



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0080974
(43) 공개일자 2023년06월07일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) G06N 3/08 (2023.01)
(52) CPC특허분류
H04L 63/1416 (2013.01)
G06N 3/08 (2023.01)
(21) 출원번호 10-2021-0168598
(22) 출원일자 2021년11월30일
심사청구일자 2021년11월30일

(71) 출원인
인하대학교 산학협력단
인천광역시 미추홀구 인하로 100(용현동, 인하대 학교)
(72) 발명자
이문규
인천광역시 연수구 컨벤시아대로42번길 95, 1005동 1403호(송도동, 더샵 엑스포)
권희용
인천광역시 연수구 원인재로 232, 103동 1305호(연수동, 솔밭마을아파트)
(74) 대리인
양성보

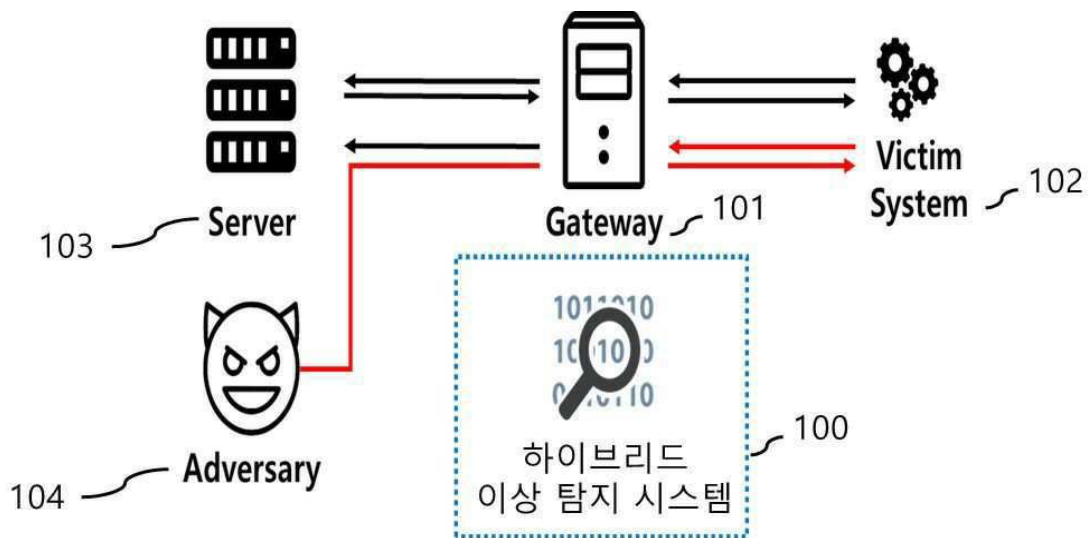
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 시그니처 기반 이상 탐지 방법과 행위 기반 이상 탐지 방법을 조합한 하이브리드 이상 탐지 방법

(57) 요약

시그니처 기반 이상 탐지 방법과 행위 기반 이상 탐지 방법을 조합한 하이브리드 이상 탐지 방법이 개시된다. 일 실시예에 따른 컴퓨터로 구현되는 하이브리드 이상 탐지 시스템에 의해 수행되는 하이브리드 이상 탐지 방법은, 동작 중인 시스템에서 생성된 데이터를 시그니처 기반의 이상 탐지 모델 및 행위 기반의 이상 탐지 모델로 구성된 하이브리드 이상 탐지 모델에 입력받는 단계; 상기 하이브리드 이상 탐지 모델을 이용하여 상기 동작 중인 시스템에서 생성된 데이터로부터 이상 탐지를 수행하는 단계; 및 상기 동작 중인 시스템에서 생성된 데이터와 상기 이상 탐지를 수행함에 따라 획득된 결과를 서버로 전달하는 단계를 포함할 수 있다.

대표도 - 도1



(52) CPC특허분류

H04L 63/0227 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711119150
과제번호	2020-0-01540
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	글로벌 핵심인재 양성지원 사업
연구과제명	[Ezbaro]스마트 그리드의 클라우드 기반 빅데이터 플랫폼을 위한 사이버 보안
기술(1차년도)	
기 여 율	60/100
과제수행기관명	인하대학교 산학협력단
연구기간	2020.06.01 ~ 2021.08.31

이 발명을 지원한 국가연구개발사업

과제고유번호	1711148097
과제번호	2020R1A2C201308912
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	중견연구
연구과제명	[Ezbaro] 블록체인 상의 기밀성 제공을 위한 암호 최적화 및 응용 기술 개발
기 여 율	20/100
과제수행기관명	인하대학교 산학협력단
연구기간	2021.03.01 ~ 2022.02.28

이 발명을 지원한 국가연구개발사업

과제고유번호	1711126259
과제번호	2020-0-01389
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	인공지능융합연구센터지원사업(국고)
연구과제명	[Ezbaro][정부] 인공지능융합연구센터지원(2차년도)
기 여 율	20/100
과제수행기관명	인하대학교 산학협력단
연구기간	2021.01.01 ~ 2021.12.31

명세서

청구범위

청구항 1

컴퓨터로 구현되는 하이브리드 이상 탐지 시스템에 의해 수행되는 하이브리드 이상 탐지 방법에 있어서,
동작 중인 시스템에서 생성된 데이터를 시그니처 기반의 이상 탐지 모델 및 행위 기반의 이상 탐지 모델로 구성된 하이브리드 이상 탐지 모델에 입력받는 단계;

상기 하이브리드 이상 탐지 모델을 이용하여 상기 동작 중인 시스템에서 생성된 데이터로부터 이상 탐지를 수행하는 단계; 및

상기 동작 중인 시스템에서 생성된 데이터와 상기 이상 탐지를 수행함에 따라 획득된 결과를 서버로 전달하는 단계

를 포함하는 하이브리드 이상 탐지 방법.

청구항 2

제1항에 있어서,

상기 입력받는 단계는,

게이트웨이에서 현재 동작 중인 시스템에서 생성된 데이터를 전달받음에 따라 이상 탐지 과정을 시작하는 단계

를 포함하는 하이브리드 이상 탐지 방법.

청구항 3

제1항에 있어서,

상기 이상 탐지를 수행하는 단계는,

상기 동작 중인 시스템에서 생성된 데이터가 상기 하이브리드 이상 탐지 모델에 구성된 시그니처 기반의 이상 탐지 모델에 입력됨에 따라 시그니처 기반의 이상 탐지 동작을 수행하는 단계

를 포함하는 하이브리드 이상 탐지 방법.

청구항 4

제3항에 있어서,

상기 이상 탐지를 수행하는 단계는,

상기 시그니처 기반의 이상 탐지 모델을 이용하여 상기 동작 중인 시스템에서 생성된 데이터를 필터링 기준에 따라 정상 동작 또는 이상 동작으로 분류하는 단계

를 포함하는 하이브리드 이상 탐지 방법.

청구항 5

제4항에 있어서,

상기 이상 탐지를 수행하는 단계는,

상기 동작 중인 시스템에서 생성된 데이터가 상기 시그니처 기반의 이상 탐지 모델에 의해 이상 동작으로 분류될 경우, 이상 탐지 과정을 종료하고, 상기 동작 중인 시스템에서 생성된 데이터가 상기 시그니처 기반의 이상 탐지 모델에 의해 정상 동작으로 분류될 경우, 상기 동작 중인 시스템에서 생성된 데이터를 행위 기반 이상 탐지 모델로 전달하는 단계

를 포함하는 하이브리드 이상 탐지 방법.

청구항 6

제1항에 있어서,

상기 이상 탐지를 수행하는 단계는,

상기 동작 중인 시스템에서 생성된 데이터가 상기 하이브리드 이상 탐지 모델에 구성된 행위 기반 이상 탐지 모델에 입력됨에 따라 행위 기반의 이상 탐지 동작을 수행하는 단계

를 포함하는 하이브리드 이상 탐지 방법.

청구항 7

제6항에 있어서,

상기 이상 탐지를 수행하는 단계는,

상기 동작 중인 시스템에서 생성된 데이터를 상기 행위 기반의 이상 탐지 모델을 이용하여 정상 동작 또는 이상 동작으로 분류하는 단계

를 포함하는 하이브리드 이상 탐지 방법.

청구항 8

제7항에 있어서,

상기 이상 탐지를 수행하는 단계는,

시그니처 기반의 이상 탐지 모델을 통해 정상 동작으로 분류된 데이터에 대하여 오토인코더를 통해 인코딩 및 디코딩하여 출력된 새로운 입력 데이터를 획득하고, 상기 정상 동작으로 분류된 데이터와 상기 획득된 새로운 입력 데이터의 차이 정보를 계산하는 단계

를 포함하는 하이브리드 이상 탐지 방법.

청구항 9

제8항에 있어서,

상기 이상 탐지를 수행하는 단계는,

상기 계산된 차이 정보를 정상 동작과 이상 동작을 분류하기 위한 임계값과 비교하여 상기 정상 동작으로 분류된 데이터의 최종 이상 여부를 판단하는 단계

를 포함하는 하이브리드 이상 탐지 방법.

청구항 10

제1항에 있어서,

상기 전달하는 단계는,

현재 동작 중인 시스템에서 생성된 데이터와 상기 이상 탐지를 수행하는 단계에서 판단된 이상 탐지 결과를 서버로 전달하는 단계

를 포함하는 하이브리드 이상 탐지 방법.

청구항 11

컴퓨터로 구현되는 하이브리드 이상 탐지 시스템에 있어서,

동작 중인 시스템에서 생성된 데이터를 시그니처 기반의 이상 탐지 모델 및 행위 기반의 이상 탐지 모델로 구성된 하이브리드 이상 탐지 모델에 입력받는 데이터 입력부;

상기 하이브리드 이상 탐지 모델을 이용하여 상기 동작 중인 시스템에서 생성된 데이터로부터 이상 탐지를 수행

하는 이상 탐지 수행부; 및

상기 동작 중인 시스템에서 생성된 데이터와 상기 이상 탐지를 수행함에 따라 획득된 결과를 서버로 전달하는 결과 전달부

를 포함하는 하이브리드 이상 탐지 시스템.

발명의 설명

기술 분야

[0001] 아래의 설명은 이상 탐지 기술에 관한 것이다.

배경 기술

[0003] 현대 사회에서는 과거에 물리적으로 제어되던 주거 시설, 차량, 공장, 사회 인프라 등의 대상들이 네트워크에 연결되고 있다. 다양한 기기들이 네트워크에 연결됨으로써 효율적으로 관리 및 통제가 가능하게 되었지만, 기존에는 불가능했던 네트워크를 통한 공격의 위협들이 생겨나게 되었다. 이는 개개인의 프라이버시를 위협하기도 하지만, 사회 인프라와 같이 특수 목적 시스템에 대한 공격은 공공의 비용적 손실과 생명의 위협을 초래할 수 있다.

[0004] 이러한 위협을 차단하기 위해 시스템으로 공격이 침투하기 전, 네트워크 단에서 공격을 차단하는 어플리케이션들이 제공되었으나 공격자는 제로 데이 공격과 같이 발견되지 않은 공격을 사용하여 시스템에 대한 공격을 수행할 수 있기 때문에 공격의 탐지 및 차단을 네트워크 보안 솔루션에만 의존할 수 없다. 이에 따라, 시스템의 현재 상태를 파악하여 시스템이 정상 동작을 하고 있는지 또는 공격에 따른 이상 동작을 하고 있는지 탐지하는 연구가 진행되었다.

[0005] 이와 같은 이상 동작 탐지 방법은 일반적으로 시그니처 기반 탐지 방법 (Signature-based anomaly detection) 과 행위 기반 탐지 방법(Behavior-based anomaly detection)으로 분류된다. 시그니처 기반 탐지 방법은 알려진 공격 또는 정상 동작의 특징을 분석하여 이를 바탕으로 입력 데이터가 정상인지 이상 동작을 하고 있는지 판단한다. 행위 기반 탐지 방법은 정상 또는 비정상 동작의 행위를 분석하여 입력 데이터의 이상 동작 여부를 판단하는 방법이다.

[0006] 일반적인 시스템은 대부분의 동작이 정상 동작이기 때문에, 정상 데이터의 양과 비교하여 이상 데이터의 양은 매우 적다. 따라서 이상 동작 탐지 연구들은 정상 데이터 또는 그 행위로부터 특징을 추출하여 이에 기반하여 이상 동작을 탐지하는 쪽으로 수행되었다.

발명의 내용

해결하려는 과제

[0008] 시그니처 기반의 이상 탐지 방법과 행위 기반의 이상 탐지 방법을 직렬 연결하여 이상 동작 탐지 성능을 높이는, 하이브리드 이상 동작 탐지 방법 및 시스템을 제공할 수 있다.

[0009] 사이버 공격으로 인한 이상 동작을 탐지하기 위해 통계적 필터링 기법과 오토인코더를 적용한 하이브리드 이상 탐지 방법 및 시스템을 제공할 수 있다.

과제의 해결 수단

[0011] 컴퓨터로 구현되는 하이브리드 이상 탐지 시스템에 의해 수행되는 하이브리드 이상 탐지 방법은, 동작 중인 시스템에서 생성된 데이터를 시그니처 기반의 이상 탐지 모델 및 행위 기반의 이상 탐지 모델로 구성된 하이브리드 이상 탐지 모델에 입력받는 단계; 상기 하이브리드 이상 탐지 모델을 이용하여 상기 동작 중인 시스템에서

생성된 데이터로부터 이상 탐지를 수행하는 단계; 및 상기 동작 중인 시스템에서 생성된 데이터와 상기 이상 탐지를 수행함에 따라 획득된 결과를 서버로 전달하는 단계를 포함할 수 있다.

- [0012] 상기 입력받는 단계는, 게이트웨이에서 현재 동작 중인 시스템에서 생성된 데이터를 전달받음에 따라 이상 탐지 과정을 시작하는 단계를 포함할 수 있다.
- [0013] 상기 이상 탐지를 수행하는 단계는, 상기 동작 중인 시스템에서 생성된 데이터가 상기 하이브리드 이상 탐지 모델에 구성된 시그니처 기반의 이상 탐지 모델에 입력됨에 따라 시그니처 기반의 이상 탐지 동작을 수행하는 단계를 포함할 수 있다.
- [0014] 상기 이상 탐지를 수행하는 단계는, 상기 시그니처 기반의 이상 탐지 모델을 이용하여 상기 동작 중인 시스템에서 생성된 데이터를 필터링 기준에 따라 정상 동작 또는 이상 동작으로 분류하는 단계를 포함할 수 있다.
- [0015] 상기 이상 탐지를 수행하는 단계는, 상기 동작 중인 시스템에서 생성된 데이터가 상기 시그니처 기반의 이상 탐지 모델에 의해 이상 동작으로 분류될 경우, 이상 탐지 과정을 종료하고, 상기 동작 중인 시스템에서 생성된 데이터가 상기 시그니처 기반의 이상 탐지 모델에 의해 정상 동작으로 분류될 경우, 상기 동작 중인 시스템에서 생성된 데이터를 행위 기반 이상 탐지 모델로 전달하는 단계를 포함할 수 있다.
- [0016] 상기 이상 탐지를 수행하는 단계는, 상기 동작 중인 시스템에서 생성된 데이터가 상기 하이브리드 이상 탐지 모델에 구성된 행위 기반 이상 탐지 모델에 입력됨에 따라 행위 기반의 이상 탐지 동작을 수행하는 단계를 포함할 수 있다.
- [0017] 상기 이상 탐지를 수행하는 단계는, 상기 동작 중인 시스템에서 생성된 데이터를 상기 행위 기반의 이상 탐지 모델을 이용하여 정상 동작 또는 이상 동작으로 분류하는 단계를 포함할 수 있다.
- [0018] 상기 이상 탐지를 수행하는 단계는, 시그니처 기반의 이상 탐지 모델을 통해 정상 동작으로 분류된 데이터에 대하여 오토인코더를 통해 인코딩 및 디코딩하여 출력된 새로운 입력 데이터를 획득하고, 상기 정상 동작으로 분류된 데이터와 상기 획득된 새로운 입력 데이터의 차이 정보를 계산하는 단계를 포함할 수 있다.
- [0019] 상기 이상 탐지를 수행하는 단계는, 상기 계산된 차이 정보를 정상 동작과 이상 동작을 분류하기 위한 임계값과 비교하여 상기 정상 동작으로 분류된 데이터의 최종 이상 여부를 판단하는 단계를 포함할 수 있다.
- [0020] 상기 전달하는 단계는, 상기 동작 중인 시스템에서 생성된 데이터와 상기 이상 탐지를 수행하는 단계에서 판단된 이상 탐지 결과가 서버로 전달될 수 있다.
- [0021] 컴퓨터로 구현되는 하이브리드 이상 탐지 시스템은, 동작 중인 시스템에서 생성된 데이터를 시그니처 기반의 이상 탐지 모델 및 행위 기반의 이상 탐지 모델로 구성된 하이브리드 이상 탐지 모델에 입력받는 데이터 입력부; 상기 하이브리드 이상 탐지 모델을 이용하여 상기 동작 중인 시스템에서 생성된 데이터로부터 이상 탐지를 수행하는 이상 탐지 수행부; 및 상기 동작 중인 시스템에서 생성된 데이터와 상기 이상 탐지를 수행함에 따라 획득된 결과를 서버로 전달하는 결과 전달부를 포함할 수 있다.

발명의 효과

- [0023] 시그니처 기반 이상 탐지 방법과 행위 기반 이상 탐지 방법을 직렬 연결하여 사용함으로써, 이상 동작 탐지의 성능을 높일 수 있다. 즉, 단독으로 시그니처 또는 행위 기반 이상 탐지를 사용하는 경우 탐지하지 못하는 이상 동작을 서로 상호 보완하여 탐지할 수 있다. 이를 통해 이상 동작의 미탐을 줄임으로써, 시스템 동작의 안전성 및 신뢰도를 향상시킬 수 있다.

도면의 간단한 설명

- [0025] 도 1은 일 실시예에 따른 하이브리드 이상 탐지 시스템에서 하이브리드 이상 탐지 동작을 설명하기 위한 도면이다.
- 도 2는 일 실시예에 있어서, 하이브리드 이상 탐지 모델을 이용하여 하이브리드 이상 탐지 동작을 설명하기 위한 도면이다.

도 3은 일 실시예에 따른 하이브리드 이상 탐지 시스템의 구성을 설명하기 위한 블록도이다.

도 4는 일 실시예에 따른 하이브리드 이상 탐지 시스템에 의해 수행되는 하이브리드 이상 탐지 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0026] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0028] 도 1은 일 실시예에 따른 하이브리드 이상 탐지 시스템에서 하이브리드 이상 탐지 동작을 설명하기 위한 도면이다.

[0029] 하이브리드 이상 탐지 시스템(100)은 컴퓨터로 구현되는 것으로서, 게이트웨이(101)에서 하이브리드 이상 탐지 알고리즘에 기초하여 동작되는 것일 수 있다. 이때, 하이브리드 이상 탐지 시스템(100)은 하이브리드 이상 탐지 알고리즘에 기초하여 이상 탐지를 수행할 수 있다. 예를 들면, 하이브리드 이상 탐지 시스템(100)은 게이트웨이(101)에서 플랫폼 또는 프로그램 형태로 구동될 수 있다.

[0030] 게이트웨이(101)란 복수의 컴퓨터와 근거리 통신망 등을 상호 접속할 때 컴퓨터와 공중 통신망, LAN과 공중 통신망 등을 접속하는 장치를 가리킨다. 실시예에서는 게이트웨이(101)를 예를 들어 설명하나, 게이트웨이(101) 이외에도 라우터 등 데이터의 송수신을 가능하게 하는 네트워크 장비이면 적용이 가능하다.

[0031] 시스템(102)에서 발생 또는 생성된 데이터가 게이트웨이(101)를 거쳐 데이터를 관리하기 위한 서버(103)로 전달될 수 있다. 예를 들면, 시스템은 게이트웨이에 연결되어 있는 동작 중인 시스템을 의미할 수 있으며, 게이트웨이에 연결된 시스템들 중 공격자(104)에 의해 공격당하는 희생 시스템에 해당될 수 있다. 이때, 외부에 위치한 공격자(104)는 게이트웨이(101)를 통해 시스템을 공격하여 이상 동작을 발생시키려고 시도할 수 있다. 그리고 발생한 이상 동작에 의해 생성된 데이터는 게이트웨이(101)를 거치게 된다. 하이브리드 이상 탐지 시스템(100)은 하이브리드 이상 탐지 알고리즘에 기초하여 게이트웨이(101)를 거치는 이상 동작에 의해 생성된 데이터를 관찰하고, 관찰을 통해 현재 시스템이 이상 동작을 하고 있는지 판단할 수 있다.

[0032] 하이브리드 이상 탐지 시스템(100)은 이상 동작 탐지를 수행하기 위해 다음의 과정이 선제적으로 수행될 수 있다. 하이브리드 이상 탐지 시스템(100)은 타겟 시스템의 정상 동작 과정에서 생성된 시계열 데이터 D 를 수집할 수 있다. 이때, 수집되는 시계열 데이터 D 는 정상 동작 과정에서 생성되는 시계열 데이터(이하, '정상 동작 데이터'로 기재하기로 함.)으로써 다수의 속성을 포함할 수 있다. 일례로, 시스템의 데이터 획득 주기가 1초일 때, 단위 데이터가 n 개의 데이터 속성을 가지며 w 초 동안 수집된 데이터(정상 동작 데이터) D 는 다음과 같이 표현될 수 있다.

$$D = \{d_1 = \{v_{1,1}, v_{1,2}, \dots, v_{1,n}\}, d_2 = \{v_{2,1}, v_{2,2}, \dots, v_{2,n}\}, \dots, d_w = \{v_{w,1}, v_{w,2}, \dots, v_{w,n}\}\}$$

[0034] 하이브리드 이상 탐지 시스템(100)은 정상 동작 데이터 D 에 대해 통계적 분석을 수행하여, 시그니처 기반 이상 동작 탐지를 위한 정상 동작 데이터의 특징을 계산할 수 있다. 하이브리드 이상 탐지 시스템(100)은 시그니처 기반 이상 탐지 방법에서 사용될 필터링 기준을 설정하기 위해 정상 동작 데이터 D 를 이용하여 평균, 표준편차, 최댓값, 최솟값 등과 같은 통계적 분석을 수행할 수 있다. 예를 들어, 하이브리드 이상 탐지 시스템(100)은 n (n 은 자연수)개의 모든 속성값들에 대해 w (w 는 자연수)초 동안 수집된 값의 표준편차인 $S_j^D = \sigma(v_{1,j}, v_{2,j}, \dots, v_{w,j})$ 를 계산할 수 있다($j=1, \dots, n$). 그리고 w 초 동안 연속된 정상 동작 데이터들의

표준편차의 하한과 상한인 $Min_{S_j} = \min_D S_j^D$ 와 $Max_{S_j} = \max_D S_j^D$ 를 계산하고, 계산된 표준편차를 필터링 기준으로 설정할 수 있다.

[0035] 하이브리드 이상 탐지 시스템(100)은 정상 동작 데이터 D 를 사용하여, 행위 기반 이상 동작 탐지를 위한 정상 동작 행위의 특징을 추출할 수 있다. 하이브리드 이상 탐지 시스템(100)은 정상 동작 데이터로부터 행위 기반 이상 탐지 방법에 사용되는 정상 동작 행위의 특징을 추출하여 정상 동작과 이상 동작을 잘 분류하는 판단 기준과 임계값(Threshold)을 설정할 수 있다. 일례로, 행위 기반 탐지 방법에는 비지도 심층 학습 방법인 오토인코더(Autoencoder)가 사용될 수 있다. 오토인코더는 정상 동작 데이터를 심층 학습의 입력으로 제공하고, 출력으

로 입력 데이터를 다시 복원하는 모델을 학습한다. 이후, 입력 데이터와 출력 데이터의 차이를 판단 기준으로 사용하여, 정상 데이터와 이상 데이터의 차이가 작은 경우 정상, 차이가 큰 경우 이상 동작으로 분류하는 임계값 θ 를 설정한다.

[0036] 도 2를 참고하면, 하이브리드 이상 탐지 모델을 이용하여 하이브리드 이상 탐지 동작을 설명하기 위한 도면이다. 하이브리드 이상 탐지 시스템은 하이브리드 이상 탐지 알고리즘 기반의 하이브리드 이상 탐지 모델(200)을 구성할 수 있다. 하이브리드 이상 탐지 모델(200)은 시그니처 기반의 이상 탐지 모델(210) 및 행위 기반의 이상 탐지 모델(220)로 구성될 수 있다.

[0037] 게이트웨이에 위치한 하이브리드 시스템에서 하이브리드 이상 탐지 방법은 다음과 같은 순서로 수행될 수 있다.

[0038] 게이트웨이가 현재 동작하는 시스템에서 생성된 데이터를 전달받음에 따라 이상 탐지 과정이 시작될 수 있다. 예를 들면, 현재 동작하는 시스템이란 게이트웨이에 연결되어 동작 중인 시스템을 의미할 수 있다. 전달받은 데이터가 시그니처 기반의 이상 탐지 모델(210)에 입력될 수 있고, 시그니처 기반의 이상 탐지 모델에서 입력받은 데이터에 대한 필터링 과정이 수행될 수 있다. 이때, 시그니처 기반의 이상 탐지 모델(210)에서 입력받은 데이터가 필터링 기준에 따라 정상 동작 또는 이상 동작으로 분류될 수 있다. 시그니처 기반의 이상 탐지 모델(210)에서 입력받은 데이터가 이상 동작으로 분류된 경우, 이상 탐지 과정이 종료될 수 있고, 입력받은 데이터가 잠재적으로 정상 동작으로 분류된 경우, 행위 기반 이상 탐지 모델(220)로 입력받은 데이터(즉, 정상 동작으로 분류된 데이터)가 전달될 수 있다.

[0039] 상세하게는, 시그니처 기반의 이상 탐지 모델(210)에서 입력받은 데이터는 필터링을 위해 설정된 기준에 따라 이상 여부가 판단될 수 있다. 일례로, 정상 여부 판정 대상인 입력받은 데이터(이하, '입력 데이터'로 기재하기로 함.) D' 를 다음과 같이 가정하기로 한다.

$$D' = \{d'_1 = \{v'_{1,1}, v'_{1,2}, \dots, v'_{1,n}\}, d'_2 = \{v'_{2,1}, v'_{2,2}, \dots, v'_{2,n}\}, \dots, d'_w = \{v'_{w,1}, v'_{w,2}, \dots, v'_{w,n}\}\}$$

[0041] 필터링 기준으로 표준편차의 하한과 상한이 설정된 경우, 입력 데이터 D' 의 n 개의 속성값에 대한 표준편차 $S_j^D = \sigma(v'_{1,j}, v'_{2,j}, \dots, v'_{w,j})$ ($j = 1, \dots, n$)가 계산된 후, S_j^D 의 값의 범위에 따라 정상 여부를 반환하는 술어논리(predicate) P_j 가 계산될 수 있다. 즉 P_j 는 다음과 같다.

$$P_j = \begin{cases} \text{True, if } \text{Min}_{S_j} \leq S_j^D \leq \text{Max}_{S_j} \\ \text{False, otherwise} \end{cases}$$

[0043] 다음으로 계산된 $P_1, P_2, \dots, P_n$ 에 대하여 $P_1 \cap P_2 \cap \dots \cap P_n = \text{True}$ 인 경우, 즉, n 개의 속성 모두가 정상 범위인 경우, 입력 데이터 D' 이 정상 동작으로 분류되고, 그렇지 않은 경우 이상 동작으로 분류될 수 있다. 이상 동작으로 분류된 경우, 이상 탐지 과정은 종료되고, 잠재적 정상 동작으로 분류된 경우, 미탐을 방지하기 위해 입력 데이터 D' 에 대해 행위 기반 이상 탐지가 추가로 수행될 수 있다.

[0044] 시그니처 기반의 이상 탐지 모델(210)에서 전달된 데이터가 행위 기반의 이상 탐지 모델(220)에 입력됨에 따라 이상 탐지 과정이 수행될 수 있다. 입력된 데이터가 행위 기반의 이상 탐지 모델(220)의 행위 기반 이상 탐지 알고리즘의 입력으로 전달될 수 있다. 행위 기반의 이상 탐지 알고리즘에 따라 입력된 데이터가 정상 동작 또는 이상 동작으로 분류될 수 있다.

[0045] 상세하게는, 잠재적 정상으로 분류된 데이터(정상 동작으로 분류된 데이터)가 행위 기반의 이상 탐지 모델(220)에 입력되어 행위 기반 이상 탐지가 수행될 수 있다. 예를 들면, 상기 기술된 비지도 심층 학습 방법 중 하나인 오토인코더가 행위 기반 이상 탐지를 위해 사용될 수 있다. 이상 탐지를 위해 입력 데이터 D' 이 오토인코더에 입력되면, 오토인코더는 입력 데이터 D' 를 인코딩 및 디코딩하여 새로운 입력 데이터 D'' 을 출력하며, D' 과 D'' 의 차이를 계산한다. 예를 들어, 평균 제곱 오차(Mean Squared Error; MSE)가 두 데이터의 차이 ($\text{Distance} = \text{MSE}(D', D'')$)를 계산하기 위해 사용될 수 있다. 다음으로 행위 기반 이상 탐지 알고리즘에 의해 계산된 거리(Distance)는 정상 동작과 이상 동작을 분류하기 위한 임계값 θ 와 비교되어 입력 데이터

D' 의 최종 이상 여부 R 이 다음과 같이 판단될 수 있다.

$$R = \begin{cases} \text{True, if } \theta < \text{Distance} \\ \text{False, otherwise} \end{cases}$$

[0046]

[0047]

이러한 이상 탐지 과정이 수행됨에 따라 이상 탐지 과정이 종료될 수 있다. 데이터 및 이상 탐지 결과가 서버로 전달될 수 있다. 입력 데이터 D' 와 시그니처 기반의 이상 탐지 동작과 행위 기반의 이상 탐지 동작을 통해 정상 동작인지 이상 동작인지 분류된 결과가 서버로 전달되며, 하이브리드 이상 탐지 과정은 종료된다.

[0048]

도 3은 일 실시예에 따른 하이브리드 이상 탐지 시스템의 구성을 설명하기 위한 블록도이고, 도 4는 일 실시예에 따른 하이브리드 이상 탐지 시스템에 의해 수행되는 하이브리드 이상 탐지 방법을 설명하기 위한 흐름도이다.

[0049]

하이브리드 이상 탐지 시스템(100)의 프로세서는 데이터 입력부(310), 이상 탐지 수행부(320) 및 결과 전달부(330)를 포함할 수 있다. 이러한 프로세서의 구성요소들은 하이브리드 이상 탐지 시스템에 저장된 프로그램 코드가 제공하는 제어 명령에 따라 프로세서에 의해 수행되는 서로 다른 기능들(different functions)의 표현들일 수 있다. 프로세서 및 프로세서의 구성요소들은 도 4의 하이브리드 이상 탐지 방법이 포함하는 단계들(410 내지 430)을 수행하도록 하이브리드 이상 탐지 시스템을 제어할 수 있다. 이때, 프로세서 및 프로세서의 구성요소들은 메모리가 포함하는 운영체제의 코드와 적어도 하나의 프로그램의 코드에 따른 명령(instruction)을 실행하도록 구현될 수 있다.

[0050]

프로세서는 하이브리드 이상 탐지 방법을 위한 프로그램의 파일에 저장된 프로그램 코드를 메모리에 로딩할 수 있다. 예를 들면, 하이브리드 이상 탐지 시스템에서 프로그램이 실행되면, 프로세서는 운영체제의 제어에 따라 프로그램의 파일로부터 프로그램 코드를 메모리에 로딩하도록 하이브리드 이상 탐지 시스템을 제어할 수 있다. 이때, 데이터 입력부(310), 이상 탐지 수행부(320) 및 결과 전달부(330) 각각은 메모리에 로딩된 프로그램 코드 중 대응하는 부분의 명령을 실행하여 이후 단계들(410 내지 430)을 실행하기 위한 프로세서의 서로 다른 기능적 표현들일 수 있다.

[0051]

단계(410)에서 데이터 입력부(310)는 동작 중인 시스템에서 생성된 데이터를 시그니처 기반의 이상 탐지 모델 및 행위 기반의 이상 탐지 모델로 구성된 하이브리드 이상 탐지 모델에 입력받을 수 있다. 데이터 입력부(310)는 게이트웨이에서 현재 동작 중인 시스템에서 생성된 데이터를 전달받음에 따라 이상 탐지 과정을 시작할 수 있다.

[0052]

단계(420)에서 이상 탐지 수행부(320)는 하이브리드 이상 탐지 모델을 이용하여 동작 중인 시스템에서 생성된 데이터로부터 이상 탐지를 수행할 수 있다. 이상 탐지 수행부(320)는 동작 중인 시스템에서 생성된 데이터가 하이브리드 이상 탐지 모델에 구성된 시그니처 기반의 이상 탐지 모델에 입력됨에 따라 시그니처 기반의 이상 탐지 동작을 수행할 수 있다. 이상 탐지 수행부(320)는 시그니처 기반의 이상 탐지 모델을 이용하여 동작 중인 시스템에서 생성된 데이터를 필터링 기준에 따라 정상 동작 또는 이상 동작으로 분류할 수 있다. 이상 탐지 수행부(320)는 동작 중인 시스템에서 생성된 데이터가 이상 동작으로 분류될 경우, 이상 탐지 과정을 종료하고, 동작 중인 시스템에서 생성된 데이터가 정상 동작으로 분류될 경우, 동작 중인 시스템에서 생성된 데이터를 행위 기반 이상 탐지 모델로 전달할 수 있다. 이상 탐지 수행부(320)는 동작 중인 시스템에서 생성된 데이터가 하이브리드 이상 탐지 모델에 구성된 행위 기반 이상 탐지 모델에 입력됨에 따라 행위 기반의 이상 탐지 동작을 수행할 수 있다. 이상 탐지 수행부(320)는 동작 중인 시스템에서 생성된 데이터를 행위 기반의 이상 탐지 모델을 이용하여 정상 동작 또는 이상 동작으로 분류할 수 있다. 이상 탐지 수행부(320)는 시그니처 기반의 이상 탐지 모델을 통해 정상 동작으로 분류된 데이터에 대하여 오토인코더를 통해 인코딩 및 디코딩하여 출력된 새로운 입력 데이터를 획득하고, 정상 동작으로 분류된 데이터와 상기 획득된 새로운 입력 데이터의 차이 정보를 계산할 수 있다. 이상 탐지 수행부(320)는 계산된 차이 정보를 정상 동작과 이상 동작을 분류하기 위한 임계값과 비교하여 정상 동작으로 분류된 데이터의 최종 이상 여부를 판단할 수 있다.

[0053]

단계(430)에서 결과 전달부(330)는 동작 중인 시스템에서 생성된 데이터와 이상 탐지를 수행함에 따라 획득된 결과를 서버로 전달할 수 있다. 결과 전달부(330)는 현재 동작 중인 시스템에서 생성된 데이터와 이상 탐지를 수행하는 과정에서 판단된 이상 탐지 결과를 서버로 전달할 수 있다. 이에, 하이브리드 이상 탐지 과정이 종료될 수 있다.

[0054]

이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어

구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0055] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

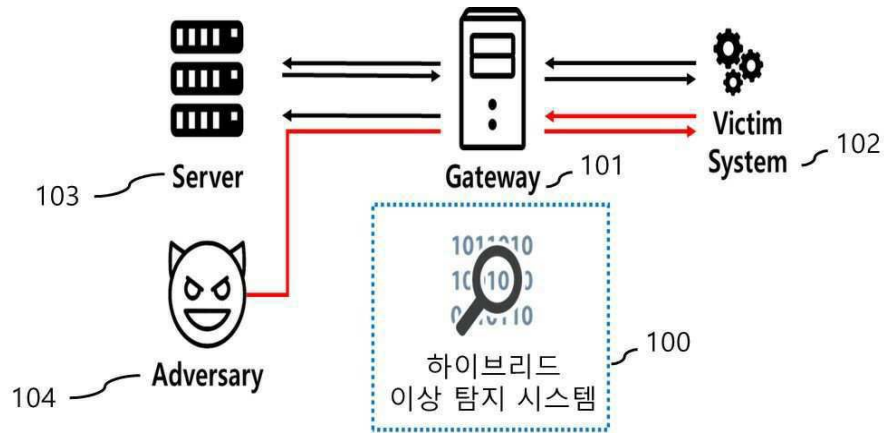
[0056] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic 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.

[0057] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

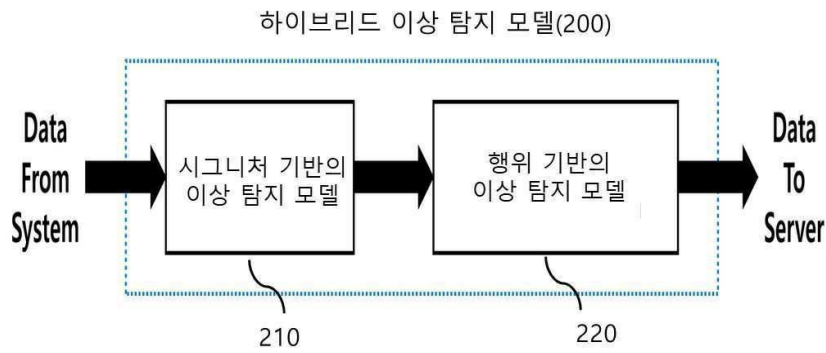
[0058] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

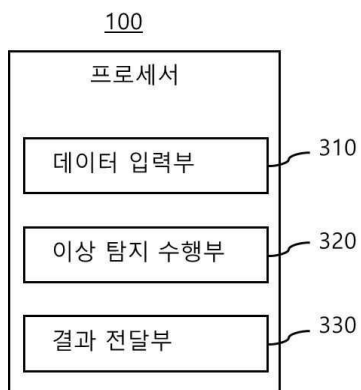
도면1



도면2



도면3



도면4

