 하드웨어로서 구현되는지 또는 소프트웨어로서 구현되는지 여부는 특정한 애플리케이션, 및 전체 시스템에 부과된 설계 제약들에 의존한다. 당업자들은 설명된 기능을 각각의 특정한 애플리케이션에 대해 다양한 방식들로 구현할 수도 있지만, 그러한 구현 결정들이 본 발명의 범위를 벗어나게 하는 것으로서 해석되지는 않아야 한다.

[0056] 본 명세서에 기재된 실시예들과 관련하여 설명된 다양한 예시적인 로직 블록들, 모듈들, 및 회로들은 범용 프로세서, 디지털 신호 프로세서(DSP), 주문형 집적회로(ASIC), 필드 프로그래밍가능 게이트 어레이(FPGA) 또는 다른 프로그래밍가능 로직 디바이스, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본 명세서에 설명된 기능들을 수행하도록 설계된 이들의 임의의 결합으로 구현 또는 수행될 수도 있다. 범용 프로세서는 마이크로프로세서일 수 있지만, 대안적으로, 프로세서는 임의의 종래의 프로세서, 제어기, 마이크로제어기, 또는 상태 머신일 수도 있다. 또한, 프로세서는 컴퓨팅 디바이스들의 결합, 예를 들어, DSP와 마이크로프로세서의 결합, 복수의 마이크로프로세서들, DSP 코어와 결합된 하나 또는 그 초과의 마이크로프로세서들, 또는 임의의 다른 그러한 구성으로서 구현될 수도 있다.

[0057] 본 명세서에 기재된 실시예들과 관련하여 설명된 방법 또는 알고리즘의 단계들은 직접적으로 하드웨어로, 프로세서에 의해 실행되는 소프트웨어 모듈로, 또는 이 둘의 결합으로 구현될 수도 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드 디스크, 착탈형 디스크, CD-ROM, 또는 당업계에 알려진 임의의 다른 형태의 저장 매체에 상주할 수도 있다. 예시적인 저장 매체는, 프로세서가 저장 매체로부터 정보를 판독하고, 저장 매체에 정보를 기입할 수 있도록 프로세서에 커플링된다. 대안적으로, 저장 매체는 프로세서에 통합될 수도 있다. 프로세서 및 저장 매체는 ASIC에 상주할 수도 있다. ASIC는 사용자 단말에 상주할 수도 있다. 대안적으로, 프로세서 및 저장 매체는 사용자 단말 내의 별개의 컴포넌트들로서 상주할 수도 있다.

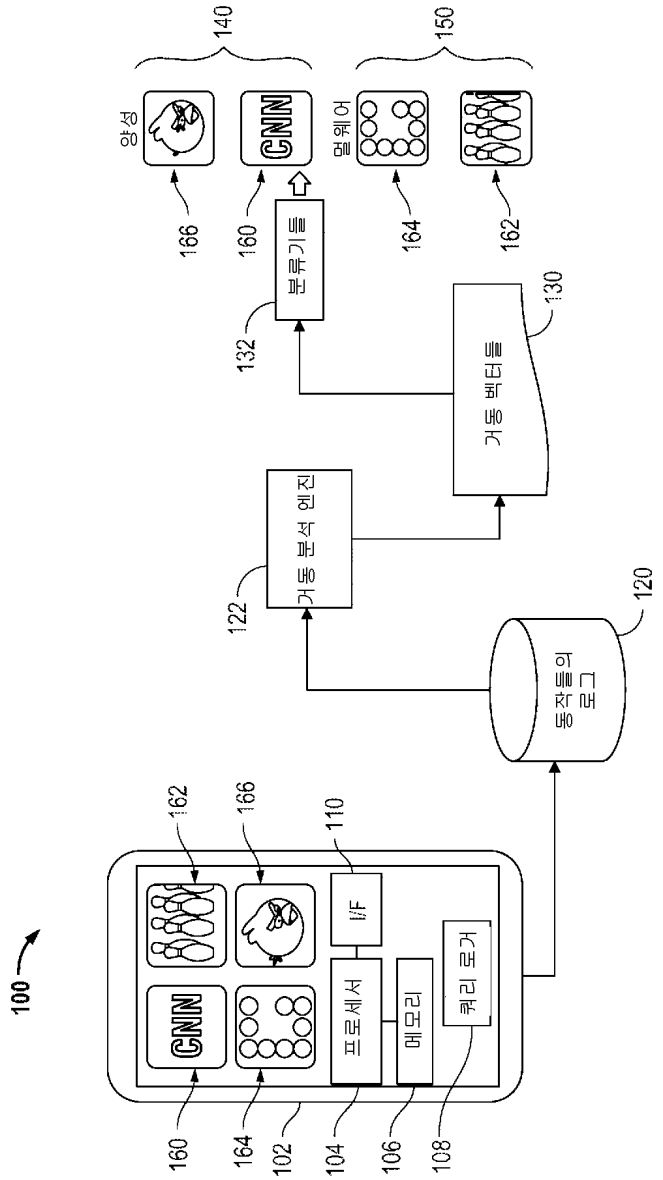
[0058] 하나 또는 그 초과의 예시적인 실시예들에서, 설명된 기능들은 하드웨어, 소프트웨어, 펌웨어, 또는 이들의 임의의 결합으로 구현될 수도 있다. 컴퓨터 프로그램 물건으로서 소프트웨어로 구현되면, 기능들은 컴퓨터 판독가능 매체 상에 하나 또는 그 초과의 명령들 또는 코드로서 저장되거나 그들을 통해 송신될 수도 있다. 컴퓨터-판독가능 매체들은, 일 장소로부터 다른 장소로의 컴퓨터 프로그램의 전달을 용이하게 하는 임의의 매체를 포함하는 통신 매체들 및 컴퓨터 저장 매체들 둘 모두를 포함한다. 저장 매체들은 컴퓨터에 의해 액세스될 수 있는 임의의 이용가능한 매체들일 수도 있다. 제한이 아닌 예로서, 그러한 컴퓨터-판독가능 매체들은 RAM, ROM, EEPROM, CD-ROM 또는 다른 광학 디스크 저장부, 자기 디스크 저장 또는 다른 자기 저장 디바이스들, 또는 명령들 또는 데이터 구조들의 형태로 원하는 프로그램 코드를 반송 또는 저장하는데 사용될 수 있고, 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있다. 또한, 임의의 접속수단(connection)이 컴퓨터-판독가능 매체로 적절히 지칭된다. 예를 들어, 소프트웨어가 동축 케이블, 광섬유 케이블, 연선(twisted pair), 디지털 가입자 라인(DSL), 또는 (적외선, 라디오, 및 마이크로파와 같은) 무선 기술들을 사용하여 웹사이트, 서버, 또

는 다른 원격 소스로부터 송신되면, 동축 케이블, 광섬유 케이블, 연선, DSL, 또는 (적외선, 라디오, 및 마이크로파와 같은) 무선 기술들은 매체의 정의에 포함된다. 본 명세서에 사용된 바와 같이, 디스크(disk) 및 디스크(disc)는 컴팩트 디스크(disc)(CD), 레이저 디스크(disc), 광학 디스크(disc), 디지털 다기능 디스크(digital versatile disc)(DVD), 플로피 디스크(disk) 및 블루-레이 디스크(disc)를 포함하며, 여기서 디스크(disk)들은 일반적으로 데이터를 자기적으로 재생하지만, 디스크(disc)들은 레이저를 이용하여 광학적으로 데이터를 재생한다. 상기한 것들의 결합들이 또한 컴퓨터-판독가능 매체들의 범위 내에 포함되어야 한다.

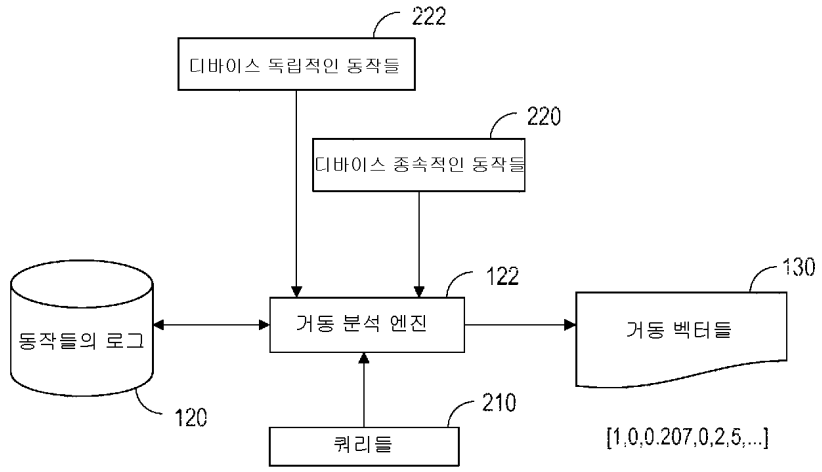
[0059] 기재된 실시예들의 이전 설명은 당업자가 본 발명을 실시하거나 또는 사용할 수 있도록 제공된다. 이들 실시예들에 대한 다양한 변형들은 당업자들에게 용이하게 명백할 것이며, 본 명세서에 정의된 일반적인 원리들은 본 발명의 사상 또는 범위를 벗어나지 않으면서 다른 실시예들에 적용될 수도 있다. 따라서, 본 발명은 본 명세서에 설명된 실시예들로 제한되도록 의도되는 것이 아니라, 본 명세서에 기재된 원리들 및 신규한 특성들과 일치하는 가장 넓은 범위에 부합할 것이다.

도면

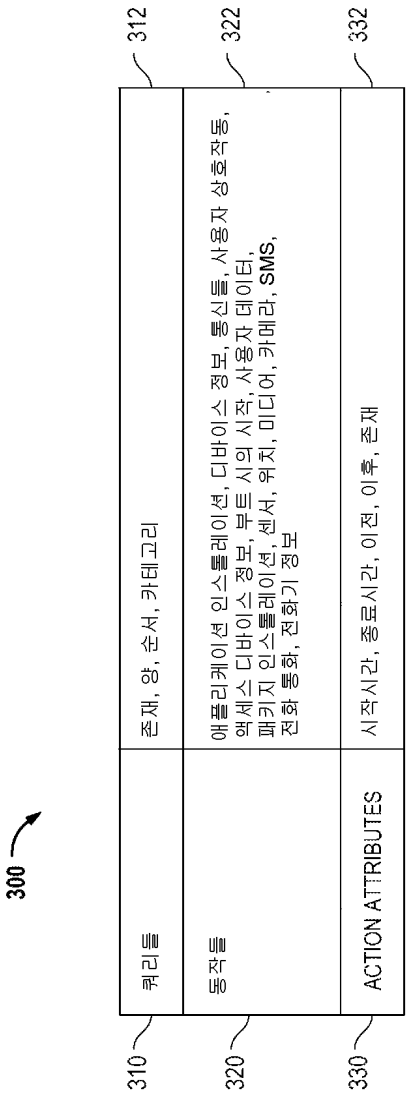
도면1



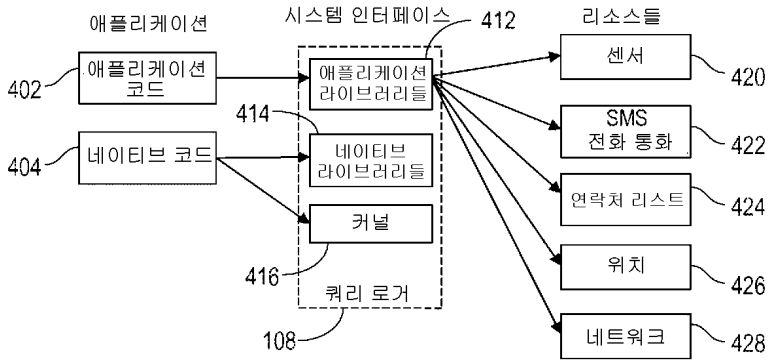
도면2


222
디바이스 독립적인 동작들
220
디바이스 종속적인 동작들
122
130
동작들의 로그
거동 분석 엔진
거동 벡터들
120
210
쿼리들
[1,0,0.207,0,2.5,...]

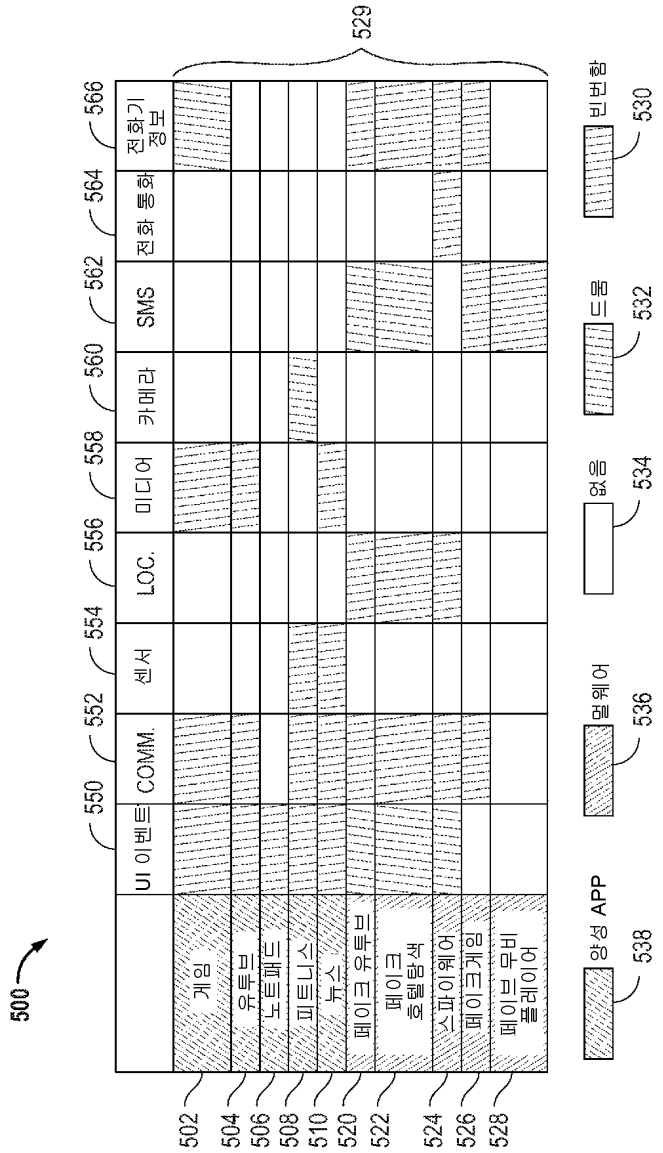
도면3


300
312
322
332
존재, 양, 순서, 카테고리
애플리케이션 인스톨레이션, 디바이스 정보, 통신들, 사용자 상호작동,
액세스 디바이스 정보, 부트 시의 시작, 사용자 데이터,
패키지 인스톨레이션, 센서, 위치, 미디어, 카메라, SMS,
전화 통화, 전화기 정보
시작시간, 종료시간, 이전, 이후, 존재
쿼리들
동작들
ACTION ATTRIBUTES
310
320
330

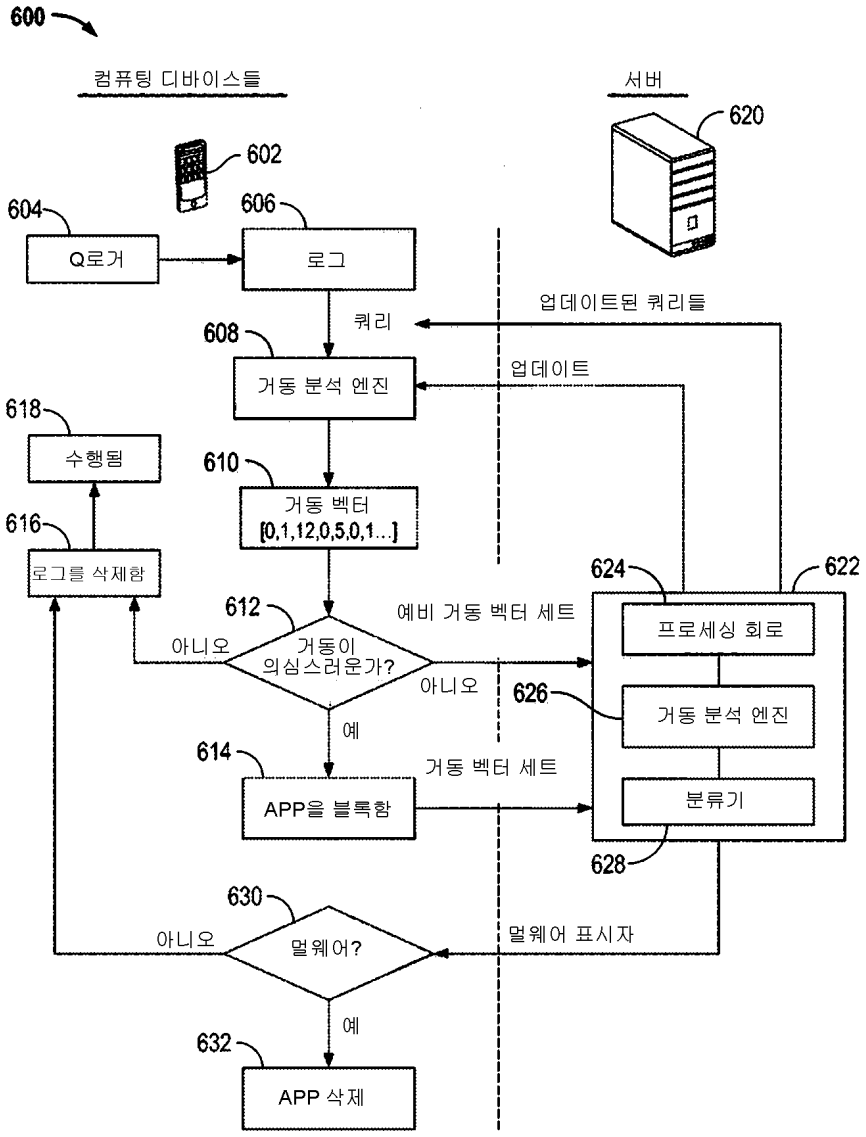
도면4


애플리케이션
시스템 인터페이스
412
리소스들
402
애플리케이션 코드
애플리케이션 라이브러리들
센서
420
414
SMS 전화 통화
422
404
네이티브 코드
네이티브 라이브러리들
연락처 리스트
424
커널
위치
426
416
쿼리 로거
108
네트워크
428

도면5


529
500
UI 이벤트
COMM.
센서
LOC.
미디어
카메라
SMS
전화 통화
전화기 정보
550
552
554
556
558
560
562
564
566
게임
유투브
노트패드
피트니스
뉴스
페이크 유투브
페이크 호텔탐색
스파이웨어
페이크게임
페이브 무비 플레이어
502
504
506
508
510
520
522
524
526
528
빈번함
530
드물
532
없음
534
멀웨어
536
양성 APP
538

도면6


600
컴퓨팅 디바이스들
서버
620
602
604
606
Q로거
로그
업데이트된 쿼리들
쿼리
608
업데이트
거동 분석 엔진
618
수행됨
610
거동 벡터
[0,1,12,0,5,0,1...]
616
로그를 삭제함
624
622
612
예비 거동 벡터 세트
프로세싱 회로
아니오
거동이
의심스러운가?
아니오
626
거동 분석 엔진
예
614
거동 벡터 세트
분류기
APP을 블록함
628
630
아니오
멀웨어?
멀웨어 표시자
예
632
APP 삭제