(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년07월01일
(11) 등록번호 10-2271449
(24) 등록일자 2021년06월25일

(51) 국제특허분류(Int. Cl.)
G06N 99/00 (2019.01) *G06F 11/22* (2017.01)
G06F 11/263 (2006.01)
(52) CPC특허분류
G06N 20/00 (2019.01)
G06F 11/2205 (2013.01)
(21) 출원번호 10-2018-0142166
(22) 출원일자 2018년11월17일
심사청구일자 2018년11월17일
(65) 공개번호 10-2020-0057903
(43) 공개일자 2020년05월27일
(56) 선행기술조사문헌
KR101623071 B1*
JP6018345 B2*
KR1020180080111 A
KR1020180120056 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
한국과학기술정보연구원
대전광역시 유성구 대학로 245 (어은동)
(72) 발명자
송중석
세종특별자치시 남세종로 469, 412동 904호 (보람동, 호려울마을4단지)
권태웅
대전광역시 유성구 농대로2번길 29-6, 306호 (어은동)
(뒷면에 계속)
(74) 대리인
이시용

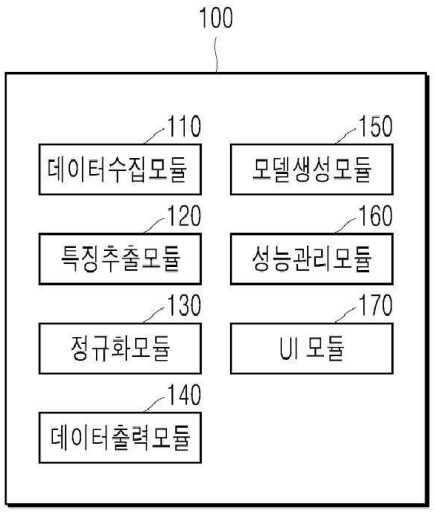
전체 청구항 수 : 총 12 항 심사관 : 박승철

(54) 발명의 명칭 **인공지능 모델 플랫폼 및 인공지능 모델 플랫폼 운영 방법**

(57) 요 약

본 발명은, 보안관제를 위한 인공지능 모델을 생성할 수 있도록 하는 인공지능 모델 플랫폼을 구현하되, 특히 인공지능 모델 성능에 직결되는 특징정보 및 정규화 방식을 최적으로 추천/적용할 수 있도록 함으로써, 보안관제 기술에 익숙하지 않은 일반 사용자도 보안관제를 위한 최적의 인공지능 모델을 생성할 수 있도록 하는 기술에 관한 것이다.

대 표 도 - 도2



(52) CPC특허분류
G06F 11/263 (2013.01)
(72) 발명자
최상수
대전광역시 유성구 노은로 353, 303동 1507호 (하기동, 송림마을아파트3단지)
최윤수
대전광역시 서구 청사로 65, 103동 1303호 (월평동, 황실타운)
이윤수
대전광역시 유성구 죽동로 39, 203동 804호 (죽동, 죽동칸타빌아파트)
박진학
서울특별시 성북구 오패산로3길 17, 105동 2102호 (하월곡동, 동신아파트)
신익수
대전광역시 유성구 대학로 245 (어은동)
이혁로
대전광역시 유성구 어은로 57, 135동 604호 (어은동, 한빛아파트)
박학수
대전광역시 유성구 진잠로149번길 30, 210동 501호 (교촌동, 한승미메이드아파트)
박진형
대전광역시 유성구 봉명로 94, 707동 2305호 (봉명동, 도안신도시7단지예미지백조의호수)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711076890
부처명	과학기술정보통신부
과제관리(전문)기관명	한국과학기술정보연구원
연구사업명	한국과학기술정보연구원연구운영비지원(주요사업비)
연구과제명	자동화 기반 과학기술정보보호서비스
기 여 율	1/1
과제수행기관명	한국과학기술정보연구원
연구기간	2018.01.01 ~ 2018.12.31

명 세 서

청구범위

청구항 1

원천 보안데이터로부터 특정 검색 조건에 의해 학습/테스트 데이터로 사용하고자 하는 보안이벤트를 수집하는 데이터수집부;

상기 수집된 보안이벤트에 대하여 기 설정된 특징정보를 추출하는 특징추출부;

상기 보안이벤트의 추출된 특징정보에 대하여 기 설정된 정규화를 수행하는 정규화부;

상기 특징정보의 정규화가 완료된 보안이벤트에서 학습 데이터 또는 테스트 데이터를 주어진 조건에 의해 추출하는 데이터출력부; 및

상기 학습 데이터에 인공지능 알고리즘을 적용하여, 보안관제를 위한 인공지능 모델을 생성하는 모델생성부을 포함하며,

상기 특징추출부는,

인공지능 모델 생성 시 설정 가능한 전체 특징정보 중 기 설정된 특징정보 학습을 기반으로 생성된 인공지능 모델에 대하여, 모델 성능을 확인하는 모델성능확인부;

상기 전체 특징정보에서 다수의 특징정보 조합을 설정하여, 상기 다수의 특징정보 조합 별로 학습을 기반으로 생성된 인공지능 모델의 성능을 확인하는 조합성능확인부; 및

상기 다수의 특징정보 조합 별 성능 중 상기 모델성능확인부에서 확인한 모델 성능 보다 높은 성능의 특정 특징정보 조합을 추천하는 추천부를 포함하는 것을 특징으로 하는 인공지능 모델 플랫폼 운영 장치.

청구항 2

제 1 항에 있어서,

상기 테스트 데이터를 활용하여, 상기 인공지능 모델의 정확도를 테스트하는 성능관리부를 더 포함하는 것을 특징으로 하는 인공지능 모델 플랫폼 운영 장치.

청구항 3

제 1 항에 있어서,

상기 데이터수집부의 특정 검색 조건, 상기 특징추출부의 특징정보, 상기 정규화부의 정규화 방식, 상기 데이터출력부의 조건 중 적어도 하나를 설정하기 위한 UI(User Interface)를 제공하는 UI부를 더 포함하는 것을 특징으로 하는 인공지능 모델 플랫폼 운영 장치.

청구항 4

제 1 항에 있어서,

상기 데이터수집부는,

수집 건의 총 수가 동시 수행 가능한 최대 수집 건수를 초과하는 경우, 상기 수집 건의 총 개수 중 최대 수집 건수를 초과하는 수집 건을 큐(queue)에 저장한 후 순차적으로 진행하며,

상기 큐에 저장한 후 진행하는 수집 건의 경우, 상기 원천 보안데이터에서 상기 수집 건의 발생시점 이전 데이터에 대해서만 상기 보안이벤트를 수집하는 것을 특징으로 하는 인공지능 모델 플랫폼 운영 장치.

청구항 5

제 2 항에 있어서,

상기 특징추출부는,

상기 성능관리부의 정확도 테스트 결과를 근거로, 상기 인공지능 모델의 정확도를 높이도록 상기 특징정보에 대한 변경을 추천하는 것을 특징으로 하는 인공지능 모델 플랫폼 운영 장치.

청구항 6

제 1 항에 있어서,

상기 정규화부는,

상기 인공지능 모델의 정확도를 높이도록 상기 정규화에 대한 정규화 방식 변경을 추천하는 것을 특징으로 하는 인공지능 모델 플랫폼 운영 장치.

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

컴퓨터로 구현되는 인공지능 모델 플랫폼 운영 장치에 의해 수행되는 인공지능 모델 플랫폼 운영 방법에 있어서,

원천 보안데이터로부터 특정 검색 조건에 의해 학습/테스트 데이터로 사용하고자 하는 보안이벤트를 수집하는 데이터수집단계;

상기 수집된 보안이벤트에 대하여 기 설정된 특징정보를 추출하는 특징추출단계;

상기 보안이벤트의 추출된 특징정보에 대하여 기 설정된 정규화를 수행하는 정규화단계;

상기 특징정보의 정규화가 완료된 보안이벤트에서 학습 데이터 또는 테스트 데이터를 주어진 조건에 의해 추출하는 데이터출력단계; 및

상기 학습 데이터에 인공지능 알고리즘을 적용하여, 보안관제를 위한 인공지능 모델을 모델생성단계를 포함하며,

상기 특징추출단계는,

인공지능 모델 생성 시 설정 가능한 전체 특징정보 중 기 설정된 특징정보 학습을 기반으로 생성된 인공지능 모델에 대하여, 모델 성능을 확인하는 모델성능확인단계;

상기 전체 특징정보에서 다수의 특징정보 조합을 설정하여, 상기 다수의 특징정보 조합 별로 학습을 기반으로 생성된 인공지능 모델의 성능을 확인하는 조합성능확인단계; 및

상기 다수의 특징정보 조합 별 성능 중 상기 모델성능확인단계에서 확인한 모델 성능 보다 높은 성능의 특정 특징정보 조합을 추천하는 추천단계를 포함하는 것을 특징으로 하는 인공지능 모델 플랫폼 운영 방법.

청구항 16

제 15 항에 있어서,

상기 테스트 데이터를 활용하여, 상기 인공지능 모델의 정확도를 테스트하는 성능관리단계를 더 포함하는 것을 특징으로 하는 인공지능 모델 플랫폼 운영 방법.

청구항 17

제 15 항에 있어서,

상기 데이터수집단계의 특정 검색 조건, 상기 특징추출단계의 특징정보, 상기 정규화단계의 정규화 방식, 상기 데이터출력단계의 조건 중 적어도 하나를 설정하기 위한 UI(User Interface)를 제공하는 단계를 더 포함하는 것을 특징으로 하는 인공지능 모델 플랫폼 운영 방법.

청구항 18

제 15 항에 있어서,

상기 데이터수집단계는,

수집 건의 총 수가 동시 수행 가능한 최대 수집 건수를 초과하는 경우, 상기 수집 건의 총 개수 중 최대 수집 건수를 초과하는 수집 건을 큐(queue)에 저장한 후 순차적으로 진행하며,

상기 큐에 저장한 후 진행하는 수집 건의 경우, 상기 원천 보안데이터에서 상기 수집 건의 발생시점 이전 데이터에 대해서만 상기 보안이벤트를 수집하는 것을 특징으로 하는 인공지능 모델 플랫폼 운영 방법.

청구항 19

제 16 항에 있어서,

상기 성능관리단계의 정확도 테스트 결과를 근거로, 상기 인공지능 모델의 정확도를 높이도록 상기 특징정보에 대한 변경을 추천하는 단계를 더 포함하는 것을 특징으로 하는 인공지능 모델 플랫폼 운영 방법.

청구항 20

제 15 항에 있어서,

상기 정규화단계는,

상기 인공지능 모델의 정확도를 높이도록 상기 정규화에 대한 정규화 방식 변경을 추천하는 것을 특징으로 하는 인공지능 모델 플랫폼 운영 방법.

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은, 보안관제를 위한 인공지능 모델 생성 기술에 관한 것으로, 더욱 상세하게는 보안관제 기술에 익숙하지 않은 일반 사용자도 보안관제를 위한 최적의 인공지능 모델을 생성할 수 있도록 하는 인공지능 모델 플랫폼을 제공하기 위한 것이다.

배 경 기 술

[0002] 현재, 과학기술사이버안전센터는 침해위협관리시스템(TMS)을 기반으로 공공연구기관에 대한 실시간 보안관제 서비스를 제공하고 있다.

[0003] 실시간 보안관제 서비스는, 침해위협관리시스템(TMS)에서 탐지 및 수집하는 보안이벤트를 기반으로, 보안관제 요원에 의한 분석 및 대응 지원이 이루어지는 서비스 구조로 제공되고 있다.

[0004] 헌데, TMS에 의해 탐지되는 보안이벤트 수가 폭발적으로 증가하고 있으며, 이와 같은 대용량의 전체 보안이벤트를 보안관제 요원이 분석하기는 현실적으로 어려운 한계 상황에 도달하고 있다.

[0005] 또한, 기존의 보안관제 서비스는, 보안관제 요원의 전문 지식 및 경험에 의존하기 때문에, 특정 보안이벤트에 대한 분석이 집중되는 업무편중 현상 발생하거나 분석 결과의 편차가 발생하는 등 분석 평준화가 실현되지 못하는 상황도 발생하고 있다.

[0006] 결국, TMS에 의해 탐지되는 보안이벤트 수가 폭발적으로 증가하고 있는 현 상황에서는, 보안관제 요원의 분석에 의존하는 기존 보안관제 서비스의 서비스 구조 자체를 혁신할 필요가 있다.

[0007] 이에, 보안관제 요원의 분석을 대체할 수 있는 인공지능 모델을 활용하는 보안관제 서비스 구조를 생각해 볼 수 있다.

[0008] 본 발명에서는, 보안관제를 위한 인공지능 모델을 생성할 수 있도록 하는 인공지능 모델 플랫폼을 제공하고자 한다.

[0009] 특히, 본 발명에서는, 보안관제 기술에 익숙하지 않은 일반 사용자도 보안관제를 위한 최적의 인공지능 모델을 생성할 수 있도록 하는 인공지능 모델 플랫폼을 제공하고자 한다.

발명의 내용

해결하려는 과제

[0010] 본 발명은 상기한 사정을 감안하여 창출된 것으로서, 본 발명에서 도달하고자 하는 목적은, 보안관제를 위한 인

공지능 모델을 생성할 수 있도록 하는 인공지능 모델 플랫폼을 구현하는 방안(기술)을 제공하는데 있다.

과제의 해결 수단

[0011] 상기 목적을 달성하기 위한 본 발명의 제 1 관점에 따른 인공지능 모델 플랫폼은, 원천 보안데이터로부터 특정 검색 조건에 의해 학습/테스트 데이터로 사용하고자 하는 보안이벤트를 수집하는 데이터수집모듈; 상기 수집된 보안이벤트에 대하여 기 설정된 특징정보를 추출하는 특징추출모듈; 상기 보안이벤트의 추출된 특징정보에 대하여 기 설정된 정규화를 수행하는 정규화모듈; 상기 특정정보 정규화가 완료된 보안이벤트에서 학습 데이터 또는 테스트 데이터를 주어진 조건에 의해 추출하는 데이터출력모듈; 및 상기 학습 데이터에 인공지능 알고리즘을 적용하여, 보안관제를 위한 인공지능 모델을 생성하는 모델생성모듈을 포함한다.

[0012] 구체적으로, 상기 테스트 데이터를 활용하여, 상기 인공지능 모델의 정확도를 테스트하는 성능관리모듈을 더 포함할 수 있다.

[0013] 구체적으로, 상기 데이터수집모듈의 특정 검색 조건, 상기 특징추출모듈의 특징정보, 상기 정규화모듈의 정규화 방식, 상기 데이터출력모듈의 조건 중 적어도 하나를 설정하기 위한 UI(User Interface)를 제공하는 UI모듈을 더 포함할 수 있다.

[0014] 구체적으로, 상기 데이터수집모듈은, 수집 건의 총 수가 동시 수행 가능한 최대 수집 건수를 초과하는 경우, 상기 수집 건의 총 개수 중 최대 수집 건수를 초과하는 수집 건을 큐(queue)에 저장한 후 순차적으로 진행하며, 상기 큐에 저장한 후 진행하는 수집 건의 경우, 상기 원천 보안데이터에서 상기 수집 건의 발생시점 이전 데이터에 대해서만 상기 보안이벤트를 수집할 수 있다.

[0015] 구체적으로, 상기 특징추출모듈은, 상기 성능관리모듈의 정확도 테스트 결과를 근거로, 상기 인공지능 모델의 정확도를 높이도록 상기 특징정보에 대한 변경을 추천할 수 있다.

[0016] 구체적으로, 상기 정규화모듈은, 상기 인공지능 모델의 정확도를 높이도록 상기 정규화에 대한 정규화 방식 변경을 추천할 수 있다.

[0017] 상기 목적을 달성하기 위한 본 발명의 제 2 관점에 따른 특징정보 추천 장치는, 인공지능 모델 생성 시 설정 가능한 전체 특징정보 중 기 설정된 특징정보 학습을 기반으로 생성된 인공지능 모델에 대하여, 모델 성능을 확인하는 모델성능확인부; 상기 전체 특징정보에서 다수의 특징정보 조합을 설정하여, 상기 다수의 특징정보 조합별로 학습을 기반으로 생성된 인공지능 모델의 성능을 확인하는 조합성능확인부; 및 상기 다수의 특징정보 조합별 성능 중 상기 모델성능확인부에서 확인한 모델 성능 보다 높은 성능의 특정 특징정보 조합을 추천하는 추천부를 포함한다.

[0018] 구체적으로, 상기 다수의 특징정보 조합은, 상기 기 설정된 특징정보에, 상기 전체 특징정보에서 상기 기 설정된 특징정보를 제외한 나머지 특정정보 중 적어도 하나씩 순차적으로 추가한 조합이며, 상기 특정 특징정보 조합은, 상기 다수의 특징정보 조합 중 상기 모델 성능 보다 높은 성능을 갖는 상위 N개일 수 있다.

[0019] 구체적으로, 상기 기 설정된 특징정보는 상기 전체 특징정보이며, 상기 조합성능확인부는, 상기 전체 특징정보 내 각 단일 특징정보 별로 학습을 기반으로 생성되는 인공지능 모델의 성능 중 최대 성능이 상기 모델 성능 보다 높은지 확인하는 단일특징정보 성능 비교과정, 상기 최대 성능이 상기 모델 성능 보다 높은 경우 상기 최대 성능의 단일 특징정보를 상기 특징정보로 재 설정하고, 상기 특징정보에 상기 전체 특징정보에서 상기 기 설정된 특징정보를 제외한 나머지 특정정보 중 하나씩 순차적으로 추가하여 상기 다수의 특징정보 조합을 설정하는 조합설정 과정, 상기 다수의 특징정보 조합 중 상기 재 설정한 특징정보의 모델 성능 보다 높은 성능을 갖는 특징정보 조합 각각을 특징정보로 재 설정하여, 재 설정한 각 특징정보에 대하여 상기 조합설정 과정이 반복 수행되도록 하는 재설정 과정, 상기 다수의 특징정보 조합 중 상기 모델 성능 보다 높은 성능을 갖는 특징정보 조합이 존재하지 않는 경우, 직전의 특징정보를 상기 특정 특징정보 조합으로서 상기 추천부로 전달하는 과정을 수행할 수 있다.

[0020] 상기 목적을 달성하기 위한 본 발명의 제 3 관점에 따른 정규화 방식 추천 장치는, 인공지능 모델 생성 시 학습에 이용되는 특징정보의 속성을 확인하는 속성확인부; 설정 가능한 전체 정규화 방식 중, 상기 특징정보의 속성에 따른 정규화 방식을 결정하는 결정부; 및 상기 결정한 정규화 방식을 추천하는 추천부를 포함한다.

[0021] 구체적으로, 상기 결정부는, 상기 특징정보 전체 필드에 동일한 정규화 방식 적용되는 경우라면, 상기 특징정보의 속성이 숫자 속성인 경우, 특징정보의 전체 숫자패턴에 따른 제1 정규화 방식을 결정하고, 상기 특징정보의

속성이 카테고리 속성인 경우, 특징정보의 전체 카테고리 개수로 정의되는 벡터(Vector) 내 특징정보의 카테고리 별로 지정된 위치에만 0이 아닌 특성값으로 표현하는 제2 정규화 방식을 결정하고, 상기 특징정보의 속성이 숫자 및 카테고리 조합 속성인 경우, 상기 제2 정규화 방식 및 제1 정규화 방식을 결정할 수 있다.

[0022] 구체적으로, 상기 제1 정규화 방식은, 기 정의된 우선순위에 따라 Standard score 정규화 방식, Mean normalization 정규화 방식, Feature scaling 정규화 방식을 포함하며, 상기 결정부는, 특징정보의 전체 숫자패턴에 대한 표준편차 및 정규화 스케일링 범위 상/하한 존재 여부를 근거로, 상기 제1 정규화 방식 중 적용 가능한 가장 우선순위가 높은 정규화 방식을 결정할 수 있다.

[0023] 구체적으로, 상기 결정부는, 상기 특징정보 전체 필드에서 필드 별로 정규화 방식 적용되는 경우라면, 상기 특징정보에서 속성이 종류 속성의 필드에 대해서는 Mean normalization 정규화 방식, Feature scaling 정규화 방식 중 적용 가능한 가장 우선순위가 높은 정규화 방식을 결정하고, 상기 특징정보에서 속성이 개수 속성의 필드에 대해서는 Mean normalization 정규화 방식, Feature scaling 정규화 방식 중 적용 가능한 가장 우선순위가 높은 정규화 방식을 결정하고, 상기 특징정보에서 속성이 비율 속성의 필드에 대해서는 정규화 방식을 미 결정하고 정규화 대상에서 제외시키거나 또는 Standard score 정규화 방식을 결정하고, 상기 특징정보에서 속성이 존재 여부 속성의 필드에 대해서는 정규화 방식을 미 결정하고 정규화 대상에서 제외시킬 수 있다.

[0024] 상기 목적을 달성하기 위한 본 발명의 제 4 관점에 따른 인공지능 모델 플랫폼 운영 방법은, 원천 보안데이터로부터 특정 검색 조건에 의해 학습/테스트 데이터로 사용하고자 하는 보안이벤트를 수집하는 데이터수집단계; 상기 수집된 보안이벤트에 대하여 기 설정된 특징정보를 추출하는 특징추출단계; 상기 보안이벤트의 추출된 특징정보에 대하여 기 설정된 정규화를 수행하는 정규화단계; 상기 특정정보 정규화가 완료된 보안이벤트에서 학습 데이터 또는 테스트 데이터를 주어진 조건에 의해 추출하는 데이터출력단계; 및 상기 학습 데이터에 인공지능 알고리즘을 적용하여, 보안관제를 위한 인공지능 모델을 생성하는 모델생성단계를 포함한다.

[0025] 구체적으로, 상기 테스트 데이터를 활용하여, 상기 인공지능 모델의 정확도를 테스트하는 성능관리단계를 더 포함할 수 있다.

[0026] 구체적으로, 상기 데이터수집단계의 특정 검색 조건, 상기 특징추출모듈의 특징정보, 상기 정규화모듈의 정규화 방식, 상기 데이터출력모듈의 조건 중 적어도 하나를 설정하기 위한 UI(User Interface)를 제공하는 단계를 더 포함할 수 있다.

[0027] 구체적으로, 상기 데이터수집단계는, 수집 건의 총 수가 동시 수행 가능한 최대 수집 건수를 초과하는 경우, 상기 수집 건의 총 개수 중 최대 수집 건수를 초과하는 수집 건을 큐(queue)에 저장한 후 순차적으로 진행하며, 상기 큐에 저장한 후 진행하는 수집 건의 경우, 상기 원천 보안데이터에서 상기 수집 건의 발생시점 이전 데이터에 대해서만 상기 보안이벤트를 수집할 수 있다.

[0028] 구체적으로, 상기 성능관리단계의 정확도 테스트 결과를 근거로, 상기 인공지능 모델의 정확도를 높이도록 상기 특징정보에 대한 변경을 추천하는 단계를 더 포함할 수 있다.

[0029] 구체적으로, 상기 정규화단계는, 상기 인공지능 모델의 정확도를 높이도록 상기 정규화에 대한 정규화 방식 변경을 추천할 수 있다.

[0030] 상기 목적을 달성하기 위한 본 발명의 제 5 관점에 따른 컴퓨터프로그램은, 하드웨어와 결합하여, 인공지능 모델 생성 시 설정 가능한 전체 특징정보 중 기 설정된 특징정보 학습을 기반으로 생성된 인공지능 모델에 대하여, 모델 성능을 확인하는 모델성능확인단계; 상기 전체 특징정보에서 다수의 특징정보 조합을 설정하여, 상기 다수의 특징정보 조합 별로 학습을 기반으로 생성된 인공지능 모델의 성능을 확인하는 조합성능확인단계; 및 상기 다수의 특징정보 조합 별 성능 중 상기 모델성능확인부에서 확인한 모델 성능 보다 높은 성능의 특정 특징정보 조합을 추천하는 추천단계를 실행시키기 위하여 매체에 저장된다.

[0031] 구체적으로, 상기 다수의 특징정보 조합은, 상기 기 설정된 특징정보에, 상기 전체 특징정보에서 상기 기 설정된 특징정보를 제외한 나머지 특정정보 중 적어도 하나씩 순차적으로 추가한 조합이며, 상기 특정 특징정보 조합은, 상기 다수의 특징정보 조합 중 상기 모델 성능 보다 높은 성능을 갖는 상위 N개일 수 있다.

[0032] 구체적으로, 상기 기 설정된 특정정보는 상기 전체 특징정보이며, 상기 조합성능확인단계는, 상기 전체 특징정보 내 각 단일 특징정보 별로 학습을 기반으로 생성되는 인공지능 모델의 성능 중 최대 성능이 상기 모델 성능 보다 높은지 확인하는 단일특징정보 성능 비교과정, 상기 최대 성능이 상기 모델 성능 보다 높은 경우 상기 최대 성능의 단일 특징정보를 상기 특징정보로 재 설정하고, 상기 특징정보에 상기 전체 특징정보에서 상기 기 설

정된 특징정보를 제외한 나머지 특징정보 중 하나씩 순차적으로 추가하여 상기 다수의 특징정보 조합을 설정하는 조합설정 과정, 상기 다수의 특징정보 조합 중 상기 재 설정한 특징정보의 모델 성능 보다 높은 성능을 갖는 특징정보 조합 각각을 특징정보로 재 설정하여, 재 설정한 각 특징정보에 대하여 상기 조합설정 과정이 반복 수행되도록 하는 재설정 과정, 상기 다수의 특징정보 조합 중 상기 모델 성능 보다 높은 성능을 갖는 특징정보 조합이 존재하지 않는 경우, 직전의 특징정보를 상기 특정 특징정보 조합으로서 상기 추천부로 전달하는 과정을 수행할 수 있다.

[0033] 구체적으로, 상기 기 설정된 특정정보는 상기 전체 특징정보이며, 상기 조합성능확인단계는, 상기 전체 특징정보 내 각 단일 특징정보 별로 학습을 기반으로 생성되는 인공지능 모델의 성능 중 최대 성능이 상기 모델 성능 보다 높은지 확인하는 단일특징정보 성능 비교과정, 상기 최대 성능이 상기 모델 성능 보다 높지 않은 경우 상기 특징정보에서 서로 다른 하나의 특정정보를 제외한 상기 다수의 특징정보 조합을 설정하는 조합설정 과정, 상기 다수의 특징정보 조합 중 상기 모델 성능 보다 높은 성능을 갖는 특징정보 조합 각각을 특징정보로 재 설정하여, 재 설정한 각 특징정보에 대하여 상기 조합설정 과정이 반복 수행되도록 하는 재설정 과정, 상기 다수의 특징정보 조합 중 상기 모델 성능 보다 높은 성능을 갖는 특징정보 조합이 존재하지 않는 경우, 직전의 특징정보를 상기 특정 특징정보 조합으로서 상기 추천부로 전달하는 과정을 수행할 수 있다.

[0034] 상기 목적을 달성하기 위한 본 발명의 제 6 관점에 따른 컴퓨터프로그램은, 하드웨어와 결합하여, 인공지능 모델 생성 시 학습에 이용되는 특징정보의 속성을 확인하는 속성확인단계; 설정 가능한 전체 정규화 방식 중, 상기 특징정보의 속성에 따른 정규화 방식을 결정하는 결정단계; 및 상기 결정한 정규화 방식을 추천하는 추천단계를 실행시키기 위하여 매체에 저장된다.

[0035] 구체적으로, 상기 결정단계는, 상기 특징정보 전체 필드에 동일한 정규화 방식 적용되는 경우라면, 상기 특징정보의 속성이 숫자 속성인 경우, 특징정보의 전체 숫자패턴에 따른 제1 정규화 방식을 결정하고, 상기 특징정보의 속성이 카테고리 속성인 경우, 특징정보의 전체 카테고리 개수로 정의되는 벡터(Vector) 내 특징정보의 카테고리 별로 지정된 위치에만 0이 아닌 특성값으로 표현하는 제2 정규화 방식을 결정하고, 상기 특징정보의 속성이 숫자 및 카테고리 조합 속성인 경우, 상기 제2 정규화 방식 및 제1 정규화 방식을 결정할 수 있다.

[0036] 구체적으로, 상기 제1 정규화 방식은, 기 정의된 우선순위에 따라 Standard score 정규화 방식, Mean normalization 정규화 방식, Feature scaling 정규화 방식을 포함하며, 상기 결정단계는, 특징정보의 전체 숫자패턴에 대한 표준편차 및 정규화 스케일링 범위 상/하한 존재 여부를 근거로, 상기 제1 정규화 방식 중 적용 가능한 가장 우선순위가 높은 정규화 방식을 결정할 수 있다.

[0037] 구체적으로, 상기 결정단계는, 상기 특징정보 전체 필드에서 필드 별로 정규화 방식 적용되는 경우라면, 상기 특징정보에서 속성이 종류 속성의 필드에 대해서는 Mean normalization 정규화 방식, Feature scaling 정규화 방식 중 적용 가능한 가장 우선순위가 높은 정규화 방식을 결정하고, 상기 특징정보에서 속성이 개수 속성의 필드에 대해서는 Mean normalization 정규화 방식, Feature scaling 정규화 방식 중 적용 가능한 가장 우선순위가 높은 정규화 방식을 결정하고, 상기 특징정보에서 속성이 비율 속성의 필드에 대해서는 정규화 방식을 미 결정하고 정규화 대상에서 제외시키거나 또는 Standard score 정규화 방식을 결정하고, 상기 특징정보에서 속성이 존재 여부 속성의 필드에 대해서는 정규화 방식을 미 결정하고 정규화 대상에서 제외시킬 수 있다.

발명의 효과

[0038] 이에, 본 발명에 따른 인공지능 모델 플랫폼 및 인공지능 모델 플랫폼 운영 방법에 의하면, 보안관제를 위한 인공지능 모델을 생성할 수 있도록 하는 인공지능 모델 플랫폼을 구현하되, 특히 인공지능 모델 성능에 직결되는 특징정보 및 정규화 방식을 최적으로 추천/적용할 수 있도록 함으로써, 보안관제 기술에 익숙하지 않은 일반 사용자도 보안관제를 위한 최적의 인공지능 모델을 생성할 수 있도록 하는 인공지능 모델 플랫폼을 구현할 수 있다.

[0039] 이로 인해, 본 발명에 따르면, 보안관제를 위한 목적 및 요구 사항에 적합한 최적의 인공지능 모델을 유연하고 다양하게 생성 및 적용할 수 있기 때문에, 보안관제 서비스의 품질 향상을 극대화시킬 수 있고, 아울러 대규모 사이버공격 및 이상행위 발생 징후를 효율적으로 분석하기 위한 인공지능 기반의 침해대응 체계 구축을 지원할 수 있는 효과까지 기대할 수 있다.

도면의 간단한 설명

[0040] 도 1은 본 발명의 실시예에 따른 인공지능 모델 플랫폼을 보여주는 개념도이다.

도 2는 본 발명의 실시예에 따른 인공지능 모델 플랫폼의 구성을 보여주는 구성도이다.

도 3은 본 발명의 실시예에 따른 특징정보 추천 장치의 구성을 보여주는 구성도이다.

도 4는 본 발명의 실시예에 따른 정규화 방식 추천 장치의 구성을 보여주는 구성도이다.

도 5는 본 발명의 실시예에 따른 인공지능 모델 플랫폼 운영 방법을 보여주는 흐름도이다.

도 6은 본 발명의 실시예에 따른 특징정보 추천 장치의 동작 방법을 보여주는 흐름도이다.

도 7은 본 발명의 실시예에 따른 정규화 방식 추천 장치의 동작 방법을 보여주는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0041] 이하, 첨부된 도면을 참조하여 본 발명의 실시예에 대하여 설명한다.

[0042] 현재, 과학기술사이버안전센터에서 제공하고 있는 실시간 보안관제 서비스는, 침해위협관리시스템(TMS)에서 탐지 및 수집하는 보안이벤트를 기반으로, 보안관제 요원에 의한 룰(Rule) 기반 분석 및 대응 지원이 이루어지는 서비스 구조를 갖는다.

[0043] 헌데, TMS에 의해 탐지되는 보안이벤트 수가 폭발적으로 증가하고 있으며, 이와 같은 대용량의 전체 보안이벤트를 보안관제 요원이 분석하기는 현실적으로 어려운 한계 상황에 도달하고 있다.

[0044] 또한, 기존의 보안관제 서비스는, 보안관제 요원의 전문 지식 및 경험에 의존하기 때문에, 특정 보안이벤트에 대한 분석이 집중되는 업무편중 현상 발생하거나 분석 결과의 편차가 발생하는 등 분석 평준화가 실현되지 못하는 상황도 발생하고 있다.

[0045] 결국, TMS에 의해 탐지되는 보안이벤트 수가 폭발적으로 증가하고 있는 현 상황에서는, 보안관제 요원의 분석에 의존하는 기존 보안관제 서비스의 서비스 구조 자체를 혁신할 필요가 있다.

[0046] 이에, 보안관제 요원의 분석을 대체할 수 있는 인공지능 모델을 활용하는 보안관제 서비스 구조를 생각해 볼 수 있다.

[0047] 본 발명에서는, 보안관제를 위한 인공지능 모델을 생성할 수 있도록 하는 인공지능 모델 플랫폼을 제공하고자 한다.

[0048] 특히, 본 발명에서는, 보안관제 기술에 익숙하지 않은 일반 사용자도 보안관제를 위한 최적의 인공지능 모델을 생성할 수 있도록 하는 인공지능 모델 플랫폼을 제공하고자 한다.

[0049] 도 1은 본 발명에서 제안하는 인공지능 모델 플랫폼의 일 실시예를 개념적으로 보여주고 있다.

[0050] 도 1에 도시된 바와 같이, 본 발명의 인공지능 모델 플랫폼은, 보안관제를 위한 인공지능 모델 생성에 필요한 각종 데이터를 수집 및 가공하는 수집 기능, 수집 기능에서 수집 및 가공된 각종 데이터를 기반으로 인공지능 모델을 생성하고 이와 관련된 성능 및 이력을 관리하는 인공지능 기능, 그리고 시스템 관리자 및 일반 사용자에게 제공하는 UI(User Interface)를 기반으로 수집/인공지능 기능과 관련된 각종 설정 및 사용자 관리를 담당하는 관리 기능으로 구분할 수 있다.

[0051] 그리고, 본 발명의 인공지능 모델 플랫폼은, 빅데이터 통합저장 스토리지로부터 신규 생성된 원천 보안데이터를 주기적으로 수집하는 검색엔진을 포함하고, 수집 기능에서의 각종 데이터를 검색엔진에 탑재하여 검색엔진을 데이터저장소로서 활용할 수 있다.

[0052] 이렇게 되면, 수집 기능에 속하는 각종 모듈(예: 수집/특징추출/정규화/출력)은 검색엔진(데이터저장소)를 기반으로 동작할 수 있다.

[0053] 이하에서는, 도 2를 참조하여 본 발명의 실시예에 인공지능 모델 플랫폼의 구성 및 각 구성의 역할을 구체적으로 설명하겠다.

[0054] 본 발명의 인공지능 모델 플랫폼(100)은, 데이터수집모듈(110), 특징추출모듈(120), 정규화모듈(130), 데이터출력모듈(140), 모델생성모듈(150)을 포함한다.

[0055] 더 나아가, 본 발명의 인공지능 모델 플랫폼(100)은, 성능관리모듈(160) 및 UI모듈(170)을 더 포함할 수 있다.

[0056] 이러한 인공지능 모델 플랫폼(100)의 구성 전체 내지는 적어도 일부는 하드웨어 모듈 형태 또는 소프트웨어 모

듈 형태로 구현되거나, 하드웨어 모듈과 소프트웨어 모듈이 조합된 형태로도 구현될 수 있다.

[0057] 여기서, 소프트웨어 모듈이란, 예컨대, 인공지능 모델 플랫폼(100) 내에서 연산을 제어하는 프로세서에 의해 실행되는 명령어로 이해될 수 있으며, 이러한 명령어는 인공지능 모델 플랫폼(100) 내 메모리에 탑재된 형태를 가질 수 있을 것이다.

[0058] 결국, 본 발명의 일 실시예에 따른 인공지능 모델 플랫폼(100)은 전술한 구성을 통해, 본 발명에서 제안하는 기술 즉 보안관제를 위한 최적의 인공지능 모델을 생성할 수 있도록 하는 기술을 실현하며, 이하에서는 이를 실현하기 위한 인공지능 모델 플랫폼(100) 내 각 구성에 대해 보다 구체적으로 설명하기로 한다.

[0059] 먼저, UI모듈(170)은, 데이터수집모듈(110)의 특정 검색 조건, 특징추출모듈(120)의 특징정보, 정규화모듈(130)의 정규화 방식, 데이터출력모듈(140)의 조건 중 적어도 하나를 설정하기 위한 UI(User Interface)를 제공한다.

[0060] 예컨대, UI모듈(170)은, 본 발명의 인공지능 모델 플랫폼(100)에서 보안관제를 위한 인공지능 모델을 생성하고자 하는 시스템 관리자 또는 일반 사용자(이하, 사용자로 통칭함)의 조작에 따라, 데이터수집모듈(110)의 특정 검색 조건, 특징추출모듈(120)의 특징정보, 정규화모듈(130)의 정규화 방식, 데이터출력모듈(140)의 조건 중 적어도 하나를 설정하기 위한 UI를 제공한다.

[0061] 이에, UI모듈(170)은, 제공한 UI를 기반으로 수집/인공지능 기능과 관련된 각종 설정, 구체적으로 후술의 생성할 인공지능 모델을 위한 데이터수집모듈(110)의 특정 검색 조건, 특징추출모듈(120)의 특징정보, 정규화모듈(130)의 정규화 방식, 데이터출력모듈(140)의 조건 등을 사용자정보/설정정보 저장소에 저장/관리하게 된다.

[0062] 데이터수집모듈(110)은, 원천 보안데이터로부터 특정 검색 조건 즉 앞서 사용자에 의해 기 설정된 특정 검색 조건에 의해 학습/테스트 데이터로 사용하고자 하는 보안이벤트를 수집한다.

[0063] 예를 들어, 데이터수집모듈(110)의 특정 검색 조건으로서, 학습/테스트 데이터로 사용하고자 하는 일자(또는 기간), 건수, IP, 탐지패턴명, 탐지패턴유형 등이 설정될 수 있다.

[0064] 여기서, 탐지패턴명이란, 침해위협관리시스템(TMS)에서 탐지되는 보안로그들의 대표 명칭을 의미하고, 탐지패턴유형이란, 유사한 탐지패턴 특징(성질, 유형)을 갖는 탐지패턴끼리 묶은 일종의 그룹을 의미하며, 예를 들면 탐지패턴유형은 웜 바이러스 피해, 자료훼손 및 유출, 경유지 악용, 홈페이지 변조, 서비스거부공격 피해, 단순침입시도의 6가지로 구분될 수 있다.

[0065] 이에, 데이터수집모듈(110)은, 특정 검색 조건이 일자(또는 기간)인 경우, 원천 보안데이터로부터 설정된 일자(또는 기간)에 속하는 보안이벤트를 수집할 수 있다.

[0066] 또는, 데이터수집모듈(110)은, 특정 검색 조건이 건수인 경우, 원천 보안데이터로부터 지정된 시점에서 설정된 건수(예: 500,000건)의 보안이벤트를 수집할 수 있다.

[0067] 또는, 데이터수집모듈(110)은, 특정 검색 조건이 IP인 경우, 원천 보안데이터로부터 설정된 IP가 Source IP 또는 Destination IP와 일치하는 보안이벤트를 수집할 수 있다.

[0068] 물론, 특정 검색 조건으로서, 일자(또는 기간), 건수, IP, 탐지패턴명, 탐지패턴유형 등의 조합이 설정될 수도 있다.

[0069] 이 경우 역시, 데이터수집모듈(110)은, 원천 보안데이터로부터 설정된 일자(또는 기간), 건수, IP, 탐지패턴명, 탐지패턴유형 등의 조합에 따른 보안이벤트를 수집할 수 있다.

[0070] 더 구체적으로, 데이터수집모듈(110)은, 전술과 같이 원천 보안데이터로부터 보안이벤트를 수집하는데 있어서, 시스템의 부하를 줄이기 위하여 동시 수행 가능한 최대 수집 건수가 한정될 수 있다.

[0071] 예를 들면, 원천 보안데이터로부터 설정된 일자(또는 기간)에 속하는 보안이벤트를 수집하는 경우, 설정된 일자(또는 기간)에 속하는 보안이벤트 수집 건의 총 수가 1000,000건이고, 동시 수행 가능한 최대 수집 건수가 500,000건이라고 가정할 수 있다.

[0072] 이 경우, 데이터수집모듈(110)은, 금번 수집 건의 총 수가 동시 수행 가능한 최대 수집 건수를 초과하는 것으로 판단, 금번 수집 건의 총 개수 중 최대 수집 건수를 초과하는 수집 건을 큐(queue)에 저장한 후 순차적으로 진행할 수 있다.

[0073] 즉, 데이터수집모듈(110)은, 금번 수집 건의 총 개수 1000,000건 중 시간순서에 따라 최대 수집 건수 500,000건

을 수집/진행하되, 최대 수집 건수 500,000건을 초과하는 수집 건 500,000건에 대해서는 큐(queue)에 저장한 후 순차적으로 수집/진행할 수 있다.

[0074] 이 경우, 데이터수집모듈(110)은, 큐에 저장한 후 진행하는 수집 건 500,000건의 경우, 원천 보안데이터에서 수집 건의 발생시점 이전 데이터에 대해서만 보안이벤트를 수집한다.

[0075] 즉, 금번 수집 건의 총 개수 1000,000건 중 큐에 저장한 후 진행하는 수집 건 500,000건의 경우는, 수집 건의 발생시점과 실제 수집/진행된 시점 간의 차이가 발생하므로, 이로 인한 보안이벤트 수집 오류를 방지하기 위해 원천 보안데이터에서 수집 건의 발생시점 이전 데이터에서만 보안이벤트를 수집하는 것이다.

[0076] 한편, 앞서 본 발명의 인공지능 모델 플랫폼(100)은, 빅데이터 통합저장 스토리지로부터 신규 생성된 원천 보안데이터를 주기적으로 수집하는 검색엔진을 포함한다고 언급한 바 있다.

[0077] 이 경우 데이터수집모듈(110)는, 검색엔진(데이터 저장소) 내 원천 보안데이터에서 보안데이터를 수집할 수 있다.

[0078] 빅데이터 통합저장 스토리지는 본 발명의 인공지능 모델 플랫폼(100) 뿐만 아니라 다른 시스템에서도 활용하는 저장소이기 때문에, 빅데이터 통합저장 스토리지로부터 대량의 데이터(보안이벤트)를 수집할 경우 빅데이터 통합저장 스토리지에 부하가 생겨 다른 시스템에도 영향을 미칠 수 있다.

[0079] 하지만, 본 발명(데이터수집모듈(110))은, 데이터수집모듈(110)가 빅데이터 통합저장 스토리지로부터 직접 보안이벤트를 수집하지 않고, 빅데이터 통합저장 스토리지로부터 신규 생성된 원천 보안데이터 만을 주기적으로 수집하는 검색엔진을 기반으로 보안이벤트를 수집하기 때문에, 전술의 빅데이터 통합저장 스토리지 부하 문제를 회피할 수 있다.

[0080] 특징추출모듈(120)은, 데이터수집모듈(110)에서 수집된 보안이벤트에 대하여 기 설정된 특징정보 즉 앞서 사용자에 의해 기 설정된 특징정보(Feature)를 추출한다.

[0081] 인공지능 모델 생성 시, 인공지능 알고리즘으로 데이터(보안이벤트)를 분류하기 위해서는 데이터(보안이벤트)가 어떤 특징으로 가지고 있는지 찾고 이를 벡터로 만들어야 하는데, 이러한 과정을 특징정보 추출 과정이라 한다.

[0082] 특징추출모듈(120)은, 데이터수집모듈(110)에서 수집된 보안이벤트에 대하여 특징정보 추출 과정을 수행하는 역할을 담당하는 것이다.

[0083] 그리고, 특징추출모듈(120)에 의해 추출된 각 보안이벤트의 특징정보는, 후술의 인공지능 모델 생성 시 기계학습(예: Deep Learning)에 사용될 것이다.

[0084] 특히, 본 발명에서는, 사용자가 특징정보로서, 단일 특징을 설정할 수 있고 복합 특징을 설정할 수 있도록 한다.

[0085] 여기서, 단일 특징이란, 하나의 보안이벤트에서 추출할 수 있는 특징들을 의미한다.

[0086] 예를 들면, 탐지시간, Source IP, Source port, Destination IP, Destination port, 프로토콜, 보안이벤트명, 보안이벤트 타입, 공격횟수, 공격방향, 패킷사이즈, 자동분석 결과, 동적분석 결과, 기관번호, 점보페이로드 여부, 페이로드, word2vec 변환 방식을 적용한 페이로드 등이, 단일 특징에 속할 수 있다.

[0087] 참고로, Word2Vec을 통한 페이로드 변환 방식은, 단어를 벡터로 변환하는 방식으로서, 주변 단어들 간의 관계를 통해 해당 단어의 벡터를 결정하는 방식이다. 일반적인 문장은 띄어쓰기 기준으로 단어를 구별할 수 있지만, 페이로드는 의미 단위로 구분하기가 매우 어려우며 다량의 특수문자들이 포함되어 있기 때문에 word2vec을 적용하기 위해서는 사전 처리가 필요하다.

[0088] 본 발명에서는, word2vec을 적용하기 위한 사전 처리로서, 다음의 4단계를 수행할 수 있다.

[0090] 1) 16진수로 인코딩된 문자열을 아스키 문자열로 변환(아스키 코드값 (32~127) 이외에는 공백으로 변환)

[0091] 2) url encoding된 부분 처리(%25 -> ‘%’, %26 -> ‘&’, %2A -> ‘*’ ...)

[0092] 3) '@', '₩', '-', ':', '%', '_', '.', '!', '/', '`'를 제외한 특수기호들을 공백으로 치환하고 모든 대문자를 소문자로 치환

[0093] 4) 한 글자로 구성된 단어를 제외하고 word2vec알고리즘 적용

[0095] 한편, 복합 특징이란, 여러 보안이벤트 간의 집계, 통계적 기법들을 활용하여 추출할 수 있는 하나의 특징을 의미한다.

[0096] 예를 들면, 기간 또는 건수 등의 기준으로 보안이벤트 그룹을 형성하고, 그룹 내 연산(예: 집계, 통계적 기법 등)을 통해 추출할 수 있는 하나의 특징(예: 연산 결과값)이, 복합 특징에 속할 수 있다.

[0097] 예를 들어, 기간(8.22~9.3)을 기준을 다음의 표 1과 같은 보안이벤트 그룹을 형성한다고 가정한다.

표 1

[0098]

	time	Source IP	Source Port	Event name	Destination IP	Destination Port
1	08.22	100.100.100.100	80	AAA	111.111.111.11	230.
2	08.25	100.100.100.100	80	CCC	123.123.12.12	222
3	08.25	100.100.100.100	1234	AAA	111.111.111.11	1122
4	08.28	100.100.100.100	80	AAA	111.111.111.11	1562
5	08.29	10.10.10.2	10022	CCC	10.10.10.1	1292
6	08.30	100.100.100.100	22	AAA	111.111.111.11	1929
7	08.30	10.10.10.1	1234	DDD	10.10.10.2	1080
8	08.30	100.100.100.100	22	BBB	10.100.10.100	2580
9	08.31	50.50.80.60	88	CCC	10.10.10.1	6543
10	09.03	100.100.100.100	8080	CCC	10.10.10.1	9874

[0099] 보안이벤트 그룹 내 연산(예: Source IP, Destination IP, 보안이벤트 명이 100.100.100.100/111.111.111.11/AAA인 보안이벤트의 개수)을 통해 추출할 수 있는 하나의 특징(예: 4개)이, 복합 특징에 속할 수 있다.

[0100] 이에, 특징추출모듈(120)은, 데이터수집모듈(110)에서 수집된 보안이벤트에 대하여, 기 설정된 특징정보(단일 특징 및/또는 복합 특징)를 추출할 수 있다.

[0101] 정규화모듈(130)은, 보안이벤트의 추출된 특징정보에 대하여 기 설정된 정규화를 수행한다.

[0102] 정규화는 추출된 특징들의 값의 범위를 일정하게 맞춰주는 과정을 말한다. 필드(field) A가 50~100, 필드 B가 0~100의 범위를 가진다면 똑같은 50이라도 서로 다른 척도에 의해서 측정된 값이기 때문에 그 의미는 상이하다. 따라서, 서로 다른 필드의 값들을 공통 척도로 조정하여 일정한 의미를 갖도록 하는 과정이 필요하고 이를 정규화라 한다.

[0103] 정규화모듈(130)은, 보안이벤트의 추출된 특징정보에 대하여, 기 설정된 정규화 방식에 따라서 서로 다른 필드의 값들을 공통 척도로 조정하여 일정한 의미를 갖도록 하는 정규화를 수행하게 된다.

[0104] 이때, 기 설정된 정규화 방식은, 앞서 사용자에 의해 기 설정된 정규화 방식을 의미한다.

[0105] 본 발명의 인공지능 모델 플랫폼(100)에서는, 다음의 3가지 정규화 방식을 제공하여 사용자로 하여금 기 설정할 수 있도록 한다.

[0106] 수학식 1은 Feature scaling [a,b] 정규화 방식을 의미하며, 수학식 2는 Mean normalization [-1,1] 정규화 방식, 수학식 3은 Standard score 정규화 방식을 의미한다.

수학식 1

[0107]

$$x' = a + \frac{(\bar{x} - \min(x))(b - a)}{\max(x) - \min(x)}$$

※ max(x) : x 중 최댓 값, min(x) : x 중 최솟 값, $\bar{x}$: original x 값, x' : 지환된 x 값,

a : 사용자가 지정한 최솟값, b : 사용자가 지정한 최댓값

[0108]

수학식 2

$$x' = \frac{\bar{x} - \text{average}(x)}{\max(x) - \min(x)}$$

[0109]

※ max(x) : x 중 최댓 값, min(x) : x 중 최솟 값, $\bar{x}$: original x 값, x' : 지환된 x 값,

average(x) : x의 평균 값

[0110]

수학식 3

$$x' = \frac{\bar{x} - average(x)}{\sigma}$$

[0111]

※ $\bar{x}$: original x 값, x' : 지환된 x 값, average(x) : x의 평균 값, σ : x의 표준편차

[0112]

[0113] 정규화모듈(130)은, 보안이벤트의 추출된 특징정보에 대하여, 전술의 3가지 정규화 방식 중 사용자에 의해 기 설정된 정규화 방식에 따라 정규화를 수행하게 된다.

[0114] 데이터출력모듈(140)은, 특정정보 정규화가 완료된 보안이벤트에서 학습 데이터 또는 테스트 데이터를 주어진 조건 즉 앞서 사용자에 의해 기 설정된(주어진) 조건에 의해 추출한다.

[0115] 구체적으로, 데이터출력모듈(140)은, 특정정보 정규화가 완료된 보안이벤트를, 사용자가 원하는 값, 순서, 포맷, 학습/테스트 데이터 비율, 파일분할방식 등에 따라 화면 또는 파일로 출력하게 된다.

[0116] 이처럼 출력된 학습 데이터 또는 테스트 데이터는, 인공지능 모델 생성 시 즉시 활용할 수 있도록 날짜, 사용자별로 Database 또는 파일 저장소를 통해 관리한다.

[0117] 모델생성모듈(150)은, 데이터출력모듈(140)에서 출력/파일 저장소에 관리되는 학습 데이터에 인공지능 알고리즘을 적용하여, 보안관제를 위한 인공지능 모델을 생성한다.

[0118] 즉, 모델생성모듈(150)은, 학습 데이터에 인공지능 알고리즘을 적용하여, 보안관제를 위한 인공지능 모델, 예컨대 사용자에 의해 요구되는 기능의 인공지능 모델을 생성할 수 있다.

[0119] 예를 들면, 모델생성모듈(150)은, 사용자 요구에 따라, 보안이벤트의 악성 여부를 탐지하기 위한 인공지능 탐지 모델을 생성할 수 있고, 보안이벤트의 정탐/오탐을 분류하기 위한 인공지능 분류모델을 생성할 수도 있다.

[0120] 구체적으로, 모델생성모듈(150)은, 데이터출력모듈(140)에서 출력/파일 저장소에 관리되는 학습 데이터를 기반으로, 인공지능 알고리즘 예컨대 사용자에 의해 기 선택된 기계학습(예: Deep Learning) 알고리즘에 따라, 보안관제를 위한 인공지능 모델을 생성할 수 있다.

[0121] 예를 들면, 모델생성모듈(150)은, Backward Propagation(오차역전파법) 계산 기반의 기계학습 기술에서 모델을 통해 예측되는 결과값과 실제 결과값 간의 편차를 나타내는 학습손실함수(Loss function)을 이용하여, 학습 데

이터를 기반으로 학습손실함수(Loss function)의 편차가 0이 되는 인공지능 모델을 생성할 수 있다.

[0122] 이상에서 설명한 바와 같이, 본 발명의 인공지능 모델 플랫폼(100)에 따르면, 별도의 프로그래밍 없이 UI를 기반으로 보안관제를 위한 인공지능 모델을 생성할 수 있도록 하는 플랫폼 환경을 제공함으로써, 보안관제 기술에 익숙하지 않은 일반 사용자도 보안관제를 위한 자신의 목적 및 요구 사항에 맞는 인공지능 모델을 생성할 수 있도록 한다.

[0123] 더 나아가, 본 발명의 인공지능 모델 플랫폼(100)에서 성능관리모듈(160)은, 데이터출력모듈(140)에서 출력/파일 저장소에 관리되는 테스트 데이터를 활용하여, 전술의 생성한 인공지능 모델의 정확도를 테스트한다.

[0124] 성능관리모듈(160)은, 모델생성모듈(150)에 의해 생성된 인공지능 모델을 관리하기 위한 것으로서, '누가' '언제' '어떤 데이터' '어떤 필드' '어떤 샘플링 방식' '어떤 정규화 방식' '어떤 모델'을 이용하여 인공지능 모델을 만든 것인지, 또한 생성된 인공지능 모델이 어느 정도의 성능(정답률)을 갖는지 등의 성능 정보를 시스템(파일저장소)에 기록 및 관리한다.

[0125] 그리고, 성능관리모듈(160)은, 이러한 성능 정보 관리를 기반으로, 모델 생성을 위한 조건들과 성능을 한눈에 비교할 수 있어 조건들과 성능의 상관 관계를 쉽게 파악할 수 있도록 한다.

[0126] 본 발명에서는, 보안관제 기술에 익숙하지 않은 일반 사용자도 인공지능 모델을 생성할 수 있도록 하는 플랫폼 환경을 제공하고 있다는 점에서, 본 발명의 플랫폼 환경에서 생성된 인공지능 모델의 정확도(성능) 테스트는 필수적일 수도 있다.

[0127] 구체적으로, 성능관리모듈(160)은, 데이터출력모듈(140)에서 출력/파일 저장소에 관리되는 테스트 데이터(정탐/오탐 분류 및 악성 여부 탐지의 실제 결과값을 알고 있는 보안이벤트)를 활용하여, 전술의 생성한 인공지능 모델의 정확도를 테스트한다.

[0128] 예를 들어, 성능관리모듈(160)은, 테스트 데이터를 활용하여 전술의 생성한 인공지능 모델을 테스트하여, 모델을 통해 예측되는 결과값과 알고 있는 실제 결과값의 일치 비율을 모델의 정확도(성능) 즉 테스트 결과로서 출력할 수 있다.

[0129] 인공지능 모델을 생성하기 위해서는, 어떠한 특징(Feature)들을 사용하는지 그리고 어떤 정규화 방식을 적용하는지가 모델 성능(정확도)에 큰 영향을 미친다.

[0130] 헌데, 사람 특히 보안관제 기술에 익숙하지 않은 일반 사용자가 자신이 원하는 인공지능 모델을 생성하는데 최적 성능을 낼 수 있는 특징정보(Feature)를 조합/설정하는 것은 어려울 것이다.

[0131] 이에, 본 발명에서 특징추출모듈(120)은, 성능관리모듈(160)의 정확도 테스트 결과를 근거로, 전술의 생성한 인공지능 모델의 정확도를 높이도록 특징정보(Feature)에 대한 변경을 추천할 수 있다.

[0132] 사람 특히 보안관제 기술에 익숙하지 않은 일반 사용자가 자신이 원하는 인공지능 모델을 생성하는데 최적 성능을 낼 수 있는 정규화 방식을 알고 설정하는 것 역시 어려울 것이다.

[0133] 또한, 본 발명에서 정규화모듈(130)은, 인공지능 모델의 정확도를 높이도록 정규화에 대한 정규화 방식 변경을 추천할 수 있다.

[0134] 이하에서는, 도 3을 참조하여, 인공지능 모델의 정확도를 높이도록 특징정보(Feature) 변경을 추천하는 기술, 구체적으로 그 기술을 실현하는 특징정보 추천 장치에 대하여 설명하겠다.

[0135] 도 3은, 본 발명의 일 실시예에 따른 특징정보 추천 장치의 구성을 도시하고 있다.

[0136] 도 3에 도시된 바와 같이, 본 발명의 특징정보 추천 장치(200)는, 모델성능확인부(210), 조합성능확인부(220), 추천부(230)를 포함한다.

[0137] 이러한 특징정보 추천 장치(200)의 구성 전체 내지는 적어도 일부는 하드웨어 모듈 형태 또는 소프트웨어 모듈 형태로 구현되거나, 하드웨어 모듈과 소프트웨어 모듈이 조합된 형태로도 구현될 수 있다.

[0138] 여기서, 소프트웨어 모듈이란, 예컨대, 특징정보 추천 장치(200) 내에서 연산을 제어하는 프로세서에 의해 실행되는 명령어로 이해될 수 있으며, 이러한 명령어는 특징정보 추천 장치(200) 내 메모리에 탑재된 형태를 가질 수 있을 것이다.

[0139] 결국, 본 발명의 일 실시예에 따른 특징정보 추천 장치(200)는 전술한 구성을 통해, 본 발명에서 제안하는 기술

즉 인공지능 모델의 정확도를 높이도록 특징정보(Feature) 변경을 추천하는 기술을 실현하며, 이하에서는 이를 실현하기 위한 특징정보 추천 장치(200) 내 각 구성에 대해 보다 구체적으로 설명하기로 한다.

[0140] 모델성능확인부(210)는, 인공지능 모델 생성 시 설정 가능한 전체 특징정보 중 기 설정된 특징정보 학습을 기반으로 생성된 인공지능 모델에 대하여, 모델 성능을 확인한다.

[0141] 즉, 모델성능확인부(210)는, 사용자에 의해 설정된 특징정보 학습을 기반으로 생성된 인공지능 모델의 성능(정확도)를 확인하는 것이다.

[0142] 구체적인 설명을 위해, 이하에서는, 본 발명의 인공지능 모델 플랫폼(100)에서 사용자에 의해 설정된 특징정보(이하, 사용자 설정 특징정보)를 학습/생성된 인공지능 모델을 가정하여 설명하겠다.

[0143] 모델성능확인부(210)는, 전술과 같이 인공지능 모델 플랫폼(100)에서 사용자 설정 특징정보를 학습하여 생성된 인공지능 모델에 대하여, 모델 성능을 확인한다.

[0144] 예를 들면, 모델성능확인부(210)는, 인공지능 모델에 대하여, 본 발명의 인공지능 모델 플랫폼(100, 특히 데이터출력모듈(140))에서 출력되는 테스트 데이터(정탐/오탐 분류 및 악성 여부 탐지의 실제 결과값을 알고 있는 보안이벤트)를 활용하여, 모델 성능(정확도)을 테스트/확인할 수 있다.

[0145] 이에 모델성능확인부(210)는, 본 발명의 인공지능 모델 플랫폼(100, 특히 데이터출력모듈(140))에서 생성되는 인공지능 모델을 대상으로, 테스트 데이터를 활용하여 인공지능 모델을 테스트함으로써, 모델을 통해 예측되는 결과값과 알고 있는 실제 결과값의 일치 비율을 모델의 정확도(성능) 즉 테스트 결과로서 출력할 수 있다.

[0146] 조합성능확인부(220)는, 전체 특징정보에서 다수의 특징정보 조합을 설정하여, 다수의 특징정보 조합 별로 학습을 기반으로 생성된 인공지능 모델의 성능을 확인한다.

[0147] 구체적으로, 조합성능확인부(220)는, 인공지능 모델 생성 시 설정 가능한 전체 특징정보에서, 금번 인공지능 모델 생성 시 학습된 사용자 설정 특징정보 외 다양한 특징정보 조합을 설정하여 다수의 특징정보 조합 별로 학습을 기반으로 생성된 인공지능 모델의 성능을 확인할 수 있다.

[0148] 추천부(230)는, 조합성능확인부(220)에서 확인한 다수의 특징정보 조합 별 성능 중에서, 모델성능확인부(210)에서 확인한 모델 성능 즉 금번 사용자 설정을 기반으로 생성된 인공지능 모델의 성능 보다 높은 성능의 특정 특징정보 조합을 추천할 수 있다.

[0149] 이하에서는, 특정 특징정보 조합을 추천하는 구체적인 실시예들을 설명하겠다.

[0150] 일 실시예에 따르면, 조합성능확인부(220)에 의해 설정되는 다수의 특징정보 조합은, 금번 인공지능 모델 생성 시 학습된 사용자 설정 특징정보에, 전체 특징정보에서 사용자 설정 특징정보를 제외한 나머지 특정정보 중 적어도 하나씩 순차적으로 추가한 조합일 수 있다.

[0151] 이하에서는, 전체 특징정보(예: a,b,c...,z(n=26)) 중 금번 인공지능 모델 생성 시 학습된 사용자 설정 특징정보(예: a,b,c,d,e,f(k=6))를 가정하여 설명하겠다. 그리고 이 경우, 모델성능확인부(210)에서 확인한 인공지능 모델 성능(m_k)이 85%라고 가정한다.

[0152] 이에, 조합성능확인부(220)는, 사용자 설정 특징정보(a,b,c,d,e,f)에 전체 특징정보(n) 중 사용자 설정 특징정보(a,b,c,d,e,f)를 제외한 나머지 특정정보 중 적어도 하나씩 순차적으로 추가하여, 다수의 특징정보 조합을 설정할 수 있다.

[0153] 예를 들면, 조합성능확인부(220)는, 사용자가 설정한 사용자 설정 특징정보(a,b,c,d,e,f)에, 전체 특징정보(n) 중 사용자 설정 특징정보(a,b,c,d,e,f)를 제외한 나머지 특정정보 중 1~(n-k)개의 특징정보를 순차적으로 추가하여, 다음과 같은 다수의 특징정보 조합을 설정할 수 있다.

[0154] a,b,c,d,e,f,g -> $m_{(k+1)}^{1}$ -> 82%

[0155] a,b,c,d,e,f,h -> $m_{(k+1)}^{2}$ -> 80%

[0156] ...

[0157] a,b,c,d,e,f,g,h,i -> $m_{(k+3)}^{1}$ -> 88%

[0158] ...

[0159] a,b,c,d,e,f,...,z -> $m_{(n)}$ -> 85%

[0160] 그리고, 조합성능확인부(220)는, 전술과 같이 다수의 특징정보 조합 별로 학습을 기반으로 생성된 인공지능 모델의 성능, 82%, 80%, ... 88%,...85%을 확인할 수 있다.

[0161] 이 경우, 추천부(230)는, 다수의 특징정보 조합 별 성능 중에서, 금번 사용자 설정을 기반으로 생성된 인공지능 모델의 성능(m_k=85%) 보다 높은 성능을 갖는 상위 N개(예: 4개)를 특정 특징정보 조합으로서 선택/추천할 수 있다.

[0162] 물론, 상위 N개는 시스템관리자 또는 사용자에 의해 지정/변경될 수 있는 개수이다.

[0163] 다른 예를 들면, 조합성능확인부(220)는, 사용자가 설정한 사용자 설정 특징정보(a,b,c,d,e,f)에, 전체 특징정보(n) 중 사용자 설정 특징정보(a,b,c,d,e,f)를 제외한 나머지 특정정보를 1개씩 순차적으로 추가하여, 다음과 같은 다수의 특징정보 조합을 설정할 수 있다.

[0164] a,b,c,d,e,f,g -> $m_{(k+1)}^{1}$ -> 82%

[0165] a,b,c,d,e,f,h -> $m_{(k+1)}^{2}$ -> 80%

[0166] ...

[0167] a,b,c,d,e,f,z -> $m_{(k+1)}^{\zeta+1}$ -> 90%

[0168] 그리고, 조합성능확인부(220)는, 전술과 같이 다수의 특징정보 조합 별로 학습을 기반으로 생성된 인공지능 모델의 성능, 82%, 80%, ...90%을 확인할 수 있다.

[0169] 이 경우, 추천부(230)는, 다수의 특징정보 조합 별 성능 중에서, 금번 사용자 설정을 기반으로 생성된 인공지능 모델의 성능(m_k=85%) 보다 높은 성능을 갖는 상위 N개(예: 3개)를 특정 특징정보 조합으로서 선택/추천할 수 있다.

[0170] 물론, 상위 N개는 시스템관리자 또는 사용자에 의해 지정/변경될 수 있는 개수이다.

[0171] 한편, 다른 실시예에 따르면, 금번 인공지능 모델 생성 시 이용된 기 설정된 특징정보는 전체 특징정보(k=n=26)일 수 있다.

[0172] 이 경우, 조합성능확인부(220)는, 기 설정된 특징정보 즉 전체 특징정보(예: a,b,c...,z(n=26)) 내 각 단일 특징정보 별로 학습을 기반으로 생성되는 인공지능 모델의 성능을 확인하고, 각 단일 특징정보의 성능 중 최대 성능(Max(m_1))이 모델 성능(m_{26}) 보다 높은지 확인하는 단일특징정보 성능 비교과정을 수행할 수 있다.

[0173] 조합성능확인부(220)는, 기 설정된 특징정보(a,b,c...,z(n=26))의 모델 성능(m_{26}) 보다 단일 특징정보(예: c)의 최대 성능(Max(m_1))이 높은 경우, 최대 성능의 단일 특징정보(c)를 특징정보로 재 설정하고, 특징정보(c)에 전체 특징정보(n)에서 특징정보(c)를 제외한 나머지 특정정보 중 하나씩 순차적으로 추가하여, 다수의 특징정보 조합을 설정하는 조합설정 과정을 수행할 수 있다.

[0174] 이렇게 되면, 조합성능확인부(220)는, 전술과 마찬가지로 다음과 같은 다수의 특징정보 조합 별 성능을 확인할 수 있다.

[0175] c,a -> m_2^{1} -> 81%

[0176] c,b -> m_2^{2} -> 90.5%

[0177] ...

[0178] c,z -> m_2^{25} -> 85%

[0179] 조합성능확인부(220)는, 다수의 특징정보 조합 중 재 설정한 특징정보(c)의 모델 성능(m_1) 보다 높은 성능을 갖는 특징정보 조합 각각을 특징정보로 재 설정하여, 재 설정한 각 특징정보에 대하여 조합설정 과정이 반복 수행되도록 하는 재설정 과정을 수행할 수 있다.

[0180] 즉, 조합성능확인부(220)는, 다수의 특징정보 조합 중 특징정보(c)의 모델 성능(m_1) 보다 낮거나 같은 성능을 갖는 특징정보 조합을 삭제하고 특징정보(c)의 모델 성능(m_1) 보다 높은 성능을 갖는 특징정보 조합 만을 다음과 같이 남기고, 이들 각각을 특징정보로 재 설정하여 다음의 표 2와 같이 재 설정한 각 특징정보에 대하여 조합설정 과정이 반복 수행되도록 하는 재설정 과정을 수행할 수 있다.

[0181] c,l -> m_2^{12} -> 92.5%

[0182] c,m -> m_2^{13} -> 93%

[0183] c,n -> m_2^{14} -> 94%

표 2

[0184]

$k=3$ sf = {c, l, a~z}	**l추가** → $k+1=3$ c, l, a ⇒ $m_{(k+1)^1}$ ⇒ m_{3^1} ⇒ 82% c, l, b ⇒ $m_{(k+1)^2}$ ⇒ m_{3^2} ⇒ 95% ..... c, l, z ⇒ $m_{(k+1)^{25}}$ ⇒ $m_{3^{25}}$ ⇒ 94%
$k=3$ sf = {c, m, a~z}	**m추가** → $k+1=3$ c, m, a ⇒ $m_{(k+1)^1}$ ⇒ m_{3^1} ⇒ 90.7% c, m, b ⇒ $m_{(k+1)^2}$ ⇒ m_{3^2} ⇒ 88% ..... c, m, z ⇒ $m_{(k+1)^{25}}$ ⇒ $m_{3^{25}}$ ⇒ 93.7%
$k=3$ sf = {c, n, a~z}	**n추가** → $k+1=3$ c, n, a ⇒ $m_{(k+1)^1}$ ⇒ m_{3^1} ⇒ 93% c, n, b ⇒ $m_{(k+1)^2}$ ⇒ m_{3^2} ⇒ 95% ..... c, n, z ⇒ $m_{(k+1)^{25}}$ ⇒ $m_{3^{25}}$ ⇒ 83%

[0185] 조합성능확인부(220)는, 전술의 조합설정 과정 및 재설정 과정을 반복하면서, 다수의 특징정보 조합 중 직전 특징정보를 기반으로 생성된 인공지능 모델의 성능 보다 높은 성능을 갖는 특징정보 조합이 존재하지 않는 경우, 직전의 특징정보를 특정 특징정보 조합으로서 선택하고 추천부(230)로 전달하는 과정을 수행한다.

[0186] 이 경우, 추천부(230)는, 다수의 특징정보 조합 별 성능 중에서, 조합성능확인부(220)로부터 전달되는 특징정보를 기 설정된 특징정보를 이용하여 생성된 인공지능 모델의 성능 보다 높은 성능을 갖는 특정 특징정보 조합으로서 추천할 수 있다.

[0187] 한편, 조합성능확인부(220)는, 기 설정된 특징정보(a,b,c...,z(n=26))의 모델 성능(m_{26}) 보다 단일 특징정보의 최대 성능(Max(m_1))이 높지 않은 경우, 특징정보(a,b,c...,z(n=26))에서 서로 다른 하나의 특정정보를 제외하여, 다수의 특징정보 조합을 설정하는 조합설정 과정을 수행할 수 있다.

[0188] 이렇게 되면, 조합성능확인부(220)는, 전술과 마찬가지로 다음과 같은 다수의 특징정보 조합 별 성능을 확인할 수 있다.

[0189] b,c,d~z -> m_{25}^{1} -> 96%

[0190] a,c,d~z -> m_{25}^{2} -> 95.6%

[0191] ...

[0192] a,b,c~y -> m_{25}^{25} -> 90%

[0193] 조합성능확인부(220)는, 다수의 특징정보 조합 중 모델 성능(m_{26}) 보다 높은 성능을 갖는 특징정보 조합 각각을 특징정보로 재 설정하여, 재 설정한 각 특징정보에 대하여 조합설정 과정이 반복 수행되도록 하는 재설정 과정을 수행할 수 있다.

[0194] 즉, 조합성능확인부(220)는, 다수의 특징정보 조합 중 모델 성능(m_{26}) 보다 낮거나 같은 성능을 갖는 특징정보 조합을 삭제하고 모델 성능(m_{26}) 보다 높은 성능을 갖는 특징정보 조합 만을 다음과 같이 남기고, 이들 각각을 특징정보로 재 설정하여 재 설정한 각 특징정보에 대하여 조합설정 과정이 반복 수행되도록 하는 재설정 과정을 수행할 수 있다.

[0195] b,c,d~z -> m_{25}^{1} -> 96%

[0196] a,c,d~z -> m_{25}^{2} -> 95.6%

[0197] a,b,d~y -> m_{25}^{3} -> 96%

[0198] 조합성능확인부(220)는, 전술의 조합설정 과정 및 재설정 과정을 반복하면서, 다수의 특징정보 조합 중 직전 특징정보를 기반으로 생성된 인공지능 모델의 성능 보다 높은 성능을 갖는 특징정보 조합이 존재하지 않는 경우, 직전의 특징정보를 특정 특징정보 조합으로서 선택하고 추천부(230)로 전달하는 과정을 수행한다.

[0199] 이 경우, 추천부(230)는, 다수의 특징정보 조합 별 성능 중에서, 조합성능확인부(220)로부터 전달되는 특징정보를 기 설정된 특징정보를 이용하여 생성된 인공지능 모델의 성능 보다 높은 성능을 갖는 특정 특징정보 조합으로서 추천할 수 있다.

[0200] 이상, 본 발명에 따르면, 인공지능 모델 플랫폼(100)에서 제공하는 환경에서 UI를 기반으로 보안관제를 위한 인공지능 모델을 생성하는 사용자에게 최적의 성능(정확도)를 갖는 최적 특징(feature)를 추천/적용할 수 있도록 함으로써, 보안관제 기술에 익숙하지 않은 일반 사용자도 보안관제를 위한 최적의 인공지능 모델을 생성할 수 있도록 한다.

[0201] 이하에서는, 도 4를 참조하여, 인공지능 모델의 정확도를 높이도록 정규화 방식 변경을 추천하는 기술, 구체적으로 그 기술을 실현하는 정규화 방식 추천 장치에 대하여 설명하겠다.

[0202] 도 4는, 본 발명의 일 실시예에 따른 정규화 방식 추천 장치의 구성을 도시하고 있다.

[0203] 도 4에 도시된 바와 같이, 본 발명의 정규화 방식 추천 장치(300)는, 속성확인부(310), 결정부(320), 추천부(330)를 포함한다.

[0204] 이러한 정규화 방식 추천 장치(300)의 구성 전체 내지는 적어도 일부는 하드웨어 모듈 형태 또는 소프트웨어 모듈 형태로 구현되거나, 하드웨어 모듈과 소프트웨어 모듈이 조합된 형태로도 구현될 수 있다.

[0205] 여기서, 소프트웨어 모듈이란, 예컨대, 정규화 방식 추천 장치(300) 내에서 연산을 제어하는 프로세서에 의해 실행되는 명령어로 이해될 수 있으며, 이러한 명령어는 정규화 방식 추천 장치(300) 내 메모리에 탑재된 형태를 가질 수 있을 것이다.

[0206] 결국, 본 발명의 일 실시예에 따른 정규화 방식 추천 장치(300)는 전술한 구성을 통해, 본 발명에서 제안하는 기술 즉 인공지능 모델의 정확도를 높이도록 정규화 방식 변경을 추천하는 기술을 실현하며, 이하에서는 이를 실현하기 위한 정규화 방식 추천 장치(300) 내 각 구성에 대해 보다 구체적으로 설명하기로 한다.

[0207] 속성확인부(310)는, 인공지능 모델 생성 시 학습에 이용되는 특징정보의 속성을 확인한다.

[0208] 여기서, 인공지능 모델 생성 시 학습에 이용되는 특징정보는, 인공지능 모델 생성 시 설정 가능한 전체 특징정보 중 UI를 기반으로 사용자에 의해 직접 설정되는 특징정보일 수 있고, 또는 전체 특징정보 중 추천되는 특정

특징정보 조합이 적용/설정되는 특징정보일 수도 있다.

[0209] 그리고, 특징정보의 속성은, 크게 숫자 속성과 카테고리 속성으로 구분될 수 있다.

[0210] 즉, 속성확인부(310)는, 인공지능 모델 생성 시 학습에 이용되는 특징정보(직접 설정 또는 추천 적용)의 속성이, 숫자 속성인지 또는 카테고리 속성인지 또는 숫자 및 카테고리 조합 속성인지를 확인할 수 있다.

[0211] 결정부(320)는, 설정 가능한 전체 정규화 방식 중, 속성확인부(310)에서 확인한 특징정보의 속성에 따른 정규화 방식을 결정한다.

[0212] 구체적으로 설명하면, 결정부(320)는, 특징정보의 속성에 따른 정규화 방식을 결정하기에 앞서, 금번 특징정보 전체 필드에 동일한 정규화 방식이 적용되는지 또는 금번 특징정보 전체 필드에서 필드 별로 정규화 방식이 적용되는지를 먼저 구분할 수 있다.

[0213] 결정부(320)는, 금번 특징정보 전체 필드에 숫자 및/또는 카테고리 데이터만 존재하는 경우(단일 특징 case 포함), 금번 특징정보 전체 필드에 동일한 정규화 방식이 적용되는 것으로 구분할 수 있다.

[0214] 이 경우, 결정부(320)는, 특징정보의 속성이 숫자 속성인 경우, 특징정보의 전체 숫자패턴에 따른 제1 정규화 방식을 결정하고, 특징정보의 속성이 카테고리 속성인 경우, 특징정보의 전체 카테고리 개수로 정의되는 벡터(Vector) 내 특징정보의 카테고리 별로 지정된 위치에만 0이 아닌 특성값으로 표현하는 제2 정규화 방식을 결정하고, 특징정보의 속성이 숫자 및 카테고리 조합 속성인 경우, 상기 제2 정규화 방식 및 제1 정규화 방식을 결정할 수 있다.

[0215] 구체적으로, 제1 정규화 방식은, 기 정의된 우선순위에 따라 Standard score 정규화 방식, Mean normalization 정규화 방식, Feature scaling 정규화 방식을 포함한다(수학식 1,2,3 참조).

[0216] 결정부(320)는, 특징정보 전체 필드에 숫자 데이터만 존재하는 경우 특징정보의 속성이 숫자 속성인 것으로 구분하고, 이 경우 특징정보의 전체 숫자패턴에 따른 제1 정규화 방식을 결정한다.

[0217] 이때, 결정부(320)는, 제1 정규화 방식 중 우선순위에 따라 Standard score 정규화 방식, Mean normalization 정규화 방식, Feature scaling 정규화 방식의 순서로 결정하되, 특징정보의 전체 숫자패턴에 대한 표준편차 및 정규화 스케일링 범위 상/하한 존재 여부를 근거로, 제1 정규화 방식 중 적용 가능한 가장 우선순위가 높은 정규화 방식을 결정할 수 있다.

[0218] 또한, 결정부(320)는, 특징정보 전체 필드에 카테고리 데이터만 존재하는 경우 특징정보의 속성이 카테고리 속성인 것으로 구분하고, 이 경우 특징정보의 전체 카테고리 개수로 정의되는 벡터(Vector) 내 특징정보의 카테고리 별로 지정된 위치에만 0이 아닌 특성값으로 표현하는 제2 정규화 방식을 결정할 수 있다.

[0219] 학습 데이터에 인공지능 알고리즘(예: 기계 학습)을 적용하여 인공지능 모델을 생성하기 위해서는, 데이터를 기계가 이해할 수 있는 수치 형태의 데이터로 변환해 주어야 하는데, 본 발명에서는 이러한 변환 방식(제2 정규화 방식)으로 One Hot Encoding을 채택할 수 있다.

[0220] 이에, 결정부(320)는, 특징정보의 속성이 카테고리 속성인 경우, 특징정보의 전체 카테고리 개수로 정의되는 벡터(Vector) 내 특징정보의 카테고리 별로 지정된 위치에만 0이 아닌 특성값(예: 1)으로 표현하는 제2 정규화 방식_One Hot Encoding을 결정할 수 있다.

[0221] 제2 정규화 방식_One Hot Encoding을 간단히 설명하면, 특징정보가 과일이라는 카테고리 속성을 가지며 사과, 배, 감(과일의 종류가 3개이므로 3차원 벡터로 표현)이 전체 카테고리 개수라고 가정한다.

[0222] 이때 사과, 배, 감 각각을 데이터로 가지는 각 특징정보는 제2 정규화 방식_One Hot Encoding에 따라 다음과 같이 표현될 수 있다.

[0223] 사과 = {1, 0, 0}

[0224] 배 = {0, 1, 0}

[0225] 감 = {0, 0, 1}

[0226] 또한, 결정부(320)는, 특징정보 전체 필드에 숫자 및 카테고리 데이터가 존재하는 경우 특징정보의 속성이 숫자 및 카테고리 조합 속성인 것으로 구분하고, 이 경우 전술의 제2 정규화 방식 및 제1 정규화 방식을 결정할 수 있다.

[0227] 즉, 결정부(320)는, 특징정보의 속성이 숫자 및 카테고리 조합 속성인 경우, 특징정보 내 카테고리 속성의 데이터에 대해서 먼저 전술의 제2 정규화 방식_One Hot Encoding이 적용된 후, 특징정보의 전체 숫자패턴에 대한 표준편차 및 정규화 스케일링 범위 상/하한 존재 여부를 근거로 제1 정규화 방식 중 적용 가능한 가장 우선순위가 높은 정규화 방식을 결정하기 위해서, 제2 정규화 방식 및 제1 정규화 방식을 결정할 수 있다.

[0228] 한편, 결정부(320)는, 특징정보가 복합 특징(여러 보안이벤트 간의 집계, 통계적 기법들을 활용하여 추출할 수 있는 하나의 특징)인 경우, 금번 특징정보 전체 필드에서 필드 별로 정규화 방식 적용되는 것으로 구분할 수 있다.

[0229] 이 경우, 결정부(320)는, 특징정보에서 속성이 종류 속성의 필드에 대해서는 Mean normalization 정규화 방식, Feature scaling 정규화 방식 중 적용 가능한 가장 우선순위가 높은 정규화 방식을 결정할 수 있다.

[0230] 또한, 결정부(320)는, 특징정보에서 속성이 개수 속성의 필드에 대해서는 Mean normalization 정규화 방식, Feature scaling 정규화 방식 중 적용 가능한 가장 우선순위가 높은 정규화 방식을 결정할 수 있다.

[0231] 또한, 결정부(320)는, 특징정보에서 속성이 비율 속성의 필드에 대해서는 정규화 방식을 미 결정하고 정규화 대상에서 제외시키도록 결정하거나 또는 Standard score 정규화 방식을 결정할 수 있다.

[0232] 또한, 결정부(320)는, 특징정보에서 속성이 존재 여부(예: 연산 결과값의 유/무)속성의 필드에 대해서는 정규화 방식을 미 결정하고 정규화 대상에서 제외시키도록 결정할 수 있다.

[0233] 추천부(330)는, 결정부(320)에서 결정한 정규화 방식을 추천한다.

[0234] 이상, 본 발명에 따르면, 인공지능 모델 플랫폼(100)에서 제공하는 환경에서 UI를 기반으로 보안관제를 위한 인공지능 모델을 생성하는 사용자에게 최적의 성능(정확도)를 갖는 최적 정규화 방식을 추천/적용할 수 있도록 함으로써, 보안관제 기술에 익숙하지 않은 일반 사용자도 보안관제를 위한 최적의 인공지능 모델을 생성할 수 있도록 한다.

[0235] 이상에서 설명한 바와 같이, 본 발명에 의하면, 보안관제를 위한 인공지능 모델을 생성할 수 있도록 하는 인공지능 모델 플랫폼을 구현하되, 특히 인공지능 모델 성능에 직결되는 특징정보 및 정규화 방식을 최적으로 추천/적용할 수 있도록 함으로써, 보안관제 기술에 익숙하지 않은 일반 사용자도 보안관제를 위한 최적의 인공지능 모델을 생성할 수 있도록 하는 인공지능 모델 플랫폼을 구현할 수 있다.

[0236] 이로 인해, 본 발명에 따르면, 보안관제를 위한 목적 및 요구 사항에 적합한 최적의 인공지능 모델을 유연하고 다양하게 생성 및 적용할 수 있기 때문에, 보안관제 서비스의 품질 향상을 극대화시킬 수 있고, 아울러 대규모 사이버공격 및 이상행위 발생 징후를 효율적으로 분석하기 위한 인공지능 기반의 침해대응 체계 구축을 지원할 수 있는 효과까지 기대할 수 있다.

[0237] 이하에서는, 도 5를 참조하여, 본 발명의 일 실시예에 따른 인공지능 모델 플랫폼 운영 방법에 대하여 설명하겠다.

[0238] 본 발명의 인공지능 모델 플랫폼(100)은, 빅데이터 통합저장 스토리지로부터 신규 생성된 원천 보안데이터를 주기적으로 수집한다(S10).

[0239] 본 발명의 인공지능 모델 플랫폼(100)은, 보안관제를 위한 인공지능 모델을 생성하고자 하는 시스템 관리자 또는 일반 사용자(이하, 사용자로 통칭함)의 조작에 따라, UI를 통해 수집/인공지능 기능과 관련된 각종 설정을 입력 받아 설정정보로 저장/관리한다(S20).

[0240] 그리고, 본 발명의 인공지능 모델 플랫폼(100)은, 원천 보안데이터로부터 특정 검색 조건 즉 앞서 사용자에 의해 기 설정된 특정 검색 조건에 의해 학습/테스트 데이터로 사용하고자 하는 보안이벤트를 수집한다(S30).

[0241] 본 발명의 인공지능 모델 플랫폼(100)은, S30단계에서 수집된 보안이벤트에 대하여 기 설정된 특징정보 즉 앞서 사용자에 의해 기 설정된 특징정보(Feature)를 추출한다(S40).

[0242] 그리고, 본 발명의 인공지능 모델 플랫폼(100)은, 보안이벤트의 추출된 특징정보에 대하여, 앞서 사용자에 의해 기 설정된 정규화를 수행한다(S50).

[0243] 본 발명의 인공지능 모델 플랫폼(100)에서는, 전술의 3가지 정규화 방식을 제공하여 사용자로 하여금 기 설정할 수 있도록 한다.

[0244] 이때, 본 발명의 인공지능 모델 플랫폼(100)은, 사용자에 의해 설정되는 정규화 방식이 최적이 아닐 수 있으므로, 인공지능 모델의 정확도를 높일 수 있는 최적의 정규화 방식을 추천할 수 있다(S50).

[0245] 정규화 방식 추천에 대한 구체적인 설명은, 후술의 도 7에서 구체적으로 언급하겠다.

[0246] 본 발명의 인공지능 모델 플랫폼(100)은, 특정정보 정규화가 완료된 보안이벤트에서 학습 데이터 또는 테스트 데이터를 주어진 조건 즉 앞서 사용자에 의해 기 설정된(주어진) 조건에 의해 추출한다(S60).

[0247] 구체적으로, 본 발명의 인공지능 모델 플랫폼(100)은, 특정정보 정규화가 완료된 보안이벤트를, 사용자가 원하는 값, 순서, 포맷, 학습/테스트 데이터 비율, 파일분할방식 등에 따라 화면 또는 파일로 출력하게 된다.

[0248] 그리고, 본 발명의 인공지능 모델 플랫폼(100)은, 학습 데이터에 인공지능 알고리즘을 적용하여, 보안관제를 위한 인공지능 모델을 생성한다(S70).

[0249] 즉, 본 발명의 인공지능 모델 플랫폼(100)은, 학습 데이터에 인공지능 알고리즘을 적용하여, 보안관제를 위한 인공지능 모델, 예컨대 사용자에 의해 요구되는 기능의 인공지능 모델을 생성할 수 있다.

[0250] 예를 들면, 본 발명의 인공지능 모델 플랫폼(100)은, 사용자 요구에 따라, 보안이벤트의 악성 여부를 탐지하기 위한 인공지능 탐지모델을 생성할 수 있고, 보안이벤트의 정탐/오탐을 분류하기 위한 인공지능 분류모델을 생성할 수도 있다.

[0251] 구체적으로, 본 발명의 인공지능 모델 플랫폼(100)은, S60단계에서 출력/파일 저장소에 관리되는 학습 데이터를 기반으로, 인공지능 알고리즘 예컨대 사용자에 의해 기 선택된 기계학습(예: Deep Learning) 알고리즘에 따라, 보안관제를 위한 인공지능 모델을 생성할 수 있다.

[0252] 예를 들면, 본 발명의 인공지능 모델 플랫폼(100)은, Backward Propagation(오차역전파법) 계산 기반의 기계학습 기술에서 모델을 통해 예측되는 결과값과 실제 결과값 간의 편차를 나타내는 학습손실함수(Loss function)을 이용하여, 학습 데이터를 기반으로 학습손실함수(Loss function)의 편차가 0이 되는 인공지능 모델을 생성할 수 있다.

[0253] 더 나아가, 본 발명의 인공지능 모델 플랫폼(100)은, S60단계에서 출력/파일 저장소에 관리되는 테스트 데이터(정탐/오탐 분류 및 악성 여부 탐지의 실제 결과값을 알고 있는 보안이벤트)를 활용하여, 전술의 생성한 인공지능 모델의 정확도를 테스트한다(S80).

[0254] 예를 들어, 본 발명의 인공지능 모델 플랫폼(100)은, 테스트 데이터를 활용하여 전술의 생성한 인공지능 모델을 테스트하여, 모델을 통해 예측되는 결과값과 알고 있는 실제 결과값의 일치 비율을 모델의 정확도(성능) 즉 테스트 결과로서 출력할 수 있다.

[0255] 이에, 본 발명의 인공지능 모델 플랫폼(100)은, '누가' '언제' '어떤 데이터' '어떤 필드' '어떤 샘플링 방식' '어떤 정규화 방식' '어떤 모델'을 이용하여 인공지능 모델을 만든 것인지, 또한 생성된 인공지능 모델이 어느 정도의 성능(정답률)을 갖는지 등의 성능 정보를 시스템(파일저장소)에 기록 및 관리할 수 있다.

[0256] 그리고, 본 발명의 인공지능 모델 플랫폼(100)은, 이러한 성능 정보 관리를 기반으로, 모델 생성을 위한 조건들과 성능을 한눈에 비교할 수 있어 조건들과 성능의 상관 관계를 쉽게 파악할 수 있도록 한다.

[0257] 이때, 본 발명의 인공지능 모델 플랫폼(100)은, S80단계의 정확도 테스트 결과를 근거로, 전술의 생성한 인공지능 모델의 정확도를 높이도록 특징정보(Feature)에 대한 변경을 추천할 수 있다(S90,S100).

[0258] 즉, 본 발명의 인공지능 모델 플랫폼(100)은, 인공지능 모델 생성 시 학습에 이용된 특징정보(이하, 사용자 설정 특징정보) 대비, 인공지능 모델의 정확도를 향상시킬 수 있는 다른 특징정보 조합이 있다면(S90 Yes), 이를 추천하는 방식이다(S100).

[0259] 이하에서는 도 6을 참조하여 본 발명의 하드웨어(추천 장치)에서 수행되는 컴퓨터프로그램 즉 특징정보 추천을 위한 컴퓨터프로그램에 대해 설명하며, 다만 설명의 편의 상 특징정보 추천 장치(200)의 동작 방법으로 지칭하여 설명하겠다.

[0260] 본 발명의 컴퓨터프로그램 즉 특징정보 추천 장치(200)의 동작 방법에 따르면, 사용자에 의해 설정된 특징정보 학습을 기반으로 생성된 인공지능 모델의 성능(정확도)를 확인한다(S110).

[0261] 구체적인 설명을 위해, 이하에서는, 본 발명의 인공지능 모델 플랫폼(100)에서 사용자에 의해 설정된 특징정보(이하, 사용자 설정 특징정보)를 학습/생성된 인공지능 모델을 가정하여 설명하겠다.

[0262] 본 발명에 따른 특징정보 추천 장치(200)의 동작 방법은, 전술과 같이 인공지능 모델 플랫폼(100)에서 사용자 설정 특징정보를 학습하여 생성된 인공지능 모델에 대하여, 모델 성능을 확인한다(S110).

[0263] 예를 들면, 본 발명에 따른 특징정보 추천 장치(200)의 동작 방법은, 인공지능 모델에 대하여, 본 발명의 인공지능 모델 플랫폼(100, 특히 데이터출력모듈(140))에서 출력되는 테스트 데이터(정탐/오탐 분류 및 악성 여부 탐지의 실제 결과값을 알고 있는 보안이벤트)를 활용하여, 모델 성능(정확도)을 테스트/확인할 수 있다.

[0264] 이에 본 발명에 따른 특징정보 추천 장치(200)의 동작 방법은, 본 발명의 인공지능 모델 플랫폼(100, 특히 데이터출력모듈(140))에서 생성되는 인공지능 모델을 대상으로, 테스트 데이터를 활용하여 인공지능 모델을 테스트함으로써, 모델을 통해 예측되는 결과값과 알고 있는 실제 결과값의 일치 비율을 모델의 정확도(성능) 즉 테스트 결과로서 출력할 수 있다.

[0265] 본 발명에 따른 특징정보 추천 장치(200)의 동작 방법은, 전체 특징정보에서 다수의 특징정보 조합을 설정하여, 다수의 특징정보 조합 별로 학습을 기반으로 생성된 인공지능 모델의 성능을 확인한다(S120,S130).

[0266] 구체적으로, 본 발명에 따른 특징정보 추천 장치(200)의 동작 방법은, 인공지능 모델 생성 시 설정 가능한 전체 특징정보에서, 금번 인공지능 모델 생성 시 학습된 사용자 설정 특징정보 외 다양한 특징정보 조합을 설정하여 다수의 특징정보 조합 별로 학습을 기반으로 생성된 인공지능 모델의 성능을 확인할 수 있다.

[0267] 이하에서는, 특정 특징정보 조합을 추천하는 구체적인 실시예들을 설명하겠다.

[0268] 이하에서는, 전체 특징정보(예: a,b,c...,z(n=26)) 중 금번 인공지능 모델 생성 시 학습된 사용자 설정 특징정보(예: a,b,c,d,e,f(k=6))를 가정하여 설명하겠다. 그리고 이 경우 확인한 인공지능 모델 성능(m_k)이 85%라고 가정한다.

[0269] 이에, 본 발명에 따른 특징정보 추천 장치(200)의 동작 방법은, 사용자 설정 특징정보(a,b,c,d,e,f)에 전체 특징정보(n) 중 사용자 설정 특징정보(a,b,c,d,e,f)를 제외한 나머지 특정정보 중 적어도 하나씩 순차적으로 추가하여, 다수의 특징정보 조합을 설정할 수 있다(S120).

[0270] 예를 들면, 본 발명에 따른 특징정보 추천 장치(200)의 동작 방법은, 사용자가 설정한 사용자 설정 특징정보(a,b,c,d,e,f)에, 전체 특징정보(n) 중 사용자 설정 특징정보(a,b,c,d,e,f)를 제외한 나머지 특정정보 중 1~(n-k)개의 특징정보를 순차적으로 추가하여, 다음과 같은 다수의 특징정보 조합을 설정할 수 있다.

[0271] a,b,c,d,e,f,g -> $m_{(k+1)}^{1}$ -> 82%

[0272] a,b,c,d,e,f,h -> $m_{(k+1)}^{2}$ -> 80%

[0273] ...

[0274] a,b,c,d,e,f,g,h,i -> $m_{(k+3)}^{1}$ -> 88%

[0275] ...

[0276] a,b,c,d,e,f,...,z -> $m_{(n)}$ -> 85%

[0277] 그리고, 본 발명에 따른 특징정보 추천 장치(200)의 동작 방법은, 전술과 같이 다수의 특징정보 조합 별로 학습을 기반으로 생성된 인공지능 모델의 성능, 82%, 80%, ... 88%,...85%을 확인할 수 있다(S130).

[0278] 이 경우, 본 발명에 따른 특징정보 추천 장치(200)의 동작 방법은, 다수의 특징정보 조합 별 성능 중에서, 금번 사용자 설정을 기반으로 생성된 인공지능 모델의 성능(m_k=85%) 보다 높은 성능을 갖는 상위 N개(예: 4개)를 특정 특징정보 조합으로서 선택/추천할 수 있다(S140 Yes, S150).

[0279] 다른 예를 들면, 본 발명에 따른 특징정보 추천 장치(200)의 동작 방법은, 사용자가 설정한 사용자 설정 특징정보(a,b,c,d,e,f)에, 전체 특징정보(n) 중 사용자 설정 특징정보(a,b,c,d,e,f)를 제외한 나머지 특정정보를 1개씩 순차적으로 추가하여, 다음과 같은 다수의 특징정보 조합을 설정할 수 있다(S120).

[0280] a,b,c,d,e,f,g -> $m_{(k+1)}^{1}$ -> 82%

[0281] a,b,c,d,e,f,h -> $m_{(k+1)}^{2}$ -> 80%

[0282] ...

[0283] a,b,c,d,e,f,z -> $m_{(k+1)}^{\zeta+1}$ -> 90%

[0284] 그리고, 본 발명에 따른 특징정보 추천 장치(200)의 동작 방법은, 전술과 같이 다수의 특징정보 조합 별로 학습을 기반으로 생성된 인공지능 모델의 성능, 82%, 80%, ...90%을 확인할 수 있다(S130).

[0285] 이 경우, 본 발명에 따른 특징정보 추천 장치(200)의 동작 방법은, 다수의 특징정보 조합 별 성능 중에서, 금번 사용자 설정을 기반으로 생성된 인공지능 모델의 성능(m_k=85%) 보다 높은 성능을 갖는 상위 N개(예: 3개)를 특정 특징정보 조합으로서 선택/추천할 수 있다(S140 Yes, S150).

[0286] 이상, 본 발명에 따르면, 인공지능 모델 플랫폼(100)에서 제공하는 환경에서 UI를 기반으로 보안관제를 위한 인공지능 모델을 생성하는 사용자에게 최적의 성능(정확도)를 갖는 최적 특징(feature)를 추천/적용할 수 있도록 함으로써, 보안관제 기술에 익숙하지 않은 일반 사용자도 보안관제를 위한 최적의 인공지능 모델을 생성할 수 있도록 한다.

[0287] 이하에서는 도 7을 참조하여 본 발명의 하드웨어(추천 장치)에서 수행되는 컴퓨터프로그램 즉 정규화 방식 추천을 위한 컴퓨터프로그램에 대해 설명하며, 다만 설명의 편의 상 정규화 방식 추천 장치(300)의 동작 방법으로 지칭하여 설명하겠다.

[0288] 본 발명의 컴퓨터프로그램 즉 정규화 방식 추천 장치(300)의 동작 방법에 따르면, 인공지능 모델 생성 시 학습에 이용되는 특징정보의 속성을 확인한다(S200).

[0289] 여기서, 인공지능 모델 생성 시 학습에 이용되는 특징정보는, 인공지능 모델 생성 시 설정 가능한 전체 특징정보 중 UI를 기반으로 사용자에 의해 직접 설정되는 특징정보일 수 있고, 또는 전체 특징정보 중 추천되는 특정 특징정보 조합이 적용/설정되는 특징정보일 수도 있다.

[0290] 그리고, 특징정보의 속성은, 크게 숫자 속성과 카테고리 속성으로 구분될 수 있다.

[0291] 즉, 본 발명에 따른 정규화 방식 추천 장치(300)의 동작 방법은, 인공지능 모델 생성 시 학습에 이용되는 특징정보(직접 설정 또는 추천 적용)의 속성이, 숫자 속성인지 또는 카테고리 속성인지 또는 숫자 및 카테고리 조합 속성인지를 확인할 수 있다(S200).

[0292] 본 발명에 따른 정규화 방식 추천 장치(300)의 동작 방법은, 설정 가능한 전체 정규화 방식 중, S200단계에서 확인한 특징정보의 속성에 따른 정규화 방식을 결정한다.

[0293] 구체적으로 설명하면, 본 발명에 따른 정규화 방식 추천 장치(300)의 동작 방법은, 특징정보의 속성에 따른 정규화 방식을 결정하기에 앞서, 금번 특징정보 전체 필드에 동일한 정규화 방식이 적용되는지 또는 금번 특징정보 전체 필드에서 필드 별로 정규화 방식이 적용되는지를 먼저 구분할 수 있다(S210).

[0294] 본 발명에 따른 정규화 방식 추천 장치(300)의 동작 방법은, 금번 특징정보 전체 필드에 숫자 및/또는 카테고리 데이터만 존재하는 경우(단일 특징 case 포함), 금번 특징정보 전체 필드에 동일한 정규화 방식이 적용되는 것으로 구분할 수 있다(S210 Yes).

[0295] 이 경우, 본 발명에 따른 정규화 방식 추천 장치(300)의 동작 방법은, 특징정보의 속성이 숫자 속성인 경우, 특징정보의 전체 숫자패턴에 따른 제1 정규화 방식을 결정하고, 특징정보의 속성이 카테고리 속성인 경우, 특징정보의 전체 카테고리 개수로 정의되는 벡터(Vector) 내 특징정보의 카테고리 별로 지정된 위치에만 0이 아닌 특성값으로 표현하는 제2 정규화 방식을 결정하고, 특징정보의 속성이 숫자 및 카테고리 조합 속성인 경우, 상기 제2 정규화 방식 및 제1 정규화 방식을 결정할 수 있다(S220).

[0296] 구체적으로, 제1 정규화 방식은, 기 정의된 우선순위에 따라 Standard score 정규화 방식, Mean normalization 정규화 방식, Feature scaling 정규화 방식을 포함한다(수학식 1,2,3 참조).

[0297] 본 발명에 따른 정규화 방식 추천 장치(300)의 동작 방법은, 특징정보 전체 필드에 숫자 데이터만 존재하는 경

우 특징정보의 속성이 숫자 속성인 것으로 구분하고, 이 경우 특징정보의 전체 숫자패턴에 따른 제1 정규화 방식을 결정한다.

[0298] 이때, 본 발명에 따른 정규화 방식 추천 장치(300)의 동작 방법은, 제1 정규화 방식 중 우선순위에 따라 Standard score 정규화 방식, Mean normalization 정규화 방식, Feature scaling 정규화 방식의 순서로 결정하되, 특징정보의 전체 숫자패턴에 대한 표준편차 및 정규화 스케일링 범위 상/하한 존재 여부를 근거로, 제1 정규화 방식 중 적용 가능한 가장 우선순위가 높은 정규화 방식을 결정할 수 있다.

[0299] 또한, 본 발명에 따른 정규화 방식 추천 장치(300)의 동작 방법은, 특징정보 전체 필드에 카테고리 데이터만 존재하는 경우 특징정보의 속성이 카테고리 속성인 것으로 구분하고, 이 경우 특징정보의 전체 카테고리 개수로 정의되는 벡터(Vector) 내 특징정보의 카테고리 별로 지정된 위치에만 0이 아닌 특성값(예: 1)으로 표현하는 제2 정규화 방식_One Hot Encoding을 결정할 수 있다.

[0300] 또한, 본 발명에 따른 정규화 방식 추천 장치(300)의 동작 방법은, 특징정보 전체 필드에 숫자 및 카테고리 데이터가 존재하는 경우 특징정보의 속성이 숫자 및 카테고리 조합 속성인 것으로 구분하고, 이 경우 전술의 제2 정규화 방식 및 제1 정규화 방식을 결정할 수 있다.

[0301] 즉, 본 발명에 따른 정규화 방식 추천 장치(300)의 동작 방법은, 특징정보의 속성이 숫자 및 카테고리 조합 속성인 경우, 특징정보 내 카테고리 속성의 데이터에 대해서 먼저 전술의 제2 정규화 방식_One Hot Encoding이 적용된 후, 특징정보의 전체 숫자패턴에 대한 표준편차 및 정규화 스케일링 범위 상/하한 존재 여부를 근거로 제1 정규화 방식 중 적용 가능한 가장 우선순위가 높은 정규화 방식을 결정하기 위해서, 제2 정규화 방식 및 제1 정규화 방식을 결정할 수 있다.

[0302] 한편, 본 발명에 따른 정규화 방식 추천 장치(300)의 동작 방법은, 특징정보가 복합 특징(여러 보안이벤트 간의 집계, 통계적 기법들을 활용하여 추출할 수 있는 하나의 특징)인 경우, 금번 특징정보 전체 필드에서 필드 별로 정규화 방식 적용되는 것으로 구분할 수 있다(S210 No).

[0303] 이 경우, 본 발명에 따른 정규화 방식 추천 장치(300)의 동작 방법은, 특징정보에서 속성이 종류 속성의 필드에 대해서는 Mean normalization 정규화 방식, Feature scaling 정규화 방식 중 적용 가능한 가장 우선순위가 높은 정규화 방식을 결정할 수 있다(S230).

[0304] 또한, 본 발명에 따른 정규화 방식 추천 장치(300)의 동작 방법은, 특징정보에서 속성이 개수 속성의 필드에 대해서는 Mean normalization 정규화 방식, Feature scaling 정규화 방식 중 적용 가능한 가장 우선순위가 높은 정규화 방식을 결정할 수 있다(S230).

[0305] 또한, 본 발명에 따른 정규화 방식 추천 장치(300)의 동작 방법은, 특징정보에서 속성이 비율 속성의 필드에 대해서는 정규화 방식을 미 결정하고 정규화 대상에서 제외시키도록 결정하거나 또는 Standard score 정규화 방식을 결정할 수 있다(S230).

[0306] 또한, 본 발명에 따른 정규화 방식 추천 장치(300)의 동작 방법은, 특징정보에서 속성이 존재 여부(예: 연산 결과값의 유/무)속성의 필드에 대해서는 정규화 방식을 미 결정하고 정규화 대상에서 제외시키도록 결정할 수 있다(S230).

[0307] 본 발명에 따른 정규화 방식 추천 장치(300)의 동작 방법은, S220단계 또는 S230단계에서 결정한 정규화 방식을 추천한다(S240).

[0308] 이상, 본 발명에 따르면, 인공지능 모델 플랫폼(100)에서 제공하는 환경에서 UI를 기반으로 보안관제를 위한 인공지능 모델을 생성하는 사용자에게 최적의 성능(정확도)를 갖는 최적 정규화 방식을 추천/적용할 수 있도록 함으로써, 보안관제 기술에 익숙하지 않은 일반 사용자도 보안관제를 위한 최적의 인공지능 모델을 생성할 수 있도록 한다.

[0309] 이상에서 설명한 바와 같이, 본 발명에 따르면, 보안관제를 위한 인공지능 모델을 생성할 수 있도록 하는 인공지능 모델 플랫폼을 구현하되, 특히 인공지능 모델 성능에 직결되는 특징정보 및 정규화 방식을 최적으로 추천/적용할 수 있도록 함으로써, 보안관제 기술에 익숙하지 않은 일반 사용자도 보안관제를 위한 최적의 인공지능 모델을 생성할 수 있도록 하는 인공지능 모델 플랫폼을 구현할 수 있다.

[0310] 이로 인해, 본 발명에 따르면, 보안관제를 위한 목적 및 요구 사항에 적합한 최적의 인공지능 모델을 유연하고 다양하게 생성 및 적용할 수 있기 때문에, 보안관제 서비스의 품질 향상을 극대화시킬 수 있고, 아울러 대규모

사이버공격 및 이상행위 발생 징후를 효율적으로 분석하기 위한 인공지능 기반의 침해대응 체계 구축을 지원할 수 있는 효과까지 기대할 수 있다.

[0311] 위 설명한 본 발명의 일 실시예에 따른 인공지능 모델 플랫폼 운영 방법은, 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0312] 지금까지 본 발명을 바람직한 실시 예를 참조하여 상세히 설명하였지만, 본 발명이 상기한 실시 예에 한정되는 것은 아니며, 이하의 특허청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 또는 수정이 가능한 범위까지 본 발명의 기술적 사상이 미친다 할 것이다.

산업상 이용가능성

[0313] 본 발명의 인공지능 모델 플랫폼 및 인공지능 모델 플랫폼 운영 방법에 따르면, 보안관제 기술에 익숙하지 않은 일반 사용자도 보안관제를 위한 최적의 인공지능 모델을 생성할 수 있도록 하는 플랫폼 환경을 제공할 수 있는 점에서, 기존 기술의 한계를 뛰어 넘음에 따라 관련 기술에 대한 이용만이 아닌 적용되는 장치의 시판 또는 영업의 가능성이 충분할 뿐만 아니라 현실적으로 명백하게 실시할 수 있는 정도이므로 산업상 이용가능성이 있는 발명이다.

부호의 설명

[0314] 100 : 인공지능 모델 플랫폼

110 : 데이터수집모듈 120 : 특징추출모듈

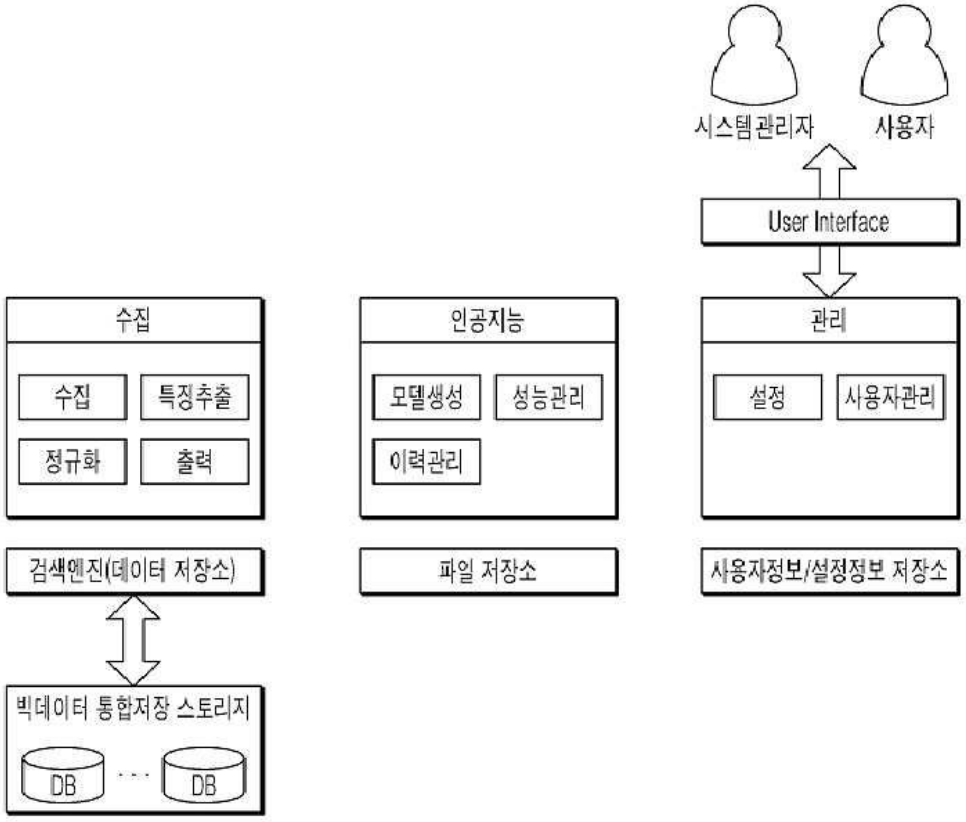
130 : 정규화모듈 140 : 데이터출력모듈

150 : 모델생성모듈 160 : 성능관리모듈

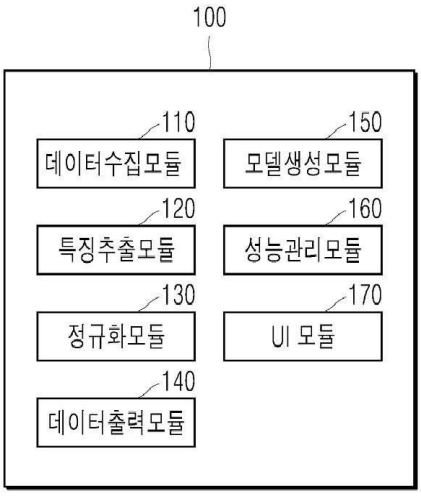
170 : UI모듈

도면

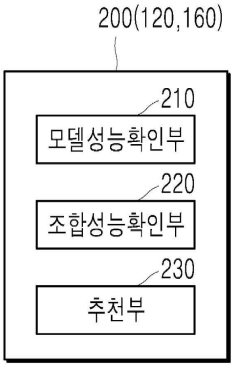
도면1


시스템관리자
사용자
User Interface
수집
수집
특징추출
정규화
출력
인공지능
모델생성
성능관리
이력관리
관리
설정
사용자관리
검색엔진(데이터 저장소)
파일 저장소
사용자정보/설정정보 저장소
빅데이터 통합저장 스토리지
DB
DB

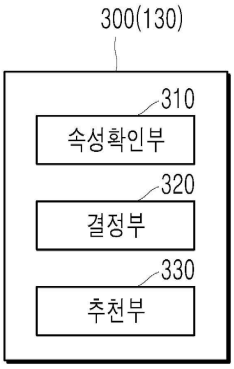
도면2


100
110
데이터수집모듈
150
모델생성모듈
120
특징추출모듈
160
성능관리모듈
130
정규화모듈
170
UI 모듈
140
데이터출력모듈

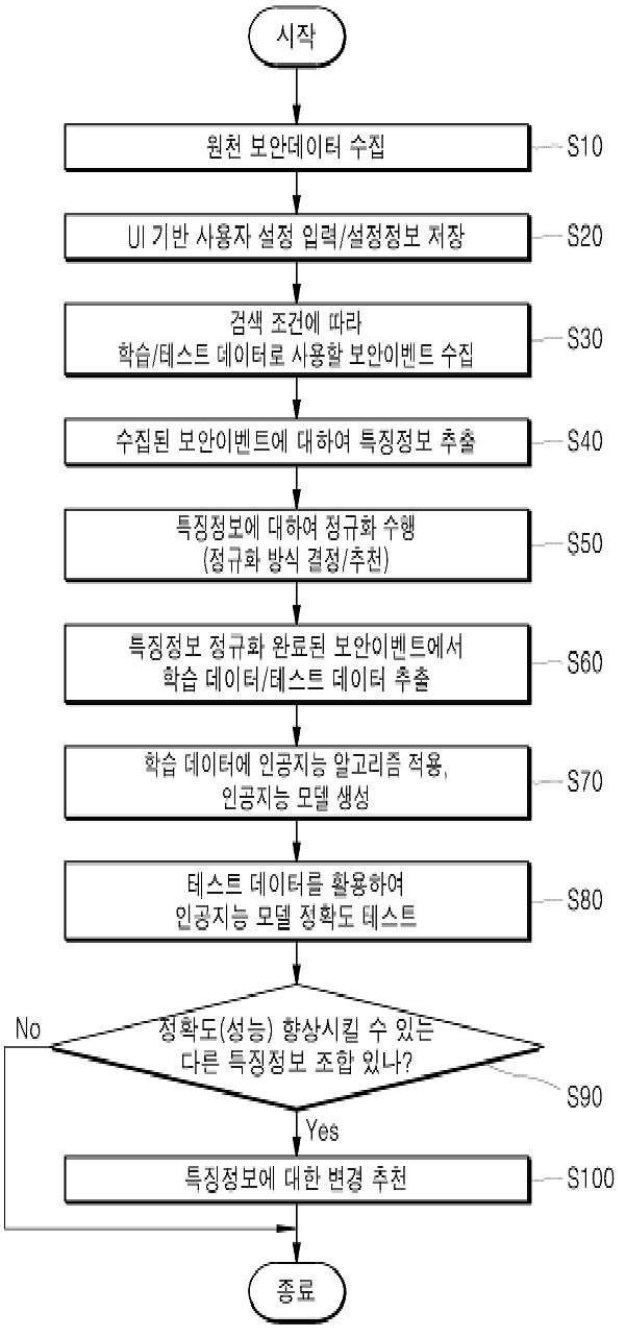
도면3


200(120,160)
210
모델성능확인부
220
조합성능확인부
230
추천부

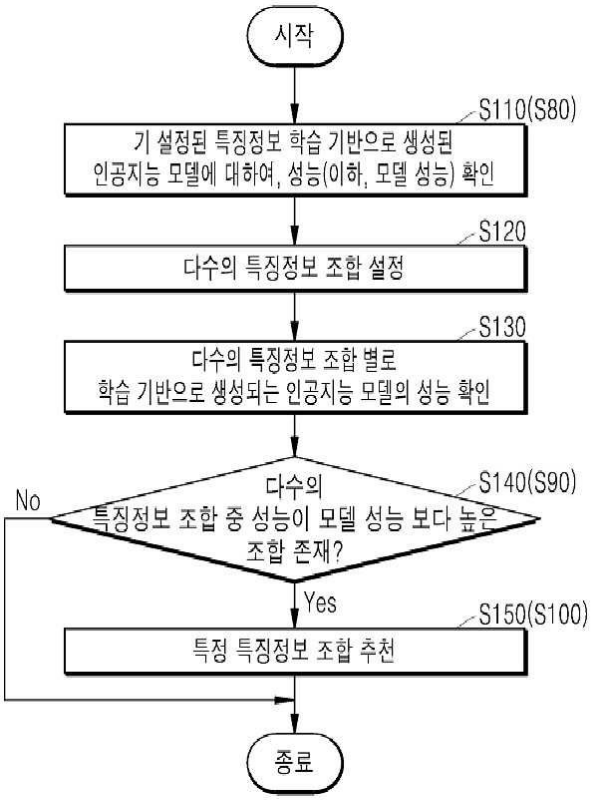
도면4


300(130)
310
속성확인부
320
결정부
330
추천부

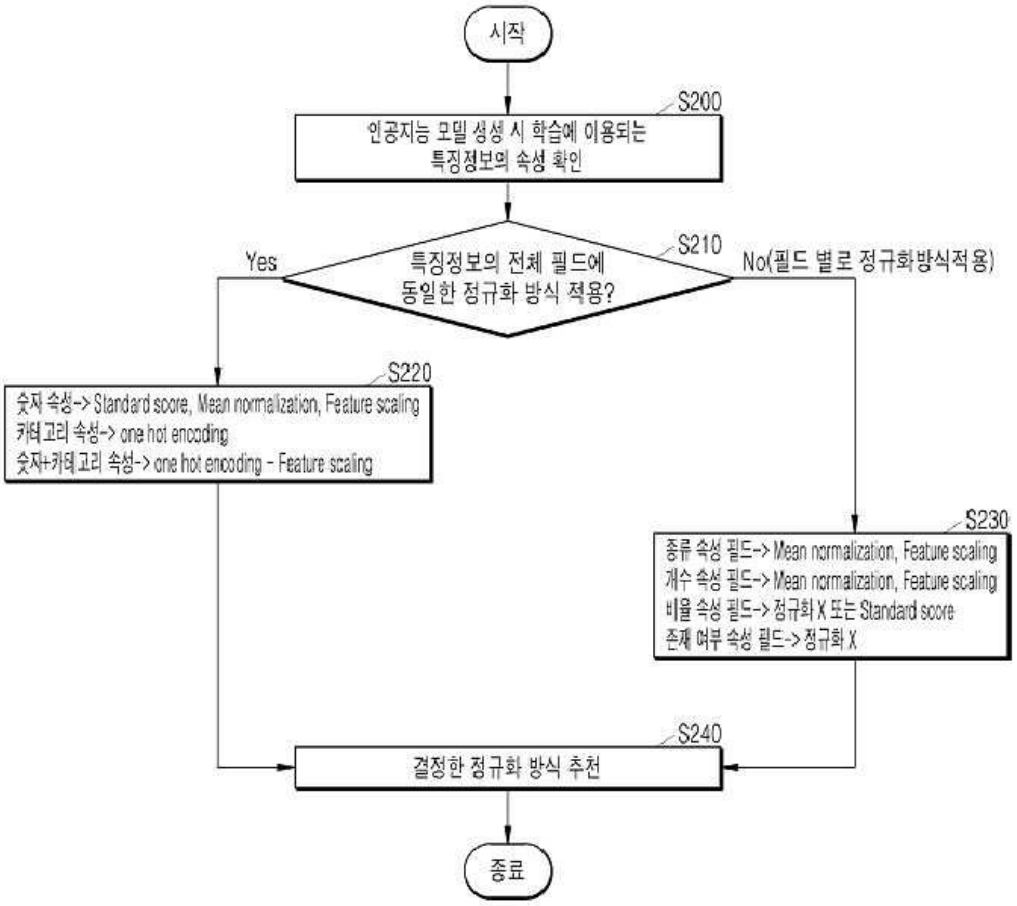
도면5


시작
원천 보안데이터 수집
S10
UI 기반 사용자 설정 입력/설정정보 저장
S20
검색 조건에 따라
학습/테스트 데이터로 사용할 보안이벤트 수집
S30
수집된 보안이벤트에 대하여 특징정보 추출
S40
특징정보에 대하여 정규화 수행
(정규화 방식 결정/추천)
S50
특징정보 정규화 완료된 보안이벤트에서
학습 데이터/테스트 데이터 추출
S60
학습 데이터에 인공지능 알고리즘 적용,
인공지능 모델 생성
S70
테스트 데이터를 활용하여
인공지능 모델 정확도 테스트
S80
No
정확도(성능) 향상시킬 수 있는
다른 특징정보 조합 있나?
S90
Yes
특징정보에 대한 변경 추천
S100
종료

도면6


시작
S110(S80)
기 설정된 특징정보 학습 기반으로 생성된
인공지능 모델에 대하여, 성능(이하, 모델 성능) 확인
S120
다수의 특징정보 조합 설정
S130
다수의 특징정보 조합 별로
학습 기반으로 생성되는 인공지능 모델의 성능 확인
S140(S90)
다수의
특징정보 조합 중 성능이 모델 성능 보다 높은
조합 존재?
No
Yes
S150(S100)
특정 특징정보 조합 추천
종료

도면7


시작
S200
인공지능 모델 생성 시 학습에 이용되는
특징정보의 속성 확인
S210
특징정보의 전체 필드에
동일한 정규화 방식 적용?
Yes
No(필드 별로 정규화방식적용)
S220
숫자 속성-> Standard score, Mean normalization, Feature scaling
카테고리 속성-> one hot encoding
숫자+카테고리 속성-> one hot encoding - Feature scaling
S230
종류 속성 필드-> Mean normalization, Feature scaling
개수 속성 필드-> Mean normalization, Feature scaling
비율 속성 필드-> 정규화 X 또는 Standard score
존재 여부 속성 필드-> 정규화 X
S240
결정한 정규화 방식 추천
종료