(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0017623
(43) 공개일자 2024년02월08일

(51) 국제특허분류(Int. Cl.)
G06N 20/20 (2019.01) *G06F 16/182* (2019.01)
H04L 9/00 (2022.01)
(52) CPC특허분류
G06N 20/20 (2021.08)
G06F 16/182 (2019.01)
(21) 출원번호 10-2022-0095552
(22) 출원일자 2022년08월01일
심사청구일자 2022년08월01일

(71) 출원인
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
도인실
인천광역시 연수구 센트럴로 194, 201동 1703호 (더샵센트럴파크2단지아파트)
김효원
경기도 수원시 장안구 천천로21번길 33, 613동 603호 청솔마을주공아파트
(74) 대리인
윤귀상

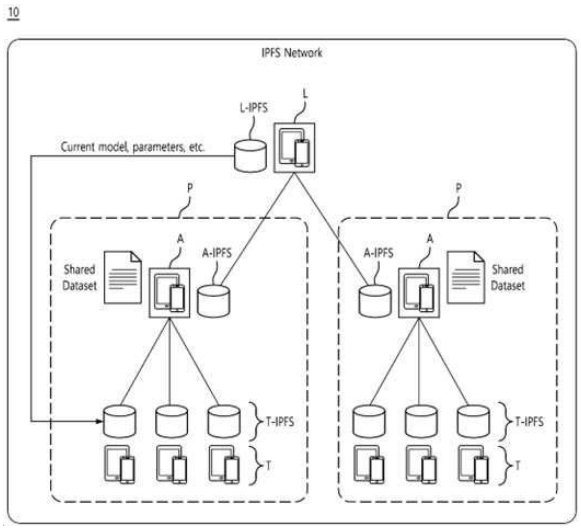
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **분산화된 연합학습 시스템 및 연합학습 방법**

(57) 요 약

본 발명은 분산화된 연합학습 시스템에 관한 것으로, 연합학습을 위한 프로젝트에 참가하여 로컬 모델을 생성하는 적어도 하나의 노드를 포함하는 참가 노드; 및 상기 로컬 모델의 파라미터에 기초하여 글로벌 모델을 생성하는 리더 노드를 포함하고, 상기 참가 노드 및 상기 리더 노드는 블록체인 네트워크 및 IPFS(Inter-Planetary File System) 네트워크를 구성하며, 상기 리더 노드는, 상기 로컬 모델을 생성하기 위한 현재 모델 및 상기 현재 모델의 파라미터를 포함하는 상기 프로젝트를 상기 IPFS 네트워크에 등록시켜 상기 참가 노드를 모집하고, 상기 글로벌 모델의 파라미터를 상기 IPFS 네트워크에 저장시킨다. 이에 의해 다양한 종류의 IoT 기기로 구성된 환경에서 사용자가 안전하고 효율적으로 연합학습에 참여할 수 있는 것은 물론, 데이터 포이즈닝 공격(Data Poisoning Attack)으로부터 데이터를 보호하여 데이터의 보안성 및 안정성을 향상시킬 수 있다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/50 (2022.05)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711154280
과제번호 2020R1A2C1006497
부처명 과학기술정보통신부
과제관리(전문)기관명 한국연구재단
연구사업명 개인기초연구(과기정통부)
연구과제명 UAV를 활용한 모바일 IoT 환경에서 효율적이고 안전한 노드 및 데이터 프라이버시 보장 기법
기 여 율 1/1
과제수행기관명 이화여자대학교
연구기간 2022.03.01 ~ 2023.02.28

명 세 서

청구범위

청구항 1

연합학습을 위한 프로젝트에 참가하여 로컬 모델을 생성하는 적어도 하나의 노드를 포함하는 참가 노드; 및

상기 로컬 모델의 파라미터에 기초하여 글로벌 모델을 생성하는 리더 노드를 포함하고,

상기 참가 노드 및 상기 리더 노드는 블록체인 네트워크 및 IPFS(Inter-Planetary File System) 네트워크를 구성하며,

상기 리더 노드는,

상기 로컬 모델을 생성하기 위한 현재 모델 및 상기 현재 모델의 파라미터를 포함하는 상기 프로젝트를 상기 IPFS 네트워크에 등록시켜 상기 참가 노드를 모집하고, 상기 글로벌 모델의 파라미터를 상기 IPFS 네트워크에 저장시키는 것을 특징으로 하는 분산화된 연합학습 시스템.

청구항 2

제1항에 있어서,

상기 참가 노드는,

상기 IPFS 네트워크로부터 상기 현재 모델 및 현재 모델의 파라미터를 저장하고, 로컬 데이터 세트에 기초하여 상기 현재 모델을 학습함으로써 상기 로컬 모델을 생성하는 학습 노드; 및

상기 로컬 모델의 파라미터 및 상기 로컬 데이터 세트를 집계(aggregates)하여 집계 데이터를 생성하고, 상기 집계 데이터를 상기 IPFS 네트워크에 저장시키는 집계 노드를 포함하고,

상기 리더 노드는,

상기 집계 데이터를 통해 상기 글로벌 모델을 생성하는 것을 특징으로 하는 분산화된 연합학습 시스템.

청구항 3

제2항에 있어서,

상기 학습 노드는,

상기 로컬 데이터 세트의 일부분에, 노이즈를 삽입하는 로컬 차등 프라이버시(LDP, Local Differential Privacy)를 적용시켜 LDP 데이터 세트를 생성하고, 상기 LDP 데이터 세트를 상기 IPFS 네트워크에 저장시키는 것을 특징으로 하는 분산화된 연합학습 시스템.

청구항 4

제3항에 있어서,

상기 집계 노드는,

상기 LDP 데이터 세트를 집계하여 공유 데이터 세트를 생성하고, 상기 집계 데이터에 상기 공유 데이터 세트가 포함되도록 하는 것을 특징으로 하는 분산화된 연합학습 시스템.

청구항 5

제4항에 있어서,

상기 집계 노드는,

상기 IPFS 네트워크에 포함된 다른 집계 노드에서 생성된 공유 데이터 세트를 공유하되, 상기 다른 집계 노드의 공유 데이터 세트와 자신의 공유 데이터 세트를 비교하여 교차 검증을 수행하고, 상기 교차 검증이 완료된 데이

터를 집계 데이터에 포함시키는 것을 특징으로 하는 분산화된 연합학습 시스템.

청구항 6

제2항에 있어서,

상기 참가 노드는,

상기 로컬 데이터 세트의 개수 또는 컴퓨팅 리소스의 정도에 따라 상기 학습 노드 또는 상기 집계 노드 중 하나로 결정되는 것을 특징으로 하는 연합학습 시스템.

청구항 7

제2항에 있어서,

상기 학습 노드는,

상기 글로벌 모델의 파라미터에 기초하여 상기 로컬 모델을 업데이트하는 것을 특징으로 하는 연합학습 시스템.

청구항 8

분산화된 연합학습 시스템에서의 연합학습 방법에 있어서,

상기 연합학습 시스템은, 블록체인 네트워크 및 IPFS 네트워크를 구성하는 학습 노드와 집계 노드를 포함하는 참가 노드 및 리더 노드를 포함하고,

상기 리더 노드가 연합학습을 위한 프로젝트를 상기 IPFS 네트워크에 등록시키고, 상기 프로젝트에 참가할 참가 노드를 모집하는 단계;

상기 참가 노드 중 학습 노드가 상기 IPFS 네트워크로부터 현재 모델 및 현재 모델의 파라미터를 저장하고, 로컬 데이터 세트에 기초하여 상기 현재 모델을 학습함으로써 상기 로컬 모델을 생성하는 단계;

상기 학습 노드가 상기 로컬 모델의 파라미터 및 상기 로컬 데이터 세트를 상기 IPFS 네트워크에 저장시키는 단계;

상기 참가 노드 중 상기 집계 노드가 상기 로컬 모델의 파라미터 및 상기 로컬 데이터 세트를 집계하여 집계 데이터를 생성하고, 상기 집계 데이터를 상기 IPFS 네트워크에 저장시키는 단계;

상기 리더 노드가 상기 집계 데이터를 통해 글로벌 모델을 생성하고, 상기 글로벌 모델의 파라미터를 상기 IPFS 네트워크에 저장시키는 단계; 및

상기 리더 노드가 상기 글로벌 모델의 정확도를 판단하는 단계를 포함하는 연합학습 방법.

청구항 9

제8항에 있어서,

상기 학습 노드가 상기 로컬 모델의 파라미터 및 상기 로컬 데이터 세트를 상기 IPFS 네트워크에 저장시키는 단계에서는,

상기 로컬 데이터 세트의 일부분에, 노이즈를 삽입하는 로컬 차등 프라이버시(LDP, Local Differential Privacy)를 적용시켜 LDP 데이터 세트를 생성하여 상기 IPFS 네트워크에 저장시키는 것을 특징으로 하는 연합학습 방법.

청구항 10

제9항에 있어서,

상기 집계 데이터를 상기 IPFS 네트워크에 저장시키는 단계에서는,

상기 집계 노드가 상기 LDP 데이터 세트를 집계하여 공유 데이터 세트를 생성하고, 상기 집계 데이터에 상기 공유 데이터 세트가 포함되도록 하는 것을 특징으로 하는 연합학습 방법.

청구항 11

제10항에 있어서,

상기 연합학습 방법은,

상기 집계 노드가 상기 IPFS 네트워크에 포함된 다른 집계 노드에서 생성된 공유 데이터 세트를 공유하되, 상기 다른 집계 노드의 공유 데이터 세트와 자신의 공유 데이터 세트를 비교하여 교차 검증을 수행하는 단계를 더 포함하고,

상기 집계 데이터를 상기 IPFS 네트워크에 저장시키는 단계에서는,

상기 교차 검증이 완료된 데이터를 집계 데이터에 포함시키는 것을 특징으로 하는 연합학습 방법.

청구항 12

제8항에 있어서,

상기 연합학습 방법은,

상기 로컬 데이터 세트의 개수 또는 컴퓨팅 리소스의 정도에 따라 상기 참가 노드를 상기 학습 노드 또는 상기 집계 노드 중 하나로 결정하는 단계를 더 포함하는 것을 특징으로 하는 연합학습 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 분산화된 연합학습 시스템 및 연합학습 방법에 관한 것으로, 보다 상세하게는 연합학습의 보안성 및 안정성을 향상시킬 수 있는 분산화된 연합학습 시스템 및 연합학습 방법에 관한 것이다.

배 경 기 술

[0002] 사람과 사물을 포함하여 모든 것이 네트워크로 연결되어 정보를 공유하는 환경인 IoE(Internet of Everything) 시대로 발전하면서 모든 데이터는 중요한 자원이 되고 있다.

[0003] 최근 스마트 도시를 이루는 도시 컴퓨팅 환경에서는 통신 기술의 발달을 기반으로 사물인터넷(Internet of Things, 이하 IoT) 기기의 수가 증가되며 매일 방대하고 다양한 종류의 데이터가 생성되고 있다. 여기서 IoT는 다양한 사물에 부착된 센서를 통해 실시간으로 데이터를 주고받을 수 있는 기술이나 환경을 의미할 수 있다.

[0004] 이러한 IoT 환경은 다양한 IoT 기기로 구성되어 있어 많은 데이터가 생성되며, IoT 기기에서 수집된 데이터가 다른 IoT 기기의 학습 데이터로 사용되는 순환 구조로 이루어져 있다. 따라서 해당 환경에서 데이터는 공유되는 자원이며 매우 중요한 요소이다.

[0005] 그리고 실시간으로 생성되는 이러한 방대한 양의 데이터를 효율적으로 사용하기 위해서는 적절한 처리가 필요하기 위해 머신러닝과 AI(Artificial intelligence)의 중요성 또한 증가되고 있다.

[0006] 하지만 머신러닝은 대체로 중앙 집중형으로서 서버가 모든 데이터를 가지고 있어야 한다는 점에서 보안적으로 한계가 있다. 이에 여러 디바이스가 각자의 데이터 세트를 가지고 학습하는 연합학습(Federate Learning)이 개개인의 프라이버시를 보장할 수 있는 방안으로 제시되었지만, 연합학습 또한 IoT 기기의 다양성 및 통신 환경의 불안정성을 보완해야 할 필요가 있다.

[0007] 구체적으로 기존의 중앙 집중식 연합학습은 중앙의 서버가 존재하고 사용자들은 자신의 데이터 세트를 통해 학습시킨 후 업데이트 값을 서버로 제출하게 된다. 이러한 연합학습 방식은 서버의 자원에 크게 의존한다는 한계가 있다.

[0008] 이를 해결하기 위해 분산형 연합학습이 연구되고 있지만, 분산형 연합학습에서는 일반적으로 IoT 기기 간의 성능 차이 때문에 특정 사용자들이 학습에 전혀 기여하지 못할 가능성이 존재한다는 문제가 있다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) 한국공개특허공보 제10-2021-0121915호

발명의 내용

해결하려는 과제

[0010] 본 발명은 상기와 같은 문제를 해결하기 위해 안출된 것으로, 본 발명의 목적은 다양한 종류의 IoT 기기로 구성된 환경에서 사용자가 안전하고 효율적으로 연합학습에 참여할 수 있는 것은 물론, 데이터 포이즈닝 공격(Data Poisoning Attack)으로부터 데이터를 보호하여 데이터의 보안성 및 안정성을 향상시킬 수 있는 분산화된 연합학습 시스템 및 연합학습 방법을 제공하는 것이다.

과제의 해결 수단

[0011] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 분산화된 연합학습 시스템은, 연합학습을 위한 프로젝트에 참가하여 로컬 모델을 생성하는 적어도 하나의 노드를 포함하는 참가 노드; 및 상기 로컬 모델의 파라미터에 기초하여 글로벌 모델을 생성하는 리더 노드를 포함하고, 상기 참가 노드 및 상기 리더 노드는 블록체인 네트워크 및 IPFS(Inter-Planetary File System) 네트워크를 구성하며, 상기 리더 노드는, 상기 로컬 모델을 생성하기 위한 현재 모델 및 상기 현재 모델의 파라미터를 포함하는 상기 프로젝트를 상기 IPFS 네트워크에 등록시켜 상기 참가 노드를 모집하고, 상기 글로벌 모델의 파라미터를 상기 IPFS 네트워크에 저장시킨다.

[0012] 그리고 상기 참가 노드는, 상기 IPFS 네트워크로부터 상기 현재 모델 및 현재 모델의 파라미터를 저장하고, 로컬 데이터 세트에 기초하여 상기 현재 모델을 학습함으로써 상기 로컬 모델을 생성하는 학습 노드; 및 상기 로컬 모델의 파라미터 및 상기 로컬 데이터 세트를 집계(aggregates)하여 집계 데이터를 생성하고, 상기 집계 데이터를 상기 IPFS 네트워크에 저장시키는 집계 노드를 포함하고, 상기 리더 노드는, 상기 집계 데이터를 통해 상기 글로벌 모델을 생성할 수 있다.

[0013] 또한 상기 학습 노드는, 상기 로컬 데이터 세트의 일부분에, 노이즈를 삽입하는 로컬 차등 프라이버시(LDP, Local Differential Privacy)를 적용시켜 LDP 데이터 세트를 생성하고, 상기 LDP 데이터 세트를 상기 IPFS 네트워크에 저장시킬 수 있다.

[0014] 그리고 상기 집계 노드는, 상기 LDP 데이터 세트를 집계하여 공유 데이터 세트를 생성하고, 상기 집계 데이터에 상기 공유 데이터 세트가 포함되도록 할 수 있다.

[0015] 또한 상기 집계 노드는, 상기 IPFS 네트워크에 포함된 다른 집계 노드에서 생성된 공유 데이터 세트를 공유하되, 상기 다른 집계 노드의 공유 데이터 세트와 자신의 공유 데이터 세트를 비교하여 교차 검증을 수행하고, 상기 교차 검증이 완료된 데이터를 집계 데이터에 포함시킬 수 있다.

[0016] 그리고 상기 참가 노드는, 상기 로컬 데이터 세트의 개수 또는 컴퓨팅 리소스의 정도에 따라 상기 학습 노드 또는 상기 집계 노드 중 하나로 결정될 수 있다.

[0017] 또한 상기 학습 노드는, 상기 글로벌 모델의 파라미터에 기초하여 상기 로컬 모델을 업데이트할 수 있다.

[0018] 한편, 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 분산화된 연합학습 시스템에서의 연합학습 방법은, 상기 연합학습 시스템은, 블록체인 네트워크 및 IPFS 네트워크를 구성하는 학습 노드와 집계 노드를 포함하는 참가 노드 및 리더 노드를 포함하고, 상기 리더 노드가 연합학습을 위한 프로젝트를 상기 IPFS 네트워크에 등록시키고, 상기 프로젝트에 참가할 참가 노드를 모집하는 단계; 상기 참가 노드 중 학습 노드가 상기 IPFS 네트워크로부터 현재 모델 및 현재 모델의 파라미터를 저장하고, 로컬 데이터 세트에 기초하여 상기 현재 모델을 학습함으로써 상기 로컬 모델을 생성하는 단계; 상기 학습 노드가 상기 로컬 모델의 파라미터 및 상기 로컬 데이터 세트를 상기 IPFS 네트워크에 저장시키는 단계; 상기 참가 노드 중 상기 집계 노드가 상기 로컬 모델의 파라미터 및 상기 로컬 데이터 세트를 집계하여 집계 데이터를 생성하고, 상기 집계 데이터를 상기 IPFS 네트워크에 저장시키는 단계; 상기 리더 노드가 상기 집계 데이터를 통해 글로벌 모델을 생성하고, 상기 글로벌 모델의 파라미터를 상기 IPFS 네트워크에 저장시키는 단계; 및 상기 리더 노드가 상기 글로벌 모델의 정확도를 판단하는 단계를 포함한다.

[0019] 그리고 상기 학습 노드가 상기 로컬 모델의 파라미터 및 상기 로컬 데이터 세트를 상기 IPFS 네트워크에 저장시키는 단계에서는, 상기 로컬 데이터 세트의 일부분에, 노이즈를 삽입하는 로컬 차등 프라이버시(LDP, Local

Differential Privacy)를 적용시켜 LDP 데이터 세트를 생성하고, 상기 LDP 데이터 세트를 상기 IPFS 네트워크에 저장시킬 수 있다.

[0020] 또한 상기 집계 데이터를 상기 IPFS 네트워크에 저장시키는 단계에서는, 상기 집계 노드가 상기 LDP 데이터 세트를 집계하여 공유 데이터 세트를 생성하고, 상기 집계 데이터에 상기 공유 데이터 세트가 포함되도록 할 수 있다.

[0021] 그리고 상기 연합학습 방법은, 상기 집계 노드가 상기 IPFS 네트워크에 포함된 다른 집계 노드에서 생성된 공유 데이터 세트를 공유하되, 상기 다른 집계 노드의 공유 데이터 세트와 자신의 공유 데이터 세트를 비교하여 교차 검증을 수행하는 단계를 더 포함하고, 상기 집계 데이터를 상기 IPFS 네트워크에 저장시키는 단계에서는, 상기 교차 검증이 완료된 데이터를 집계 데이터에 포함시킬 수 있다.

[0022] 또한 상기 연합학습 방법은, 상기 로컬 데이터 세트의 개수 또는 컴퓨팅 리소스의 정도에 따라 상기 참가 노드를 상기 학습 노드 또는 상기 집계 노드 중 하나로 결정하는 단계를 더 포함할 수 있다.

발명의 효과

[0023] 상술한 본 발명의 일측면에 따르면, 분산화된 연합학습 시스템 및 연합학습 방법을 제공함으로써, 다양한 종류의 IoT 기기로 구성된 환경에서 사용자가 안전하고 효율적으로 연합학습에 참여할 수 있는 것은 물론, 데이터 포이즈닝 공격(Data Poisoning Attack)으로부터 데이터를 보호하여 데이터의 보안성 및 안정성을 향상시킬 수 있다.

도면의 간단한 설명

[0024] 도 1은 본 발명의 일 실시예에 따른 연합학습 시스템을 설명하기 위한 도면,

도 2는 본 발명의 일 실시예에 따른 연합학습 시스템에서의 연합학습 방법을 설명하기 위한 흐름도,

도 3은 도 2의 연합학습 방법을 보다 구체적으로 설명하기 위한 도면, 그리고

도 4 및 도 5는 본 발명의 일 실시예에 따른 연합학습 시스템의 효과를 설명하기 위한 실험결과를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0025] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예와 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.

[0026] 본 발명에 따른 구성요소들은 물리적인 구분이 아니라 기능적인 구분에 의해서 정의되는 구성요소들로써 각각이 수행하는 기능들에 의해서 정의될 수 있다. 각각의 구성요소들은 하드웨어 또는 각각의 기능을 수행하는 프로그램 코드 및 프로세싱 유닛으로 구현될 수 있을 것이며, 두 개 이상의 구성요소의 기능이 하나의 구성요소에 포함되어 구현될 수도 있을 것이다. 따라서 이하의 실시예에서 구성요소에 부여되는 명칭은 각각의 구성요소를 물리적으로 구분하기 위한 것이 아니라 각각의 구성요소가 수행되는 대표적인 기능을 암시하기 위해서 부여된 것이며, 구성요소의 명칭에 의해서 본 발명의 기술적 사상이 한정되지 않는 것임에 유의하여야 한다.

[0027] 이하에서는 도면들을 참조하여 본 발명의 바람직한 실시예들을 보다 상세하게 설명하기로 한다.

[0028] 도 1은 본 발명의 일 실시예에 따른 연합학습 시스템(10)을 설명하기 위한 도면이다.

[0029] 본 발명의 연합학습 시스템(10, 이하 시스템)은 데이터 포이즈닝 공격을 방어하기 위해 악성 노드의 영향을 감소시키고, 중앙 집중식 연합학습에서 발생하는 통신 병목 문제를 해결할 수 있다.

[0030] 이를 위해 본 발명의 시스템(10)은 블록체인 네트워크 및 IPFS 네트워크에 기반하여 마련된다.

[0031] 블록체인은 ICT(Information & Communication Technology)의 핵심 기술 중 하나로, 차세대 네트워크 기술로 주목받고 있다. 블록체인이란 분산 데이터베이스의 일종으로 중앙 서버가 없으므로 모든 노드가 동등하다는 특징을 가진다.

[0032] 이러한 블록체인은 누구나 자유롭게 네트워크에 참여할 수 있는 퍼블릭 블록체인과 허가 받은 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.

[0033] 블록체인에서 데이터는 "블록"으로 불리며, 각 블록은 해시값을 통해 체인 형태로 연결되어 저장된다. 블록체인의 참여자들은 모든 거래 내용을 검증하고 보관하기 때문에, 만약 악의적인 사용자가 거래 내용을 수정한다고 하더라도 하나의 거래를 수정하기 위해 모든 참여자의 원장을 수정해야 한다.

[0034] 이에 블록체인은 제3자가 아닌 참여자들의 합의를 통해 데이터가 검증되므로 데이터의 신뢰성이 보장되며, 모두가 같은 정보를 가지고 있으므로 무결성이 보장된다는 특징을 가지고 있다.

[0035] 한편 IPFS(Inter-Planetary File System)는 상호 연결된 분산 파일 시스템으로 콘텐츠 자체가 주소 역할을 하는 content-addressing 방식을 사용한다. 이러한 IPFS를 활용하면 고용량의 파일을 빠르고 효율적으로 저장할 수 있다는 이점이 있으며, 무결성, 위조방지 및 탈중앙화의 효과를 얻을 수 있다. 이에 IPFS는 주로 블록체인에 담기에는 블록체인 네트워크에 업로드하기에는 용량이 데이터를 저장하는 오프체인 저장소의 역할을 할 수 있다.

[0036] 본 발명의 실시예에 따른 시스템(10)은 참가 노드(P) 및 리더 노드(L)를 포함하고, 참가 노드(P) 및 리더 노드(L)는 블록체인 네트워크 및 IPFS 네트워크를 구성할 수 있다.

[0037] 그리고 참가 노드(P) 및 리더 노드(L)의 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 기기로 지칭할 수 있다.

[0038] 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.

[0039] 이러한 참가 노드(P)는 리더 노드(L)가 연합학습을 위해 등록한 프로젝트에 참가하는 노드로써, 로컬 모델을 생성하는 적어도 하나의 노드를 포함할 수 있다.

[0040] 참가 노드(P)는 IPFS 네트워크에 등록되어 스웜 키(swarm key)를 공유하고, 공유한 스웜 키를 통해 IPFS 네트워크에 공유된 서로의 저장소에 접근할 수 있다.

[0041] 도 1에 도시된 바와 같이 참가 노드(P)는 학습 노드(T) 및 집계 노드(A)로 구성될 수 있는데, 참가 노드(P)에 포함되는 적어도 하나의 노드는 학습 노드(T) 또는 집계 노드(A) 중 하나로 결정된다. 구체적으로 참가 노드(P)에 포함되는 적어도 하나의 노드는, 자신이 수집하는 데이터인 로컬 데이터 세트의 개수 또는 컴퓨팅 리소스의 정도에 따라 학습 노드(T) 또는 집계 노드(A) 중 하나로 결정될 수 있다.

[0042] 학습 노드(T)는 프로젝트에 참가하는 노드로써 기존의 연합학습에서의 일반 참여자에 해당할 수 있다.

[0043] 본 발명에서의 학습 노드(T)는 IPFS 네트워크로부터 현재 모델(Current model) 및 현재 모델의 파라미터(parameters)를 저장하고, 현재 모델(Current model)을 로컬 데이터 세트에 기초하여 학습함으로써 로컬 모델을 생성할 수 있다.

[0044] 여기서 현재 모델(Current model)은, 로컬 모델을 생성하기 위한 학습 전 모델로써, 리더 노드(L)가 연합학습을 위한 프로젝트를 등록할 때 IPFS 네트워크에 저장시킨 초기 모델일 수도 있고, 리더 노드(L)가 연합학습을 수행하는 과정에서 업데이트한 글로벌 모델일 수도 있다.

[0045] 그리고 학습 노드(T)는 리더 노드(L)의 글로벌 모델의 파라미터에 기초하여 로컬 모델을 업데이트할 수 있다.

[0046] 학습 노드(T)가 다른 노드와 공유하는 로컬 데이터 세트의 양은 프로젝트마다 다를 수 있다.

[0047] 또한 본 발명의 실시예에 따른 학습 노드(T)는 로컬 데이터 세트의 일부에 로컬 차등 프라이버시(이하 LDP, Local Differential Privacy)를 적용시켜 LDP 데이터 세트를 생성할 수 있다.

[0048] 여기서 LDP는 로컬 데이트 세트에 적절한 노이즈를 삽입하여 사용자의 로컬 데이터 세트를 보호하는 방법이다. 일반적으로 IoT 센서에서 수집된 데이터 셋에서는 민감한 개인 정보가 포함될 가능성이 있으며, 로우(raw) 데이터를 공유하게 되면 개인 정보 문제가 발생할 수 있다.

[0049] 하지만 개인 정보 보호를 위해 데이터를 과도하게 가공하면 머신러닝 서비스 측면에서 데이터의 품질이 저하된다는 문제가 있다.

[0050] 이를 해결하기 위해 본 발명의 실시예에 따른 학습 노드(T)는 공유되는 데이터 세트의 정확성 향상 및 개인 정보 보호를 위해 LDP를 적용할 수 있다. 그리고 로컬 데이터 세트에 LDP 적용을 위한 파라미터는 리더 노드(L)가 프로젝트 등록 시 초기에 지정한 값의 범위 내에서 자유롭게 설정될 수 있다.

[0051] 또한 본 발명의 학습 노드(T)는 여러 쿼리를 수신할 때 더 효율적으로 개인 정보 보호를 보장할 수 있고 다양한 응용프로그램에 적합한 가우시안(Gaussian)에 기반한 LDP를 적용할 수 있다. 물론 LDP의 방식이 꼭 이에 한정되는 것은 아니며 라플라시안(Laplacian)과 같은 다른 모델을 사용할 수도 있다.

[0052] 그리고 각 학습 노드(T)들은 LDP 데이터 세트를 자체 IPFS 저장소인 학습 IPFS 저장소(T-IPFS)에 저장함으로써 LDP 데이터 세트를 IPFS 네트워크에 저장시킬 수 있다.

[0053] 이러한 방식을 통해 생성된 LDP 데이터 세트는 노드들과 공유될 수 있는데, LDP 데이터 세트는 차등 프라이버시 노이즈를 통해 보호되기 때문에 개인 정보를 추출할 수 없게 된다.

[0054] 그리고 학습 노드(T)는 로컬 모델의 파라미터도 IPFS 네트워크에 저장시켜 IPFS 네트워크를 구성하는 다른 노드들과 공유할 수 있다.

[0055] 이러한 학습 노드(T)를 포함하는 본 발명의 시스템(10)은 예상하지 못한 노드 이탈이 발생하더라도 다른 노드에 로컬 데이터 세트의 일부가 존재하고, 로컬 데이터 세트를 다운로드 하는데 문제가 없게 되므로, IPFS 네트워크에서 최소 중복성이 보장될 수 있다. 또한 통신 환경 문제나 네트워크 문제로 노드가 해당 프로젝트에서 나가더라도 인증을 받으면 다시 프로젝트에 참여할 수 있게 된다.

[0056] 한편 집계 노드(A)는 프로젝트에 참가하는 노드로써 IPFS 네트워크에서 로컬 데이터 세트 대신에 컴퓨팅 파워를 제공하는 노드일 수 있다. 즉, 집계 노드(A)는 IoT 환경에서 의미있는 데이터를 보유하지 않고도 자체 컴퓨팅 리소스를 활용할 수 있다.

[0057] 이러한 집계 노드(A)는 공유 데이터 세트를 생성하여 배포하고, 학습 노드(T)에서 생성된 로컬 모델의 파라미터를 검증하기 위해 마련될 수 있다.

[0058] 이를 위해 집계 노드(A)는 IPFS 네트워크에 저장된 로컬 모델의 파라미터 및 로컬 데이터 세트를 집계(aggregates)하여 집계 데이터를 생성할 수 있다. 다시 말해, 집계 노드(A)는 IPFS 네트워크에 분산된 여러 학습 노드(T)에서 제공하는 데이터를 다운로드하여 집계 데이터를 생성할 수 있다.

[0059] 그리고 집계 노드(A)는 집계 데이터를 자체 IPFS 저장소인 집계 IPFS 저장소(A-IPFS)에 저장함으로써 IPFS 네트워크에 저장시킬 수 있다.

[0060] 또한 집계 노드(A)는, 학습 노드(T)가 저장시킨 LDP 데이터 세트를 집계하여 공유 데이터 세트(Shared Dataset)를 생성하고, 집계 데이터에 공유 데이터 세트(Shared Dataset)가 포함되도록 할 수 있다.

[0061] 그리고 집계 노드(A)는 공유 데이터 세트(Shared Dataset)를 생성함에 있어, IPFS 네트워크에 있는 전체 학습 노드(T) 중 일정 비율에 해당하는 학습 노드(T)로부터 수집한 LDP 데이터 세트가 포함되도록 할 수 있다.

[0062] 예를 들어 일정 비율이 50%로 설정된다면, 집계 노드(A)는 IPFS 네트워크에 존재하는 모든 학습 노드(T)의 50%에 해당하는 학습 노드(T)로부터 수집한 LDP 데이터 세트를 다운로드하여 공유 데이터 세트(Shared Dataset)를 생성할 수 있다.

[0063] 여기서 일정 비율은, IPFS 네트워크 상에 존재하는 모든 악성 노드가 집계 노드(A)와 결합되었더라도 생성된 공유 데이터 세트에는 양성 노드로부터 집계된 로컬 데이터 세트가 대부분을 차지할 수 있도록 하는 비율일 수 있다. 즉, 50% 이상의 학습 노드(T)에 의해 공유 데이터 세트가 생성되면, IPFS 네트워크의 모든 악성 노드가 해당 집계 노드(A)와 결합되었더라도 해당 집계 노드(A)에서 생성한 공유 데이터 세트에는 양성 노드로부터 집계

된 로컬 데이터 세트가 대부분을 차지할 수 있음을 의미한다. 상술한 일정 비율은 설명의 편의를 위한 예시적 사항에 불과하며, 얼마든지 변경 가능하다.

[0064] 구체적으로 집계 노드(A)에서 수행되는 집계 과정에 대해 설명하기로 한다.

[0065] 총 K개의 학습 노드(T)가 있다고 가정하고, F_k를 학습 노드(T) k의 로컬 파라미터로 가정하면 집계 노드(A)의 집계에 영향을 미치는 계수를 계산하기 위한 본 발명에서의 메커니즘은 수학식 1과 같을 수 있다.

[0066] [수학식 1]

[0067] $$F_k / 1 + 2 + 3 + \cdots + K$$

[0068] 모든 악성 노드가 집계에 참여하는 경우 이상적으로 악성 노드의 영향력은 (1+2+쪈+2/K)/K이므로 이 방정식을 간단히 확장하면 $((\frac{2}{K})^2 + 1)/K$ 가 될 수 있다.

[0069] 따라서 IPFS 네트워크의 노드 수가 증가할수록 악성 노드는 영향력을 잃게 되며, 노드 수가 증가하더라도 안정적인 네트워크를 유지할 수 있다.

[0070] 또한 집계 노드(A)는, IPFS 네트워크에 포함된 다른 집계 노드에서 생성된 공유 데이터 세트(Shared Dataset)를 공유하되, 다른 집계 노드의 공유 데이터 세트와 자신의 공유 데이터 세트를 비교하여 교차 검증을 수행하고 교차 검증이 완료된 데이터를 집계 데이터에 포함시킬 수 있다.

[0071] 구체적으로 집계 노드(A)는 도 1에 도시된 바와 같이 한 프로젝트 내에서 2개 이상 존재할 수 있다. 그리고 집계 노드(A)들은 서로 P2P 통신을 통해 최종적으로 생성된 공유 데이터 세트(Shared Dataset)를 포함하는 집계 데이터를 비교하고, 그 결과를 리더 노드(L)에서 확인하도록 할 수 있다. 다시 말해 두 집계 노드(A)는 서로의 정당성을 확인할 수 있다.

[0072] 한편, 리더 노드(L)는 연합학습의 총 책임자이며, 참가 노드(P)에서 생성된 로컬 모델의 파라미터에 기초하여 글로벌 모델을 생성할 수 있다. 구체적으로는 리더 노드(L)는 집계 노드(A)에서 생성한 집계 데이터를 통해 글로벌 모델을 생성할 수 있다.

[0073] 또한 리더 노드(L)는, 연합학습을 위한 프로젝트를 IPFS 네트워크에 등록시켜 참가 노드(P)를 모집할 수 있으며, 참가 노드(P)의 모집은 브로드캐스팅을 통해 이루어질 수 있다.

[0074] 그리고 프로젝트에는 참가 노드(P)에서 로컬 모델을 생성하기 위한 현재 모델(Current model), 현재 모델의 파라미터(parameters), 프로젝트에 참가가능한 참가 노드(P)의 최대 수, 참가 노드(P) 내에서의 학습 노드(T) 및 집계 노드(A)의 비율, 학습 노드(T)로 참여가능한 조건 등이 설정될 수 있다.

[0075] 그리고 리더 노드(L)는 글로벌 모델의 파라미터를 IPFS 네트워크에 저장시킬 수 있다. 다시 말해 리더 노드(L)는 글로벌 모델의 파라미터를 자체 IPFS 저장소인 리더 IPFS 저장소(L-IPFS)에 저장할 수 있다.

[0076] 또한 본 발명의 실시예에 따른 리더 노드(L)는 자신을 세미 집계 노드로 선택하여 학습에 참여할 수도 있다.

[0077] 이를 통해 만약 모든 집계 노드(A)가 악성 노드라고 할지라도 악성 노드는 리더 노드(L)에 의해 차단될 수 있다. 즉, 리더 노드(L)가 세미 집계 노드로써 학습에 참여하게 되면 리더 노드(L)는 집계 노드(A) 간에 서로 다른 이상한 집계 데이터를 발견할 수 있다. 즉 본 발명의 리더 노드(L)는 프로젝트의 옵저버로 참여할 수 있다.

[0078] 따라서 상술한 학습 노드(T), 집계 노드(A) 및 리더 노드(L)를 포함하는 본 발명의 실시예에 따른 시스템(10)의 장점은 효율적인 연합학습을 위해 참가 노드(P)가 자신의 능력에 맞는 역할을 수행하면서 개인 정보가 보호된 학습에서 자신의 분산 데이터를 사용할 수 있다는 점이다.

[0079] 예를 들어 양질의 로컬 데이터 세트를 가진 노드는 학습 노드(T)로써 프로젝트에 참가할 수 있고, 적절한 로컬 데이터 세트를 가지지 못한 노드는 집계 노드(A)로써 프로젝트에 참가할 수 있다.

[0080] 또한 본 발명의 실시예에 따른 시스템(10)은 LDP가 적용된 로컬 데이터 세트를 공유 데이터 세트에 적용하므로 집계 노드는 해당 로컬 데이터 세트가 어느 노드에 속하는지를 구별하기 어렵기 때문에 개인 정보를 보호할 수 있다.

[0081] 그리고 본 발명의 실시예에 따른 시스템(10)은 LDP 로컬 데이터 세트를 이용하여 공유 데이터 세트를 생성하므로 다양한 IoT 기기가 노드로 구성되는 연합학습에서 발생하는 non-IID 문제를 완화할 수 있다.

[0082] 특히 본 발명의 실시예에 따른 시스템(10)은, 한 세션에서 빠르게 훈련을 마친 노드의 값을 더하기 때문에 IoT 기기간의 성능 격차로 인해 학습에 참여하지 않거나 인센티브를 받지 못하는 클라이언트가 있을 수 있는 기존의 집계 방식의 문제를 해결할 수 있다.

[0084] 도 2는 본 발명의 일 실시예에 따른 연합학습 시스템(10)에서의 연합학습 방법을 설명하기 위한 흐름도로써, 본 발명의 일 실시예에 따른 연합학습 방법은 도 1에 도시된 연합학습 시스템(10)과 실질적으로 동일한 구성 상에서 진행되므로, 도1의 연합학습 시스템(10)과 동일한 구성요소에 대해 동일한 도면 부호를 부여하고, 반복되는 설명은 생략하기로 한다.

[0085] 본 발명의 연합학습 시스템(10)은, 블록체인 네트워크 및 IPFS 네트워크를 구성하는 학습 노드(T)와 집계 노드(A)를 포함하는 참가 노드(P) 및 리더 노드(L)를 포함할 수 있다.

[0086] 그리고 리더 노드(L)가 연합학습을 위한 프로젝트를 IPFS 네트워크에 등록시키고, 프로젝트에 참가할 참가 노드(P)를 모집한다(S110).

[0087] 참가 노드(P) 중 학습 노드가 IPFS 네트워크로부터 현재 모델(Current model) 및 현재 모델의 파라미터(parameters)를 저장하고, 로컬 데이터 세트에 기초하여 현재 모델(Current model)을 학습함으로써 로컬 모델을 생성할 수 있다(S120).

[0088] 그리고나서 학습 노드(T)가 로컬 모델의 파라미터 및 로컬 데이터 세트를 IPFS 네트워크에 저장시킬 수 있다(S130).

[0089] 이러한 학습 노드가 상기 로컬 모델의 파라미터 및 상기 로컬 데이터 세트를 상기 IPFS 네트워크에 저장시키는 단계(S130)에서는, 로컬 데이터 세트의 일부분에, 노이즈를 삽입하는 로컬 차등 프라이버시(LDP, Local Differential Privacy)를 적용시켜 LDP 데이터 세트를 생성하고, LDP 데이터 세트를 IPFS 네트워크에 저장시킬 수 있다.

[0090] 이후 참가 노드(P) 중 집계 노드(A)가 로컬 모델의 파라미터 및 로컬 데이터 세트를 집계하여 집계 데이터를 생성하고, 집계 데이터를 IPFS 네트워크에 저장시킬 수 있다(S140).

[0091] 여기서 집계 데이터는, LDP 데이터 세트를 집계하여 생성될 수 있다.

[0092] 그리고 집계 데이터를 IPFS 네트워크에 저장시키는 단계(S140)에서는, 집계 노드(A)가 LDP 데이터 세트를 집계하여 공유 데이터 세트(Shared Dataset)를 생성하고, 집계 데이터에 공유 데이터 세트(Shared Dataset)가 포함되도록 할 수 있다.

[0093] 그리고 리더 노드(L)가 집계 데이터를 통해 글로벌 모델을 생성하고, 글로벌 모델의 파라미터를 IPFS 네트워크에 저장시킬 수 있다(S150).

[0094] 이후 리더 노드가 글로벌 모델의 정확도를 판단할 수 있다(S160).

[0095] 또한 본 발명의 실시예에 따른 연합학습 방법은, 집계 노드(A)가 IPFS 네트워크에 포함된 다른 집계 노드에서 생성된 공유 데이터 세트(Shared Dataset)를 공유하되, 다른 집계 노드의 공유 데이터 세트(Shared Dataset)와 자신의 공유 데이터 세트(Shared Dataset)를 비교하여 교차 검증을 수행하는 단계를 더 포함할 수 있다.

[0096] 이에 상술한 집계 데이터를 IPFS 네트워크에 저장시키는 단계(S140)에서는, 교차 검증이 완료된 데이터를 집계 데이터에 포함시킬 수 있다.

[0097] 그리고 본 발명의 실시예에 따른 연합학습 방법은, 로컬 데이터 세트의 개수 또는 컴퓨팅 리소스의 정도에 따라 참가 노드(P)를 학습 노드(T) 또는 집계 노드(A) 중 하나로 결정하는 단계를 더 포함할 수 있다. 이러한 참가 노드(P)를 학습 노드(T) 또는 집계 노드(A) 중 하나로 결정하는 단계는 참가 노드(P)를 모집하는 단계(S110) 이후에 수행될 수 있다.

[0098] 도 3은 도 2의 연합학습 방법을 보다 구체적으로 설명하기 위한 도면이다.

[0099] 먼저 다양한 노드들이 블록체인 네트워크를 구성한다(S210).

[0100] 따라서 시스템(10)을 구성하는 리더 노드(L), 학습 노드(T) 및 집계 노드(A)는 연합학습에 참여하고자 하는 노드들로써 블록체인 네트워크에 자신을 사전에 인증이 완료된 노드들이다.

[0101] 연합 학습의 초기에 블록체인 네트워크에 속한 노드 중 하나로써, 리더 노드(L)는 프로젝트를 등록할 수 있다(S220).

[0102] 리더 노드(L)는 블록체인 네트워크에 속한 노드 중에서 프로젝트에 참가할 노드를 브로드캐스팅을 통해 모집할 수 있다.

[0103] 이후 브로드캐스팅을 통해 모집된 참가 노드(P)가 프로젝트에 참가할 수 있다(S230)

[0104] 그리고 IPFS 네트워크를 위해 IPFS 라이브러리에는 스웜 키가 마련되는데, 각 스웜 키는 동일한 프로젝트에 참여하는 참가 노드(P)들이 공유할 수 있다(S240). 구체적으로 참가 노드(P)들이 공유하는 단계(S240)에서는 프로젝트에 참가할 참가 노드(P)의 모집이 완료되면, 스웜 키는 해당 프로젝트에 참여하여 IPFS 네트워크에 액세스할 수 있는 각 참가 노드(P)에 저장될 수 있다. 따라서 프로젝트에 참여하는 참가 노드(P)는 블록체인 네트워크와 IPFS 네트워크를 통한 인증을 통해 연합학습의 참가자로써 참여할 수 있게 된다.

[0105] 그리고 스웜 키가 저장된 참가 노드(P)는 서로의 저장소에 접근할 수 있는 것은 물론, IPFS 네트워크에서 로컬 데이터 세트를 배포하고 저장할 수도 있다. 만약 IPFS 네트워크를 떠나는 노드가 있다면 리더 노드(L)는 다시 스웜 키를 생성하여 리더 IPFS 저장소(L-IPFS)에 저장하고 브로드캐스트 메시지를 모든 노드로 라우팅할 수 있다.

[0106] 그러면 프로젝트에 참여하는 다른 학습 노드(T) 또는 집계 노드(A)는 다시 리더 노드(L)의 리더 IPFS 저장소(L-IPFS)에 접근하여 스웜 키를 받아올 수 있고, 받아온 스웜 키는 해당 IPFS 네트워크를 떠나는 노드가 발생할 때까지 유지될 수 있다.

[0107] 그리고 스웜 키를 공유한 참가 노드들 각각은 학습 노드(T) 또는 집계 노드(A) 중 하나로 결정될 수 있다(S250).

[0108] 만약 학습 노드(T)로 결정되면(S250-예), 학습 노드(T)는 LDP가 적용된 로컬 데이터 세트를 학습 IPFS 저장소(T-IPFS)에 저장하여 IPFS 네트워크에 저장시킬 수 있다(S260)

[0109] 그리고 학습 노드(T)는 IPFS 네트워크로부터 현재 모델(Current model) 및 현재 모델의 파라미터(parameters)를 저장할 수 있다(S270).

[0110] 이후 학습 노드(T)는 로컬 데이터 세트로 현재 모델(Current model)을 학습하여 로컬 모델을 생성할 수 있다(S280).

[0111] 그리고 학습 노드(T)는 로컬 모델의 파라미터를 학습 IPFS 저장소(T-IPFS)에 저장하여 IPFS 네트워크에 저장시킬 수 있다(S290).

[0112] 반면, 참가 노드(P)가 집계 노드(A)로 결정되면(S250-아니오), 집계 노드(A)는 IPFS 네트워크에서 학습 노드(T)의 로컬 데이터 세트를 검색할 수 있다.

[0113] 그리고 나서 집계 노드(A)는 로컬 데이터 세트를 집계하여 공유 데이터 세트(Shared Dataset)를 생성할 수 있다(S310).

[0114] 그리고 집계 노드(A)는 학습 노드(T)의 로컬 모델의 파라미터를 IPFS 네트워크로부터 다운로드하여 집계할 수 있다(S320).

[0115] 이후 집계 노드(A)는 공유 데이터 세트(Shared Dataset)와 집계된 로컬 모델의 파라미터를 집계 데이터로써 집계 IPFS 저장소(A-IPFS)에 저장하여 IPFS 네트워크에 저장시킬 수 있다.

[0116] 리더 노드(L)는 주기적으로 집계 노드(A)의 집계 IPFS 저장소(A-IPFS)에서 로컬 모델의 파라미터를 확인하고, 로컬 모델의 파라미터에 기초하여 글로벌 모델을 생성하고, 글로벌 모델의 파라미터를 저장할 수 있다(S340).

[0117] 그리고 리더 노드(L)는 글로벌 모델의 정확도가 이상적인 정확도인지 판단(S350)하고, 이상적인 정확도에 도달하지 못한 것으로 판단되면(S350-아니오), 학습 노드(T)가 현재 모델(Current model) 및 현재 모델의 파라미터(parameters)를 저장하는 단계(S270)로 회귀할 수 있다. 이때 학습 노드(T)가 저장하게 되는 현재 모델(Current model)은 업데이트된 글로벌 모델이며, 현재 모델의 파라미터는 업데이트된 글로벌 모델의 파라미터이다.

[0118] 반면 이상적인 정확도에 도달한 것으로 판단되면(S350-예), 종료할 수 있다.

[0120] 한편 도 4 및 도 5는 본 발명의 일 실시예에 따른 연합학습 시스템(10)의 효과를 설명하기 위한 실험결과를 도시한 도면이다.

[0121] 성능 및 개인정보 분석을 위해 python 환경에서 몇 가지 시나리오를 시뮬레이션 하였다. 그리고 CNN 모델을 통해 MNIST 이미지를 분류하였으며, MNIST 데이터 세트는 머신 러닝 실험에서 자주 사용되는 데이터 세트이다. 실제 시나리오에서는 학습을 위한 모든 모델이 통합되는 것은 물론이고, 프로젝트를 설정하고자 하는 회사, 조직 또는 개인이 연합학습을 개시하게 된다.

[0122] Python 코드로 연합학습을 구현하는 오픈 소스 코드를 사용하였으며, 구현된 메커니즘은 미니 유효성 검사 세트(공유 데이터 세트)와 공유 데이터 세트에서 높은 정확도를 얻은 노드를 집계 단계에서 유리하게 만들었다. 그리고 각 클라이언트 학습 세션의 에폭(epoch) 및 배치(batch)는 각 10으로 설정되었다.

[0123] MNIST 데이터 세트로 테스트하여 기존 집계 함수의 정확도를 악의적인 사용자가 제시하는 환경에서 생성한 함수와 비교하였다. 이 시나리오에서는 데이터 포이즈닝 공격을 테스트하기 위해 전체 네트워크 노드의 20%가 악성 노드인 것으로 가정한다. 참가 인원은 1,000명이고 각 학습 세션마다 고객 100명을 무작위로 선발한다. 악성 노드의 경우 데이터 세트의 레이블을 의도적으로 조작하여 불량 데이터 세트를 만들었다.

[0124] 본 발명의 실시예에 따른 시스템(10)은 악성 노드가 학습 세션에 미치는 영향을 효율적으로 억제하고 정확도를 유지하였다. 구체적으로 도 4는 본 발명의 시스템(10)이 악의적인 상황에서 정확성을 원활하게 유지하여 약 95%의 정확도를 획득했음을 보여준다.

[0125] 한편 도 5는 악성 노드의 수가 0%와 20%인 환경을 추가로 시뮬레이션한 결과로써, 20% 환경에서는 안정성이 떨어지긴 했지만 정확도가 높아지면서 결국 수렴이 가능했음을 알 수 있다.

[0126] 또한 공유 데이터 세트를 IPFS 네트워크에 저장하는 과정에서 개인정보 문제가 발생할 수 있는데, 이때 가우시안 차등 프라이버시를 사용하여 전송하는 로컬 데이터 세트에 노이즈를 추가하였다. 개인에 대한 메타데이터도 노드의 익명성을 위해 암호화하였다. 그리고 공유 데이터 세트의 개인 정보를 분석한 결과, 통해 로컬 데이터 세트를 수집하여 공유 데이터 세트를 생성할 때 집계 노드(A)는 개인의 개인정보를 알 수 없으며 공유 데이터 세트에서 개인을 추측할 수 없음을 확인하였다.

[0127] 이와 같은 본 발명의 연합학습 방법은 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다.

[0128] 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다.

[0129] 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD 와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다.

[0130] 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0131] 이상에서는 본 발명의 다양한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어져서는 안될 것이다.

부호의 설명

[0132] 10 : 연합학습 시스템 L : 리더 노드

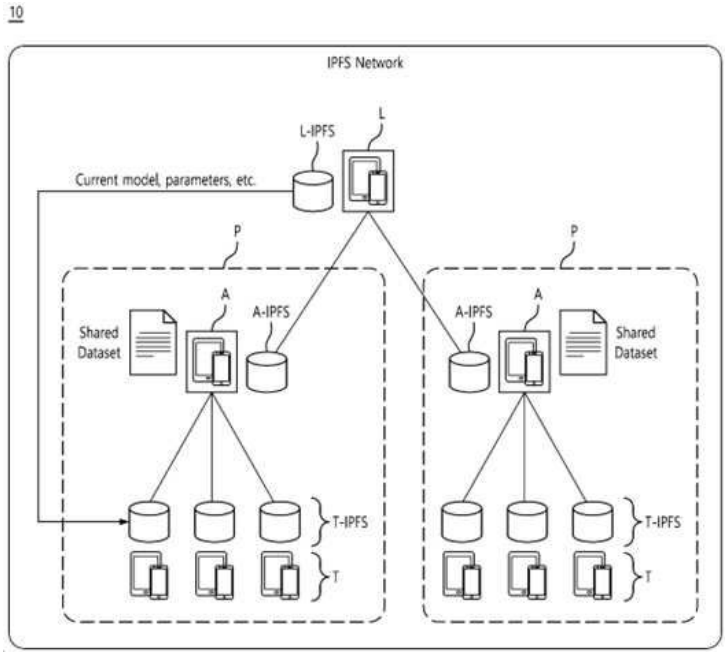
L-IPFS : 리더 IPFS 저장소 P : 참가 노드

A : 집계 노드 A-IPFS : 집계 IPFS 저장소

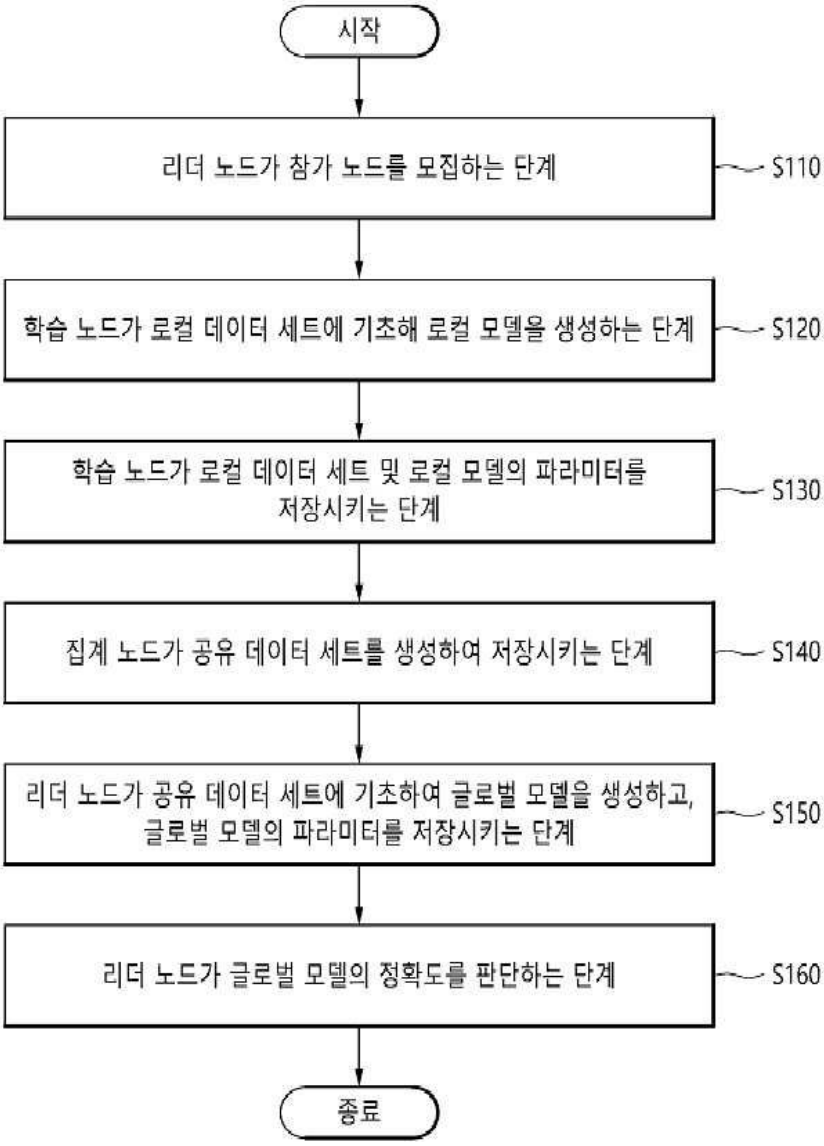
T : 학습 노드 T-IPFS : 학습 IPFS 저장소

도면

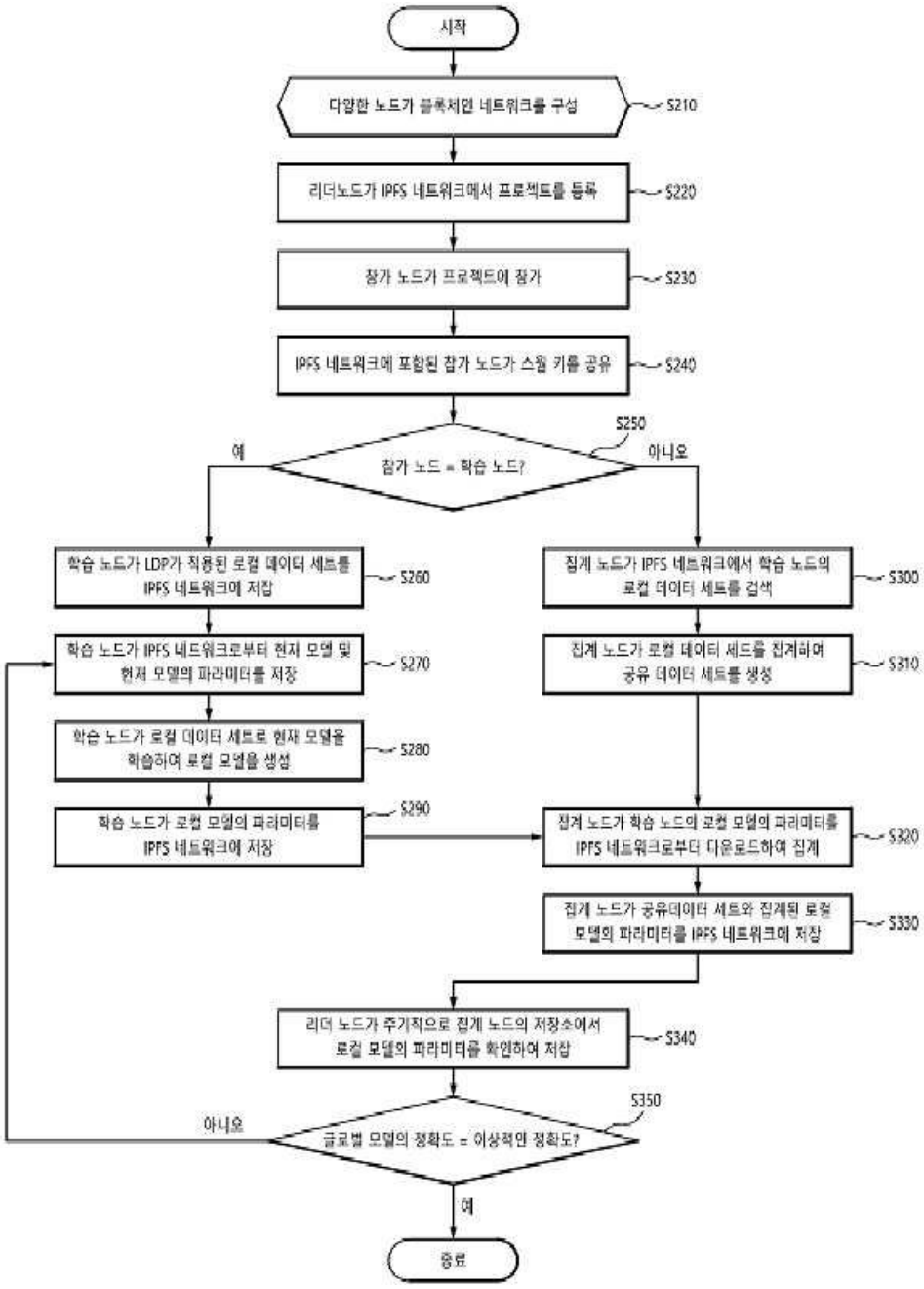
도면1



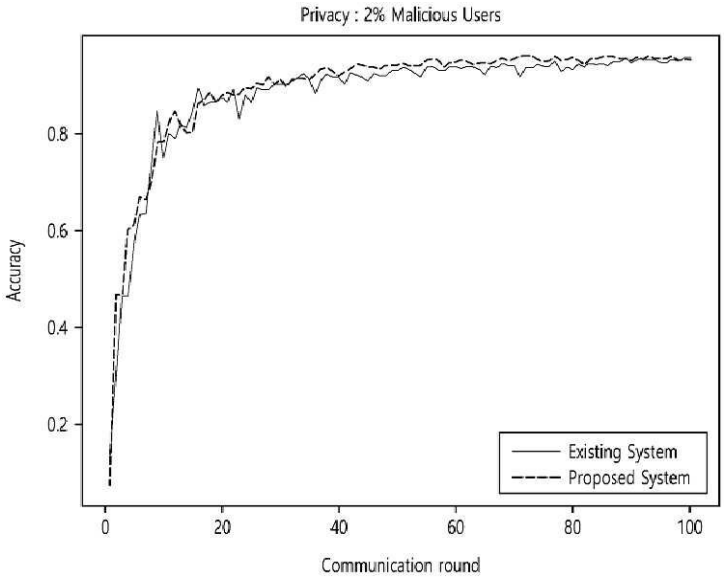
도면2


시작
리더 노드가 참가 노드를 모집하는 단계
S110
학습 노드가 로컬 데이터 세트에 기초해 로컬 모델을 생성하는 단계
S120
학습 노드가 로컬 데이터 세트 및 로컬 모델의 파라미터를 저장시키는 단계
S130
집계 노드가 공유 데이터 세트를 생성하여 저장시키는 단계
S140
리더 노드가 공유 데이터 세트에 기초하여 글로벌 모델을 생성하고, 글로벌 모델의 파라미터를 저장시키는 단계
S150
리더 노드가 글로벌 모델의 정확도를 판단하는 단계
S160
종료

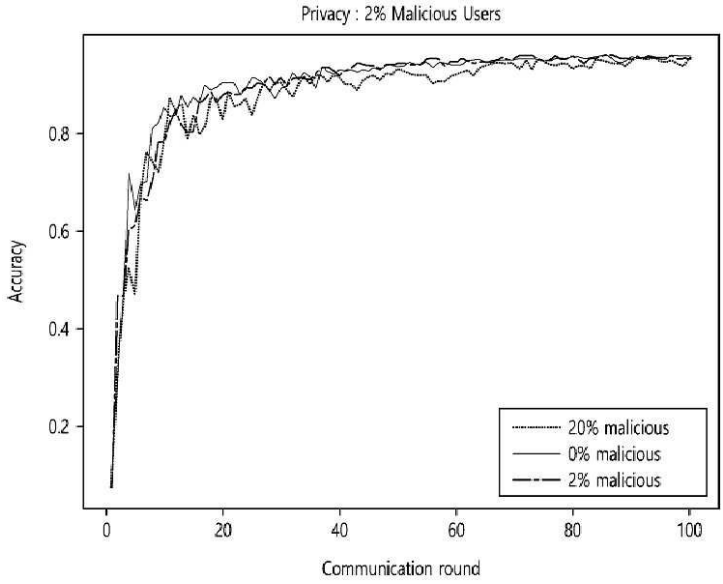
도면3


시작
다양한 노드가 블록체인 네트워크를 구성
S210
리더노드가 IPFS 네트워크에서 프로젝트를 등록
S220
참가 노드가 프로젝트에 참가
S230
IPFS 네트워크에 포함된 참가 노드가 스왐 키를 공유
S240
S250
참가 노드 = 학습 노드?
예
아니오
학습 노드가 LDP가 적용된 로컬 데이터 세트를 IPFS 네트워크에 저장
S260
학습 노드가 IPFS 네트워크로부터 현재 모델 및 현재 모델의 파라미터를 저장
S270
학습 노드가 로컬 데이터 세트로 현재 모델을 학습하여 로컬 모델을 생성
S280
학습 노드가 로컬 모델의 파라미터를 IPFS 네트워크에 저장
S290
집계 노드가 IPFS 네트워크에서 학습 노드의 로컬 데이터 세트를 검색
S300
집계 노드가 로컬 데이터 세트를 집계하여 공유 데이터 세트를 생성
S310
집계 노드가 학습 노드의 로컬 모델의 파라미터를 IPFS 네트워크로부터 다운로드하여 집계
S320
집계 노드가 공유데이터 세트와 집계된 로컬 모델의 파라미터를 IPFS 네트워크에 저장
S330
리더 노드가 주기적으로 집계 노드의 저장소에서 로컬 모델의 파라미터를 확인하여 저장
S340
S350
글로벌 모델의 정확도 = 이상적인 정확도?
아니오
예
종료

도면4


Privacy : 2% Malicious Users
Accuracy
0.2
0.4
0.6
0.8
0
20
40
60
80
100
Communication round
Existing System
Proposed System

도면5


Privacy : 2% Malicious Users
Accuracy
0.2
0.4
0.6
0.8
0
20
40
60
80
100
Communication round
20% malicious
0% malicious
2% malicious