



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2023년01월03일

(11) 등록번호 10-2483797

(24) 등록일자 2022년12월28일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) G06N 20/00 (2019.01)
G06N 3/08 (2006.01)

(52) CPC특허분류
H04L 63/1416 (2013.01)
G06N 20/00 (2021.08)

(21) 출원번호 10-2022-0065476

(22) 출원일자 2022년05월27일

심사청구일자 2022년05월27일

(56) 선행기술조사문헌

JP2007060233 A*

KR1020200133644 A*

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

엘아이지넥스원 주식회사

경기도 용인시 기흥구 마북로 207 (마북동)

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

유재관

경기도 성남시 분당구 판교로 333 (삼평동)

박성진

경기도 성남시 분당구 판교로 333 (삼평동)

(뒷면에 계속)

(74) 대리인

특허법인우인

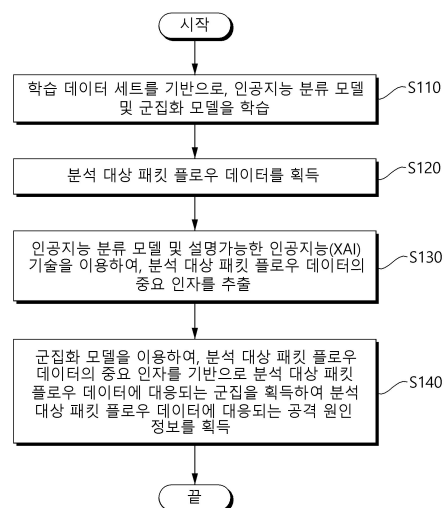
전체 청구항 수 : 총 6 항

심사관 : 문형섭

(54) 발명의 명칭 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 방법, 이를 수행하는 장치 및 컴퓨터 프로그램

(57) 요약

본 발명의 바람직한 실시예에 따른 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 방법, 이를 수행하는 장치 및 컴퓨터 프로그램은, 설명가능한 인공지능(explainable artificial intelligence, XAI)을 이용하여 네트워크 패킷 공격의 원인을 분석함으로써, 군집 분류 성능을 향상시킬 수 있어 보다 정확한 공격 원인의 분석이 가능하다.

대표도 - 도2

(52) CPC특허분류

G06N 3/08 (2013.01)

(72) 발명자

조병모

경기도 성남시 분당구 판교로 333 (삼평동)

이상근

서울특별시 성북구 안암로 73-15(안암동5가)

김혜은

서울특별시 성북구 안암로 61-1, 704호 (안암동5가, 구결발당)

정관영

경기도 안양시 동안구 귀인로 294 (평촌동)

한성민

서울특별시 동대문구 무학로45길 10, 401호(용두동)

명세서

청구범위

청구항 1

동일한 송신자 및 수신자의 통신으로 구성된 패킷들로 이루어진 분석 대상 패킷 플로우(packet flow) 데이터를 획득하는 단계;

미리 학습되어 구축된 인공지능 분류 모델과 설명가능한 인공지능(explainable artificial intelligence, XAI) 기술을 이용하여, 상기 분석 대상 패킷 플로우 데이터의 중요 인자를 추출하는 단계; 및

군집화 모델을 이용하여, 상기 분석 대상 패킷 플로우 데이터의 중요 인자를 기반으로 상기 분석 대상 패킷 플로우 데이터에 대응되는 군집을 획득하여 상기 분석 대상 패킷 플로우 데이터에 대응되는 공격 원인 정보를 획득하는 단계;

를 포함하고,

상기 인공지능 분류 모델은, 패킷 플로우 데이터를 입력으로 하고, 입력된 패킷 플로우 데이터가 정상인지 악성인지 여부를 나타내는 값 및 입력된 패킷 플로우 데이터에 대응되는 설명 맵(saliency map)을 출력으로 하며,

상기 군집화 모델은, 패킷 플로우 데이터를 입력으로 하고, 입력된 패킷 플로우 데이터가 속하는 군집을 출력으로 하고,

상기 중요 인자 추출 단계는, 상기 분석 대상 패킷 플로우 데이터를 상기 인공지능 분류 모델에 입력하고, 상기 설명가능한 인공지능(XAI) 기술을 활용하여 도출한 설명 맵을 기반으로 상기 분석 대상 패킷 플로우 데이터의 중요 인자를 추출하는 것으로 이루어지며,

상기 공격 원인 정보 획득 단계는, 상기 분석 대상 패킷 플로우 데이터의 중요 인자를 기반으로 상기 분석 대상 패킷 플로우 데이터에서 중요 인자에 대한 값을 유지하고 중요 인자가 아닌 부분에 대한 값은 미리 설정된 대체 값으로 교체하고, 대체값으로 교체된 상기 분석 대상 패킷 플로우 데이터를 상기 군집화 모델에 입력하고, 상기 군집화 모델의 출력인 군집을 상기 분석 대상 패킷 플로우 데이터에 대응되는 군집으로 획득하며, 상기 분석 대상 패킷 플로우 데이터에 대응되는 군집의 공격 원인을 상기 분석 대상 패킷 플로우 데이터에 대응되는 공격 원인 정보로 획득하는 것으로 이루어지는 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

제1항에서,

학습 데이터 세트를 기반으로, 상기 인공지능 분류 모델 및 상기 군집화 모델을 학습하는 단계;

를 더 포함하며,

상기 학습 데이터 세트는,

동일한 송신자 및 수신자의 통신으로 구성된 패킷들로 이루어진 패킷 플로우 학습 데이터, 상기 패킷 플로우 학습 데이터가 정상인지 악성인지 여부를 나타내는 제1 정답 레이블(label) 및 상기 패킷 플로우 학습 데이터에 대응되는 군집을 나타내는 제2 정답 레이블을 포함하는,

설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 방법.

청구항 6

제5항에서,

상기 학습 단계는,

패킷 내의 미리 설정된 대체 대상 정보의 값을 미리 설정된 대체값으로 교체하고, 상기 인공지능 분류 모델의 입력 데이터 정보를 기반으로 패킷의 크기를 조정하여, 상기 패킷 플로우 학습 데이터를 전처리하는 단계;

전처리한 상기 패킷 플로우 학습 데이터 및 상기 제1 정답 레이블을 이용하여, 상기 인공지능 분류 모델을 학습하는 단계;

전처리한 상기 패킷 플로우 학습 데이터를 상기 인공지능 분류 모델에 입력하고, 상기 설명가능한 인공지능(XAI) 기술을 활용하여 도출한 설명 맵을 기반으로 전처리한 상기 패킷 플로우 학습 데이터의 중요 인자를 추출하는 단계; 및

전처리한 상기 패킷 플로우 학습 데이터의 중요 인자를 이용하여, 상기 군집화 모델을 학습하는 단계;

를 포함하는 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 방법.

청구항 7

제6항에서,

상기 군집화 모델 학습 단계는,

전처리한 상기 패킷 플로우 학습 데이터의 중요 인자를 기반으로 상기 패킷 플로우 학습 데이터에서 중요 인자에 대한 값은 유지하고 중요 인자가 아닌 부분에 대한 값은 미리 설정된 대체값으로 교체하고, 대체값으로 교체된 상기 패킷 플로우 학습 데이터 및 상기 제2 정답 레이블을 이용하여, 상기 군집화 모델을 학습하는 것으로 이루어지는,

설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 방법.

청구항 8

제1항, 제5항 내지 제7항 중 어느 한 항에 기재된 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 방법을 컴퓨터에서 실행시키기 위하여 컴퓨터 판독 가능한 저장 매체에 저장된 컴퓨터 프로그램.

청구항 9

설명가능한 인공지능(explainable artificial intelligence, XAI) 기술을 이용하여 네트워크 패킷 공격의 원인을 분석하는 공격 원인 분석 장치로서,

설명가능한 인공지능(XAI) 기술을 이용하여 네트워크 패킷 공격의 원인을 분석하기 위한 하나 이상의 프로그램을 저장하는 메모리; 및

상기 메모리에 저장된 상기 하나 이상의 프로그램에 따라 설명가능한 인공지능(XAI) 기술을 이용하여 네트워크 패킷 공격의 원인을 분석하기 위한 동작을 수행하는 하나 이상의 프로세서;

를 포함하며,

상기 프로세서는,

동일한 송신자 및 수신자의 통신으로 구성된 패킷들로 이루어진 분석 대상 패킷 플로우(packet flow) 데이터를 획득하고,

미리 학습되어 구축된 인공지능 분류 모델과 설명가능한 인공지능(XAI) 기술을 이용하여, 상기 분석 대상 패킷 플로우 데이터의 중요 인자를 추출하며,

군집화 모델을 이용하여, 상기 분석 대상 패킷 플로우 데이터의 중요 인자를 기반으로 상기 분석 대상 패킷 플로우 데이터에 대응되는 군집을 획득하여 상기 분석 대상 패킷 플로우 데이터에 대응되는 공격 원인 정보를 획득

특하고,

상기 인공지능 분류 모델은, 패킷 플로우 데이터를 입력으로 하고, 입력된 패킷 플로우 데이터가 정상인지 악성인지 여부를 나타내는 값 및 입력된 패킷 플로우 데이터에 대응되는 설명 맵(saliency map)을 출력으로 하며,

상기 군집화 모델은, 패킷 플로우 데이터를 입력으로 하고, 입력된 패킷 플로우 데이터가 속하는 군집을 출력으로 하고,

상기 프로세서는, 상기 분석 대상 패킷 플로우 데이터를 상기 인공지능 분류 모델에 입력하고, 상기 설명가능한 인공지능(XAI) 기술을 활용하여 도출한 설명 맵을 기반으로 상기 분석 대상 패킷 플로우 데이터의 중요 인자를 추출하며,

상기 프로세서는, 상기 분석 대상 패킷 플로우 데이터의 중요 인자를 기반으로 상기 분석 대상 패킷 플로우 데이터에서 중요 인자에 대한 값을 유지하고 중요 인자가 아닌 부분에 대한 값은 미리 설정된 대체값으로 교체하고, 대체값으로 교체된 상기 분석 대상 패킷 플로우 데이터를 상기 군집화 모델에 입력하고, 상기 군집화 모델의 출력인 군집을 상기 분석 대상 패킷 플로우 데이터에 대응되는 군집으로 획득하며, 상기 분석 대상 패킷 플로우 데이터에 대응되는 군집의 공격 원인을 상기 분석 대상 패킷 플로우 데이터에 대응되는 공격 원인 정보로 획득하는,

설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 장치.

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

발명의 설명

기술 분야

[0001] 본 발명은 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 방법, 이를 수행하는 장치 및 컴퓨터 프로그램에 관한 것으로서, 더욱 상세하게는 네트워크 패킷 공격의 원인을 분석하는, 방법, 장치 및 컴퓨터 프로그램에 관한 것이다. 본 연구는 2021년 5월 1일 ~ 2022년 4월 30일에 LIG넥스원의 주관으로 수행된 XAI 기반 사이버 공격 원인 분석 기술(과제고유번호 : LIGNEX1-2021-0414(00) / 수행부서 : C4I연구소 사이버전연구팀)과 관련된다.

배경 기술

[0002] 한국공개특허 제10-2018-0042019호는 심층 신경망의 한 종류인 순환 신경망을 활용하여 패킷의 임베딩을 학습하고, 이를 활용해 다음 패킷의 특성을 예측하여, 예측한 패킷의 특성과 제2 입력 패킷 특성 간의 유사도를 기초로 위험 여부를 판단하는 제1 위험 요소 결정부와 가상 머신으로 실제 패킷의 위험 여부를 판단하는 제2 위험 요소 결정부로 구성된 패킷 위험 요소 분석 장치와 방법을 제안하고 있다.

[0003] 그리고, 한국공개특허 제10-2020-0068608호는 주성분 분석을 기반으로 하여 패킷에서 대표 특징 필드들을 결정하고, 이에 기초하여 복수 패킷 데이터들에 대해 DBSCAN 군집화 알고리즘 수행하여, 네트워크 공격을 탐지하는 방법을 제안하고 있다.

[0004] 그리고, 한국등록특허 제 10-2247179호는 수집된 데이터 일부를 활용한 정상 및 비정상 데이터를 이용해 이상 행위 탐지를 위한 지도 학습 모델을 생성하고, 설명가능한 인공지능(explainable artificial intelligence, XAI) 기술을 활용하여 지도 학습 모델을 사용해 이상 기준 수치 범위를 설정해 수집된 데이터셋의 정상 데이터셋 라벨을 형성하는 기술을 제안하고 있다.

[0005] 그러나, 종래 기술 중 공격 원인을 분석하는 방식에는 규칙 기반 분석 방식(한국공개특허 제10-2019-0049322

호)이나 하나 이상의 대표 특징 필드를 직접 추출하는 방식(한국공개특허 제10-2020-0068608호]을 사용하고 있다. 이는 규칙에 지정되어 있지 않은 공격에는 대응할 수 없으며, 특징 필드를 직접 추출하는 데에 사용자의 개입이 필요하다는 한계가 있다. 데이터 자체를 군집화하여 유사도 비교를 통해 네트워크 공격의 원인을 분석하는 방법은 종래에 제안되지 않았으며 본래 데이터를 그대로 사용하기에는 성능이 낮아 활용에 다소 어려움이 있는 현황이다.

발명의 내용

해결하려는 과제

[0006] 본 발명이 이루고자 하는 목적은, 설명가능한 인공지능(explainable artificial intelligence, XAI)을 이용하여 네트워크 패킷 공격의 원인을 분석하는, 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 방법, 이를 수행하는 장치 및 컴퓨터 프로그램을 제공하는 데 있다.

[0007] 본 발명의 명시되지 않은 또 다른 목적들은 하기의 상세한 설명 및 그 효과로부터 용이하게 추론할 수 있는 범위 내에서 추가적으로 고려될 수 있다.

과제의 해결 수단

[0008] 상기의 기술적 과제를 달성하기 위한 본 발명의 바람직한 실시예에 따른 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 방법은, 동일한 송신자 및 수신자의 통신으로 구성된 패킷들로 이루어진 분석 대상 패킷 플로우(packet flow) 데이터를 획득하는 단계; 미리 학습되어 구축된 인공지능 분류 모델과 설명가능한 인공지능(explainable artificial intelligence, XAI) 기술을 이용하여, 상기 분석 대상 패킷 플로우 데이터의 중요 인자를 추출하는 단계; 및 군집화 모델을 이용하여, 상기 분석 대상 패킷 플로우 데이터의 중요 인자를 기반으로 상기 분석 대상 패킷 플로우 데이터에 대응되는 군집을 획득하여 상기 분석 대상 패킷 플로우 데이터에 대응되는 공격 원인 정보를 획득하는 단계;를 포함한다.

[0009] 여기서, 상기 인공지능 분류 모델은, 패킷 플로우 데이터를 입력으로 하고, 입력된 패킷 플로우 데이터가 정상인지 악성인지 여부를 나타내는 값 및 입력된 패킷 플로우 데이터에 대응되는 설명 맵(saliency map)을 출력으로 하며, 상기 군집화 모델은, 패킷 플로우 데이터를 입력으로 하고, 입력된 패킷 플로우 데이터가 속하는 군집을 출력으로 할 수 있다.

[0010] 여기서, 상기 중요 인자 추출 단계는, 상기 분석 대상 패킷 플로우 데이터를 상기 인공지능 분류 모델에 입력하고, 상기 설명가능한 인공지능(XAI) 기술을 활용하여 도출한 설명 맵을 기반으로 상기 분석 대상 패킷 플로우 데이터의 중요 인자를 추출하는 것으로 이루어질 수 있다.

[0011] 여기서, 상기 공격 원인 정보 획득 단계는, 상기 분석 대상 패킷 플로우 데이터의 중요 인자를 기반으로 상기 분석 대상 패킷 플로우 데이터에서 중요 인자에 대한 값을 유지하고 중요 인자가 아닌 부분에 대한 값은 미리 설정된 대체값으로 교체하고, 대체값으로 교체된 상기 분석 대상 패킷 플로우 데이터를 상기 군집화 모델에 입력하고, 상기 군집화 모델의 출력인 군집을 상기 분석 대상 패킷 플로우 데이터에 대응되는 군집으로 획득하며, 상기 분석 대상 패킷 플로우 데이터에 대응되는 군집의 공격 원인을 상기 분석 대상 패킷 플로우 데이터에 대응되는 공격 원인 정보로 획득하는 것으로 이루어질 수 있다.

[0012] 여기서, 학습 데이터 세트를 기반으로, 상기 인공지능 분류 모델 및 상기 군집화 모델을 학습하는 단계;를 더 포함하며, 상기 학습 데이터 세트는, 동일한 송신자 및 수신자의 통신으로 구성된 패킷들로 이루어진 패킷 플로우 학습 데이터, 상기 패킷 플로우 학습 데이터가 정상인지 악성인지 여부를 나타내는 제1 정답 레이블(label) 및 상기 패킷 플로우 학습 데이터에 대응되는 군집을 나타내는 제2 정답 레이블을 포함할 수 있다.

[0013] 여기서, 상기 학습 단계는, 패킷 내의 미리 설정된 대체 대상 정보의 값을 미리 설정된 대체값으로 교체하고, 상기 인공지능 분류 모델의 입력 데이터 정보를 기반으로 패킷의 크기를 조정하여, 상기 패킷 플로우 학습 데이터를 전처리하는 단계; 전처리한 상기 패킷 플로우 학습 데이터 및 상기 제1 정답 레이블을 이용하여, 상기 인공지능 분류 모델을 학습하는 단계; 전처리한 상기 패킷 플로우 학습 데이터를 상기 인공지능 분류 모델에 입력하고, 상기 설명가능한 인공지능(XAI) 기술을 활용하여 도출한 설명 맵을 기반으로 전처리한 상기 패킷 플로우 학습 데이터의 중요 인자를 추출하는 단계; 및 전처리한 상기 패킷 플로우 학습 데이터의 중요 인자를 이용하여, 상기 군집화 모델을 학습하는 단계;를 포함할 수 있다.

[0014] 여기서, 상기 군집화 모델 학습 단계는, 전처리한 상기 패킷 플로우 학습 데이터의 중요 인자를 기반으로 상기

패킷 플로우 학습 데이터에서 중요 인자에 대한 값은 유지하고 중요 인자가 아닌 부분에 대한 값은 미리 설정된 대체값으로 교체하고, 대체값으로 교체된 상기 패킷 플로우 학습 데이터 및 상기 제2 정답 레이블을 이용하여, 상기 군집화 모델을 학습하는 것으로 이루어질 수 있다.

[0016] 상기의 기술적 과제를 달성하기 위한 본 발명의 바람직한 실시예에 따른 컴퓨터 프로그램은 컴퓨터 판독 가능한 저장 매체에 저장되어 상기한 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 방법 중 어느 하나를 컴퓨터에서 실행시킨다.

[0018] 상기의 기술적 과제를 달성하기 위한 본 발명의 바람직한 실시예에 따른 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 장치는, 설명가능한 인공지능(explainable artificial intelligence, XAI) 기술을 이용하여 네트워크 패킷 공격의 원인을 분석하는 공격 원인 분석 장치로서, 설명가능한 인공지능(XAI) 기술을 이용하여 네트워크 패킷 공격의 원인을 분석하기 위한 하나 이상의 프로그램을 저장하는 메모리; 및 상기 메모리에 저장된 상기 하나 이상의 프로그램에 따라 설명가능한 인공지능(XAI) 기술을 이용하여 네트워크 패킷 공격의 원인을 분석하기 위한 동작을 수행하는 하나 이상의 프로세서;를 포함하며, 상기 프로세서는, 동일한 송신자 및 수신자의 통신으로 구성된 패킷들로 이루어진 분석 대상 패킷 플로우(packet flow) 데이터를 획득하고, 미리 학습되어 구축된 인공지능 분류 모델과 설명가능한 인공지능(XAI) 기술을 이용하여, 상기 분석 대상 패킷 플로우 데이터의 중요 인자를 추출하며, 군집화 모델을 이용하여, 상기 분석 대상 패킷 플로우 데이터의 중요 인자를 기반으로 상기 분석 대상 패킷 플로우 데이터에 대응되는 군집을 획득하여 상기 분석 대상 패킷 플로우 데이터에 대응되는 공격 원인 정보를 획득한다.

[0019] 여기서, 상기 인공지능 분류 모델은, 패킷 플로우 데이터를 입력으로 하고, 입력된 패킷 플로우 데이터가 정상인지 악성인지 여부를 나타내는 값 및 입력된 패킷 플로우 데이터에 대응되는 설명 맵(saliency map)을 출력으로 하며, 상기 군집화 모델은, 패킷 플로우 데이터를 입력으로 하고, 입력된 패킷 플로우 데이터가 속하는 군집을 출력으로 할 수 있다.

[0020] 여기서, 상기 프로세서는, 상기 분석 대상 패킷 플로우 데이터를 상기 인공지능 분류 모델에 입력하고, 상기 설명가능한 인공지능(XAI) 기술을 활용하여 도출한 설명 맵을 기반으로 상기 분석 대상 패킷 플로우 데이터의 중요 인자를 추출할 수 있다.

[0021] 여기서, 상기 프로세서는, 상기 분석 대상 패킷 플로우 데이터의 중요 인자를 기반으로 상기 분석 대상 패킷 플로우 데이터에서 중요 인자에 대한 값을 유지하고 중요 인자가 아닌 부분에 대한 값은 미리 설정된 대체값으로 교체하고, 대체값으로 교체된 상기 분석 대상 패킷 플로우 데이터를 상기 군집화 모델에 입력하고, 상기 군집화 모델의 출력인 군집을 상기 분석 대상 패킷 플로우 데이터에 대응되는 군집으로 획득하며, 상기 분석 대상 패킷 플로우 데이터에 대응되는 군집의 공격 원인을 상기 분석 대상 패킷 플로우 데이터에 대응되는 공격 원인 정보로 획득할 수 있다.

발명의 효과

[0022] 본 발명의 바람직한 실시예에 따른 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 방법, 이를 수행하는 장치 및 컴퓨터 프로그램에 의하면, 설명가능한 인공지능(explainable artificial intelligence, XAI)을 이용하여 네트워크 패킷 공격의 원인을 분석함으로써, 군집 분류 성능을 향상시킬 수 있어 보다 정확한 공격 원인의 분석이 가능하다.

[0023] 본 발명의 효과들은 이상에서 언급한 효과들로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0024] 도 1은 본 발명의 바람직한 실시예에 따른 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 장치를 설명하기 위한 블록도이다.

도 2는 본 발명의 바람직한 실시예에 따른 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 방법을 설명하기 위한 흐름도이다.

도 3은 본 발명의 바람직한 실시예에 따른 학습 데이터 세트를 설명하기 위한 도면이다.

도 4는 본 발명의 바람직한 실시예에 따른 인공지능 분류 모델에 설명가능한 인공지능(XAI) 기술의 적용 과정을

설명하기 위한 도면이다.

도 5는 본 발명의 바람직한 실시예에 따른 군집화 모델의 학습 과정을 설명하기 위한 도면이다.

도 6은 본 발명의 바람직한 실시예에 따른 공격 원인 정보의 획득 과정을 설명하기 위한 도면이다.

도 7은 본 발명의 바람직한 실시예에 따른 공격 원인 정보의 분석 일례를 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0025] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 상세히 설명한다. 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나, 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.
- [0026] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또한, 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.
- [0027] 본 명세서에서 "제1", "제2" 등의 용어는 하나의 구성 요소를 다른 구성 요소로부터 구별하기 위한 것으로, 이들 용어들에 의해 권리범위가 한정되어서는 아니 된다. 예컨대, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고, 유사하게 제2 구성 요소도 제1 구성 요소로 명명될 수 있다.
- [0028] 본 명세서에서 각 단계들에 있어 식별부호(예컨대, a, b, c 등)는 설명의 편의를 위하여 사용되는 것으로 식별 부호는 각 단계들의 순서를 설명하는 것이 아니며, 각 단계들은 문맥상 명백하게 특정 순서를 기재하지 않는 이상 명기된 순서와 다르게 일어날 수 있다. 즉, 각 단계들은 명기된 순서와 동일하게 일어날 수도 있고 실질적으로 동시에 수행될 수도 있으며 반대의 순서대로 수행될 수도 있다.
- [0029] 본 명세서에서, "가진다", "가질 수 있다", "포함한다" 또는 "포함할 수 있다" 등의 표현은 해당 특징(예컨대, 수치, 기능, 동작, 또는 부품 등의 구성 요소)의 존재를 가리키며, 추가적인 특징의 존재를 배제하지 않는다.
- [0032] 이하에서 첨부한 도면을 참조하여 본 발명에 따른 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 방법, 이를 수행하는 장치 및 컴퓨터 프로그램의 바람직한 실시예에 대해 상세하게 설명한다.
- [0034] 먼저, 도 1을 참조하여 본 발명의 바람직한 실시예에 따른 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 장치에 대하여 설명한다.
- [0035] 도 1은 본 발명의 바람직한 실시예에 따른 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 장치를 설명하기 위한 블록도이다.
- [0036] 도 1을 참조하면, 본 발명의 바람직한 실시예에 따른 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 장치(이하 '공격 원인 분석 장치'라 한다)(100)는 설명가능한 인공지능(explainable artificial intelligence, XAI) 기술을 이용하여 네트워크 패킷 공격의 원인을 분석할 수 있다.
- [0037] 즉, 본 발명은 설명가능한 인공지능(XAI) 기술을 활용한 네트워크 패킷 플로우 데이터의 중요 인자 추출을 제안하고 이를 활용한 분석 방법을 제안한다. 인공지능 분류 모델이 중요하다고 판단한 인자를 기준으로 원인 분석을 수행하며, 이를 통해 사용자의 개입이나 등록되지 않은 규칙 등에 제약받지 않는 공격 원인 분석 기술을 제공할 수 있다.
- [0038] 보다 자세히 설명하면, 설명가능한 인공지능(XAI) 기술을 활용한 네트워크 패킷 공격 원인 분석 기술은 네트워크 공격 유형에 따라 각 공격 유형별 패킷 플로우(packet flow) 데이터들이 어떤 공통된 특성을 보이는지를 분석해 그룹화하는데, 효과적인 분석을 위해서는 패킷 플로우 데이터들의 공격에 대한 유사성을 잘 표현할 수 있는 기술이 필요하다. 여기서, 데이터 간 유사성을 확인하기 위해 군집화 알고리즘을 사용하는데, 일반적인 네트워크 패킷 플로우 데이터들을 기준으로 군집화를 수행할 시 유형과 관계없이 한 군집에 여러 유형의 데이터가 섞여 공격 원인을 분석하기 어렵다는 문제점이 있다.
- [0039] 이처럼 효과적인 공격 원인 분석을 위해 동일 유형의 공격을 이루는 패킷 플로우 데이터들끼리 군집이 되도록

하는 공격 원인 분석 기술이 필요한 상황이다. 본 발명에서는 악성 패킷과 정상 패킷을 탐지하는 인공지능 분류 모델 및 설명가능한 인공지능(XAI) 기술을 활용해 패킷 플로우 데이터 내 중요 인자를 추출한다. 나아가, 본 발명은 추출된 중요 인자를 기반으로 군집화를 수행했을 때 일반 데이터를 기준으로 군집화를 수행했을 때보다 더 나은 공격 유형별 군집화 성능을 보이는 기술을 제안한다. 이에 따라, 본 발명은 악성 패킷과 정상 패킷의 분류 원인 분석 및 악성 패킷의 공격 유형별 원인 분석 등 설명가능한 인공지능(XAI) 기법을 통한 중요 인자 추출 기술을 필요한 기술의 기반 기술로 사용될 수 있다.

- [0040] 또한, 본 발명은 설명가능한 인공지능(XAI) 기술을 이용하여 네트워크 패킷 공격의 원인을 분석함으로써, 군집 분류 성능을 향상시킬 수 있어 보다 정확한 공격 원인의 분석이 가능하다.
- [0041] 즉, 본 발명에서 제안하는 설명가능한 인공지능(XAI) 기술로 도출된 새로운 패킷 데이터는 기존 패킷 데이터에 남아 있는 불필요한 정보가 제거되고, 인공지능 모델의 의사결정에 중요한 영향을 미치는 인자만 남아 있는 상태이다. 따라서, 공격 유형별 패킷의 공통된 특성을 보기에 더 적합하며, 동일 유형에서의 데이터들 사이의 유사성을 높일 수 있으므로, 일반 패킷 데이터를 통해 군집화를 수행한 결과와 비교했을 때 더 높은 군집 정확도를 보인다.
- [0042] 모든 데이터가 포함된 일반적인 네트워크 패킷의 경우, 중요 인자가 포함되어 있으나 인공지능 모델의 의사결정과 관계없는(혹은 부정적인 영향을 미치는) 입력값도 포함되어 있다. 따라서, 임의의 공간에 데이터들을 배치했을 때 같은 공격 유형의 데이터일지라도 산점도가 높으며 다른 공격 유형 집단에 섞여 있어 공격 원인을 분석하기가 어렵다. 반면, 본 발명에서 제안하는 기술을 사용한다면, 설명가능한 인공지능(XAI) 기술에 기반해 모델의 의사결정에 영향을 미친 중요 인자들만 남긴 후 나머지 데이터들에 대한 영향력은 제거되므로 공격 원인 분석에 더 용이하다.
- [0043] 위와 같은 이유로 본 발명에서 제안하는 설명가능한 인공지능(XAI) 기술에 기반한 네트워크 패킷 데이터의 중요 인자 도출 기술을 활용할 때 공격 원인 분석을 위한 유사도 군집 분석을 용이하게 한다. 또한, 본 발명에서 제안하는 설명가능한 인공지능(XAI) 기술에 기반한 패킷 데이터 중요 인자 도출 기술은 실제로 사용하는 인공지능 모델이 합리적인 근거에 기반하여 의사결정을 내리고 있는지 점검할 수 있는 효과가 있다.
- [0045] 이를 위해, 공격 원인 분석 장치(100)는 하나 이상의 프로세서(110), 컴퓨터 판독 가능한 저장 매체(130) 및 통신 버스(150)를 포함할 수 있다.
- [0046] 프로세서(110)는 공격 원인 분석 장치(100)가 동작하도록 제어할 수 있다. 예컨대, 프로세서(110)는 컴퓨터 판독 가능한 저장 매체(130)에 저장된 하나 이상의 프로그램(131)을 실행할 수 있다. 하나 이상의 프로그램(131)은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 컴퓨터 실행 가능 명령어는 프로세서(110)에 의해 실행되는 경우 공격 원인 분석 장치(100)로 하여금 설명가능한 인공지능(XAI) 기술을 이용하여 네트워크 패킷 공격의 원인을 분석하기 위한 동작을 수행하도록 구성될 수 있다.
- [0047] 컴퓨터 판독 가능한 저장 매체(130)는 설명가능한 인공지능(XAI) 기술을 이용하여 네트워크 패킷 공격의 원인을 분석하기 위한 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능한 저장 매체(130)에 저장된 프로그램(131)은 프로세서(110)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능한 저장 매체(130)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 디바이스들, 광학 디스크 저장 디바이스들, 플래시 메모리 디바이스들, 그 밖에 공격 원인 분석 장치(100)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적절한 조합일 수 있다.
- [0048] 통신 버스(150)는 프로세서(110), 컴퓨터 판독 가능한 저장 매체(130)를 포함하여 공격 원인 분석 장치(100)의 다른 다양한 컴포넌트들을 상호 연결한다.
- [0049] 공격 원인 분석 장치(100)는 또한 하나 이상의 입출력 장치를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(170) 및 하나 이상의 통신 인터페이스(190)를 포함할 수 있다. 입출력 인터페이스(170) 및 통신 인터페이스(190)는 통신 버스(150)에 연결된다. 입출력 장치(도시하지 않음)는 입출력 인터페이스(170)를 통해 공격 원인 분석 장치(100)의 다른 컴포넌트들에 연결될 수 있다.
- [0052] 그러면, 도 2 내지 도 7을 참조하여 본 발명의 바람직한 실시예에 따른 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 방법에 대하여 설명한다.

- [0053] 도 2는 본 발명의 바람직한 실시예에 따른 설명가능한 인공지능을 이용한 네트워크 패킷 공격의 원인 분석 방법을 설명하기 위한 흐름도이고, 도 3은 본 발명의 바람직한 실시예에 따른 학습 데이터 세트를 설명하기 위한 도면이며, 도 4는 본 발명의 바람직한 실시예에 따른 인공지능 분류 모델에 설명가능한 인공지능(XAI) 기술의 적용 과정을 설명하기 위한 도면이고, 도 5는 본 발명의 바람직한 실시예에 따른 군집화 모델의 학습 과정을 설명하기 위한 도면이며, 도 6은 본 발명의 바람직한 실시예에 따른 공격 원인 정보의 획득 과정을 설명하기 위한 도면이고, 도 7은 본 발명의 바람직한 실시예에 따른 공격 원인 정보의 분석 일례를 설명하기 위한 도면이다.
- [0054] 도 2를 참조하면, 공격 원인 분석 장치(100)의 프로세서(110)는 학습 데이터 세트를 기반으로, 인공지능 분류 모델 및 군집화 모델을 학습할 수 있다(S110).
- [0055] 여기서, 인공지능 분류 모델은 패킷 플로우 데이터를 입력으로 하고, 입력된 패킷 플로우 데이터가 정상인지 악성인지 여부를 나타내는 값 및 입력된 패킷 플로우 데이터에 대응되는 설명 맵(saliency map)을 출력으로 할 수 있다. 설명 맵은 입력된 패킷 플로우 데이터의 어떤 지점이 인공지능 분류 모델의 의사결정에 얼마나 영향을 미쳤는지에 대한 정보를 말한다. 즉, 본 발명에 따른 인공지능 분류 모델에 설명가능한 인공지능(XAI) 기술을 적용해 입력 데이터에 대한 설명 맵을 제공받을 수 있는 형태라면 인공지능 분류 모델은 인공지능 구조에 무관하게 사용될 수 있다. 예컨대, 설명가능한 인공지능(XAI) 기술은 임베딩 벡터, 민감도 정보 등과 같은 설명 맵을 출력할 수 있다. 임베딩 벡터는 범주형 데이터 또는 수치형 데이터 등을 잘 표현할 수 있는 저차원의 연속형 벡터(특징)를 의미할 수 있다. 민감도 정보는 모델의 입력으로 들어온 데이터의 각 부분이 결과 값 출력에 얼마나 영향을 미쳤는지에 대한 정보를 의미할 수 있다.
- [0056] 그리고, 패킷 플로우 데이터는 동일한 송신자 및 수신자의 통신으로 구성된 패킷들로 이루어질 수 있다.
- [0057] 그리고, 군집화 모델은 패킷 플로우 데이터를 입력으로 하고, 입력된 패킷 플로우 데이터가 속하는 군집을 출력으로 할 수 있다.
- [0058] 그리고, 학습 데이터 세트는 도 3에 도시된 바와 같이, 동일한 송신자 및 수신자의 통신으로 구성된 패킷들로 이루어진 패킷 플로우 학습 데이터(PFD-L), 패킷 플로우 학습 데이터(PFD-L)가 정상인지 악성인지 여부를 나타내는 제1 정답 레이블(label)(PFD-L-T1) 및 패킷 플로우 학습 데이터(PFD-L)에 대응되는 군집을 나타내는 제2 정답 레이블(PFD-L-T2)을 포함할 수 있다. 즉, 네트워크를 통해 송신 패킷과 수집 패킷을 수집하고, 수집한 패킷들의 헤더 필드에 있는 정보인 송신 정보(송신 IP주소, 송신 MAC 주소 등)와 수신 정보(수신 IP주소, 수신 MAC 주소 등)를 이용하여 패킷 플로우 학습 데이터(PFD-L)들을 획득할 수 있다. 이때, 수집한 패킷들의 헤더 필드를 확인하여 수집한 패킷들을 TCP 패킷들과 UDP 패킷들로 1차 분류를 수행하고, 1차 분류된 TCP 패킷들과 UDP 패킷들의 송신 정보와 수신 정보를 이용하여 패킷 플로우 학습 데이터(PFD-L)들을 획득할 수 있다. 그리고, 획득한 패킷 플로우 학습 데이터(PFD-L)가 정상 패킷인지 악성 패킷인지를 나타내는 제1 정답 레이블(PFD-L-T1)을 획득할 수 있다. 그리고, 획득한 패킷 플로우 학습 데이터(PFD-L)에 대응되는 공격 원인을 통해 해당 패킷 플로우 학습 데이터(PFD-L)가 속하는 군집을 나타내는 제2 정답 레이블(PFD-L-T2)을 획득할 수 있다. 이때, 공격 원인의 유형별로 서로 다른 군집에 소속되도록 하기 위해, 공격 원인 유형이 상이한 패킷 플로우 학습 데이터(PFD-L)들은 동일한 제2 정답 레이블(PFD-L-T2)을 가지며, 공격 원인 유형이 상이한 패킷 플로우 학습 데이터(PFD-L)들은 상이한 제2 정답 레이블(PFD-L-T2)을 가지게 된다.
- [0059] 보다 자세히 설명하면, 프로세서(110)는 도 4에 도시된 바와 같이, 패킷 플로우 학습 데이터(PFD-L)를 전처리하여, 전처리한 패킷 플로우 학습 데이터(PFD-L-P)를 획득할 수 있다. 즉, 프로세서(110)는 인공지능 분류 모델(132)의 과적합을 방지하기 위해 패킷 내의 미리 설정된 대체 대상 정보의 값을 미리 설정된 대체값으로 교체하고, 인공지능 분류 모델(132)의 입력 데이터 정보를 기반으로 패킷의 크기를 조정하여, 패킷 플로우 학습 데이터(PFD-L)를 전처리할 수 있다. 여기서, 과적합이란 인공지능 분류 모델(132)이 통상적인 데이터 상황을 고려하지 않고 학습 데이터 상황에 과하게 적합하도록 학습되어 실제 데이터에 대해 검증 성능이 떨어지는 것을 의미한다. 그리고, 대체 대상 정보는 인공지능 분류 모델(132)의 학습에 있어 편향성을 줄 수 있는 값으로, 송신 IP 주소, 송신 포트 번호, 수신 IP 주소, 수신 포트 번호 및 MAC 주소를 포함할 수 있다. 그리고, 대체값은 무작위로 부여된 임의의 값(random value)일 수 있다. 그리고, 인공지능 분류 모델의 입력 데이터 정보는 인공지능 분류 모델에 입력되는 값의 크기 등과 같이 입력 데이터 형상에 대해 미리 설정된 정보를 말한다.
- [0060] 그런 다음, 프로세서(110)는 도 4에 도시된 바와 같이, 인공지능 분류 모델(132)을 학습할 수 있다. 즉, 프로세서(110)는 전처리한 패킷 플로우 학습 데이터(PFD-L-P) 및 전처리한 패킷 플로우 학습 데이터(PFD-L-P)에 대응되는 제1 정답 레이블(PFD-L-T1)을 이용하여, 인공지능 분류 모델(132)을 학습할 수 있다.

- [0061] 그런 다음, 프로세서(110)는 도 5에 도시된 바와 같이, 학습되어 구축된 인공지능 분류 모델(132) 및 설명가능한 인공지능(XAI) 기술을 이용하여, 전처리한 패킷 플로우 학습 데이터(PFD-L-P)의 중요 인자를 추출할 수 있다. 즉, 프로세서(110)는 전처리한 패킷 플로우 학습 데이터(PFD-L-P)를 인공지능 분류 모델(132)에 입력하고, 설명가능한 인공지능(XAI) 기술을 활용하여 도출한 설명 맵을 기반으로 전처리한 패킷 플로우 학습 데이터(PFD-L-P)의 중요 인자를 추출할 수 있다.
- [0062] 그런 다음, 프로세서(110)는 도 5에 도시된 바와 같이, 군집화 모델(133)을 학습할 수 있다. 즉, 프로세서(110)는 전처리한 패킷 플로우 학습 데이터(PFD-L-P)의 중요 인자 및 전처리한 패킷 플로우 학습 데이터(PFD-L-P)에 대응되는 제2 정답 레이블(PFD-L-T2)을 이용하여, 군집화 모델(133)을 학습할 수 있다. 이때, 프로세서(110)는 전처리한 패킷 플로우 학습 데이터(PFD-L-P)의 중요 인자를 기반으로 패킷 플로우 학습 데이터(PFD-L-P)에서 중요 인자에 대한 값은 유지하고 중요 인자가 아닌 부분에 대한 값은 미리 설정된 대체값으로 교체하고, 대체값으로 교체된 패킷 플로우 학습 데이터(PFD-L-R) 및 제2 정답 레이블(PFD-L-T2)을 이용하여, 군집화 모델(133)을 학습할 수 있다. 여기서, 대체값은 군집화에 영향을 미치지 않을 정도의 값을 나타낼 수 있다. 예컨대, 군집화의 대상이 되는 입력 데이터들의 각 위치별 평균값을 대체값으로 사용할 수 있고, 물론 중요 인자들을 기반으로 군집화를 진행할 때 영향을 미치지 않는 값이라면 다른 값을 대체값으로 사용할 수도 있다. 이와 같은 유사도 군집 분석은 입력 데이터 간의 유사도를 측정하여 유사한 데이터들을 하나의 군집으로 묶는 역할을 수행할 수 있다. 예컨대, 유사도 군집 기술에는 다양한 종류가 있지만, 대표적으로 k-평균 유사도 군집 알고리즘의 예시의 유사도는 임베딩 간 유클리디안 거리를 의미하고, 유사하다는 것은 입력 데이터 간의 유클리디안 거리가 가깝다는 것을 의미한다. 따라서, 이러한 유사도 군집 분석으로 획득된 군집은 비슷한 공격 특성, 흐름을 가지는 복수의 패킷 플로우 데이터로 구성되게 된다.
- [0064] 이후, 프로세서(110)는 분석 대상 패킷 플로우 데이터를 획득할 수 있다(S120).
- [0065] 여기서, 분석 대상 패킷 플로우 데이터는 공격 원인을 분석하고자 하는 임의 패킷 플로우 데이터로서, 동일한 송신자 및 수신자의 통신으로 구성된 패킷들로 이루어질 수 있다. 예컨대, 분석 대상 패킷 플로우 데이터는 송신 정보(송신 IP 주소와 송신 MAC 주소)와 수신 정보(수신 IP 주소와 수신 MAC 주소)가 동일한 패킷들로 이루어질 수 있다.
- [0067] 그런 다음, 프로세서(110)는 미리 학습되어 구축된 인공지능 분류 모델 및 설명가능한 인공지능(XAI) 기술을 이용하여, 분석 대상 패킷 플로우 데이터의 중요 인자를 추출할 수 있다(S130).
- [0068] 보다 자세히 설명하면, 프로세서(110)는 도 6에 도시된 바와 같이, 인공지능 분류 모델(132) 및 설명가능한 인공지능(XAI) 기술을 이용하여 분석 대상 패킷 플로우 데이터(PFD-T)의 중요 인자를 추출할 수 있다. 즉, 프로세서(110)는 분석 대상 패킷 플로우 데이터(PFD-T)를 인공지능 분류 모델(132)에 입력하고, 설명가능한 인공지능(XAI) 기술을 활용하여 도출한 설명 맵을 기반으로 분석 대상 패킷 플로우 데이터(PFD-T)의 중요 인자를 추출할 수 있다.
- [0070] 그런 다음, 프로세서(110)는 군집화 모델을 이용하여, 분석 대상 패킷 플로우 데이터의 중요 인자를 기반으로 분석 대상 패킷 플로우 데이터에 대응되는 군집을 획득하여 분석 대상 패킷 플로우 데이터에 대응되는 공격 원인 정보를 획득할 수 있다(S140).
- [0071] 보다 자세히 설명하면, 프로세서(110)는 도 6에 도시된 바와 같이, 군집화 모델(133)을 이용하여, 분석 대상 패킷 플로우 데이터(PFD-T)의 중요 인자를 기반으로 분석 대상 패킷 플로우 데이터(PFD-T)에 대응되는 공격 원인 정보(PFD-T-AR)를 획득할 수 있다. 즉, 프로세서(110)는 분석 대상 패킷 플로우 데이터(PFD-T)의 중요 인자를 기반으로 분석 대상 패킷 플로우 데이터(PFD-T)에서 중요 인자에 대한 값을 유지하고 중요 인자가 아닌 부분에 대한 값은 미리 설정된 대체값으로 교체할 수 있다. 여기서, 대체값은 군집화에 영향을 미치지 않을 정도의 값을 나타낼 수 있다. 예컨대, 군집화의 대상이 되는 입력 데이터들의 각 위치별 평균값을 대체값으로 사용할 수 있고, 물론 중요 인자들을 기반으로 군집화를 진행할 때 영향을 미치지 않는 값이라면 다른 값을 대체값으로 사용할 수도 있다. 그리고, 프로세서(110)는 대체값으로 교체된 분석 대상 패킷 플로우 데이터(PFD-T-R)를 군집화 모델(133)에 입력하고, 군집화 모델(133)의 출력인 군집을 분석 대상 패킷 플로우 데이터(PFD-T)에 대응되는 군집으로 획득할 수 있다. 그리고, 프로세서(110)는 분석 대상 패킷 플로우 데이터(PFD-T)에 대응되는 군집의 공격 원인을 분석 대상 패킷 플로우 데이터(PFD-T)에 대응되는 공격 원인 정보로 획득할 수 있다. 예컨대, 분석 대상 패킷 플로우 데이터(PFD-T)에 대응되는 군집이 "group 1"이면, 군집 "group 1"의 공격 원인을 분석 대상 패킷 플로우 데이터(PFD-T)에 대응되는 공격 원인 정보로 획득할 수 있다.

[0074] 본 실시예들에 따른 동작은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능한 저장 매체에 기록될 수 있다. 컴퓨터 판독 가능한 저장 매체는 실행을 위해 프로세서에 명령어를 제공하는데 참여한 임의의 매체를 나타낸다. 컴퓨터 판독 가능한 저장 매체는 프로그램 명령, 데이터 파일, 데이터 구조 또는 이들의 조합을 포함할 수 있다. 예컨대, 자기 매체, 광기록 매체, 메모리 등이 있을 수 있다. 컴퓨터 프로그램은 네트워크로 연결된 컴퓨터 시스템 상에 분산되어 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수도 있다. 본 실시예를 구현하기 위한 기능적인(Functional) 프로그램, 코드, 및 코드 세그먼트들은 본 실시예가 속하는 기술 분야의 프로그래머들에 의해 용이하게 추론될 수 있을 것이다.

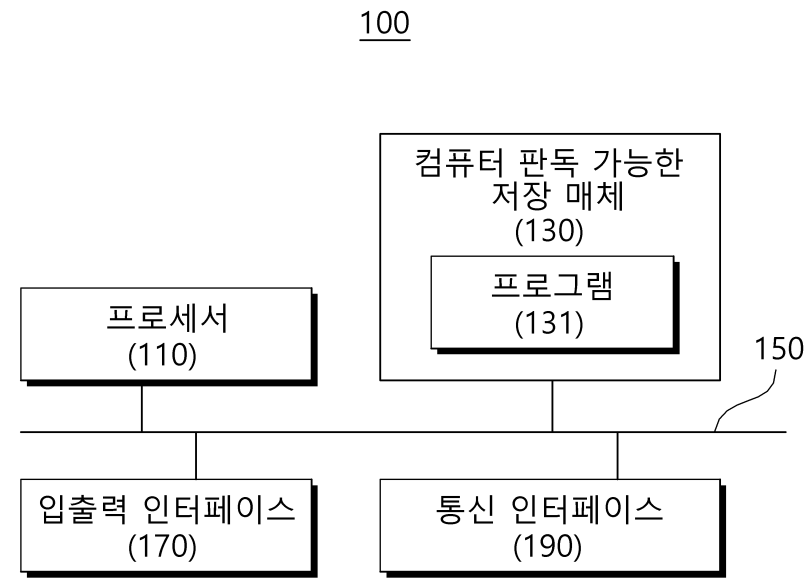
[0075] 본 실시예들은 본 실시예의 기술 사상을 설명하기 위한 것이고, 이러한 실시예에 의하여 본 실시예의 기술 사상의 범위가 한정되는 것은 아니다. 본 실시예의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 실시예의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

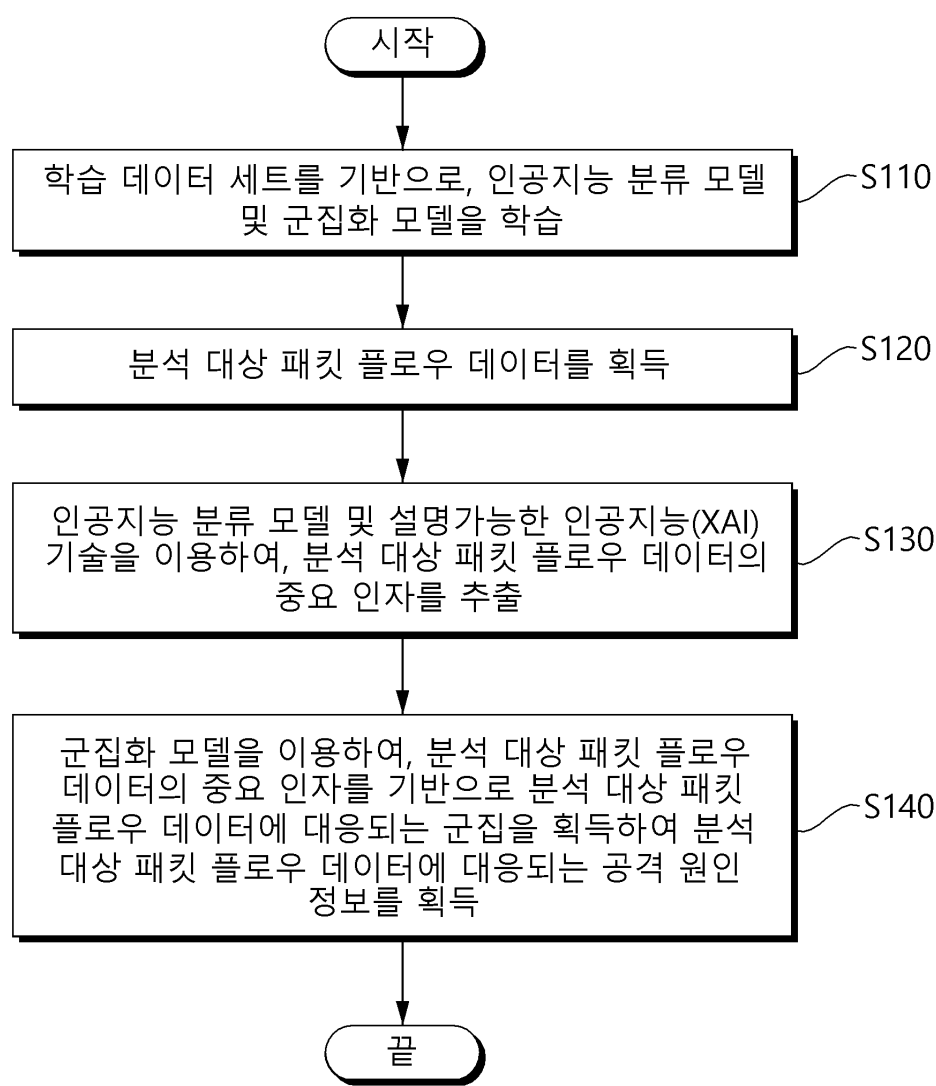
- [0076] 100 : 공격 원인 분석 장치,
110 : 프로세서,
130 : 컴퓨터 판독 가능한 저장 매체,
131 : 프로그램,
150 : 통신 버스,
170 : 입출력 인터페이스,
190 : 통신 인터페이스

도면

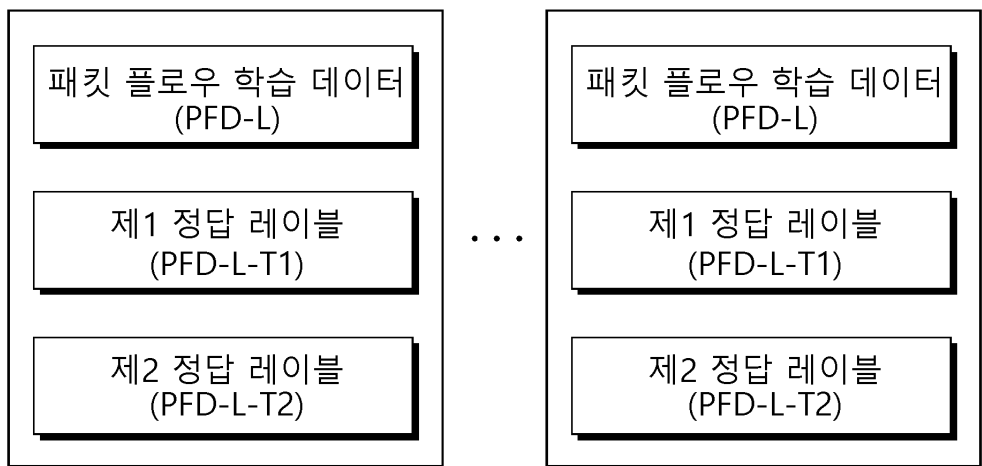
도면1



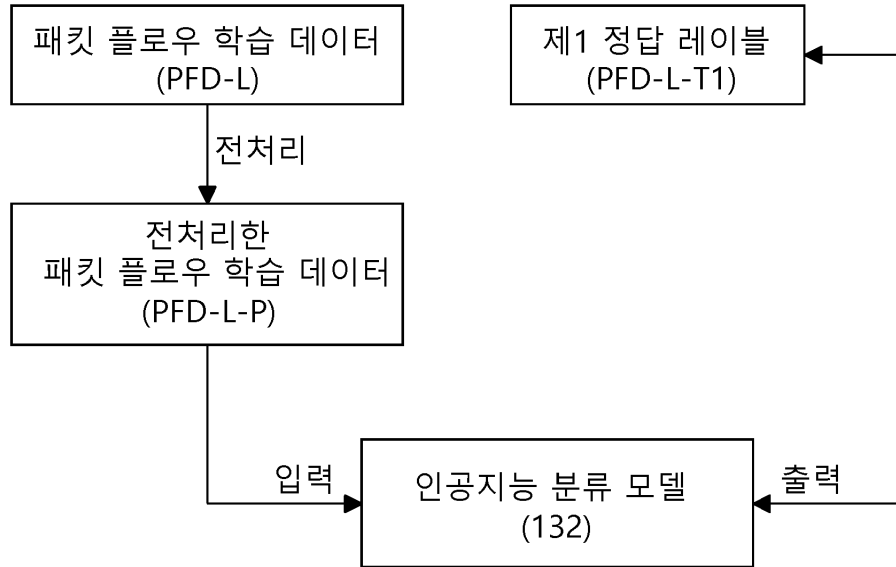
도면2



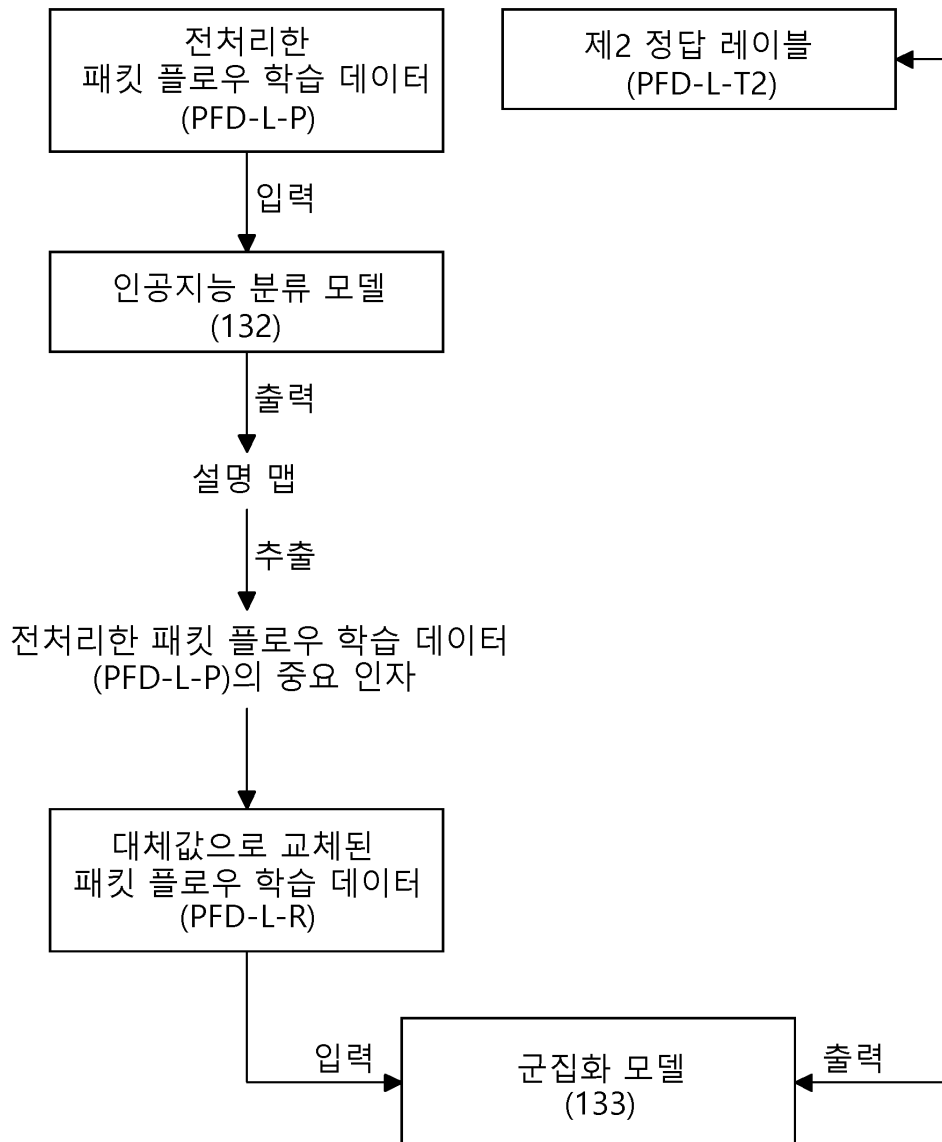
도면3



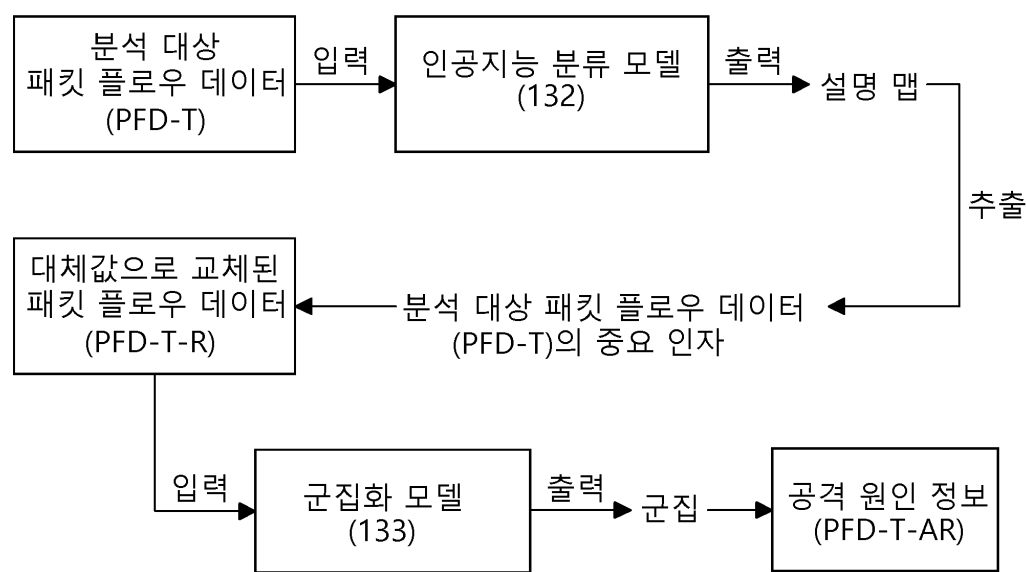
도면4



도면5



도면6



도면7

