



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0040110
(43) 공개일자 2023년03월22일

(51) 국제특허분류(Int. Cl.)

H04L 9/40 (2022.01) G06F 16/13 (2019.01)
G06F 21/57 (2013.01) G16Y 30/10 (2020.01)
G16Y 40/50 (2020.01) H04L 43/00 (2022.01)
H04L 65/40 (2022.01) H04L 9/06 (2006.01)

(52) CPC특허분류

H04L 63/1416 (2013.01)
G06F 16/137 (2019.01)

(21) 출원번호 10-2021-0123317

(22) 출원일자 2021년09월15일

심사청구일자 2021년09월15일

(71) 출원인

이화여자대학교 산학협력단

서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)

(72) 발명자

도인실

인천광역시 연수구 센트럴로 194, 201동 1703호
(더샵센트럴파크2단지아파트)

채기준

서울특별시 강남구 강남대로136길 34, 402호 (논현동, 월드노블레스빌)

김효원

경기도 수원시 장안구 천천로21번길 33, 613동
603호 청솔마을주공아파트

(74) 대리인

윤귀상

전체 청구항 수 : 총 16 항

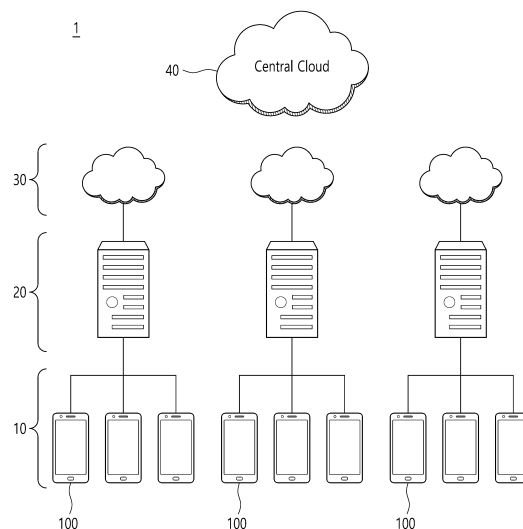
(54) 발명의 명칭 도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 시스템 및 그 방법

(57) 요약

본 발명은 도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 시스템 및 그 방법에 대한 것이다.

본 발명에 따른 도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 시스템은, 최하위 계층을 형성하고 IoT 기기의 트래픽 데이터를 가지고 있는 복수의 엔드 노드와, 복수의 IoT 기기들로 형성되는 복수의 그룹에 각각 연결되고, 상기 IoT 기기들로부터 전달되는 트래픽 데이터를 이용하여 특징 정보 모음을 생성하여 전달하는 복수의 엣지 노드 및 각 엣지 노드에 연결되어 해당 엣지 노드를 통해 상기 특징 정보 모음을 전달받아 블록체인 네트워크상의 F-Env(Feature-Environment) 목록에 상기 특징 정보 모음에 대응하는 F-Env가 존재하는지 판단하고, 판단 결과에 따른 IoT 기기에 대한 공격 탐지 모델을 상기 엣지 노드에 전달하는 복수의 포그 노드를 포함한다.

대표도 - 도1



(52) CPC특허분류

G06F 21/57 (2013.01)
G16Y 30/10 (2020.01)
G16Y 40/50 (2020.01)
H04L 43/18 (2022.05)
H04L 63/1458 (2013.01)
H04L 67/06 (2022.05)
H04L 67/1089 (2022.05)
H04L 67/2885 (2022.05)
H04L 9/0643 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711129577
과제번호	2020R1A2C1006497
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	개인기초연구(과기정통부)(R&D)
연구과제명	UAV를 활용한 모바일 IoT 환경에서 효율적이고 안전한 노드 및 데이터 프라이버시
보장 기법	
기 여 율	1/1
과제수행기관명	이화여자대학교
연구기간	2020.03.01 ~ 2021.02.28

명세서

청구범위

청구항 1

도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 시스템에 있어서,

최하위 계층을 형성하고, IoT 기기의 트래픽 데이터를 가지고 있는 복수의 엔드 노드;

복수의 IoT 기기들로 형성되는 복수의 그룹에 각각 연결되고, 상기 IoT 기기들로부터 전달되는 트래픽 데이터를 이용하여 특징 정보 모음을 생성하여 전달하는 복수의 엣지 노드; 및

각 엣지 노드에 연결되어 해당 엣지 노드를 통해 상기 특징 정보 모음을 전달받아 블록체인 네트워크상의 F-Env(Feature-Environment) 목록에 상기 특징 정보 모음에 대응하는 F-Env가 존재하는지 판단하고, 판단 결과에 따른 IoT 기기에 대한 공격 탐지 모델을 상기 엣지 노드에 전달하는 복수의 포그 노드를 포함하고,

상기 엣지 노드는,

상기 공격 탐지 모델을 전달받아 해당 IoT 네트워크에서 적용하는 공격 탐지 모델 공유 시스템.

청구항 2

제1항에 있어서,

상기 엣지 노드는,

상기 트래픽 데이터를 통해 트래픽 특징 정보를 수집하여 패킷의 크기와 프로토콜의 분포 정보를 산출하고, 산출한 패킷의 크기와 프로토콜의 분포 정보가 포함된 상기 특징 정보 모음을 생성하여 상기 엣지 노드에 연결된 상기 포그 노드에 전달하는 공격 탐지 모델 공유 시스템.

청구항 3

제1항에 있어서,

상기 포그 노드는,

상기 특징 정보 모음을 이용하여 패킷의 크기와 프로토콜의 종류별로 임의의 임계치가 설정된 상기 F-Env를 생성하며, 생성된 F-Env를 상기 블록체인 네트워크상의 F-Env 목록에 추가시키는 공격 탐지 모델 공유 시스템.

청구항 4

제1항에 있어서,

상기 포그 노드는,

중앙 클라우드와 가장 가까운 최상위 계층을 형성하고,

상기 최상위 계층은,

분산된 환경에서 암호학적 해쉬를 통한 콘텐츠 식별자를 이용하여 파일의 위치를 찾아 각 포그 노드 간의 파일 업로드와 다운로드를 지원하는 IPFS(InterPlanetary File System) 환경을 기반으로 하며,

각각의 포그 노드는,

저장소를 포함하여 자신이 생성하거나 타 포그 노드로부터 다운로드 받은 공격 탐지 모델을 해당 저장소에 저장하는 공격 탐지 모델 공유 시스템.

청구항 5

제4항에 있어서,

상기 포그 노드는,

상기 F-Env 목록에 상기 특징 정보 모음에 대응하는 F-Env가 존재하는 경우,

상기 공격 탐지 모델을 보유하고 있는지 판단하여 상기 공격 탐지 모델을 보유하고 있으면 상기 공격 탐지 모델을 연결된 엣지 노드에 전달하고,

상기 공격 탐지 모델을 보유하고 있지 않으면 상기 IPFS 환경에서 타 포그 노드들의 저장소를 검색하여 상기 공격 탐지 모델을 보유한 포그 노드로부터 상기 공격 탐지 모델을 다운로드 받아 상기 엣지 노드에 전달하는 공격 탐지 모델 공유 시스템.

청구항 6

제4항에 있어서,

상기 포그 노드는,

상기 F-Env 목록에 상기 특징 정보 모음에 대응하는 F-Env가 존재하지 않는 경우,

상기 전달받은 특징 정보 모음을 이용하여 IoT 기기에 대한 공격 탐지를 위한 머신러닝 공격 탐지 모델과 F-Env를 생성하여 저장소에 저장하고, 상기 공격 탐지 모델을 연결된 엣지 노드에 전달하는 공격 탐지 모델 공유 시스템.

청구항 7

제6항에 있어서,

상기 포그 노드는,

타 포그 노드들과의 합의 알고리즘에 의해 통과되면 상기 생성된 F-Env를 프라이빗 블록체인 네트워크상의 F-Env 목록에 추가시키는 공격 탐지 모델 공유 시스템.

청구항 8

제1항에 있어서,

상기 엣지 노드는,

상기 공격 탐지 모델을 해당 IoT 네트워크에서 적용하여 트래픽을 탐지하고, 탐지 결과에 따라 트래픽을 제한하는 공격 탐지 모델 공유 시스템.

청구항 9

도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 시스템에 의해 수행되는 공격 탐지 모델 공유 방법에 있어서

제2 계층을 형성하는 엣지 노드가 제1 계층을 형성하는 엔드 노드를 통해 IoT 기기의 트래픽 데이터를 전달받는 단계;

상기 엣지 노드가 상기 트래픽 데이터를 이용하여 특징 정보 모음을 생성하고 생성된 특징 정보 모음을 제3 계층을 형성하는 포그 노드에 전달하는 단계;

상기 포그 노드가 블록체인 네트워크상의 F-Env(Feature-Environment) 목록에 상기 특징 정보 모음에 대응하는 F-Env가 존재하는지 판단하는 단계;

상기 판단 결과에 따른 IoT 기기에 대한 공격 탐지 모델을 상기 엣지 노드에 전달하는 단계; 및

상기 엣지 노드가 해당 IoT 네트워크에서 상기 공격 탐지 모델을 적용하는 단계를 포함하는 공격 탐지 모델 공유 방법.

청구항 10

제9항에 있어서,

상기 포그 노드에 전달하는 단계는,

상기 트래픽 데이터를 통해 트래픽 특징 정보를 수집하여 패킷의 크기와 프로토콜의 분포 정보를 산출하고, 산출한 패킷의 크기와 프로토콜의 분포 정보가 포함된 상기 특징 정보 모음을 생성하여 상기 엣지 노드에 연결된 상기 포그 노드에 전달하는 공격 탐지 모델 공유 방법.

청구항 11

제9항에 있어서,

상기 포그 노드는,

상기 특징 정보 모음을 이용하여 패킷의 크기와 프로토콜의 종류별로 임의의 임계치가 설정된 상기 F-Env를 생성하며, 생성된 F-Env를 상기 블록체인 네트워크상의 F-Env 목록에 추가시키는 공격 탐지 모델 공유 방법.

청구항 12

제9항에 있어서,

상기 포그 노드는,

중앙 클라우드와 가장 가까운 최상위 계층을 형성하고,

상기 최상위 계층은,

분산된 환경에서 암호학적 해쉬를 통한 콘텐츠 식별자를 이용하여 파일의 위치를 찾아 각 포그 노드 간의 파일 업로드와 다운로드를 지원하는 IPFS(InterPlanetary File System) 환경을 기반으로 하며,

각각의 포그 노드는,

저장소를 포함하여 자신이 생성하거나 타 포그 노드로부터 다운로드 받은 공격 탐지 모델을 해당 저장소에 저장하는 공격 탐지 모델 공유 방법.

청구항 13

제12항에 있어서,

상기 엣지 노드에 전달하는 단계는,

상기 F-Env 목록에 상기 특징 정보 모음에 대응하는 F-Env가 존재하는 경우,

상기 공격 탐지 모델을 보유하고 있는지 판단하여 상기 공격 탐지 모델을 보유하고 있으면 상기 공격 탐지 모델을 연결된 엣지 노드에 전달하고,

상기 공격 탐지 모델을 보유하고 있지 않으면 상기 IPFS 환경에서 타 포그 노드들의 저장소를 검색하여 상기 공격 탐지 모델을 보유한 포그 노드로부터 상기 공격 탐지 모델을 다운로드 받아 연결된 엣지 노드에 전달하는 공격 탐지 모델 공유 방법.

청구항 14

제12항에 있어서,

상기 엣지 노드에 전달하는 단계는,

상기 F-Env 목록에 상기 특징 정보 모음에 대응하는 F-Env가 존재하지 않는 경우,

상기 전달받은 특징 정보 모음을 이용하여 IoT 기기에 대한 공격 탐지를 위한 머신러닝 공격 탐지 모델과 F-Env를 생성하여 해당 포그 노드의 저장소에 저장하고, 상기 공격 탐지 모델을 연결된 엣지 노드에 전달하는 공격 탐지 모델 공유 방법.

청구항 15

제14항에 있어서,

상기 포그 노드는,

타 포그 노드들과의 합의 알고리즘에 의해 통과되면 상기 생성된 F-Env를 프라이빗 블록체인 네트워크상의 F-Env 목록에 추가시키는 공격 탐지 모델 공유 방법.

청구항 16

제9항에 있어서,

상기 공격 탐지 모델을 적용하는 단계는,

상기 공격 탐지 모델을 해당 IoT 네트워크에서 적용하여 트래픽을 탐지하고, 탐지 결과에 따라 트래픽을 제한하는 공격 탐지 모델 공유 방법.

발명의 설명

기술 분야

- [0001] 본 발명은 도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 시스템 및 그 방법에 관한 것으로서, 더욱 상세하게는 다양성과 변동성이 높은 IoT 기기에 대한 공격 탐지 모델을 효율적으로 공유하기 위한 도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 시스템 및 그 방법에 관한 것이다.

배경 기술

- [0002] 최근 스마트 도시를 이루는 도시 컴퓨팅 환경에서는 통신 기술의 발달을 기반으로 사물인터넷(Internet of Things, 이하 IoT) 기기의 수가 증가하며 매일 방대하고 다양한 종류의 데이터가 생성되고 있다. 여기서 IoT는 다양한 사물에 부착된 센서를 통해 실시간으로 데이터를 주고받을 수 있는 기술이나 환경을 말한다.
- [0003] IoT를 통해 많은 양의 빅데이터가 수집됨에 따라 현대의 도시 컴퓨팅 환경에서 IoT가 미치는 영향은 점점 증가하고 있으며, 인터넷에 연결되는 IoT 기기의 수는 2022년을 기준으로 약 350억 개에 달할 것으로 예상된다.
- [0004] 이와 같이 IoT가 도시 컴퓨팅에서 차지하는 비중이 증가할수록, 보안 위협의 종류와 심각성 또한 커지고 있다. 이러한 위협들은 IoT를 통한 DDoS(Distributed Denial of Service), 데이터 유출 등 다양한 종류가 있다. 이에 따라, 통일된 보안 방법을 적용하는 것이 아니라 다양한 공격에 대처할 수 있는 IoT 보안 환경의 필요성이 높아지고 있다.
- [0005] 그러나 저전력, 저용량과 같은 IoT 기기의 물리적인 한계는 IoT 단말 자체에 보안 모듈을 구현하는 것을 어렵게 만든다. 또한, IoT의 다양성과 변동성으로 인해 기존의 보안 모듈이나 통일된 종류의 보안 방법을 적용하는 것도 쉽지 않은 실정이다.
- [0006] 또한, 딥러닝을 통해 네트워크에서 비정상적인 트래픽을 탐지하는 AI 보안 방안이 활발히 연구되고 있지만 머신러닝 공격 탐지 기법은 다양한 환경에서 모델을 지속적으로 업데이트해야 하므로 시스템에 부하를 일으킬 수 있다는 문제점을 가지고 있다.
- [0007] 따라서 유동적이고 다양한 IoT 환경에서 효율적으로 공격을 탐지할 수 있는 보안 시스템의 개발이 필요하다.
- [0009] 본 발명의 배경이 되는 기술은 대한민국 공개특허공보 제10-2018-0119162호(2018. 11. 01. 공개)에 개시되어 있다.

발명의 내용

해결하려는 과제

- [0010] 본 발명이 이루고자 하는 기술적 과제는 중앙으로 트래픽이 집중되어 전체적인 시스템의 성능이 저하되는 것을 방지하기 위해 엣지 컴퓨팅을 기반으로 다양성과 변동성이 높은 IoT 기기에 대한 공격 탐지 모델을 효율적으로 공유하기 위한 도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 시스템 및 그 방법을 제공하는 것이다.
- [0011] 또한, 공격 탐지 모델을 지속적으로 생성 및 업데이트 하는 대신 블록체인 네트워크 상의 F-Env(Feature-Environment) 목록을 이용하여 적합한 모델을 검색하여 공유하고 이를 IoT 기기에 적용할 수 있도록 하는 도시

컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 시스템 및 그 방법을 제공하기 위한 것이다.

[0012] 또한, IPFS(InterPlanetary File System) 환경을 기반으로 하여 같은 계층의 포그 노드 간에 공격 탐지 모델을 효율적으로 공유하도록 하는 도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 시스템 및 그 방법을 제공하기 위한 것이다.

과제의 해결 수단

[0013] 이러한 기술적 과제를 이루기 위한 본 발명의 실시 예에 따른 도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 시스템은, 최하위 계층을 형성하고, IoT 기기의 트래픽 데이터를 가지고 있는 복수의 엔드 노드; 복수의 IoT 기기들로 형성되는 복수의 그룹에 각각 연결되고, 상기 IoT 기기들로부터 전달되는 트래픽 데이터를 이용하여 특징 정보 모음을 생성하여 전달하는 복수의 엣지 노드; 및 각 엣지 노드에 연결되어 해당 엣지 노드를 통해 상기 특징 정보 모음을 전달받아 블록체인 네트워크상의 F-Env(Feature-Environment) 목록에 상기 특징 정보 모음에 대응하는 F-Env가 존재하는지 판단하고, 판단 결과에 따른 IoT 기기에 대한 공격 탐지 모델을 상기 엣지 노드에 전달하는 복수의 포그 노드를 포함하고, 상기 엣지 노드는 상기 공격 탐지 모델을 전달받아 해당 IoT 네트워크에서 적용할 수 있다.

[0014] 이때, 상기 엣지 노드는 상기 트래픽 데이터를 통해 트래픽 특징 정보를 수집하여 패킷의 크기와 프로토콜의 분포 정보를 산출하고, 산출한 패킷의 크기와 프로토콜의 분포 정보가 포함된 상기 특징 정보 모음을 생성하여 상기 엣지 노드에 연결된 상기 포그 노드에 전달할 수 있다.

[0015] 또한, 상기 포그 노드는 상기 특징 정보 모음을 이용하여 패킷의 크기와 프로토콜의 종류별로 임의의 임계치가 설정된 상기 F-Env를 생성하며, 생성된 F-Env를 상기 블록체인 네트워크상의 F-Env 목록에 추가시킬 수 있다.

[0016] 또한, 상기 포그 노드는 중앙 클라우드와 가장 가까운 최상위 계층을 형성하고, 상기 최상위 계층은 분산된 환경에서 암호학적 해쉬를 통한 콘텐츠 식별자를 이용하여 파일의 위치를 찾아 각 포그 노드 간의 파일 업로드와 다운로드를 지원하는 IPFS(InterPlanetary File System) 환경을 기반으로 하며, 각각의 포그 노드는 저장소를 포함하여 자신이 생성하거나 타 포그 노드로부터 다운로드 받은 공격 탐지 모델을 해당 저장소에 저장할 수 있다.

[0017] 또한, 상기 포그 노드는 상기 F-Env 목록에 상기 특징 정보 모음에 대응하는 F-Env가 존재하는 경우, 상기 공격 탐지 모델을 보유하고 있는지 판단하여 상기 공격 탐지 모델을 보유하고 있으면 상기 공격 탐지 모델을 연결된 엣지 노드에 전달하고, 상기 공격 탐지 모델을 보유하고 있지 않으면 상기 IPFS 환경에서 타 포그 노드들의 저장소를 검색하여 상기 공격 탐지 모델을 보유한 포그 노드로부터 상기 공격 탐지 모델을 다운로드 받아 상기 엣지 노드에 전달할 수 있다.

[0018] 또한, 상기 포그 노드는 상기 F-Env 목록에 상기 특징 정보 모음에 대응하는 F-Env가 존재하지 않는 경우, 상기 전달받은 특징 정보 모음을 이용하여 IoT 기기에 대한 공격 탐지를 위한 머신러닝 공격 탐지 모델과 F-Env를 생성하여 저장소에 저장하고, 상기 공격 탐지 모델을 연결된 엣지 노드에 전달할 수 있다.

[0019] 또한, 상기 포그 노드는 타 포그 노드들과의 합의 알고리즘에 의해 통과되면 상기 생성된 F-Env를 프라이빗 블록체인 네트워크상의 F-Env 목록에 추가시킬 수 있다.

[0020] 또한, 상기 엣지 노드는 상기 공격 탐지 모델을 해당 IoT 네트워크에서 적용하여 트래픽을 탐지하고, 탐지 결과에 따라 트래픽을 제한할 수 있다.

[0021] 또한, 본 발명의 다른 실시 예에 따른 도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 방법은, 제2 계층을 형성하는 엣지 노드가 제1 계층을 형성하는 엔드 노드를 통해 IoT 기기의 트래픽 데이터를 전달받는 단계; 상기 엣지 노드가 상기 트래픽 데이터를 이용하여 특징 정보 모음을 생성하고 생성된 특징 정보 모음을 제3 계층을 형성하는 포그 노드에 전달하는 단계; 상기 포그 노드가 블록체인 네트워크상의 F-Env(Feature-Environment) 목록에 상기 특징 정보 모음에 대응하는 F-Env가 존재하는지 판단하는 단계; 상기 판단 결과에 따른 IoT 기기에 대한 공격 탐지 모델을 상기 엣지 노드에 전달하는 단계; 및 상기 엣지 노드가 해당 IoT 네트워크에서 상기 공격 탐지 모델을 적용하는 단계를 포함한다.

발명의 효과

[0022] 이와 같이 본 발명에 따르면, 중앙으로 트래픽이 집중되어 전체적인 시스템의 성능이 저하되는 것을 방지하기 위해 엣지 컴퓨팅을 기반으로 다양성과 변동성이 높은 IoT 기기에 대한 공격 탐지 모델을 효율적으로 공유할 수

있다.

- [0023] 또한 본 발명에 따르면, 공격 탐지 모델을 지속적으로 생성 및 업데이트 하는 대신 블록체인 네트워크 상의 F-Env(Feature-Environment) 목록을 이용하여 적합한 모델을 검색하여 공유하고 이를 IoT 기기에 적용할 수 있도록 함으로써 모델을 훈련하여 업데이트해야 하는 부담을 경감시킬 수 있는 효과가 있다.
- [0024] 또한 본 발명에 따르면, IPFS(InterPlanetary File System) 환경을 기반으로 하여 같은 계층의 포그 노드 간에 공격 탐지 모델을 효율적으로 공유하도록 함으로써 비슷한 환경 간에 새로운 모델을 생성하거나 업데이트할 필요가 없으므로 효율성과 경량화를 동시에 달성하여 시스템 내에서 네트워크 및 컴퓨팅 자원을 절약할 수 있는 효과가 있다.
- [0025] 또한 본 발명에 따르면, 트래픽의 데이터 셋에 대해 일정 수준 이상의 정확도를 보장하도록 하며, 공격 탐지 모델을 계속 업데이트하는 과정에서 낭비되는 컴퓨팅 자원을 절약할 수 있도록 하는 효과가 있다.
- [0026] 또한 본 발명에 따르면, 새로 등록하고자 하는 포그 노드가 있으면, 프라이빗 블록체인 네트워크에서 인증받아 등록하고, 기존의 F-Env를 검색하여 필요한 공격 탐지 모델을 다운로드 받을 수 있기 때문에 기존의 환경에 빠르게 적응할 수 있는 효과가 있다.
- [0027] 또한 본 발명에 따르면, 트래픽의 데이터 셋에 대한 과적합(overfitting)을 줄여 같은 모델로도 일정 시간 네트워크 내에서 효율적으로 공격을 탐지할 수 있도록 하는 효과가 있다.
- [0028] 또한 본 발명에 따르면, 상대적으로 사용도가 떨어지는 공격 탐지 모델은 각 포그 노드에서 시간순으로 삭제되고, 삭제된 모델이 타 포그 노드에 존재하면 해당 공격 탐지 모델을 공유받을 수 있어 시스템 내에서 네트워크 및 컴퓨팅 자원을 절약할 수 있는 효과가 있다.
- [0029] 또한 본 발명에 따르면, 시스템의 보안과 더불어 경량화를 보장하므로 도시 컴퓨팅 환경뿐만 아니라, 전력 사용의 효율성이 중요한 가정 내부의 IoT 가전 환경 등에서도 효과적으로 적용할 수 있다.

도면의 간단한 설명

- [0030] 도 1은 본 발명의 실시 예에 따른 도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 시스템을 나타낸 시스템 구성도이다.
- 도 2는 도 1의 시스템에서 특징 정보 모음과 F-Env를 예시적으로 도시한 도면이다.
- 도 3은 본 발명의 실시 예에 따른 도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 방법의 동작 흐름을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0031] 이하 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시 예를 상세히 설명하기로 한다. 이 과정에서 도면에 도시된 선들의 두께나 구성요소의 크기 등은 설명의 명료성과 편의상 과장되게 도시되어 있을 수 있다.
- [0032] 또한 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서, 이는 사용자, 운용자의 의도 또는 관례에 따라 달라질 수 있다. 그러므로 이러한 용어들에 대한 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.
- [0033] 본 발명에 따른 실시 예를 설명하기에 앞서, 본 발명은 엣지 컴퓨팅(Edge Computing)과 포그 컴퓨팅(Fog Computing)을 기반으로 하며, 이때, 엣지 컴퓨팅은 중앙 집중 서버가 모든 데이터를 처리하는 클라우드 컴퓨팅(Cloud Computing)과 다르게 분산된 소형 서버를 통해 실시간으로 처리하는 기술을 일컫는다.
- [0034] 즉, 방대한 데이터를 중앙 집중 서버가 아닌 분산된 소형 서버를 통해 실시간으로 처리하는 기술이다. IoT 기기가 본격적으로 보급되면서 데이터 양이 폭증했고, 이 때문에 클라우드 컴퓨팅이 한계에 부딪히게 됐는데, 이를 보완하기 위해 엣지 컴퓨팅 기술이 개발됐다.
- [0035] 이러한 엣지 컴퓨팅 기술은 실시간으로 대응해야 하는 자율주행차, 스마트 팩토리, 가상현실 등 4차 산업혁명을 구현하는데 핵심적인 역할을 한다.
- [0036] 또한, 포그 컴퓨팅은 기존의 클라우드를 중심으로 한 중앙화된 네트워크 운영기법 대신 유저들에게 더 가까운 거리에서 클라우드와 같은 편의를 제공할 수 있는 가벼운 노드를 만들기 위해 개발된 방식이다. 포그 노드는 유

저와 가까운 거리에서 로컬 서비스 애플리케이션을 운영하게 된다.

- [0037] 포그 컴퓨팅은 IoT 환경에서 적은 지연과 실시간 통신이 가능한 환경을 제공하며, 기존의 클라우드 방식에서 크게 소모되었던 대역폭을 절약할 수 있다.
- [0039] 이하, 도면들을 참조하여 본 발명의 바람직한 실시예들을 보다 상세하게 설명하기로 한다.
- [0040] 먼저, 도 1 및 도 2를 통해 본 발명의 실시 예에 따른 도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 시스템에 대하여 설명한다.
- [0041] 도 1은 본 발명의 실시 예에 따른 도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 시스템을 나타낸 시스템 구성도이다.
- [0042] 도 1에서와 같이 본 발명의 실시 예에 따른 도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 시스템(1)은 제1 계층(10), 제2 계층(20) 및 제3 계층(30)을 포함한다.
- [0043] 먼저, 제1 계층(10)은 최하위 계층을 형성하고, IoT 기기(100)의 트래픽 데이터를 가지고 있는 복수의 엔드 노드를 포함한다.
- [0044] 즉, 제1 계층(10)은 실제 IoT 어플리케이션을 이용하는 사용자들의 계층이다.
- [0045] 따라서, 엔드 노드는 실제 트래픽 데이터를 가지고 있는 노드이며, 하나의 엣지 노드에 복수의 엔드 노드가 연결될 수 있다. 엔드 노드의 예로는 사용자의 태블릿, 스마트폰, 스마트 워치, 노트북 등일 수 있으며, 디바이스(device), 기구(apparatus), 단말(terminal), UE(user equipment), MS(mobile station), 무선기기(wireless device), 휴대기기(handheld device) 등 다른 용어로 불릴 수도 있다. 본 발명의 실시 예에서는 이와 같은 기기들을 통합하여 IoT 기기(100)로 지칭하기로 한다.
- [0046] IoT는 사물과 그에 부착된 센서를 통해 실시간으로 데이터를 주고받고 이용할 수 있는 기술이나 환경을 말한다. IoT 환경에 기반한 IoT 서비스는 인간의 조작이 필요하지 않고, 사물 간의 인터넷 통신과 정보 교환이 가능하다는 특징이 있다.
- [0047] 그리고 제2 계층(20)은 복수의 엣지 노드를 포함한다.
- [0048] 이때, 엣지 노드는 복수의 IoT 기기(100)들로 형성되는 복수의 그룹에 각각 연결되어 IoT 기기(100)들로부터 전달되는 트래픽 데이터를 이용하여 특징 정보 모음을 생성하여 전달한다.
- [0049] 자세히는, 엣지 노드와 연결된 엔드 노드를 통해 IoT 기기(100)들로부터 전달되는 트래픽 데이터로부터 트래픽 특징 정보를 수집하여 패킷의 크기와 프로토콜의 분포 정보를 산출하고, 산출한 패킷의 크기와 프로토콜의 분포 정보가 포함된 특징 정보 모음을 생성하여 엣지 노드와 연결된 포그 노드에 전달한다.
- [0050] 즉, 제2 계층(20)은 제1 계층(10)과 제3 계층(30)의 중간에 위치하는 계층으로, 제2 계층(20)에 포함된 엣지 노드는 IoT 기기(100)와 접촉하여 지나가는 수많은 패킷으로부터 트래픽 데이터를 수집한다. 이때, 트래픽 데이터는 여러 가지 특징 정보(Feature)로 이루어져 있으며, 엣지 노드는 이 특징 정보에서 패킷의 크기와 프로토콜의 분포 정보를 모아 최상위 계층을 형성하는 제3 계층(30)에 포함된 포그 노드에 전달한다.
- [0051] 또한, 엣지 노드는 연결된 포그 노드로부터 IoT 기기(100)에 대한 공격 탐지 모델을 전달받아 해당 IoT 네트워크에서 적용한다. 자세히는, 엣지 노드는 공격 탐지 모델을 해당 IoT 네트워크에서 적용하여 트래픽을 탐지하고, 탐지 결과에 따라 트래픽을 제한한다.
- [0052] 즉, 엣지 노드는 포그 노드로부터 전달받은 공격 탐지 모델을 직접 IoT 네트워크에서 적용하고, IoT 환경을 위협할 수 있는 트래픽을 제한하는 주체이다.
- [0053] 마지막으로 제3 계층(30)은 중앙 클라우드(Central Cloud)와 가장 가까운 최상위 계층을 형성하고, 각 엣지 노드에 연결되는 복수의 포그 노드를 포함한다.
- [0054] 따라서 제3 계층(30)에 포함된 포그 노드는 연결된 엣지 노드로부터 특징 정보 모음을 전달받아 블록체인 네트워크상의 F-Env(Feature-Environment) 목록에 특징 정보 모음에 대응하는 F-Env가 존재하는지 판단하고, 판단 결과에 따라 IoT 기기에 대한 공격 탐지 모델을 해당 엣지 노드에 전달한다.
- [0055] 자세히는, 포그 노드는 블록체인 네트워크상의 F-Env 목록에 해당 엣지 노드로부터 전달받은 특징 정보 모음에

대응하는 F-Env가 존재하는 경우, 자신이 공격 탐지 모델을 보유하고 있는지 판단한다.

- [0056] 판단 결과, 포그 노드는 자신이 해당 공격 탐지 모델을 보유하고 있으면 보유한 공격 탐지 모델을 연결된 엡지 노드에 전달한다.
- [0057] 만약, 포그 노드가 해당 공격 탐지 모델을 보유하고 있지 않으면 IPFS(InterPlanetary File System) 환경에서 타 포그 노드들의 저장소를 검색하여 공격 탐지 모델을 보유한 포그 노드로부터 공격 탐지 모델을 다운로드 받아 연결된 엡지 노드에 전달한다.
- [0058] 여기서, IPFS는 대용량 데이터를 탈 중앙화 네트워크에 공유할 수 있는 P2P (Peer-to-Peer) 분산 파일 시스템이다. 기존 HTTP(HyperText Transfer Protocol) 방식은 데이터가 위치한 곳의 주소를 찾아가서 원하는 콘텐츠를 가져오는 방식이었으나, IPFS는 중앙화 서버 없이 노드들의 P2P통신으로 대용량 파일을 여러 조각으로 나누어 가진다.
- [0059] 즉, IPFS는 본질적으로는 콘텐츠 어드레스 지정이 가능하고, 버전관리와 P2P 하이퍼미디어 구현이 가능한 분산 저장 및 전송 프로토콜이라고 할 수 있으며, 지난 30년간 사용해 온 HTTP, HTTP(HyperText Transfer Protocol Secure) 프로토콜을 보완 또는 대체함으로써 더욱 빠르고 안전하며 자유로운 인터넷 시대를 여는 것이 목표이다.
- [0060] 본 발명은 상술한 바와 같이 분산된 환경에서 암호학적 해쉬를 통한 콘텐츠 식별자를 이용하여 파일의 위치를 찾아 각 포그 노드 간의 파일 업로드와 다운로드를 지원하는 IPFS 환경을 기반으로 한다.
- [0061] 따라서, 각각의 포그 노드는 저장소를 포함하여 자신이 생성하거나 타 포그 노드로부터 다운로드 받은 공격 탐지 모델을 저장소에 저장할 수 있다.
- [0062] 또한, 사용도가 떨어지는 공격 탐지 모델은 이후 시간순으로 각 포그 노드에서 삭제되며, 삭제된 공격 탐지 모델이라도 IPFS 네트워크에서 공격 탐지 모델을 다운로드 받은 포그 노드가 존재한다면 다시 해당 공격 탐지 모델을 다운로드 할 수도 있어, 같은 계층의 포그 노드 간에 효율적으로 공유할 수 있고 시스템 내에서 네트워크 및 컴퓨팅 자원을 절약할 수도 있다.
- [0063] 또한, 포그 노드는 블록체인 네트워크상의 F-Env 목록에 해당 엡지 노드로부터 전달받은 특징 정보 모음에 대응하는 F-Env가 존재하지 않는 경우, 전달받은 특징 정보 모음을 이용하여 IoT 기기(100)에 대한 공격 탐지를 위한 머신러닝 공격 탐지 모델과 F-Env를 생성하여 자신의 저장소에 저장하고, 공격 탐지 모델을 연결된 엡지 노드에 전달한다.
- [0064] 이때, 포그 노드는 타 포그 노드들과의 합의 알고리즘에 의해 통과되면 새로 생성된 F-Env를 프라이빗 블록체인 네트워크상의 F-Env 목록에 추가시킬 수도 있다.
- [0065] 즉, 포그 노드는 자신이 생성한 F-Env에 대한 정보를 다른 포그 노드들과의 합의 알고리즘을 거쳐 프라이빗 블록체인 네트워크에 등록할 수도 있다.
- [0066] 여기서, 블록체인은 누구나 자유롭게 네트워크에 참여할 수 있는 퍼블릭 블록체인과 허가받은 사람만 네트워크에 참여할 수 있는 프라이빗 블록체인으로 나누어지며, 블록체인의 특징에 따라 PoW(Proof of Work), PoS(Proof of Stake), 또는 PBFT(Practical Byzantine Fault Tolerance) 등 다양한 합의 알고리즘을 사용하여 블록을 생성한다.
- [0067] 블록체인은 제3자가 아닌 참여자들의 합의를 통해 데이터가 검증되므로 데이터의 신뢰성이 보장되며, 모두가 같은 정보를 가지고 있으므로 무결성이 보장된다는 특징을 가지고 있다.
- [0068] 또한, 포그 노드는 연결된 엡지 노드로부터 전달받은 특징 정보 모음을 이용하여 패킷의 크기와 프로토콜의 종류별로 임의의 임계치가 설정된 F-Env를 생성하며, 생성된 F-Env를 블록체인 네트워크상의 F-Env 목록에 추가시킬 수도 있다.
- [0069] 도 2는 도 1의 시스템에서 특징 정보 모음과 F-Env를 예시적으로 도시한 도면이다.
- [0070] 도 2에서와 같이, 포그 노드는 엡지 노드로부터 전달받은 특징 정보 모음(도 2의 (a)에 해당)의 분포 정보를 토대로 네트워크에서 임의의 임계치를 설정하여 F-Env(도 2의 (b)에 해당)를 생성할 수도 있다.
- [0071] 이를 자세히 설명하자면, 포그 노드는 특징 정보 모음에 포함된 구성(도 2에는 프로토콜과 패킷의 크기만 예시함)별로 임의의 임계치를 설정하여 F-Env 정보를 생성할 수 있다. 도 2를 예로 들어 설명하자면, 프로토콜

(Protocol)의 종류별, 패킷의 크기(Size of Packet)별로 임의의 비중을 두어 F-Env 정보를 생성하여 생성된 F-Env를 블록체인 네트워크상의 F-Env 목록에 추가시킬 수도 있다.

- [0073] 이하에서는 도 3을 통해 본 발명의 실시 예에 따른 도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 방법에 대하여 설명한다.
- [0074] 도 3은 본 발명의 실시 예에 따른 도시 컴퓨팅 환경에서 엣지 컴퓨팅 기반의 공격 탐지 모델 공유 방법의 동작 흐름을 도시한 순서도로서, 이를 참조하여 본 발명의 구체적인 동작을 설명한다.
- [0075] 본 발명의 실시 예에 따르면, 엔드 노드는 IoT 기기(100)의 트래픽 데이터를 연결된 엣지 노드에 전달한다(S10).
- [0076] 자세히는, 제1 계층(10)을 형성하는 엔드 노드가 해당 엔드 노드와 연결된 엣지 노드를 통해 IoT 기기(100)의 트래픽 데이터를 전달한다. 이때, 엔드 노드는 복수개가 그룹핑되어 하나의 엣지 노드에 연결된다.
- [0077] 그 다음, 제2 계층(20)을 형성하는 엣지 노드가 엔드 노드를 통해 전달된 IoT 기기(100)의 트래픽 데이터를 수집한다(S20).
- [0078] 자세히는, 엣지 노드는 복수의 IoT 기기(100)들로 형성되는 복수의 그룹에 각각 연결되어 IoT 기기(100)들로부터 트래픽 데이터를 수집한다.
- [0079] 그 다음, 엣지 노드는 S20 단계에서 수집한 트래픽 데이터를 이용하여 특징 정보 모음을 생성한다(S30).
- [0080] 그리고 엣지 노드는 S30 단계에서 생성된 특징 정보 모음을 제3 계층(30)에 포함된 포그 노드에 전달한다(S40).
- [0081] 자세히는, 트래픽 데이터를 통해 트래픽 특징 정보를 수집하여 패킷의 크기와 프로토콜의 분포 정보를 산출하고, 산출한 패킷의 크기와 프로토콜의 분포 정보가 포함된 특징 정보 모음을 생성하여 엣지 노드에 연결된 포그 노드에 전달한다.
- [0082] 그 다음, 제3 계층(30)을 형성하는 포그 노드는 블록체인 네트워크상의 F-Env(Feature-Environment) 목록에 특징 정보 모음에 대응하는 F-Env가 존재하는지 판단한다(S50).
- [0083] 이때, 제3 계층(30)은 중앙 클라우드(Central Cloud)와 가장 가까운 최상위 계층을 형성하고, 각 엣지 노드에 연결되는 복수의 포그 노드를 포함한다.
- [0084] S50 단계의 판단 결과, F-Env 목록에 특징 정보 모음에 대응하는 F-Env가 존재하지 않는 경우, 포그 노드는 전달받은 특징 정보 모음을 이용하여 IoT 기기(100)에 대한 공격 탐지를 위한 머신러닝 공격 탐지 모델과 F-Env를 생성한다(S51).
- [0085] 이때, 포그 노드는 생성된 공격 탐지 모델과 F-Env를 자신의 저장소에 저장하고, 공격 탐지 모델을 연결된 엣지 노드에 전달할 수도 있다.
- [0086] 또한, 포그 노드는 타 포그 노드들과의 합의 알고리즘에 의해 통과되면 새로 생성된 F-Env를 프라이빗 블록체인 네트워크상의 F-Env 목록에 추가시킬 수도 있다.
- [0087] 즉, 포그 노드는 자신이 생성한 F-Env에 대한 정보를 다른 포그 노드들과의 합의 알고리즘을 거쳐 프라이빗 블록체인 네트워크에 등록할 수도 있다.
- [0088] S50 단계의 판단 결과, F-Env 목록에 특징 정보 모음에 대응하는 F-Env가 존재하는 경우, 포그 노드는 자신이 공격 탐지 모델을 보유하고 있는지 판단한다(S60).
- [0089] S60 단계의 판단 결과, 포그 노드가 공격 탐지 모델을 보유하고 있지 않으면 IPFS 환경에서 타 포그 노드들의 저장소를 검색한다(S61).
- [0090] 본 발명은 상술한 바와 같이 분산된 환경에서 암호학적 해쉬를 통한 콘텐츠 식별자를 이용하여 파일의 위치를 찾아 각 포그 노드 간의 파일 업로드와 다운로드를 지원하는 IPFS 환경을 기반으로 한다.
- [0091] 따라서, 각각의 포그 노드는 저장소를 포함하여 자신이 생성하거나 타 포그 노드로부터 다운로드 받은 공격 탐지 모델을 저장소에 저장할 수 있다.
- [0092] 그리고 포그 노드는 검색 결과에 따라 공격 탐지 모델을 보유한 포그 노드로부터 공격 탐지 모델을 다운로드 받

아 연결된 엣지 노드에 전달한다(S62).

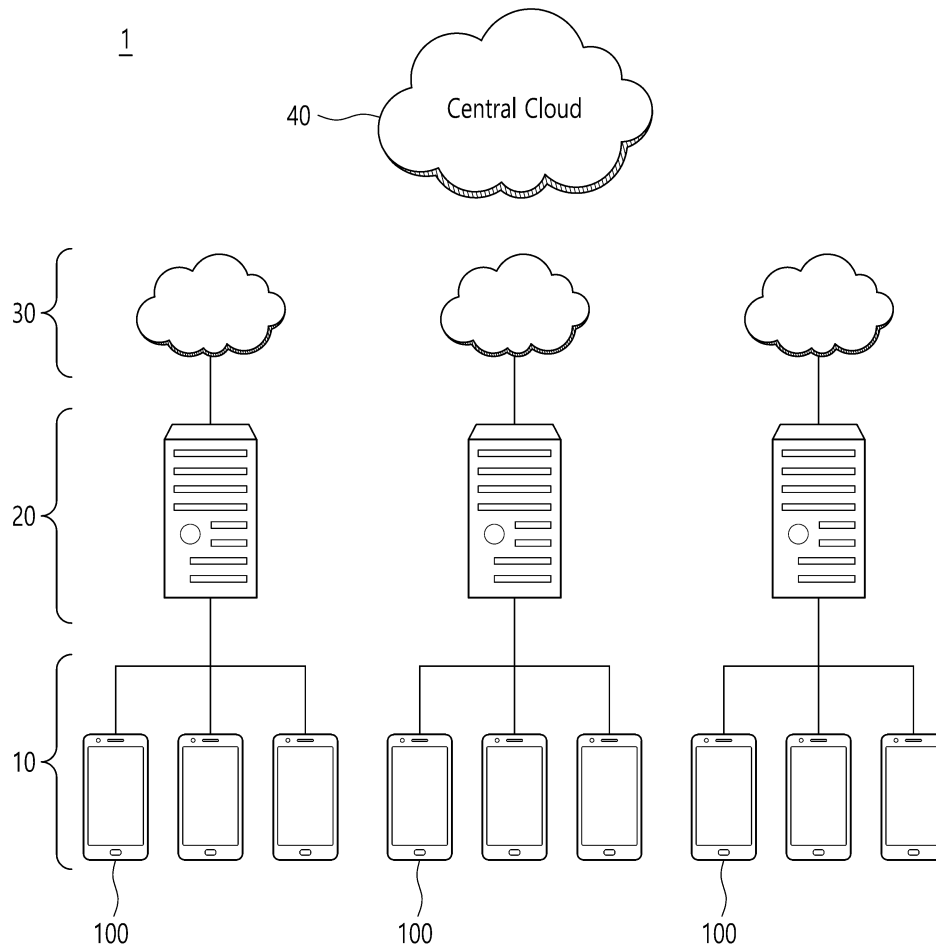
- [0093] S60 단계의 판단 결과, 포그 노드가 공격 탐지 모델을 보유하고 있으면 공격 탐지 모델을 연결된 엣지 노드에 전달한다(S70).
- [0094] 마지막으로, 엣지 노드가 포그 노드로부터 전달받은 공격 탐지 모델을 해당 IoT 네트워크에서 적용한다(S80).
- [0095] 즉, 엣지 노드는 연결된 포그 노드로부터 IoT 기기(100)에 대한 공격 탐지 모델을 전달받아 해당 IoT 네트워크에서 적용한다.
- [0096] 따라서 엣지 노드는 포그 노드로부터 전달받은 공격 탐지 모델을 직접 IoT 네트워크에서 적용하고, IoT 환경을 위협할 수 있는 트래픽을 제한하는 주체이다.
- [0097] 따라서, S80 단계에서 엣지 노드는 공격 탐지 모델을 해당 IoT 네트워크에서 적용하여 트래픽을 탐지하고, 탐지 결과에 따라 트래픽을 제한한다.
- [0098] 상술한 바와 같이, 본 발명의 실시 예에 따르면 중앙으로 트래픽이 집중되어 전체적인 시스템의 성능이 저하되는 것을 방지하기 위해 엣지 컴퓨팅을 기반으로 다양성과 변동성이 높은 IoT 기기에 대한 공격 탐지 모델을 효율적으로 공유할 수 있다.
- [0099] 또한 본 발명의 실시 예에 따르면, 공격 탐지 모델을 지속적으로 생성 및 업데이트 하는 대신 블록체인 네트워크 상의 F-Env(Feature-Environment) 목록을 이용하여 적합한 모델을 검색하여 공유하고 이를 IoT 기기에 적용할 수 있도록 함으로써 모델을 훈련하여 업데이트해야 하는 부담을 경감시킬 수 있다.
- [0100] 또한 본 발명의 실시 예에 따르면, IPFS(InterPlanetary File System) 환경을 기반으로 하여 같은 계층의 포그 노드 간에 공격 탐지 모델을 효율적으로 공유하도록 함으로써 비슷한 환경 간에 새로운 모델을 생성하거나 업데이트할 필요가 없으므로 효율성과 경량화를 동시에 달성하여 시스템 내에서 네트워크 및 컴퓨팅 자원을 절약할 수 있다.
- [0101] 또한 본 발명의 실시 예에 따르면, 트래픽의 데이터 셋에 대해 일정 수준 이상의 정확도를 보장하도록 하며, 공격 탐지 모델을 계속 업데이트하는 과정에서 낭비되는 컴퓨팅 자원을 절약할 수 있다.
- [0102] 또한 본 발명의 실시 예에 따르면, 새로 등록하고자 하는 포그 노드가 있으면, 프라이빗 블록체인 네트워크에서 인증받아 등록하고, 기존의 F-Env를 검색하여 필요한 공격 탐지 모델을 다운로드 받을 수 있기 때문에 기존의 환경에 빠르게 적응할 수 있다.
- [0103] 또한 본 발명의 실시 예에 따르면, 트래픽의 데이터 셋에 대한 과적합(overfitting)을 줄여 같은 모델로도 일정 시간 네트워크 내에서 효율적으로 공격을 탐지할 수 있다.
- [0104] 또한 본 발명의 실시 예에 따르면, 상대적으로 사용도가 떨어지는 공격 탐지 모델은 각 포그 노드에서 시간순으로 삭제되고, 삭제된 모델이 타 포그 노드에 존재하면 해당 공격 탐지 모델을 공유받을 수 있어 시스템 내에서 네트워크 및 컴퓨팅 자원을 절약할 수 있다.
- [0105] 또한 본 발명의 실시 예에 따르면, 시스템의 보안과 더불어 경량화를 보장하므로 도시 컴퓨팅 환경뿐만 아니라, 전력 사용의 효율성이 중요한 가정 내부의 IoT 가전 환경 등에서도 효과적으로 적용할 수 있다.
- [0106] 본 발명은 도면에 도시된 실시 예를 참고로 하여 설명되었으나 이는 예시적인 것에 불과하며, 당해 기술이 속하는 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서 본 발명의 진정한 기술적 보호범위는 아래의 특허청구범위의 기술적 사상에 의하여 정해져야 할 것이다.

부호의 설명

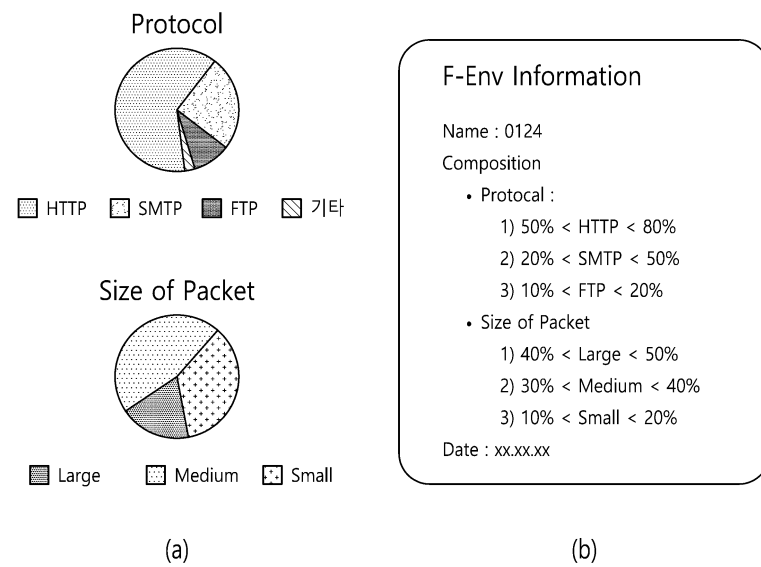
- [0107] 1 : 공격 탐지 모델 공유 시스템 10 : 제1 계층
20 : 제2 계층 30 : 제3 계층
40 : 중앙 클라우드 100 : IoT 기기

도면

도면1



도면2



도면3

