(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년08월14일
(11) 등록번호 10-1767454
(24) 등록일자 2017년08월07일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)
(52) CPC특허분류
H04L 63/1425 (2013.01)
H04L 67/22 (2013.01)
(21) 출원번호 10-2015-0158592
(22) 출원일자 2015년11월12일
심사청구일자 2015년11월12일
(65) 공개번호 10-2017-0056045
(43) 공개일자 2017년05월23일
(56) 선행기술조사문헌
US20150106926 A1*
KR1020120037865 A*
JP2004220373 A*
KR1020100001786 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 엔젠소프트
서울특별시 강남구 테헤란로77길 11-9, 7층(삼성동, 삼성타워)
(72) 발명자
김성
경기도 성남시 분당구 분당로201번길 17 114동 801호 (서현동,효자촌현대아파트)
박경철
서울 양천구 월정로 306
(74) 대리인
박종한

전체 청구항 수 : 총 12 항 심사관 : 문형섭

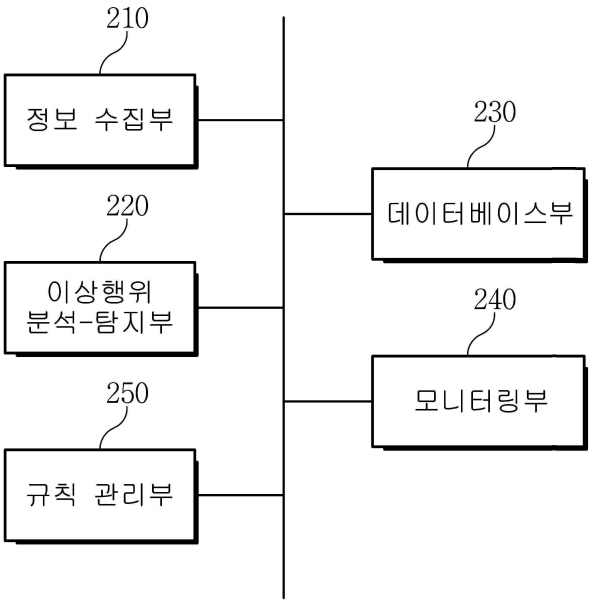
(54) 발명의 명칭 **다양한 웹 서비스 환경에서 사용자의 행위 패턴 분석을 통한 이상행위 탐지 방법과 그를 위한 장치**

(57) 요 약

본 발명은 이상행위 탐지 방법에 관한 것으로, 보다 상세하게는 프로파일 기반 분석과 기계학습 기반 분석을 통해 이상행위를 탐지할 수 있도록 하며, 사용자의 행위 파라미터 값을 통해 이상행위 분석 규칙을 추가 혹은 삭제하며, 기계학습을 통한 이상행위 분석 모델을 생성하여 이상행위를 탐지하기 위한 방법, 그를 위한 장치에 관한

(뒷면에 계속)

대 표 도 - 도2



것이다.

이를 위한 본 발명의 일 실시 예에 따른 이상행위 탐지 방법은 사용자의 행위 파라미터 값을 실시간으로 수집하는 단계; 상기 수집된 사용자의 행위 파라미터 값을 해당 사용자의 이상행위 분석 규칙과 비교하여, 이상행위 여부를 탐지하는 제1 탐지 단계; 상기 제1 탐지 단계에서 이상행위로 판단되지 않은 사용자의 행위 파라미터 값을 이상행위 분석 모델에 입력하여, 상기 이상행위 분석 모델의 연산을 통해, 이상행위 여부를 탐지하는 제2 탐지 단계; 상기 제1 탐지 단계의 탐지 결과 및 상기 제2 탐지 단계의 탐지 결과를 조합하여, 이상행위 여부를 판단하는 단계; 를 포함하여 구현된다.

(52) CPC특허분류
H04L 67/306 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 R-20150521-001431
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 방송통신융합미디어원천기술개발 사업
연구과제명 다양한 웹 서비스 환경에서 사용자의 행위패턴 분석을 통한 이상행위 탐지기술개발
기 여 율 1/1
주관기관 (주)엔젠소프트
연구기간 2015.06.01 ~ 2016.05.31

명 세 서

청구범위

청구항 1

사용자별 이상행위 분석 규칙을 생성하는 단계;

사용자의 행위 파라미터 값을 실시간으로 수집하는 단계;

상기 수집된 사용자의 행위 파라미터 값을 해당 사용자의 이상행위 분석 규칙과 비교하여, 이상행위 여부를 탐지하는 제1 탐지 단계;

상기 제1 탐지 단계에서 이상행위로 판단되지 않은 사용자의 행위 파라미터 값을 이상행위 분석 모델에 입력하여, 상기 이상행위 분석 모델의 연산을 통해, 이상행위 여부를 탐지하는 제2 탐지 단계;

상기 제1 탐지 단계의 탐지 결과 및 상기 제2 탐지 단계의 탐지 결과를 조합하여, 이상행위 여부를 판단하는 단계;를 포함하고,

상기 사용자의 행위 파라미터 값은, 사용자가 이용하는 사용자 단말 장치, 사용자 단말 장치의 사용 행위, 웹 서비스 서버에 대한 접근 행위의 속성을 추출하거나 패턴화시킬 수 있는 정보로서,

사용자가 제공받는 서비스에 관한 고유 정보, 사용자 단말 장치에 관한 환경 정보, 사용자 단말 장치의 주변 하드웨어 정보, 사용자 단말 장치의 소프트웨어 정보 중 하나 이상을 포함하는 디바이스 핑거프린팅 속성과 관련된 행위 파라미터 값,

사용자가 이용하는 입력 장치에 대한 입력 패턴 정보, 입력 장치 자체의 변동 정보, 입력 장치에 대한 이용 행위에 관한 정보, 사용자 인증 방식에 관한 정보 중 하나 이상을 포함하는 입력 기기 이용행위에 관련된 행위 파라미터 값, 및

사용자가 이용하는 웹 서비스 서버와의 거래 사전 행위와 관련된 패턴 정보, 인증 행위와 관련된 정보, 거래 행위 패턴 정보, 거래 패턴 정보, 비정상 행위와 관련된 사전 정보 중 하나 이상을 포함하는 웹 네비게이션 행위에 관련된 파라미터 값을 포함하는 것을 특징으로 하는 이상행위 탐지 방법.

청구항 2

제1항에 있어서,

상기 판단하는 단계의 결과가 정상행위인 경우, 이상행위에 앞서 연속적으로 발생하는 행위와 이상행위 간 상관관계를 분석하여 위험도를 산출하는 단계;

상기 위험도를 기반으로 상기 이상행위 여부를 재판단하는 단계;

를 더 포함하는 것을 특징으로 하는 이상행위 탐지 방법.

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 제1 탐지 단계는,

상기 실시간으로 수집한 행위 파라미터 값을 기반으로 해당 사용자에 대한 프로파일 정보를 생성하고,

상기 프로파일 정보의 특성을 추출하며,

상기 추출된 프로파일 특성을 상기 이상행위 분석 규칙과 비교하여 이상행위를 탐지하는 것을 특징으로 하는 이상행위 탐지 방법.

청구항 5

제1항에 있어서,

상기 제1 탐지 단계는,

기 설정된 블랙리스트 및 화이트리스트와 상기 행위 파라미터 값을 비교하여 이상 행위를 탐지하는 것을 특징으로 하는 이상행위 탐지 방법.

청구항 6

제1항에 있어서,

상기 사용자 별 이상행위 분석 규칙을 생성하는 단계는,

상기 이상행위 분석 규칙과의 비교를 통해 정상행위 또는 이상행위로 판단된 행위 파라미터 값을 기반으로 해당 사용자의 이상행위 분석 규칙을 추가 또는 삭제하는 것을 특징으로 하는 이상행위 탐지 방법.

청구항 7

제1항에 있어서,

사용자의 행위 파라미터값 중 정상행위로 판단된 행위 파라미터 값을 학습 데이터로 추출하고, 상기 학습 데이터를 기반으로 상기 이상행위 분석 모델에 대한 기계학습을 수행하는 단계를 더 포함하는 것을 특징으로 하는 이상행위 탐지 방법.

청구항 8

제1항에 있어서,

상기 이상행위 분석 모델은,

SVDD(Support Vector Data Description) 기법을 이용한 분석 모델인 것을 특징으로 하는 이상행위 탐지 방법.

청구항 9

삭제

청구항 10

제6항에 있어서,

상기 사용자 별 이상행위 분석 규칙을 생성하는 단계는

위험도 산출 결과를 기반으로 이상행위 분석 규칙을 추가 또는 삭제하는 것을 특징으로 하는 이상행위 탐지 방법.

청구항 11

이상 징후 식별에 필요한 사용자 별로 발생한 사용자의 행위 파라미터 값을 실시간으로 수집하는 정보 수집부; 및

상기 수집된 사용자의 행위 파라미터 값을, 기 생성된 이상행위 분석 규칙과 비교하여 이상행위 여부를 1차 탐지하고 이상행위 분석 모델을 통해 연산하여 이상행위 여부를 2차 탐지하고, 상기 1차 탐지 및 2차 탐지 판단 결과를 조합하여 최종 이상행위 여부를 판단하는 이상행위 분석 탐지부;를 포함하며,

상기 사용자의 행위 파라미터 값은, 사용자가 이용하는 사용자 단말 장치, 사용자 단말 장치의 사용 행위, 웹 서비스 서버에 대한 접근 행위의 속성을 추출하거나 패턴화시킬 수 있는 정보로서,

사용자가 제공받는 서비스에 관한 고유 정보, 사용자 단말 장치에 관한 환경 정보, 사용자 단말 장치의 주변 하드웨어 정보, 사용자 단말 장치의 소프트웨어 정보 중 하나 이상을 포함하는 디바이스 핑거프린팅 속성과 관련된 행위 파라미터 값,

사용자가 이용하는 입력 장치에 대한 입력 패턴 정보, 입력 장치 자체의 변동 정보, 입력 장치에 대한 이용 행

위에 관한 정보, 사용자 인증 방식에 관한 정보 중 하나 이상을 포함하는 입력 기기 이용행위에 관련된 행위 파라미터 값, 및

사용자가 이용하는 웹 서비스 서버와의 거래 사전 행위와 관련된 패턴 정보, 인증 행위와 관련된 정보, 거래 행위 패턴 정보, 거래 패턴 정보, 비정상 행위와 관련된 사전 정보 중 하나 이상을 포함하는 웹 네비게이션 행위에 관련된 파라미터 값을 포함하는 것을 특징으로 하는 이상행위 탐지 장치.

청구항 12

제11항에 있어서, 상기 정보 수집부는,

사용자의 PC로부터 사용자의 행위 파라미터 값을 수집하는 PC 정보 수집부, 사용자의 모바일 단말 장치로부터 사용자의 행위 파라미터 값을 수집하는 모바일 정보 수집부, 사용자가 이용하는 웹 서버로부터 사용자의 행위 파라미터 값을 수집하는 웹 서버 정보 수집부를 포함하는 것을 특징으로 하는 이상행위 탐지 장치.

청구항 13

제11항에 있어서,

상기 이상행위 분석 탐지부의 탐지 결과를 기반으로, 기 수집된 행위 파라미터 값 중 정상행위로 판단된 행위 파라미터 값을 기반으로 사용자 별로 상기 이상행위 분석 규칙을 추가 및 삭제하는 규칙 관리부;

를 더 포함하는 것을 특징으로 하는 이상행위 탐지 장치.

청구항 14

제11항에 있어서,

상기 이상행위 분석 탐지부의 탐지 결과를 출력하며, 이상행위 탐지시 이를 관리자에게 통지하는 모니터링부;

를 더 포함하는 이상행위 탐지 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 이상행위 탐지 방법에 관한 것으로, 보다 상세하게는 프로파일 기반 분석과 기계학습 기반 분석을 통해 이상행위를 탐지할 수 있도록 하며, 사용자의 행위 파라미터 값을 통해 이상행위 분석 규칙을 추가 혹은 삭제하며, 기계학습을 통한 이상행위 분석 모델을 생성하여 이상행위를 탐지하기 위한 방법, 그를 위한 장치에 관한 것이다.

배 경 기 술

[0002] 이 부분에 기술된 내용은 단순히 본 실시 예에 대한 배경 정보를 제공할 뿐 종래기술을 구성하는 것은 아니다.

[0003] 다양한 해킹 기법으로 개인정보 유출이 쉬운 사회적 환경에서, 탈취한 사용자 계정, 주민번호, 신용카드 정보 등을 이용하여 웹 해킹 및 온라인 사기 시도 시 이에 대해 효과적으로 대응하기 위한 이상행위 탐지 기술의 필요성이 대두되고 있다. 보험, 금융, 증권, 이동통신 등 다양한 분야에서 다양한 형태의 사기 사건이 발생함에 따라, 사기 여부를 지능적으로 판단할 수 있도록 개선되고 다양한 유형의 웹사이트에 범용적으로 적용될 수 있는 기술 역시 필요하다.

[0004] 웹 서비스의 논리적인 결함이나 미비점을 이용한 이상행위, 사기행위를 탐지하기 위해서는 각 서비스의 논리적인 정상행위 패턴과 비정상 행위 패턴을 분리해 낼 수 있어야 하며, 정상행위 패턴 벡터를 기반으로 비정상 행위를 판단하는 기능이 필요하다.

[0005] 그러나 기존의 이상행위 패턴 탐지 기술은 정적 룰 기반으로 구성되어, 지능화되는 변종 사기 및 다양한 해킹시도에 대하여 적절히 대응할 수 없는 문제점이 있다.

[0006] 이상행위 탐지 기술의 실용성은 사건 발생 전 사전 차단에 있으며 이를 위하여 행위 패턴 분석, 탐지 및 결정까지 소요시간이 적을수록 보다 실효성 있는 시스템이라 할 수 있다.

[0007] 이에 따라 기존 시스템과 같이 사전에 생성된 정적 룰뿐 아니라 신규 패턴을 자동으로 인식할 수 있는 인공지능

기계학습을 통해 능동적 정상 행위 패턴의 범위를 넓힐 수 있는 기술적인 대안의 필요성이 커지고 있다.

[0008] 또한 전자상거래 분야에서 공인인증서 의무사용 정책이 폐지됨에 따라, 보안 취약성에 관한 문제가 야기되었으며, 이 문제를 해결하기 위한 이상행위 탐지 기술이 주목을 받고 있고, 시장 공개에 따른 원천 기술 확보 역시 이슈가 되고 있다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) 한국등록특허공보 제10-1153968호, 2012년 05월 31일 등록 (명칭: 금융사기 방지 시스템 및 방법)

발명의 내용

해결하려는 과제

[0010] 이에 본 발명은, 다양한 웹 서비스 환경에서 사용자의 행위 패턴 분석을 통해 이상행위 분석 규칙을 추가 또는 삭제하고 기계 학습을 통한 이상행위 분석 모델을 형성하여 이상행위 탐지의 정확도를 높이기 위한 이상행위 탐지 방법과 그를 위한 장치를 제공하고자 한다.

[0011] 본 발명에서 이루고자 하는 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급하지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0012] 본 발명은 상술한 과제를 해결하기 위한 수단으로서, 사용자의 행위 파라미터 값을 실시간으로 수집하는 단계; 상기 수집된 사용자의 행위 파라미터 값을 해당 사용자의 이상행위 분석 규칙과 비교하여, 이상행위 여부를 탐지하는 제1 탐지 단계; 상기 제1 탐지 단계에서 이상행위로 판단되지 않은 사용자의 행위 파라미터 값을 이상행위 분석 모델에 입력하여, 상기 이상행위 분석 모델의 연산을 통해, 이상행위 여부를 탐지하는 제2 탐지 단계; 상기 제1 탐지 단계의 탐지 결과 및 상기 제2 탐지 단계의 탐지 결과를 조합하여, 이상행위 여부를 판단하는 단계; 를 포함하는 이상행위 탐지 방법을 제공한다.

[0013] 본 발명의 다른 일 양상은, 이상 징후 식별에 필요한 사용자 별로 발생한 행위 파라미터 값을 실시간으로 수집하는 정보 수집부; 및 상기 수집된 사용자의 행위 파라미터 값을, 기 생성된 이상행위 분석 규칙과 비교하여 1차 이상행위 여부를 탐지하고 이상행위 분석 모델을 통해 연산하여 2차 이상행위 여부를 탐지하는 이상행위 분석 탐지부; 를 포함하며, 상기 이상행위 분석 탐지부는, 상기 1차 이상행위 여부 및 2차 이상행위 여부의 판단 결과를 조합하여 최종 이상행위 여부를 판단하는 것을 특징으로 하는 이상행위 탐지 장치를 더 제공한다.

발명의 효과

[0014] 본 발명에 따르면, 사용자의 사용 환경 정보(PC, 모바일 등의 핑거프린트 속성 정보)와 사용자의 사용패턴(입력기기 이용 행위 파라미터, 웹 네비게이션 행위 파라미터) 및 특정 웹의 사용자 접근 패턴(사용자 이동 패턴, 시간 별 접속 페이지 정보/분류, 시간대별 사용자 접근 방식) 등의 정보를 기반으로 화이트 리스트(white list)를 구성하고 인공지능 기법(SVDD)의 기계학습을 통해 공격행동을 빠르게 판단할 수 있다.

[0015] 본 발명에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0016] 본 발명에 관한 이해를 돕기 위해 상세한 설명의 일부로 포함되는, 첨부 도면은 본 발명에 대한 실시 예를 제공하고, 상세한 설명과 함께 본 발명의 기술적 특징을 설명한다.

도 1은 본 발명의 실시 예에 따른 이상행위 탐지 방법을 제공하기 위한 시스템의 구성을 설명하기 위한 도면이

다.

도 2는 본 발명의 실시 예에 따른 이상행위 탐지 장치의 개략적인 구성을 설명하기 위한 블록도이다.

도 3은 본 발명의 실시 예에 따른 이상행위 탐지 장치 내 정보 수집부의 개략적인 구성을 설명하기 위한 블록도이다.

도 4는 본 발명의 실시 예에 따른 이상행위 탐지 장치 내 데이터베이스부의 개략적인 구성을 설명하기 위한 블록도이다.

도 5는 본 발명의 실시 예에 따른 이상행위 탐지 장치 내 이상행위 분석 탐지부의 개략적인 구성을 설명하기 위한 블록도이다.

도 6은 본 발명의 실시 예에 다른 이상행위 분석 모델의 형성 과정을 나타낸 흐름도이다.

도 7은 본 발명의 일 실시 예에 따른 이상행위 탐지 방법의 과정을 설명하기 위한 흐름도이다.

도 8은 본 발명의 다른 실시 예에 따른 이상행위 탐지 과정을 나타낸 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0017] 이하, 본 발명에 따른 바람직한 실시 형태를 첨부된 도면을 참조하여 상세하게 설명한다. 첨부된 도면과 함께 이하에 개시될 상세한 설명은 본 발명의 예시적인 실시형태를 설명하고자 하는 것이며, 본 발명이 실시될 수 있는 유일한 실시형태를 나타내고자 하는 것이 아니다. 이하의 상세한 설명은 본 발명의 완전한 이해를 제공하기 위해서 구체적 세부사항을 포함한다. 그러나, 본 발명이 속하는 분야의 통상의 기술자는 본 발명이 이러한 구체적 세부사항 없이도 실시될 수 있음을 안다.

[0018] 몇몇 경우, 본 발명의 개념이 모호해지는 것을 피하기 위하여 공지의 구조 및 장치는 생략되거나, 각 구조 및 장치의 핵심기능을 중심으로 한 블록도 형식으로 도시될 수 있다.

[0019] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함(comprising 또는 including)"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "부", "기", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다. 또한, "일(a 또는 an)", "하나(one)", "그(the)" 및 유사어는 본 발명을 기술하는 문맥에 있어서(특히, 이하의 청구항의 문맥에서) 본 명세서에 달리 지시되거나 문맥에 의해 분명하게 반박되지 않는 한, 단수 및 복수 모두를 포함하는 의미로 사용될 수 있다.

[0020] 또한, 제1, 제2 등과 같이 서수를 포함하는 용어는 다양한 구성요소들을 설명하기 위해 사용하는 것으로, 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용될 뿐, 상기 구성요소들을 한정하기 위해 사용되지 않는다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제2 구성요소는 제1 구성요소로 명명될 수 있고, 유사하게 제1 구성요소도 제2 구성요소로 명명될 수 있다.

[0021] 이하의 설명에서 사용되는 특정 용어들은 본 발명의 이해를 돕기 위해서 제공된 것이며, 이러한 특정 용어의 사용은 본 발명의 기술적 사상을 벗어나지 않는 범위에서 다른 형태로 변경될 수 있다.

[0022] 본 발명은 통신망을 이용한 다양한 서비스 환경에 있어서, 사용자의 행위패턴 분석을 통해 이상행위 탐지 방법을 제공하기 위한 것이다. 이하 도면을 참조하여 본 발명에서 제안하는 방식에 대해 서술한다.

[0023] 도 1은 본 발명의 실시 예에 따른 이상행위 탐지 방법을 제공하기 위한 시스템의 구성을 설명하기 위한 도면이다.

[0024] 도 1을 참조하면, 본 발명에 따른 이상행위 탐지 장치(120)는 통신망(150)을 통해 연결된 하나 이상의 사용자 단말 장치(100)와, 하나 이상의 웹 서비스 서버(110)를 포함하여 이루어질 수 있다.

[0025] 본 발명의 실시를 위한 사용자 단말 장치(100)는 본 발명에 의해 제공되는 통신망에 접속하여 데이터를 송수신하는 장치를 의미한다. 여기서, 단말(100)은 UE(User Equipment), MS(Mobile Station), MSS(Mobile Subscriber Station), SS(Subscriber Station), AMS(Advanced Mobile Station), WT(Wireless terminal), MTC(Machine-Type Communication) 장치, M2M(Machine-to-Machine) 장치, D2D 장치(Device-to-Device), 스테이션(STA: Station) 등의 용어에 의해 대체될 수 있다.

[0026] 이러한 본 발명의 실시 예에 따른 사용자 단말 장치(100)는 다양한 형태로 구현될 수 있다. 예를 들어, 스마트폰(smart phone), 타블렛 PC(Tablet PC), PDA(Personal Digital Assistants), PMP(Portable Multimedia Player), MP3 Player 등의 이동 단말기는 물론, 스마트 TV(Smart TV), 데스크탑 컴퓨터 등과 같은 고정 단말기가 사용될 수도 있다.

[0027] 그러나 이에 한정되지 않으며, 유/무선을 구분하지 않고, 사용자를 통신망(150)에 접속할 수 있도록 하여 일정한 기능을 수행하는 장치는 모두 본 발명에서 서술하는 단말에 해당할 수 있다.

[0028] 사용자 단말 장치(100)는 통신망(150)을 경유하여 다른 단말이나 웹 서비스 서버(110), 이상행위 탐지 장치(120)와 연결된다. 여기서 통신망(150)은 컴퓨터 시스템들 및/또는 모듈들 간의 전자 데이터를 전송할 수 있게 하는 하나 이상의 데이터 링크로서 정의된다. 예컨대, WLAN(Wireless LAN), 와이파이(Wi-Fi), 와이브로(Wibro), 와이맥스(Wimax), HSDPA(High Speed Downlink Packet Access) 등의 무선 통신 방식 또는 이더넷(Ethernet), xDSL(ADSL, VDSL), HFC(Hybrid Fiber Coaxial Cable), FTTC(Fiber to The Curb), FTTH(Fiber To The Home) 등의 유선 통신 방식을 이용할 수 있다. 또한, 상술한 통신 방식 이외에도 기타 널리 공지되었거나 향후 개발될 모든 형태의 통신 방식을 포함할 수 있다.

[0029] 정보가 네트워크 또는 다른 (유선, 무선, 또는 유선 또는 무선의 조합인) 통신 접속을 통하여 컴퓨터 시스템에 전송되거나 제공될 때, 이 접속은 컴퓨터-판독가능매체로서 이해될 수 있다. 컴퓨터 판독가능 명령어는, 예를 들면, 범용 컴퓨터 시스템 또는 특수 목적 컴퓨터 시스템이 특정 기능 또는 기능의 그룹을 수행하도록 하는 명령어 및 데이터를 포함한다. 컴퓨터 실행가능 명령어는, 예를 들면, 어셈블리어, 또는 심지어는 소스코드와 같은 이진, 중간 포맷 명령어일 수 있다.

[0030] 웹 서비스 서버(110) 역시 통신망(150)을 경유하여 다른 웹 서비스 서버나 사용자 단말 장치(100), 이상행위 탐지 장치(120)와 연결된다. 웹 서비스 서버(110)는 사용자 단말 장치(100)를 통해 사용자가 이용하는 서비스를 제공하는 주체이다. 예를 들어, 본 발명의 웹 서비스 서버(110)는 보험, 금융 서비스 제공사의 온라인 거래 제공을 위한 서버가 될 수 있으며, 증권 거래를 위한 HTS(Home Trading System) 혹은 MTS(Mobile Trading System)과 연결되는 서비스 제공 서버일 수도 있다. 서비스 제공 분야가 전자상거래로 한정되는 것은 아니며, 온라인 서버를 이용해 제공되는 게임, 음악, 영상 등 각종 컨텐츠 제공 서비스를 위한 서버가 될 수 있으며, 그 분야를 한정하지 않는다.

[0031] 이상행위 탐지 장치(120)는 본 발명의 주요한 구성을 이루는 부분으로, 이하 도 2 내지 도 5에 그 구성이 나타나 있다.

[0032] 도 2는 본 발명의 실시 예에 따른 이상행위 탐지 장치의 개략적인 구성을 설명하기 위한 블록도이다.

[0033] 도 2를 참조하면, 본 발명에 따른 이상행위 탐지 장치(120)는 정보 수집부(210)와, 이상행위 분석 탐지부(220), 데이터베이스부(230), 모니터링부(240) 및 규칙 관리부(250)를 포함하여 이루어질 수 있다.

[0034] 정보 수집부(210)는 PC 또는 모바일 등 웹 서비스 이용 과정에서 이상 징후 식별에 필요한 익명성 보장 행위 파라미터 값을 추출 및 수집하기 위한 구성으로, 자세한 구성은 도 3에 나타나 있다.

[0035] 도 3은 본 발명의 실시 예에 따른 이상행위 탐지 장치 내 정보 수집부의 개략적인 구성을 설명하기 위한 블록도이다.

[0036] 도 3을 참조하면, 본 발명에 따른 정보 수집부(210)는 PC 정보 수집부(310), 모바일 정보 수집부(320), 웹 서버 정보 수집부(330)를 포함하여 이루어질 수 있다.

[0037] PC 정보 수집부(310) 및 모바일 정보 수집부(320)는 통신망(150)을 경유하여 PC 또는 모바일 특성에 맞는 하나 이상의 사용자 단말 장치(100)와 연결되며, 웹 서버 정보 수집부(330)는 통신망(150)을 경유하여 하나 이상의 웹 서비스 서버(110)와 연결된다.

[0038] 각 정보 수집부(210)는 정보 수집 대상으로부터 정보를 수집하기 위한 에이전트(Agent)를 구비할 수 있다. 에이전트는 정보 수집을 위하여 관리자를 대신하여 작업을 수행하는 자율적 프로세스로, 독자적으로 존재하지 않고 정보 수집부의 일부로 존재하는 시스템이다. 정보 수집용 에이전트는 사용자 단말 장치(100)의 종류와 이에 설치된 브라우저의 종류에 따라 다르게 구성될 수 있다. 에이전트는 관리자의 개입이 없어도 정해진 스케줄에 따라 통신망(150)을 통하여 정보를 수집하며, 미리 제공된 행위 파라미터의 종류에 관한 정보를 이용하여 전체 또는 일부 통신망(150)을 검색하여 관심이 있는 정보를 모으고, 그것을 매일 또는 일정 시간대 별로 제공하는 기

능을 수행할 수 있다.

[0039] 정보 수집부(210)는 에이전트를 통하여 사용자의 사용자 단말 장치(100) 사용에 관한 정보 또는 웹 서비스 서버(120)에 대한 접근 기록이나 패턴을 수집할 수 있다. 속성을 추출하거나 패턴화 시킬 수 있는 각각의 항목을 파라미터(parameter)라 지칭하며, 추출된 결과를 파라미터 값이라 지칭한다.

[0040] 특히, 본 발명에서 수집하는 파라미터 값은 디바이스 핑거프린팅(Device Fingerprinting) 속성, 입력기기 이용행위, 웹 네비게이션(Web Navigation) 중 하나 이상에 관련된 행위 파라미터 값을 포함할 수 있다.

[0041] 핑거프린팅 기술은 통신과정에서 발생되는 무선신호 특성으로부터 디바이스를 고유하게 식별하는 핑거프린트(모뎀 등 물리적 하드웨어 계층정보, 비콘 헤더 등 MAC 소프트웨어 계층정보 등)를 추출하여 송신 디바이스가 가짜 클론 디바이스인지 아닌지 여부를 식별하는 기술이다. 이는 크게 핑거프린트 생성 및 분류 단계로 나누어진다.

[0042] 본 발명의 실시 예에서 수집하는 디바이스 핑거프린팅 속성과 관련된 파라미터 값은, 사용자가 제공받는 서비스에 관한 고유 정보(거래 번호, 트랜잭션(Transaction) 번호, 서비스 등록 번호 등), 사용자 단말 장치에 관한 환경 정보(M/B ID, CPU ID, HDD S/N, USB S/N과 같은 하드웨어 정보, OS의 버전, 이용 브라우저나 주변 기기의 patch/plugin의 버전, 브라우저의 버전/타입/언어와 같은 소프트웨어 정보, IP주소, MAC 주소, G/W IP 주소, G/W MAC 주소와 같은 네트워크 정보, USIM 정보 등), 사용자 단말 장치(100)의 주변 하드웨어 정보(키보드, 마우스, USB 저장소, 터치패드, 이동식 키보드, 마우스 등의 BLE 제품 등의 정보), 사용자 단말 장치(100)의 소프트웨어 정보(동작 프로세스, 특정 레지스트 정보 등)에 관련된 값을 포함할 수 있다.

[0043] 입력 기기 이용행위에 관련된 파라미터 값은 사용자 단말 장치(100) 내 입력장치에서 수집하며, 여기서 입력 장치는 현재 상용화되어 있거나 향후 상용화가 가능한 다양한 입력 수단으로 구현될 수 있으며, 예를 들면, 키보드, 마우스, 조이스틱, 터치 스크린, 터치 패드 등과 같은 일반적인 입력 장치뿐만 아니라, 사용자의 모션을 감지하여 특정 입력 신호를 발생하는 제스처 입력 수단, 사용자의 음성을 인식하는 음성 인식 수단을 포함할 수 있다. 여기서, 입출력 인터페이스는 예를 들면, 직렬 포트 인터페이스, PS/2 인터페이스, 병렬 포트 인터페이스, USB 인터페이스, IEEE(Institute of Electrical and Electronics Engineers) 1394 인터페이스(즉, 파이어 와이어(FireWire) 인터페이스)와 같은 매우 다양한 서로 다른 인터페이스 중 임의의 것을 논리적으로 나타내거나, 다른 인터페이스의 조합까지도 논리적으로 나타낼 수 있다.

[0044] 입력 기기 이용행위에 관련된 파라미터 종류는 앞서 설명한 바와 같은 입력 장치에 대한 입력 패턴 정보, 입력 장치 자체의 변동 정보, 주된 이용 행위에 관한 정보, 인증 방식에 관한 정보(패턴 터치, 지문 인식, 비밀번호 설정, PC를 통한 브라우징(browsing) 중 모바일 기기를 이용한 인증 등)를 포함할 수 있다.

[0045] 웹 네비게이션 행위에 관련된 파라미터 값은 거래 사전 행위와 관련된 패턴 정보(공인인증서의 발급과 등록, 로그인 행위, 개인정보 변경 행위 등), 인증 행위와 관련된 정보(인증 수단의 추가나 변경, 인증 행위 자체의 패턴 등), 거래 행위 패턴 정보(방문 횟수, 순서, 경로 등), 거래 패턴 정보(거래 금액, 빈도, 일자 등), 비정상 행위와 관련된 사전 정보(로그인 한도 초과, 오류 발생 빈도, 개인정보 변경 시도, 거래 위치와 시간)에 관련된 파라미터 값을 포함할 수 있다. 웹 네비게이션 행위와 관련된 파리미터 값은 웹 트래픽 (Web Traffic) 정보 수집을 통해 수집 및 추출될 수 있다.

[0046] 분류된 각 파라미터 값은 정보 수집부 내에 구비된 저장장치에 저장되거나 별도의 데이터베이스부(230)에 저장될 수도 있다.

[0047] 이상행위 분석 탐지부(210)는 수집된 파라미터 값을 이용한 이상행위 분석 탐지를 수행하기 위한 수단으로서, 자세한 구성은 도 4에 나타나 있다.

[0048] 도 4를 참조하면, 본 발명에 따른 이상행위 분석 탐지부(230)는 사용자 식별부(410), 실시간 처리용 분산 저장 데이터베이스(420), 특징 추출부(430), 제1이상행위 분석부(440) 및 제2이상행위 분석부(450)를 포함하여 이루어질 수 있다.

[0049] 사용자 식별부(410)는 수집된 파라미터 값이 어떤 사용자의 파라미터 값인지 판별하는 기능을 수행하기 위한 구성이다. 사용자 식별부(410)에 의해 각각의 사용자가 구분되며, 사용자별로 파라미터 값을 구분하기 위하여 사용자 단말 장치(100)에 관한 정보(IP, MAC 주소 등) 또는 로그인 ID를 이용하여 각 사용자 별로 프로파일링을 실시할 수 있다. 이러한 프로파일링 시 수집한 IP, ID 정보를 기반으로 정상 사용자 여부를 판단할 수 있다.

[0050] 실시간 처리용 분산 저장 데이터베이스(420)는 본 발명의 실시에 따른 실시간 정보를 처리하기 위한 데이터베이스이다. 실시간 처리를 위해 별도로 구성된 데이터베이스부(230)가 아닌 이상행위 분석 탐지부(220) 내에 구성

되어 있으며, 실시간 처리용 분산 저장 데이터베이스(420) 내에 사용자 별 프로파일 정보를 생성하고 저장하는 기능을 수행한다.

[0051] 특징 추출부(430)는 각 사용자 별 프로파일 정보를 이용하여 실시간으로 특징 추출 결과를 이용한 특징 벡터를 생성하기 위한 구성이다. 특징 벡터의 차원과 항목은 수집된 행위 파라미터 값에 의해 결정되며, 항목이 많을수록 차원이 높아지며 성능이 높아질 수 있다. 본 발명을 수행하기 위하여 필요한 항목의 수는 디바이스 핑거 프린팅에 관련된 행위 파라미터 값 4종, 입력 기기 이용행위 파라미터 값 450종 이상이 적정하나, 이에 한정되는 것은 아니다.

[0052] 제1 이상행위 분석부(440)는 행위 파라미터 값을 해당 사용자의 이상행위 분석 규칙과 비교하여, 이상행위 여부를 탐지하기 위한 구성이다. 이를 제1 탐지 단계라 지칭한다. 이상행위 규칙은 각 사용자 별로 생성될 수 있다.

[0053] 또한, 제1 이상행위 분석부(440)는 프로파일 정보를 기반으로 이상행위를 분석하고 탐지할 수 있다. 이는 특징 추출부(430)에서 추출한 특징 벡터를 이용하여 수행할 수 있으며, 추출한 특징 벡터 또는 프로파일 특성을 이상행위 분석 규칙과 비교하여 이상행위 여부를 탐지한다.

[0054] 아울러, 제1 이상행위 분석부(440)에는 정상행위에 대응하는 화이트리스트(White List)와 이상행위에 대응하는 블랙리스트(Black List)가 기 설정 또는 저장되어 있을 수 있다. 제1 이상행위 분석부(440)는 기 설정된 화이트리스트와 블랙리스트를 행위 파라미터 값과 비교하여 이상행위 여부를 탐지한다.

[0055] 제2 이상행위 분석부(450)는 학습데이터를 기반으로 이상행위 분석 모델을 생성하고 이상행위를 탐지하기 위한 구성이다. 이를 제2 탐지 단계라 지칭한다. 제2 이상행위 분석부(450)에는 이상행위 분석 모델이 기 저장되어 있을 수 있다. 또한, 제2 이상행위 분석부(450)는 특징 추출부(430)에서 생성된 특징 벡터에 관한 정보를 수신하여 이를 기반으로 학습데이터를 추출하고, 기계학습을 수행한다. 기계학습의 수행을 통해 이상행위 분석 모델이 수정될 수 있다. 여기서 이상행위 분석 모델은 SVDD(Support Vector Data Description) 기법을 이용해 생성된 분석 모델일 수 있다.

[0056] SVDD는 분류 대상이 되는 하나의 학습 클래스에 속한 데이터만을 이용하여 학습을 수행할 수 있는 단일 클래스 문제(One-Class Classification Problems)를 해결하는데 유용한 기법 중 하나이다. SVDD는 특이점을 검출하여 주어진 목적 데이터 대부분을 포함하는 경계면을 찾는다. 경계면은 목적 데이터를 최대한 포함하며, 특이점을 가정 적게 포함하는 구로 구성된다. 학습 데이터의 집합은 중심 a와 반지름 r을 가지는 경계면 내부 혹은 외부에 분포되며, 학습 데이터 수만큼의 제곱에 해당하는 구를 이용해 학습 클래스의 영역을 표현한다. 학습 데이터가 경계면 외부에 분포하는 경우에는 패널티가 부과된다. 특이점과 구의 크기는 각종 변수와 상수, Lagrangean Multiplier를 이용한 함수로 나타낼 수 있으며, 고차원 특정 공간(Feature Space)을 표현하기 위한 커널이 더 이용될 수 있다.

[0057] 제2 이상행위 분석부(450)는 기계학습을 이용하여 생성된 이상행위 분석 모델과 현재 사용자 단말 장치(100)를 통해 수집되고 있는 행위 파라미터 값을 상호 비교하여, 상기 행위 파라미터 값이 생성된 이상행위 분석 모델의 경계면 안에 포함되는지, 경계면 밖에 존재하는지를 판단하여 이상행위 여부를 탐지한다.

[0058] 이상행위 분석 탐지부(220)는 제1 탐지 단계의 결과와 제2 탐지 단계의 결과를 조합하여 이상행위 여부를 최종 판단할 수 있다.

[0059] 도 5는 본 발명의 실시 예에 따른 이상행위 탐지 장치 내 데이터베이스부(230)의 개략적인 구성을 설명하기 위한 블록도이다.

[0060] 데이터베이스부(230)는 이를 관리하는 데이터베이스 관리 시스템(DBMS, DataBase Management System)을 포함한다. DBMS는 데이터베이스부(230)를 관리하며 본 발명인 이상행위 탐지 시스템과 관련된 응용 프로그램들이 데이터베이스부(230)를 공유 및 사용할 수 있는 환경을 제공한다. DBMS에 의해 데이터베이스 구축 틀이 형성되며 응용 프로그램이 데이터베이스부(230)에 접근할 수 있는 인터페이스, 데이터베이스부(230)의 장애에 따른 복구, 보안 유지 기능 등을 제공한다.

[0061] 도 5를 참조하면, 본 발명에 따른 데이터베이스부(230)는 대용량 로그 저장 데이터베이스(410), 이상행위 프로파일 데이터베이스(420), 특성추출벡터 데이터베이스(430), 서비스 접근 기록 데이터베이스(440)를 포함하여 이루어질 수 있다.

[0062] 대용량 로그 저장 데이터베이스(510)는 실시간 처리용 분산 저장 데이터베이스(420)로부터 각 사용자 별 로그 데이터를 수신하여 저장하기 위한 구성이다. 로그 데이터에는 로그인 및 로그아웃 기록, 접속 시 연결된 파일의

수(히트, Hits), 사용자의 웹 브라우저가 HTML로 구성된 웹 문서를 다운받은 횟수(페이지뷰, PageView), 방문자가 사이트에 접속하여 다른 사이트로 떠날 때까지의 상태(세션, Session), 특정 사이트에 머무른 시간(Duration Time)이 포함될 수 있다.

[0063] 이상 행위 프로파일 데이터베이스(520)는 실시간 처리용 분산 저장 데이터베이스(420)로부터 프로파일 정보를 수신하여 저장하기 위한 구성이다.

[0064] 특성 추출 벡터 데이터베이스(530)는 특성 추출부(430)가 추출해낸 특성 벡터를 수신하여 저장하기 위한 구성이다.

[0065] 이상행위 분석 규칙 데이터베이스(540)는 기 설정된 블랙리스트와 화이트리스트를 저장하거나, 그 외 기 설정된 이상행위 분석 규칙을 저장하기 위한 구성이다. 이상행위 분석 규칙 데이터베이스(540)는 제1 이상행위 분석부(440) 및 제2 이상행위 분석부(450), 규칙 관리부(250)와 연결되어 추가된 학습 데이터를 수신하고 변경된 이상행위 분석 규칙을 저장할 수 있다.

[0066] 데이터베이스부(230)는 하나의 서버 혹은 저장장치로 구성되거나, 다수의 서버 혹은 저장장치에 나뉘어 구성될 수 있다. 저장장치는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM(Compact Disk Read Only Memory), DVD(Digital Video Disk)와 같은 광 기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media) 및 롬(ROM), 램(RAM, Random Access Memory), 플래시 메모리를 포함한다.

[0067] 모니터링부(240)는 이상행위 분석 탐지부(220)의 탐지 결과를 출력하며, 이상행위 탐지 시 이를 관리자에게 통지하기 위한 구성이다. 모니터링부(240)는 관리를 위한 별도의 웹 서버나 시스템을 구비할 수 있으며, 대시보드를 포함할 수 있다. 대시보드는 한 화면에서 다양한 정보를 중앙 집중적으로 관리하고 찾을 수 있는 사용자 인터페이스 기능을 포함한다.

[0068] 규칙 관리부(250)는 이상행위 분석 탐지부(220)의 탐지 결과를 기반으로, 기 수집된 행위 파라미터 값들 중 정상행위로 판단된 행위 파라미터 값을 정상행위 학습 데이터로 추출하고, 추출된 정상행위 학습 데이터를 기반으로 사용자 별로 상기 이상행위 분석 규칙을 추가 및 삭제하기 위한 구성이다.

[0069] 또한 규칙 관리부(250)를 통해 새로운 기기 및 웹 서비스 접근 형태에 의한 이상행위들에 관하여, 규칙의 추가 또는 삭제가 이루어질 수 있다.

[0070] 이러한 규칙의 추가 또는 삭제는 관리자의 판단 하에 이루어질 수도 있으나, 규칙 관리부(250)에서 이상행위 분석 규칙과의 비교를 통해 정상행위 또는 이상행위로 판단된 행위 파라미터 값을 기반으로 해당 사용자의 이상행위 분석 규칙을 추가 또는 삭제할 수 있다. 예를 들어, 일정 횟수 이상 이상행위로 판단된 행위 파라미터 값의 조합은 이후부터 이상행위로 판단하도록 하는 이상행위 분석 규칙을 추가 및 적용하도록 규칙 관리부(250)에서 데이터베이스부(230) 또는 이상행위 분석탐지부(220)를 제어할 수 있다.

[0071] 도 6은 본 발명의 실시 예에 다른 이상행위 분석 모델의 형성 과정을 나타낸 흐름도이다.

[0072] 제2 이상행위 분석부(450)는 사용자의 행위 파라미터 값 중 정상행위로 판단된 행위 파라미터 값을 학습 데이터로 추출한다(S600). 제2 이상행위 분석부(450)는 이상행위 분석 모델 생성을 위해 상기 학습 데이터를 특징 벡터화하며(S602), 이후, 상기 학습 데이터를 기반으로 기계학습을 수행한다(S604). 기계학습의 방식으로는 SVDD를 이용할 수 있다. 기계학습의 수행을 통해 이상행위 분석 모델이 생성된다(S606).

[0073] 도 7은 본 발명의 일 실시 예에 따른 이상행위 탐지 방법의 과정을 설명하기 위한 흐름도이다.

[0074] 도 7을 참조하면, 먼저 정보 수집부(210)에서 사용자의 행위 파라미터 값을 수집한다(S700). 제1 이상행위 분석부(440)는 행위 파라미터 값을 이상행위 분석 규칙 데이터베이스(540) 내에 저장된, 이상행위로 기 설정된 이상행위 분석 규칙과 비교(S702)하여 대응되는 부분이 존재하는지 판단하며(S704), 이상행위 분석 규칙에 이상행위로 지정된 부분이 있는 경우 이상행위로 판단할 수 있다(S710a). 이상행위 분석 규칙에는 블랙리스트 및 화이트리스트가 포함될 수 있다. 블랙리스트에는 이상행위를 일으킨 IP나 계좌가 등록되어 있을 수 있으며, 화이트리스트에는 정상사용자로 인증 및 등록된 특정 IP나 사용자 단말이 포함될 수 있다.

[0075] 이상행위로 판단되지 않은 경우에는, 제2 이상행위 분석부(450)에서 행위 파라미터 값을 이상행위 분석 모델에 입력하여 이상행위 여부를 판단하는 기계학습 기반의 탐지를 수행한다(S706). 도 5에서 설명한 바와 같이, 기계학습, 특히 SVDD를 통해 이상행위 분석 모델이 생성될 수 있다. 제2 이상행위 분석부(450)는 실시간으로 수집된

사용자의 행위 파라미터 값이 이상행위 분석 모델의 경계면 안에 포함되는지, 경계면 밖에 존재하는지를 판단하여 이상행위에 해당하는지 탐지한다(S708).

[0076] 정상행위로 판단(S710b)되는 경우 이상행위 분석 규칙을 추가 또는 삭제할 수 있으며, 필요에 따라 이상행위 분석 모델을 변경하기 위한 기계 학습을 수행할 수 있다. 이상행위로 탐지된 경우에는 관리자에게 통지할 수 있다(S710a).

[0077] 여기서 이상행위로 기 설정된 이상행위 분석 규칙은, 사용자 별로 기 수집된 행위 파라미터를 이용하여 생성된 것일 수 있다. 또한, 위험도 산출의 결과를 이용하여 분석 규칙의 추가 또는 삭제가 이루어질 수 있다.

[0078] 도 8은, 본 발명의 다른 실시 예에 따른 이상행위 탐지 방법의 과정을 설명하기 위한 흐름도이다.

[0079] 도 8을 참조하면, 먼저 정보 수집부(210)에서 사용자의 행위 파라미터 값을 추출 및 수집한다(S800).

[0080] 수집된 파라미터 값은 프로파일 기반 체크(S802) 및 기계학습 기반 체크(S806) 과정을 거치며, 이상행위 여부를 판단하게 된다(S804, S808).

[0081] 이후 기계학습 기반 이상행위 탐지 단계(제1 탐지 단계)의 탐지 결과와 프로파일 기반 이상행위 탐지 단계(제2 탐지 단계)의 탐지 결과를 조합하여 이상행위 여부를 최종 판단하여(S810) 이상행위로 판단되면 판단 결과를 관리자에게 통지한다(S818).

[0082] 이상행위 여부의 판단이 확실하지 않은 경우, 또는 판단 결과가 정상행위인 경우, 상관도를 분석하여 위험도를 산출할 수 있다(S812). 상관도 분석에는 피어슨 상관계수를 이용할 수 있다. 피어슨 상관계수는 각 변수를 x, y라 칭할 때, r = x와 y가 함께 변하는 정도 / x와 y가 따로 변하는 정도로 나타내어지며, 수식으로 나타내면

[0083] $$r = \frac{\Sigma(x-\bar{x})(y-\bar{y})}{\sqrt{\Sigma(x-\bar{x})^2\Sigma(y-\bar{y})^2}}$$

[0084] 와 같다. r은 -1<0<1 사이에서 형성되며, r의 양수이면 양의 선형관계, r이 음수이면 음의 선형관계, 0인 경우는 선형 상관관계가 아님을 뜻한다.

[0085] 이러한 상관관계를 통해 이상행위에 앞서 연속적으로 발생하는 행위와 이상행위 간 상관관계를 분석하여 위험도를 산출하고(S812) 이를 이상행위 분석 규칙에 추가하여 이를 기반으로 이상행위를 탐지할 수 있다(S814).

[0086] 탐지 결과 및 위험도 산출 결과는 이상행위 분석 규칙 데이터베이스(540)에 저장될 수 있으며(S816), 상기 결과는 관리자에게 통지되며 이상행위 분석 규칙에 반영될 수 있다(S818).

[0087] 본 명세서와 도면에서는 예시적인 장치 구성을 기술하고 있지만, 본 명세서에서 설명하는 기능적인 동작과 주제의 구현물은 다른 유형의 디지털 전자 회로로 구현되거나, 본 명세서에서 개시하는 구조 및 그 구조적인 등가물들을 포함하는 컴퓨터 소프트웨어, 펌웨어 혹은 하드웨어로 구현되거나, 이들 중 하나 이상의 결합으로 구현 가능하다. 본 명세서에서 설명하는 주제의 구현물은 하나 이상의 컴퓨터 프로그램 제품, 다시 말해 본 발명에 따른 장치의 동작을 제어하기 위하여 혹은 이것에 의한 실행을 위하여 유형의 프로그램 저장매체 상에 인코딩된 컴퓨터 프로그램 명령에 관한 하나 이상의 모듈로서 구현될 수 있다. 컴퓨터로 판독 가능한 매체는 기계로 판독 가능한 저장 장치, 기계로 판독 가능한 저장 기판, 메모리 장치, 기계로 판독 가능한 전파형 신호에 영향을 미치는 물질의 조성물 혹은 이들 중 하나 이상의 조합일 수 있다.

[0088] 본 명세서는 다수의 특정한 구현물의 세부사항들을 포함하지만, 이들은 어떠한 발명이나 청구 가능한 것의 범위에 대해서도 제한적인 것으로서 이해되어서는 안되며, 오히려 특정한 발명의 특정한 실시형태에 특유할 수 있는 특징들에 대한 설명으로서 이해되어야 한다. 개별적인 실시형태의 문맥에서 본 명세서에 기술된 특정한 특징들은 단일 실시형태에서 조합하여 구현될 수도 있다. 반대로, 단일 실시형태의 문맥에서 기술한 다양한 특징들 역시 개별적으로 혹은 어떠한 적절한 하위 조합으로도 복수의 실시형태에서 구현 가능하다. 나아가, 특징들이 특정한 조합으로 동작하고 초기에 그와 같이 청구된 바와 같이 묘사될 수 있지만, 청구된 조합으로부터의 하나 이상의 특징들은 일부 경우에 그 조합으로부터 배제될 수 있으며, 그 청구된 조합은 하위 조합이나 하위 조합의 변형물로 변경될 수 있다.

[0089] 마찬가지로, 특정한 순서로 도면에서 동작들을 묘사하고 있지만, 이는 바람직한 결과를 얻기 위하여 도시된 그 특정한 순서나 순차적인 순서대로 그러한 동작들을 수행하여야 한다거나 모든 도시된 동작들이 수행되어야 하는 것으로 이해되어서는 안 된다. 특정한 경우, 멀티태스킹과 병렬 프로세싱이 유리할 수 있다. 또한, 상술한 실시

형태의 다양한 시스템 컴포넌트의 분리는 그러한 분리를 모든 실시형태에서 요구하는 것으로 이해되어서는 안되며, 설명한 프로그램 컴포넌트와 시스템들은 일반적으로 단일의 소프트웨어 제품으로 함께 통합되거나 다중 소프트웨어 제품에 패키징 될 수 있다는 점을 이해하여야 한다.

산업상 이용가능성

[0090] 본 발명은, 이상행위 탐지 방법에 관한 것으로, 사용자 단말 장치의 환경 및 사용자의 행동 패턴 분석을 통해 실시간 이상 행위 탐지 기술을 제공할 수 있다.

[0091] 특히 본 발명에 따르면, 익명성 보장 파라미터 값의 추출 수집을 통해 파라미터 값에 대한 이상행위 분석 탐지를 수행한다. 구체적으로, 다수의 이상행위 분석 및 탐지 규칙을 적용하고 기계학습을 수행하여 높은 이상행위 여부 탐지 성공률을 보장할 수 있다.

부호의 설명

[0092] 100: 사용자 단말 장치

110: 웹 서비스 서버

120: 이상행위 탐지 장치

210: 정보 수집부

220: 이상행위 분석 탐지부

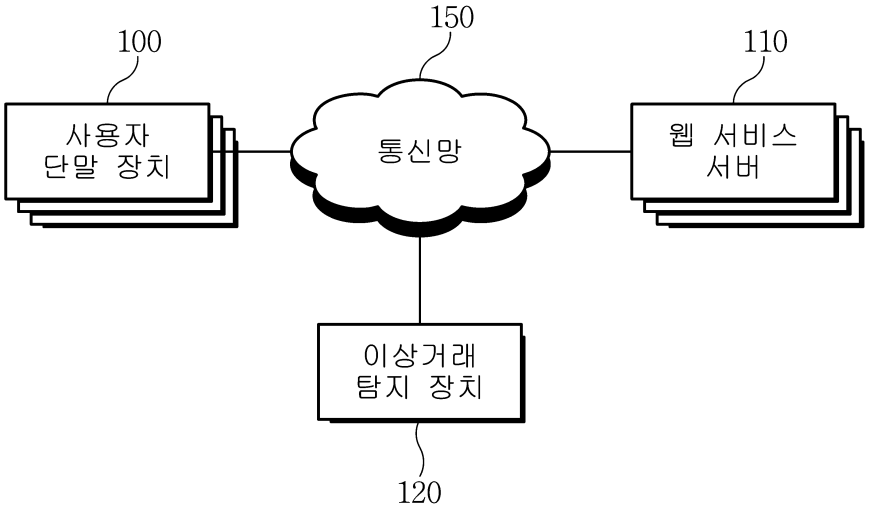
230: 데이터베이스부

240: 모니터링부

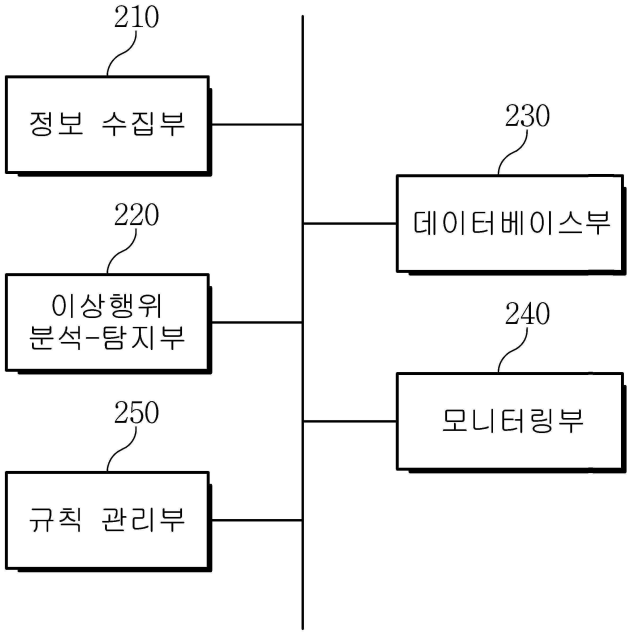
250: 규칙 관리부

도면

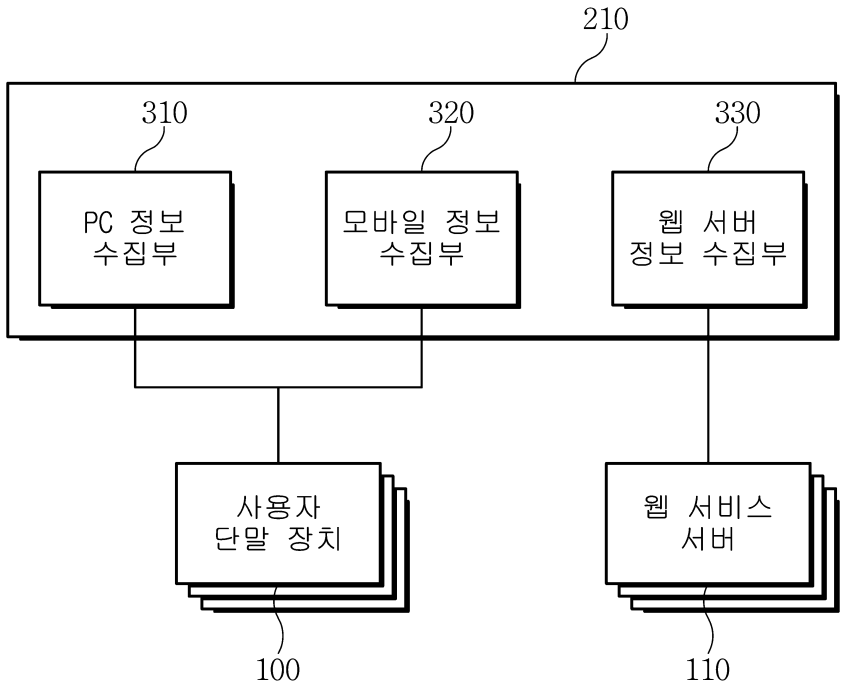
도면1



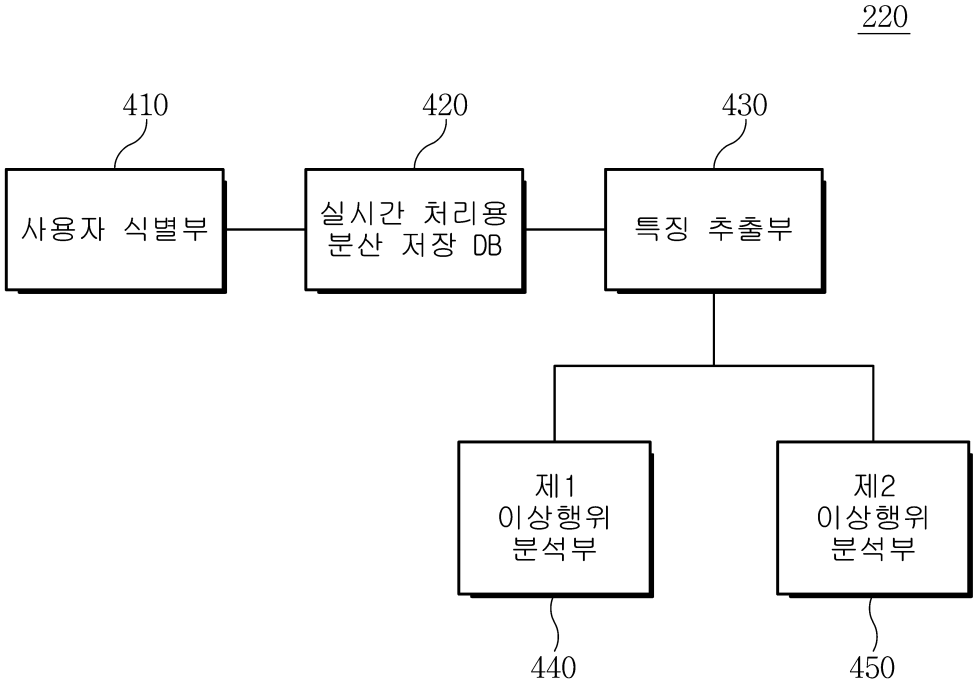
도면2


210
정보 수집부
230
데이터베이스부
220
이상행위
분석-탐지부
240
모니터링부
250
규칙 관리부

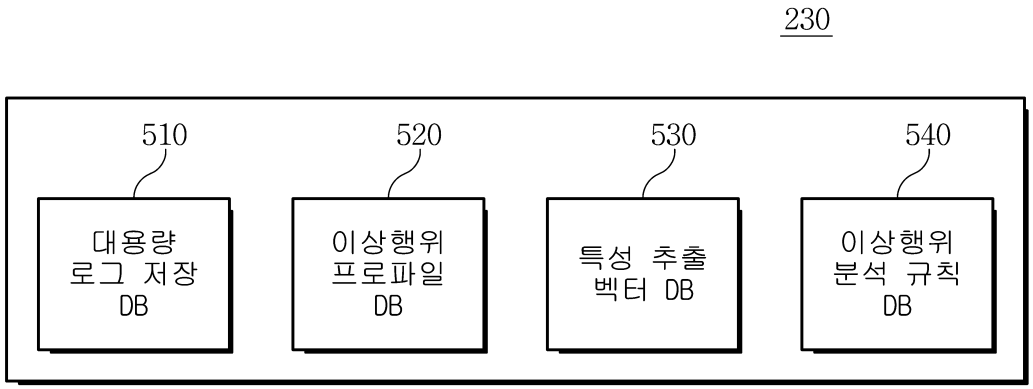
도면3


210
310
320
330
PC 정보
수집부
모바일 정보
수집부
웹 서버
정보 수집부
사용자
단말 장치
웹 서비스
서버
100
110

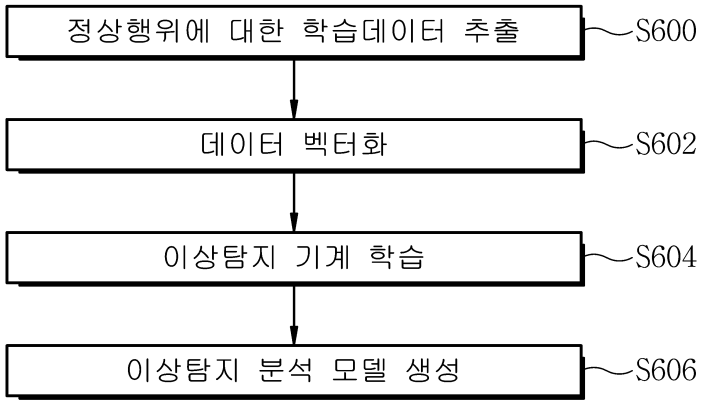
도면4


220
410
420
430
사용자 식별부
실시간 처리용 분산 저장 DB
특징 추출부
제1 이상행위 분석부
제2 이상행위 분석부
440
450

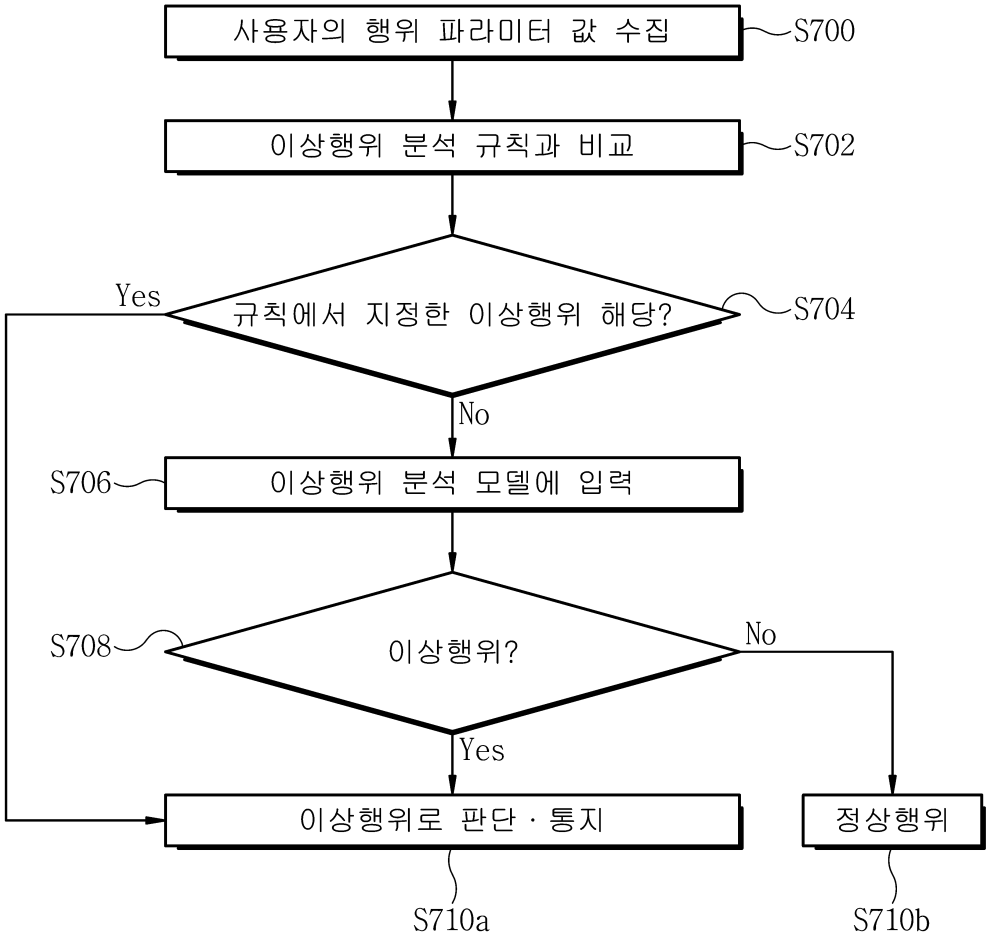
도면5


230
510
520
530
540
대용량 로그 저장 DB
이상행위 프로파일 DB
특성 추출 벡터 DB
이상행위 분석 규칙 DB

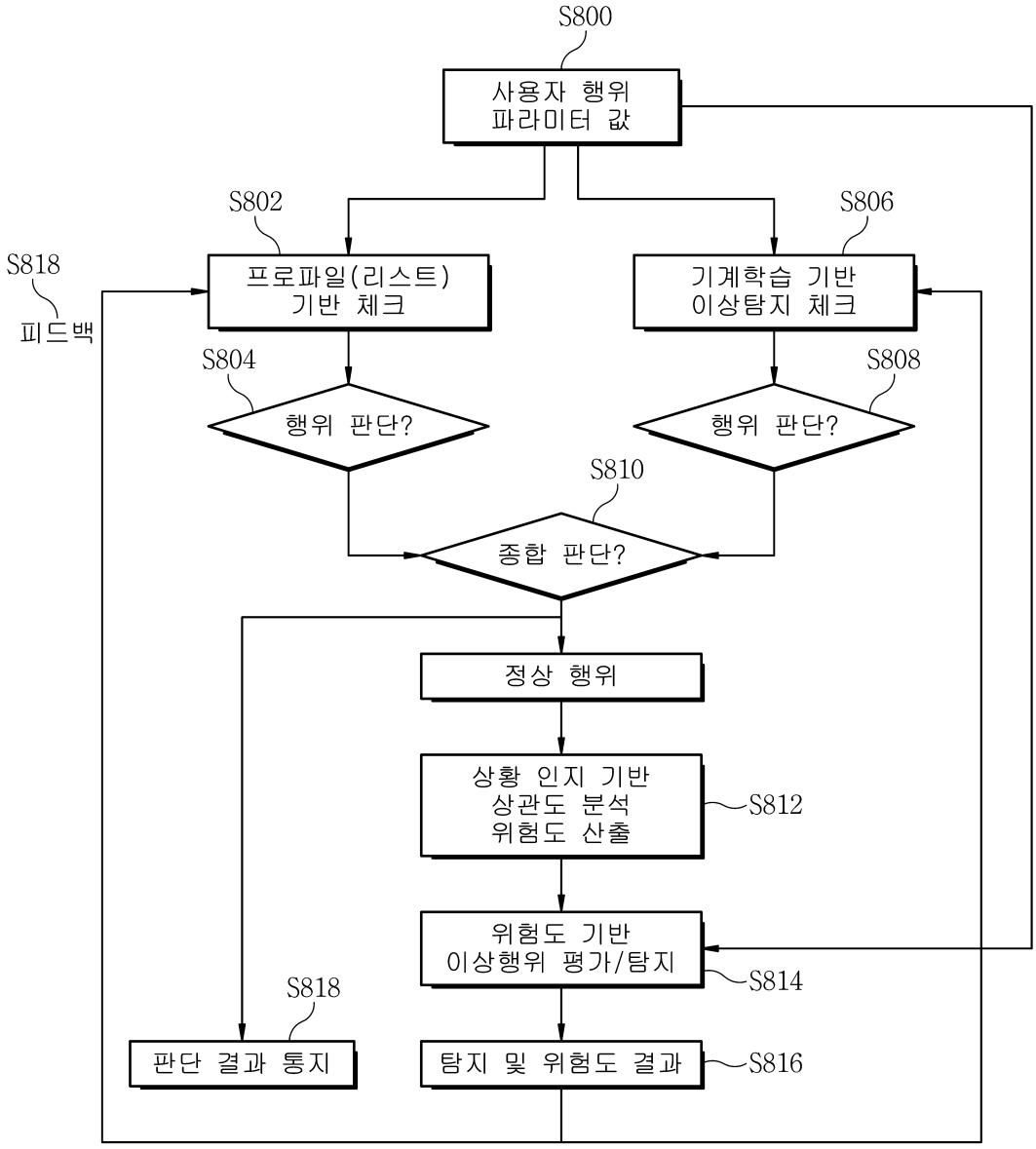
도면6


정상행위에 대한 학습데이터 추출
S600
데이터 벡터화
S602
이상탐지 기계 학습
S604
이상탐지 분석 모델 생성
S606

도면7


사용자의 행위 파라미터 값 수집
S700
이상행위 분석 규칙과 비교
S702
규칙에서 지정한 이상행위 해당?
S704
Yes
No
S706
이상행위 분석 모델에 입력
S708
이상행위?
No
Yes
이상행위로 판단 · 통지
정상행위
S710a
S710b

도면8


S800
사용자 행위
파라미터 값
S802
프로파일(리스트)
기반 체크
S806
기계학습 기반
이상탐지 체크
S818
피드백
S804
행위 판단?
S808
행위 판단?
S810
종합 판단?
정상 행위
상황 인지 기반
상관도 분석
위험도 산출
S812
위험도 기반
이상행위 평가/탐지
S814
S818
판단 결과 통지
탐지 및 위험도 결과
S816