



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0094891
(43) 공개일자 2023년06월28일

(51) 국제특허분류(Int. Cl.)
G06N 20/20 (2019.01) H04L 9/00 (2022.01)
H04L 9/06 (2006.01)
(52) CPC특허분류
G06N 20/20 (2021.08)
H04L 9/008 (2013.01)
(21) 출원번호 10-2021-0184384
(22) 출원일자 2021년12월21일
심사청구일자 2021년12월21일

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)
(72) 발명자
홍충선
경기도 용인시 수지구 상현로 30-10, 233동 101호 (상현동, 상현마을성원상떼빌아파트)
마지드 우머
경기도 용인시 기흥구 덕영대로 1732, 경희대학교 국제캠퍼스 전자정보대학 352호
(뒷면에 계속)
(74) 대리인
두호특허법인

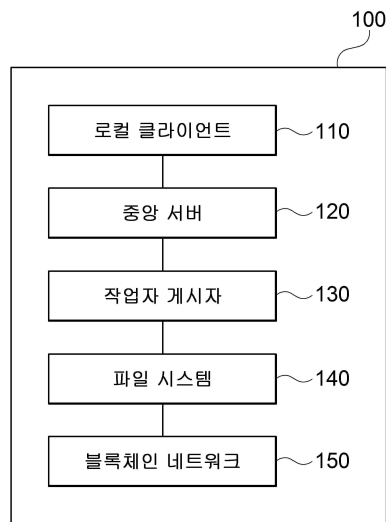
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 연합 학습 시스템 및 그 동작 방법

(57) 요약

구조화된 투명성을 지원하는 블록체인 기반의 연합 학습 시스템 및 그 동작 방법이 개시된다. 일 실시예에 따른 연합 학습 시스템은 서로 다른 로컬 학습 데이터를 이용하여 로컬 학습 모델을 생성하는 하나 이상의 로컬 클라이언트; 하나 이상의 로컬 클라이언트로부터 각각의 로컬 학습 모델을 수신하여 연합 학습 모델을 생성하는 중앙 서버; 하나 이상의 로컬 클라이언트 및 중앙 서버가 수행할 연합 학습 작업(federated learning task)의 모델 구조를 스마트 계약에 게시하는 작업 게시자; 로컬 학습 모델 및 연합 학습 모델을 공유 및 저장하며, 로컬 학습 모델 및 연합 학습 모델에 대한 해시를 생성하는 파일 시스템; 및 스마트 계약, 로컬 학습 모델에 대한 해시 및 연합 학습 모델에 대한 해시를 저장하는 블록체인 네트워크를 포함할 수 있다.

대표도 - 도1



(52) CPC특허분류

H04L 9/0643 (2013.01)

H04L 9/50 (2022.05)

(72) 발명자

김기태

경기도 용인시 기흥구 서천서로12번길 4-5, 302호
(서천동)

라티프 우라 칸

경기도 용인시 기흥구 덕영대로 1732, 경희대학교
국제캠퍼스 전자정보대학 352호

박성배

경기도 용인시 기흥구 덕영대로 1732 전자정보대학
323-1호

이 발명을 지원한 국가연구개발사업

과제고유번호	1711135177
과제번호	2020R1A4A1018607
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	집단연구지원(R&D)
연구과제명	Meta Federated Learning기반 이동엣지 컴퓨팅시스템 핵심구조 개발
기 여 율	30/100
과제수행기관명	경희대학교(국제캠퍼스)
연구기간	2021.06.01 ~ 2022.02.28

이 발명을 지원한 국가연구개발사업

과제고유번호	1415174513
과제번호	20209810400030
부처명	산업통상자원부
과제관리(전문)기관명	한국에너지기술평가원
연구사업명	미래형스마트그리드실증(R&D)
연구과제명	전기차 PnC 기반 충전서비스, 보안 인증체계 구축
기 여 율	30/100
과제수행기관명	한국전기연구원
연구기간	2021.02.01 ~ 2021.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호	1711139517
과제번호	2021-0-02068-001
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보통신방송혁신인재양성(R&D)
연구과제명	인공지능 혁신 허브 연구 개발
기 여 율	40/100
과제수행기관명	고려대학교산학협력단
연구기간	2021.07.01 ~ 2021.12.31

명세서

청구범위

청구항 1

서로 다른 로컬 학습 데이터를 이용하여 로컬 학습 모델을 생성하는 하나 이상의 로컬 클라이언트;
상기 하나 이상의 로컬 클라이언트로부터 각각의 로컬 학습 모델을 수신하여 연합 학습 모델을 생성하는 중앙 서버;
상기 하나 이상의 로컬 클라이언트 및 상기 중앙 서버가 수행할 연합 학습 작업(federated learning task)의 모델 구조를 스마트 계약에 게시하는 작업 게시자;
상기 로컬 학습 모델 및 상기 연합 학습 모델을 공유 및 저장하며, 상기 로컬 학습 모델 및 상기 연합 학습 모델에 대한 해시를 생성하는 파일 시스템; 및
상기 스마트 계약, 상기 로컬 학습 모델에 대한 해시 및 상기 연합 학습 모델에 대한 해시를 저장하는 블록체인 네트워크를 포함하는, 연합 학습 시스템.

청구항 2

제 1 항에 있어서,
상기 작업 게시자는
매 에포크(epoch)마다 새로운 동형 암호화 개인 컨텍스트(context) 및 동형 암호화 공개 컨텍스트를 생성하는, 연합 학습 시스템.

청구항 3

제 2 항에 있어서,
상기 로컬 클라이언트는
상기 작업 게시자로부터 동형 암호화 공개 컨텍스트를 수신하며,
생성한 로컬 학습 모델을 상기 동형 암호화 공개 컨텍스트에 기초하여 암호화하는, 연합 학습 시스템.

청구항 4

제 3 항에 있어서,
상기 중앙 서버는
상기 동형 암호화 공개 컨텍스트에 기초하여 암호화된 로컬 학습 모델을 집계하여 암호화된 연합 학습 모델을 생성하며,
생성된 암호화된 연합 학습 모델을 상기 파일 시스템에 전송하며,
상기 파일 시스템은
상기 암호화된 연합 학습 모델에 대한 해시를 스마트 계약에 기록하는, 연합 학습 시스템.

청구항 5

제 1 항에 있어서,

상기 중앙 서버가 생성한 연합 학습 모델을 검증하는 연합 학습 검증자를 더 포함하는, 연합 학습 시스템.

청구항 6

제 5 항에 있어서,

상기 연합 학습 검증자는

동형 암호화 공개 컨텍스트에 기초하여 암호화된 로컬 학습 모델을 집계하여 암호화된 검증 연합 학습 모델을 생성하며,

상기 암호화된 검증 연합 학습 모델의 해시와 중앙 서버가 생성한 암호화된 연합 학습 모델의 해시를 비교하여 중앙 서버가 생성한 암호화된 연합 학습 모델을 검증하는, 연합 학습 시스템.

청구항 7

제 4 항에 있어서,

상기 작업 게시자는

상기 동형 암호화 개인 컨텍스트를 기초로 상기 중앙 서버가 생성한 암호화된 연합 학습 모델을 해독하며,

상기 해독된 연합 학습 모델을 상기 파일 시스템에 전송하며,

상기 파일 시스템은

상기 해독된 연합 학습 모델에 대한 해시를 스마트 계약에 기록하는, 연합 학습 시스템.

청구항 8

작업 게시자가 하나 이상의 로컬 클라이언트 및 중앙 서버가 수행할 연합 학습 작업(federated learning task)의 모델 구조를 스마트 계약에 게시하는 단계;

상기 하나 이상의 로컬 클라이언트가 서로 다른 로컬 학습 데이터를 이용하여 로컬 학습 모델을 생성하는 단계;

상기 중앙 서버가 상기 하나 이상의 로컬 클라이언트로부터 각각의 로컬 학습 모델을 수신하여 연합 학습 모델을 생성하는 단계;

파일 시스템이 상기 로컬 학습 모델 및 상기 연합 학습 모델을 공유 및 저장하며, 상기 로컬 학습 모델 및 상기 연합 학습 모델에 대한 해시를 생성하는 단계; 및

블록체인 네트워크가 상기 스마트 계약, 상기 로컬 학습 모델에 대한 해시 및 상기 연합 학습 모델에 대한 해시를 저장하는 단계를 포함하는, 연합 학습 시스템의 동작 방법.

발명의 설명

기술 분야

[0001] 연합 학습을 위한 기술로서 특히, 구조화된 투명성을 지원하는 블록체인 기반의 연합 학습 시스템 및 그 방법에 관한 것이다.

배경 기술

[0002] 연합 학습은 학습에 참여하는 노드들의 로컬 학습 데이터를 직접 공유하지 않고 로컬 학습 모델들의 파라미터를 중앙 서버에서 통합하여 글로벌 모델을 생성하고 이를 다시 학습 참여 노드로 전송하는 분산 기계 학습 기법이

다.

[0003] 구조화된 투명성(Structured Transparency)은 입력 프라이버시, 입력 검증, 출력 프라이버시, 출력 검증 및 플로우 거버넌스(Flow Governance)로 구성되어 있는 프레임워크다. 구조화된 투명성은 프라이버시와 투명성 트레이드 오프 문제를 해결하고 미리 정의된 플로우 거버넌스를 구축하여 원활한 정보의 흐름을 보장한다.

발명의 내용

해결하려는 과제

[0004] 구조화된 투명성을 지원하는 블록체인 기반의 연합 학습 시스템 및 그 동작 방법을 제공하는데 목적이 있다.

과제의 해결 수단

[0005] 일 양상에 따르면, 연합 학습 시스템은 서로 다른 로컬 학습 데이터를 이용하여 로컬 학습 모델을 생성하는 하나 이상의 로컬 클라이언트; 하나 이상의 로컬 클라이언트로부터 각각의 로컬 학습 모델을 수신하여 연합 학습 모델을 생성하는 중앙 서버; 하나 이상의 로컬 클라이언트 및 중앙 서버가 수행할 연합 학습 작업(federated learning task)의 모델 구조를 스마트 계약에 게시하는 작업 게시자; 로컬 학습 모델 및 연합 학습 모델을 공유 및 저장하며, 로컬 학습 모델 및 연합 학습 모델에 대한 해시를 생성하는 파일 시스템; 및 스마트 계약, 로컬 학습 모델에 대한 해시 및 연합 학습 모델에 대한 해시를 저장하는 블록체인 네트워크를 포함할 수 있다.

[0006] 작업 게시자는 매 에포크(epoch)마다 새로운 동형 암호화 개인 컨텍스트(context) 및 동형 암호화 공개 컨텍스트를 생성할 수 있다.

[0007] 로컬 클라이언트는 작업 게시자로부터 동형 암호화 공개 컨텍스트를 수신하며, 생성한 로컬 학습 모델을 동형 암호화 공개 컨텍스트에 기초하여 암호화할 수 있다.

[0008] 중앙 서버는 동형 암호화 공개 컨텍스트에 기초하여 암호화된 로컬 학습 모델을 집계하여 암호화된 연합 학습 모델을 생성하며, 생성된 암호화된 연합 학습 모델을 파일 시스템에 전송하며, 파일 시스템은 암호화된 연합 학습 모델에 대한 해시를 스마트 계약에 기록할 수 있다.

[0009] 연합 학습 시스템은 중앙 서버가 생성한 연합 학습 모델을 검증하는 연합 학습 검증자를 더 포함할 수 있다.

[0010] 연합 학습 검증자는 동형 암호화 공개 컨텍스트에 기초하여 암호화된 로컬 학습 모델을 집계하여 암호화된 검증 연합 학습 모델을 생성하며, 암호화된 검증 연합 학습 모델의 해시와 중앙 서버가 생성한 암호화된 연합 학습 모델의 해시를 비교하여 중앙 서버가 생성한 암호화된 연합 학습 모델을 검증할 수 있다.

[0011] 작업 게시자는 동형 암호화 개인 컨텍스트를 기초로 중앙 서버가 생성한 암호화된 연합 학습 모델을 해독하며, 해독된 연합 학습 모델을 파일 시스템에 전송하며, 파일 시스템은 해독된 연합 학습 모델에 대한 해시를 스마트 계약에 기록할 수 있다.

[0012] 일 양상에 따르면, 연합 학습 시스템의 동작 방법은 작업 게시자가 하나 이상의 로컬 클라이언트 및 중앙 서버가 수행할 연합 학습 작업(federated learning task)의 모델 구조를 스마트 계약에 게시하는 단계; 하나 이상의 로컬 클라이언트가 서로 다른 로컬 학습 데이터를 이용하여 로컬 학습 모델을 생성하는 단계; 중앙 서버가 하나 이상의 로컬 클라이언트로부터 각각의 로컬 학습 모델을 수신하여 연합 학습 모델을 생성하는 단계; 파일 시스템이 로컬 학습 모델 및 연합 학습 모델을 공유 및 저장하며, 로컬 학습 모델 및 연합 학습 모델에 대한 해시를 생성하는 단계; 및 블록체인 네트워크가 스마트 계약, 로컬 학습 모델에 대한 해시 및 연합 학습 모델에 대한 해시를 저장하는 단계를 포함할 수 있다.

발명의 효과

[0013] 일 실시예에 따른 경우, 구조화된 투명성을 지원하는 블록체인 기반의 연합 학습 시스템을 구현할 수 있다.

도면의 간단한 설명

[0014] 도 1은 일 실시예에 따른 연합 학습 시스템의 구성도이다.

도 2는 일 실시예에 따른 연합 학습 시스템을 설명하기 위한 예시도이다.

도 3은 일 실시예에 따른 연합 학습 시스템의 동작 방법을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0015] 이하, 첨부된 도면을 참조하여 본 발명의 일 실시예를 상세하게 설명한다. 본 발명을 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 또한, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로, 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.
- [0016] 이하, 연합 학습 시스템 및 그 동작 방법의 실시예들을 도면들을 참고하여 자세히 설명한다.
- [0017] 구조적 투명성은 프라이버시와 투명성 사이의 트레이드오프를 관리하기 위한 프레임워크(framework)이며 연합 학습 시 데이터 교환 안정성을 보장한다. 구조적 투명성에는 입력 프라이버시(Input Privacy), 입력 검증(Input Verification), 출력 프라이버시(Output Privacy), 출력 검증(Output Verification) 및 흐름 거버넌스(Flow Governance)와 같이 다섯 가지로 구성되어 있다. 입력 프라이버시는 정보의 흐름에 대해 개인 정보를 유출하지 않도록 요구된다. 입력 검증은 입력 프라이버시에 대한 검증 메커니즘이 요구된다. 출력 프라이버시는 정보 흐름의 출력이 계획된 엔티티(entity)에게만 접근을 허용하고 프라이버시 문제가 없음을 보장한다. 출력 검증은 정보 흐름의 출력이 흐름 거버넌스에 의해 정의된 정책에 따라 문제가 없음을 보장한다. 마지막으로 흐름 거버넌스는 정보 흐름을 조정하고 거버넌스 관련 문제를 처리한다.
- [0018] 기존의 연합 학습 체계인 바닐라 연합 학습(Vanilla Federated Learning)에서 연합 학습에 참여하는 학습 장치들은 연합 학습 모델 생성을 위해 로컬 학습 모델을 중앙 집계 서버에 전송한다. 이 경우 중앙 집계 서버에 문제가 생기는 경우 전체 연합 학습 과정이 중단될 수 있다. 또한 악의적인 공격에 취약하여 성능이 저하된 연합 학습 모델을 생성할 가능성이 있다. 또한 중앙 집계 서버는 로컬 학습 모델의 추론 공격을 통하여 학습 데이터의 프라이버시가 침해될 수 있다.
- [0019] 일 예로, 구조화된 투명성을 지원하는 블록체인 기반 연합 학습 프레임워크는 입력 프라이버시, 출력 프라이버시, 출력 검증, 흐름 거버넌스와 같이 구조화된 투명성을 보장하는 블록체인 기반 연합 학습 프레임워크일 수 있다.
- [0020] 일 예로, 연합 학습 프로세스에서 입력 프라이버시와 출력 프라이버시는 각각 로컬 학습 모델과 연합 학습 모델에 대한 단일키 동형 암호화 체계를 통해 입력 및 출력 프라이버시를 지킬 수 있다. 또한 스마트 계약은 로컬 학습 모델 및 연합 학습 모델에 대한 무단 접근을 방지하여 입력 및 출력 개인정보를 보호할 수 있다.
- [0021] 일 예로, 암호화된 연합 학습 모델은 중앙 서버에서 해당 글로벌 에포크(Epoch)의 로컬 학습 모델들을 동형 집계하여 만들어지며 연합 학습 검증자는 출력 검증을 위하여 동형 집계 방식에 맞는지 확인한다.
- [0022] 일 예로, 흐름 거버넌스를 위하여 연합 학습 작업과 관련된 작업 게시자, 스마트 계약 및 연합 학습 작업과 관련된 블록체인 오라클을 통해 연합 학습 과정이 조정될 수 있다. 연합 학습 작업용 블록체인 오라클 서비스를 통해 스마트 계약이 서비스 관리자와 상호 작용하여 현재 에포크(Epoch)를 위한 중앙 서버 및 연합 학습 검증자에 대한 정보를 확인 할 수 있다.
- [0023] 도 1은 일 실시예에 따른 연합 학습 시스템의 구성도이다.
- [0024] 일 실시예에 따르면, 연합 학습 시스템(100)은 로컬 클라이언트(110), 중앙 서버(120), 작업 게시자(130), 파일 시스템(140) 및 블록체인 네트워크(150)를 포함할 수 있다.
- [0025] 일 예에 따르면, 연합 학습 시스템(100)은 4개의 계층으로 구성될 수 있다. 예를 들어, 클라이언트 계층(Client Layer)은 작업 게시자(130)와 로컬 클라이언트(110)가 포함될 수 있다. 각 연합 학습 작업에는 고유한 클라이언트 계층이 있을 수 있다. 분산계층(Distributed decentralized layer)은 파일 시스템(InterPlanetary File System, 140), 블록체인 네트워크, 블록체인 오라클에 해당하는 스마트 계약으로 구성될 수 있다. 연합 학습 집계 계층(aggregation layer)은 중앙 서버(120)로 구성될 수 있다. 이때, 중앙 서버(120)는 하나 이상의 연합 학습 집계자를 포함할 수 있다. 이에 따라, 이후 중앙 서버에 대한 실시예는 연합 학습 집계자에 대한 실시예로 해석될 수 있다.
- [0026] 연합 학습 검증 계층(verification layer)은 하나 이상의 연합 학습 검증자(210)로 구성될 수 있다.
- [0027] 일 실시예에 따르면, 로컬 클라이언트(110)는 서로 다른 로컬 학습 데이터를 이용하여 로컬 학습 모델을 생성할 수 있다.

- [0028] 일 예에 따르면, 로컬 클라이언트(110)는 각 글로벌 에포크(Epoch)에 대한 로컬 학습 모델을 이전 글로벌 에포크에서 생성된 해독된(Decrypted) 연합 학습 모델을 초기 모델로 각 로컬 데이터 세트를 사용하여 훈련할 수 있다. 각 로컬 클라이언트(110)는 단일키 동형 암호화 체계의 공개 컨텍스트를 사용하여 로컬 학습 모델을 암호화할 수 있다. 이후, 로컬 클라이언트(110)는 암호화된 로컬 학습 모델을 파일 시스템(140)에 업로드할 수 있다. 이때, 로컬 학습 모델은 트랜잭션을 통해 스마트 계약서에 기록될 수 있다.
- [0029] 일 실시예에 따르면, 중앙 서버(120)는 하나 이상의 로컬 클라이언트로부터 각각의 로컬 학습 모델을 수신하여 연합 학습 모델을 생성할 수 있다.
- [0030] 일 예에 따르면, 중앙 서버(120) 및 연합 학습 검증자(210)는 현재 글로벌 에포크에 해당하는 암호화된 로컬 학습 모델을 다운로드 할 수 있다. 중앙 서버(120)는 암호화된 로컬 학습 모델들을 암호화된 연합 학습 모델로 집계할 수 있다. 중앙 서버(120)는 암호화된 연합 학습 모델을 파일 시스템(140)에 업로드하고 획득한 파일 시스템(140) 해시를 스마트 계약에 기록할 수 있다.
- [0031] 일 실시예에 따르면, 작업 게시자(130)는 하나 이상의 로컬 클라이언트 및 중앙 서버가 수행할 연합 학습 작업(federated learning task)의 모델 구조를 스마트 계약에 게시할 수 있다.
- [0032] 일 예에 따르면, 작업 게시자(130)와 로컬 클라이언트(110)는 연합 학습 시스템의 클라이언트 계층이 될 수 있다. 작업 게시자(130)는 연합 학습 프로세스를 조정하고 기록하기 위하여 연합 학습 작업에 대한 스마트 계약을 배포할 수 있다. 이후, 작업 게시자(130)는 로컬 학습 모델에 대한 집계 방법, 모델 구조 및 암호화되지 않은 초기 전역 가중치들을 파일 시스템(140)에 업로드할 수 있다. 이때, 파일 시스템(140)은 집계 방법, 모델 구조 및 암호화되지 않은 초기 전역 가중치에 대한 해시를 생성하여 스마트 계약에 기록할 수 있다.
- [0033] 일 예에 따르면, 작업 게시자(130)는 중앙 서버(120) 및 연합 학습 검증자(210)가 로컬 학습 모델을 연합 학습 모델로 집계하는 방법을 스마트 계약에 게시할 수 있다.
- [0034] 일 예에 따르면, 작업 게시자(130)는 로컬 클라이언트(110)가 로컬 학습 모델들을 학습하고 중앙 서버(120) 및 연합 학습 검증자(210)가 로컬 학습 모델을 연합 학습 모델로 집계하기 위한 연합 학습 작업의 모델 구조를 게시할 수 있다. 초기화된 연합 학습 모델의 가중치는 연합 학습 프로세스의 첫 번째 에포크(Epoch)에서 게시될 수 있다.
- [0035] 일 예에 따르면, 작업 게시자(130)는 이더리움에서 연합 학습 작업을 위한 스마트 계약을 배포할 수 있다. 일 예로, 이더리움은 스마트 계약을 실행하고 트랜잭션을 불변의 방식으로 저장할 수 있는 탈 중앙화 컴퓨팅 플랫폼일 수 있다.
- [0036] 일 실시예에 따르면, 작업 게시자(130)는 매 에포크(epoch)마다 새로운 동형 암호화 개인 컨텍스트(context) 및 동형 암호화 공개 컨텍스트를 생성할 수 있다.
- [0037] 일 예에 따르면, 작업 게시자(130)는 매 글로벌 에포크(Epoch)마다 새로운 단일키 동형 암호화(Single-Key Homomorphic Encryption) 개인 컨텍스트 및 공개 컨텍스트를 생성할 수 있다. 이후, 공개 컨텍스트와 개인 컨텍스트는 파일 시스템(140)에 업로드될 수 있으며, 공개 컨텍스트 및 개인 컨텍스트에 대한 해시는 스마트 계약에 기록될 수 있다. 개인 컨텍스트는 작업 게시자(130)만 접근할 수 있으며, 그 외 다른 구성요소는 스마트 계약에 포함된 개인 정보 보호 정책에 따라 공개 컨텍스트에만 접근할 수 있다.
- [0038] 일 실시예에 따르면, 로컬 클라이언트(110)는 작업 게시자(130)로부터 동형 암호화 공개 컨텍스트를 수신하며, 생성한 로컬 학습 모델을 동형 암호화 공개 컨텍스트에 기초하여 암호화할 수 있다.
- [0039] 일 예에 따르면, 로컬 클라이언트(110)는 각 글로벌 에포크(Epoch)에 대하여 로컬 데이터 세트를 통해 로컬 학습 모델을 훈련시킬 수 있다. 또한, 로컬 클라이언트(110)는 동형 암호화 공개 컨텍스트에 대한 암호키를 사용하여 로컬 학습 모델을 동형적으로 암호화할 수 있다.
- [0040] 일 실시예에 따르면, 중앙 서버(120)는 동형 암호화 공개 컨텍스트에 기초하여 암호화된 로컬 학습 모델을 집계하여 암호화된 연합 학습 모델을 생성하며, 생성된 암호화된 연합 학습 모델을 파일 시스템(140)에 전송할 수 있다.
- [0041] 일 예에 따르면, 중앙 서버(120)는 하나 이상의 연합 학습 집계자를 포함할 수 있다.
- [0042] 일 예에 따르면, 중앙 서버(120) 및 연합 학습 검증자(210)는 현재 글로벌 에포크에 해당하는 암호화된 로컬 학습 모델을 다운로드 할 수 있다. 중앙 서버(120)는 암호화된 로컬 학습 모델들을 암호화된 연합 학습 모델로 집

계할 수 있다.

- [0043] 일 실시예에 따르면, 파일 시스템(140)은 암호화된 연합 학습 모델에 대한 해시를 스마트 계약에 기록할 수 있다. 일 예로, 중앙 서버(120)는 암호화된 연합 학습 모델을 파일 시스템(140)에 업로드하고 획득한 파일 시스템(140) 해시를 스마트 계약에 기록할 수 있다.
- [0044] 일 실시예에 따르면, 작업 게시자(130)는 동형 암호화 개인 컨텍스트를 기초로 중앙 서버(120)가 생성한 암호화된 연합 학습 모델을 해독하며, 해독된 연합 학습 모델을 파일 시스템(140)에 전송할 수 있다.
- [0045] 일 예에 따르면, 작업 게시자(130)는 현재 글로벌 에포크에 해당하는 단일 키 동형 암호화 체계의 개인 컨텍스트를 사용하여 암호화된 연합 학습 모델의 암호를 해독할 수 있다. 일 예로, 작업 게시자(130)는 해독된 연합 학습 모델의 정확성을 테스트 세트를 통해 측정하고 스마트 계약서에 기록할 수 있다.
- [0046] 일 실시예에 따르면, 파일 시스템(140)은 로컬 학습 모델 및 연합 학습 모델을 공유 및 저장하며, 로컬 학습 모델 및 연합 학습 모델에 대한 해시를 생성할 수 있다. 또한, 파일 시스템(140)은 해독된 연합 학습 모델에 대한 해시를 스마트 계약에 기록할 수 있다. 일 예로, 작업 게시자(130)는 해독된 연합 학습 모델을 파일 시스템(140)에 업로드할 수 있으며, 파일 시스템(140)은 해독된 연합 학습 모델에 대한 해시를 생성하여 스마트 계약에 기록할 수 있다.
- [0047] 일 예로, 파일 시스템(140)은 콘텐츠를 식별할 수 있는 콘텐츠 주소 지정 해시를 제공하는 분산형 파일 스토리지 시스템일 수 있다.
- [0048] 일 실시예에 따르면, 블록체인 네트워크(150)는 스마트 계약, 로컬 학습 모델에 대한 해시 및 연합 학습 모델에 대한 해시를 저장할 수 있다.
- [0049] 도 2를 참조하면, 연합 학습 시스템(100)은 중앙 서버(120)가 생성한 연합 학습 모델을 검증하는 연합 학습 검증자(210)를 더 포함할 수 있다.
- [0050] 일 실시예에 따르면, 연합 학습 검증자(210)는 동형 암호화 공개 컨텍스트에 기초하여 암호화된 로컬 학습 모델을 집계하여 암호화된 검증 연합 학습 모델을 생성하며, 암호화된 검증 연합 학습 모델의 해시와 중앙 서버가 생성한 암호화된 연합 학습 모델의 해시를 비교하여 중앙 서버가 생성한 암호화된 연합 학습 모델을 검증할 수 있다.
- [0051] 일 예로, 연합 학습 검증자(210)는 현재 글로벌 에포크에 해당하는 암호화된 로컬 학습 모델을 다운로드할 수 있다.
- [0052] 일 예에 따르면, 하나 이상의 연합 학습 검증자(210) 각각은 암호화된 로컬 학습 모델들을 암호화된 연합 학습 모델로 집계할 수 있으며, 집계된 암호화된 연합 학습 모델에 대한 파일 시스템(140) 해시를 중앙 서버(120)가 제출한 파일 시스템(140) 해시와 비교할 수 있다. 일 예로, 두 해시가 일치하는 경우, 중앙 서버(120)가 암호화된 로컬 학습 모델들을 집계 방법에 따라 암호화된 연합 학습 모델로 올바르게 집계했음을 의미한다.
- [0053] 일 예에 따르면, 하나 이상의 연합 학습 검증자(210)들 각각은 스마트 계약 거래를 통해 현재 글로벌 에포크(Epoch)에 대한 연합 학습 검증자(210)의 암호화된 연합 학습 모델의 정확성에 대해 투표할 수 있다. 이때, 투표 결과가 미리 정의된 임계값을 초과하면 암호화된 연합 학습 모델이 유효한 것으로 간주할 수 있다. 반면, 투표 결과가 미리 정의된 임계값 이하이면 중앙 서버(120)에 포함된 다른 연합 학습 집계자와 다른 연합 학습 검증자(210)의 배치(Batch)를 선택할 수 있다.
- [0054] 일 예에 따르면, 현재 글로벌 에포크(Epoch)에 대한 암호화된 연합 학습 모델이 유효한 경우, 현재 글로벌 에포크에 해당하는 단일 키 동형 암호화 체계의 개인 컨텍스트를 사용하여 작업 게시자(130)에 의해 암호화된 연합 학습 모델의 암호가 해독될 수 있다. 일 예로, 작업 게시자(130)는 해독된 연합 학습 모델의 정확성을 테스트 세트를 통해 측정하고 스마트 계약서에 기록할 수 있다.
- [0055] 일 예에 따르면, 연합 학습 시스템(100)은 서비스 관리자(220)를 더 포함할 수 있다.
- [0056] 일 예에 따르면, 서비스 관리자(220)는 연합 학습 집계 계층 및 연합 학습 검증 계층에서 현재 글로벌 에포크(Epoch)의 중앙 서버(120)에 포함된 연합 학습 집계자와 연합 학습 검증자(210)를 임의로 선택할 수 있다. 일 예로, 서비스 관리자(220)는 글로벌 에포크(epoch)당 하나의 연합 학습 집계자를 선택할 수 있다. 일 예로, 서비스 관리자(220)는 하나 이상의 연합 학습 검증자(210)를 선택할 수 있다. 예를 들어, 서비스 관리자(220)는 작업 게시자(130)가 지불한 비용에 따라 하나 이상의 연합 학습 검증자(210)를 선택할 수 있다. 이후, 선택된

중앙 서버(120)의 연합 학습 집계자와 연합 학습 검증자(210)의 주소가 블록체인 오라클의 도움을 받아 스마트 계약서에 기록될 수 있다.

- [0057] 일 예로, 선택된 중앙 서버(120)의 연합 학습 집계자와 연합 학습 검증자(210)는 스마트 계약을 통해 집계 방법, 모델 구조, 공개 단일키 동형 암호화 컨텍스트를 다운로드 할 수 있다.
- [0058] 도 3은 일 실시예에 따른 연합 학습 시스템의 동작 방법을 도시한 흐름도이다.
- [0059] 일 실시예에 따르면, 작업 게시자는 하나 이상의 로컬 클라이언트 및 중앙 서버가 수행할 연합 학습 작업 (federated learning task)의 모델 구조를 스마트 계약에 게시할 수 있다(310).
- [0060] 일 예에 따르면, 작업 게시자는 연합 학습 프로세스를 조정하고 기록하기 위하여 연합 학습 작업에 대한 스마트 계약을 배포할 수 있다. 이후, 작업 게시자는 로컬 학습 모델에 대한 집계 방법, 모델 구조 및 암호화되지 않은 초기 전역 가중치들을 파일 시스템에 업로드할 수 있다. 이때, 파일 시스템은 집계 방법, 모델 구조 및 암호화 되지 않은 초기 전역 가중치에 대한 해시를 생성하여 스마트 계약에 기록할 수 있다.
- [0061] 일 실시예에 따르면, 하나 이상의 로컬 클라이언트는 서로 다른 로컬 학습 데이터를 이용하여 로컬 학습 모델을 생성할 수 있다(320).
- [0062] 일 예에 따르면, 로컬 클라이언트는 각 글로벌 에포크(Epoch)에 대한 로컬 학습 모델을 이전 글로벌 에포크에서 생성된 해독된 연합 학습 모델을 초기 모델로 각 로컬 데이터 세트를 사용하여 훈련할 수 있다. 각 로컬 클라이언트는 단일키 동형 암호화 체계의 공개 컨텍스트를 사용하여 로컬 학습 모델을 암호화할 수 있다. 이후, 로컬 클라이언트는 암호화된 로컬 학습 모델을 파일 시스템에 업로드할 수 있다. 이때, 로컬 학습 모델은 트랜잭션을 통해 스마트 계약서에 기록될 수 있다.
- [0063] 일 실시예에 따르면, 중앙 서버는 하나 이상의 로컬 클라이언트로부터 각각의 로컬 학습 모델을 수신하여 연합 학습 모델을 생성할 수 있다(330).
- [0064] 일 예에 따르면, 중앙 서버 및 연합 학습 검증자는 현재 글로벌 에포크에 해당하는 암호화된 로컬 학습 모델을 다운로드 할 수 있다. 중앙 서버는 암호화된 로컬 학습 모델들을 암호화된 연합 학습 모델로 집계할 수 있다. 중앙 서버는 암호화된 연합 학습 모델을 파일 시스템에 업로드하고 획득한 파일 시스템 해시를 스마트 계약에 기록할 수 있다.
- [0065] 일 실시예에 따르면, 파일 시스템은 로컬 학습 모델 및 연합 학습 모델을 공유 및 저장하며, 로컬 학습 모델 및 연합 학습 모델에 대한 해시를 생성할 수 있다(340). 또한, 파일 시스템은 해독된 연합 학습 모델에 대한 해시를 스마트 계약에 기록할 수 있다. 일 예로, 작업 게시자는 해독된 연합 학습 모델을 파일 시스템에 업로드할 수 있으며, 파일 시스템은 해독된 연합 학습 모델에 대한 해시를 생성하여 스마트 계약에 기록할 수 있다.
- [0066] 일 실시예에 따르면, 블록체인 네트워크는 스마트 계약, 로컬 학습 모델에 대한 해시 및 연합 학습 모델에 대한 해시를 저장할 수 있다(350).
- [0067] 본 발명의 일 양상은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로서 구현될 수 있다. 상기의 프로그램을 구현하는 코드들 및 코드 세그먼트들은 당해 분야의 컴퓨터 프로그래머에 의하여 용이하게 추론될 수 있다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함할 수 있다. 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 광 디스크 등을 포함할 수 있다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드로 작성되고 실행될 수 있다.
- [0068] 이제까지 본 발명에 대하여 그 바람직한 실시 예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 따라서, 본 발명의 범위는 전술한 실시 예에 한정되지 않고 특허 청구범위에 기재된 내용과 동등한 범위 내에 있는 다양한 실시 형태가 포함되도록 해석되어야 할 것이다.

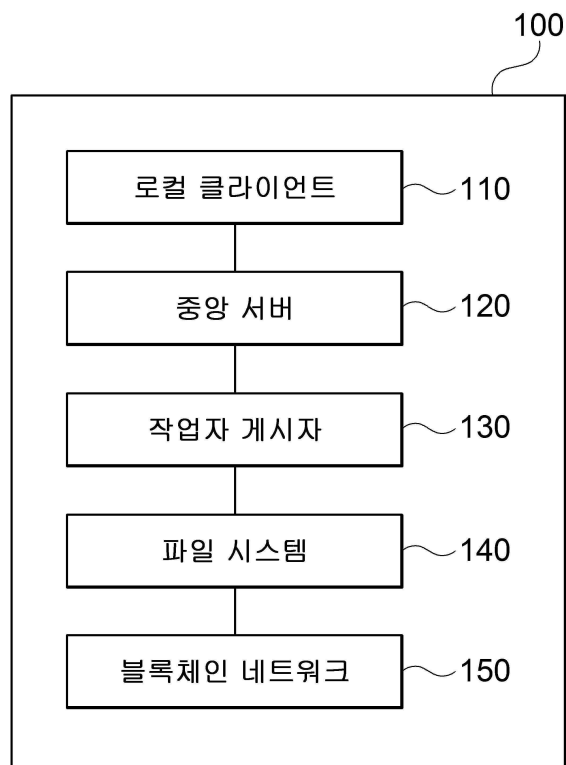
부호의 설명

- [0069] 100: 연합 학습 시스템
- 110: 로컬 클라이언트

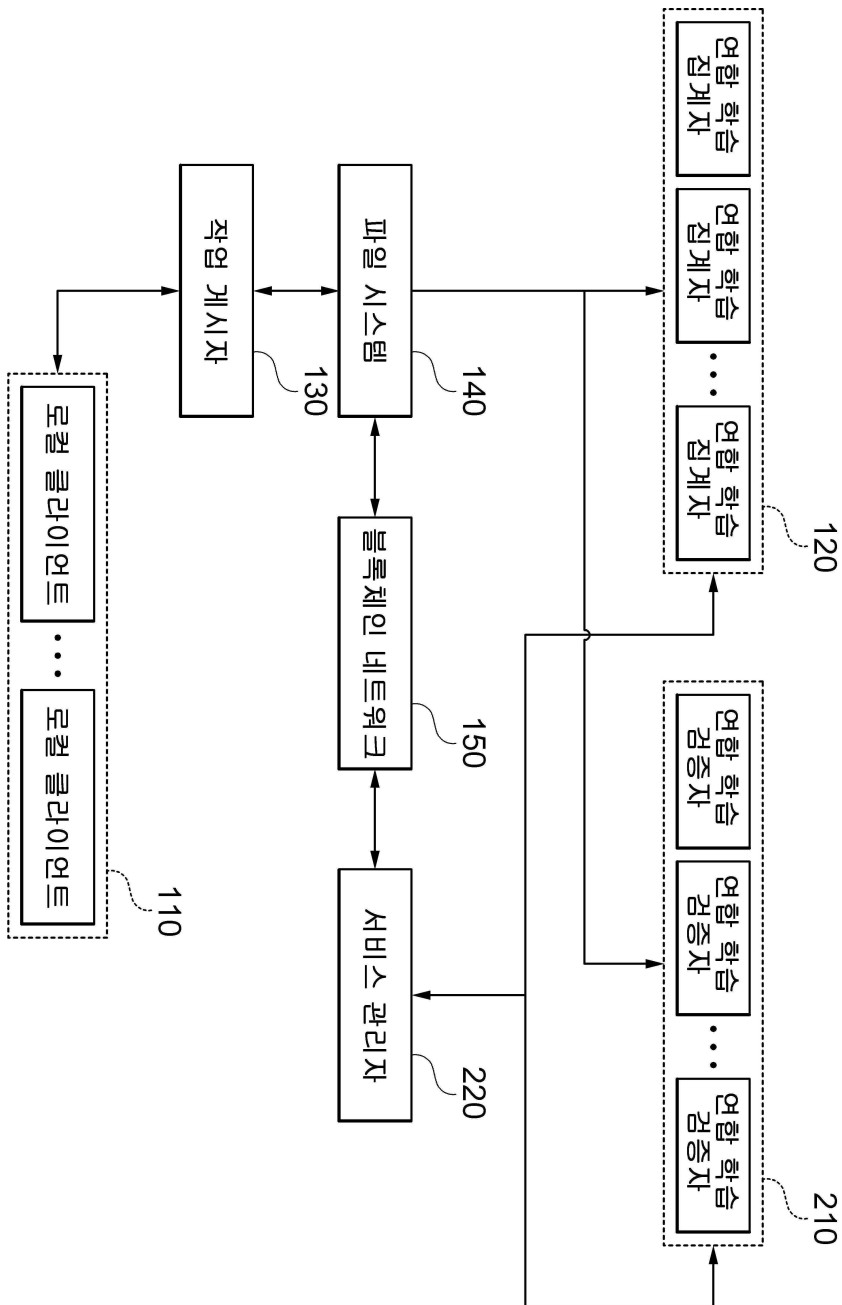
- 120: 중앙 서버
- 130: 작업 게시자
- 140: 파일 시스템
- 150: 블록체인 네트워크
- 210: 연합 학습 검증자
- 220: 서비스 관리자

도면

도면1



도면2



도면3

