(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2023 년 7 월 13 일 (13.07.2023)

WIPO | PCT

(10) 국제공개번호
WO 2023/132597 A1

(51) 국제특허분류:
G06N 20/20 (2019.01)

(21) 국제출원번호: PCT/KR2023/000064

(22) 국제출원일: 2023 년 1 월 3 일 (03.01.2023)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2022-0000892 2022 년 1 월 4 일 (04.01.2022) KR

(71) 출원인: 숭실대학교 산학협력단 (**FOUNDATION OF SOONGSIL UNIVERSITY-INDUSTRY COOPERATION**) [KR/KR]; 06978 서울특별시 동작구 상도로 369, Seoul (KR).

(72) 발명자: **최봉준 (CHOI, Bongjun)**; 04397 서울특별시 용산구 서빙고로 79가길 8, 201호, Seoul (KR). **쿠마아짓 (KUMAR, Ajit)**; 07024 서울특별시 동작구 상도로 61길 65, 501호, Seoul (KR).

(74) 대리인: **윤귀상 (YUN, Kuisang)**; 08511 서울특별시 금천구 디지털로 9길 47 804호(가산동, 한신IT 타워2차), Seoul (KR).

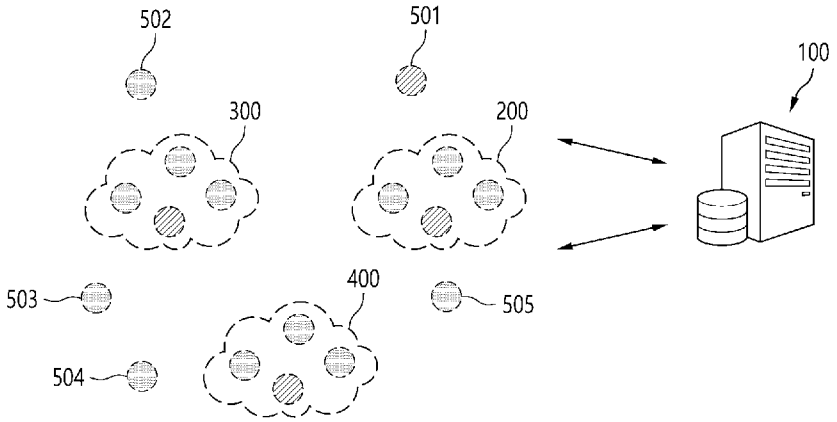
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:
— 국제조사보고서와 함께 (조약 제21조(3))

(54) Title: LOCAL GROUP-BASED FEDERATED LEARNING SYSTEM AND FEDERATED LEARNING CONTROL METHOD

(54) 발명의 명칭: 로컬 그룹 기반의 연합학습 시스템 및 연합학습 제어방법



(57) Abstract: A federated learning system according to an embodiment of the present invention comprises at least one central server and a plurality of local groups, wherein each of the plurality of local groups is configured by including a master node and a plurality of nodes, and the plurality of local groups are formed by the central server by using information of a feature set (C) for federated learning.

(57) 요약서: 본 발명의 일실시예에 따른 연합학습 시스템은 적어도 하나의 중앙 서버와 다수의 로컬 그룹을 포함하고, 상기 다수의 로컬 그룹 각각은 하나의 마스터 노드(Node)와 다수의 노드를 포함하여 구성되며, 상기 다수의 로컬 그룹은 상기 중앙 서버가 연합학습을 위한 특징 세트(C)의 정보를 이용하여 형성하는 것을 특징으로 한다.

WO 2023/132597 A1

명세서

발명의 명칭: 로컬 그룹 기반의 연합학습 시스템 및 연합학습 제어방법

기술분야

[1] 본 발명은 로컬 그룹 기반의 연합학습 시스템 및 연합학습 제어방법에 관한 것으로, 특히 신뢰가치평가에 의해 로컬 그룹을 형성하여 연합학습을 수행하는 연합학습 시스템 및 연합학습 제어방법에 관한 것이다.

배경기술

[2] 연합학습(Federated Learning)은 다수의 로컬 클라이언트와 하나의 중앙 서버가 협력하여 데이터가 탈중앙화된 상황에서 글로벌 모델을 학습하는 기계학습 기술이다. 여기서, 로컬 클라이언트는 예컨대 사물 인터넷 기기, 스마트 폰 등이 될 수 있다.

[3] 이러한 연합학습은 McMahan이 2017년에 처음 논문으로 발표한 이후, 2017년 구글 AI 블로그에서 공식적으로 소개되고, 제로 모바일 Google Gboard에 적용되고 있는 기술로서 많은 주목을 받기 시작했다.

[4] 특히, 연합학습은 데이터 희소성 및 데이터 불균형으로 인해 발생하는 non-iid(non-independent and identically distributed) 문제를 줄이기 위해, 학습을 그룹화(grouping, clustering)하는 방법들이 제안되고 있다.

[5] 그러나, 이렇게 그룹화를 하면서도 중앙 집중식으로 학습을 할 때보다 학습 정확도(Accuracy)가 저하되는 문제가 있고, 로컬 그룹 내부에 구성된 로컬 클라이언트 간의 데이터 공유시 충분하지 않은 자원을 가지고 있거나 또는 불성실하게 참여하지 않는 클라이언트로 인한 안정성 및 성능이 저하되는 문제가 있으며, 로컬 그룹 내 데이터 공유시 악의적으로 시스템의 취약점을 공격하는 다양한 보안상의 문제가 발생한다.

[6] [선행기술문헌]

[7] [특허문헌]

[8] (특허문헌 1) 특허문헌 : 공개특허공보 제 10-2021-0121915호

발명의 상세한 설명

기술적 과제

[9] 본 발명은 상기 문제점을 해소하기 위하여 안출된 것으로, 본 발명의 목적은 신뢰가치평가에 의해 로컬 그룹을 형성하여 그룹 내 데이터 공유를 개선하고 연합학습을 수행하는 연합학습 시스템을 제공하는 데 있다.

[10] 본 발명의 다른 목적은 신뢰가치평가에 의해 로컬 그룹을 형성하여 그룹 내 데이터 공유를 개선하고 연합학습을 수행하는 연합학습 제어방법을 제공하는 데 있다.

과제 해결 수단

[11] 본 발명의 일실시예에 따른 연합학습 시스템은 적어도 하나의 중앙 서버와 다수의 로컬 그룹을 포함하고, 상기 다수의 로컬 그룹 각각은 하나의 마스터 노드(Node)와 다수의 노드를 포함하여 구성되며, 상기 다수의 로컬 그룹은 상기 중앙 서버가 연합학습을 위한 특징 세트(C)의 정보를 이용하여 형성하는 것을 특징으로 한다.

[12] 본 발명의 일실시예에 따른 연합학습 시스템에서 상기 다수의 로컬 그룹 각각은 상기 마스터 노드에 연결된 참여 DB(participation DB)를 더 포함하는 것을 특징으로 한다.

[13] 본 발명의 일실시예에 따른 연합학습 시스템에서 상기 특징 세트(C)의 정보는 신뢰도 점수(T), 수행능력(E), 가용성(A), 참여유무(P), 로컬 데이터품질(Q) 및 디바이스 정보(D) 중 어느 하나를 포함하는 것을 특징으로 한다.

[14] 또는, 본 발명의 다른 실시예에 따른 연합학습 제어방법은 (ㄱ) 중앙서버가 연합학습에 참여할 다수의 노드에게 특징 세트(C)의 정보를 요청하는 단계; (ㄴ) 상기 중앙서버가 상기 특징 세트(C)의 정보를 이용하여 상기 다수의 노드중에서 임시의 마스터 노드를 지정하는 단계; (ㄷ) 상기 중앙서버가 상기 마스터 노드와 상기 마스터 노드에 인접한 노드들로 이루어진 다수의 로컬 그룹을 생성하는 단계; 및 (ㄹ) 상기 중앙서버는 상기 마스터 노드를 통해 상기 로컬 그룹을 구성하는 노드로부터 연합학습 정책정보를 수신하는 단계;를 포함한다.

[15] 본 발명의 다른 실시예에 따른 연합학습 제어방법은 상기 (ㄷ) 단계에서 다수의 로컬 그룹 각각이 상기 마스터 노드에 연결된 참여 DB(participation DB)를 더 포함하는 것을 특징으로 한다.

[16] 본 발명의 다른 실시예에 따른 연합학습 제어방법에서 상기 특징 세트(C)의 정보는 신뢰도 점수(T), 수행능력(E), 가용성(A), 참여유무(P), 로컬 데이터품질(Q) 및 디바이스 정보(D) 중 어느 하나를 포함하는 것을 특징으로 한다.

[17] 본 발명의 다른 실시예에 따른 연합학습 제어방법에서 상기 신뢰도 점수(T)는 상기 다수의 노드 각각의 행동특성수치(B) 및 추천 점수(RB)에 의해 결정되는 것을 특징으로 한다.

[18] 본 발명의 다른 실시예에 따른 연합학습 제어방법에서 상기 (ㄴ)단계는 상기 신뢰도 점수(T), 수행능력(E), 참여유무(P) 및 가용성(A)의 정보를 이용하여 상기 임시의 마스터 노드를 지정하는 것을 특징으로 한다.

[19]

[20] 본 발명의 특징 및 이점들은 첨부도면에 의거한 다음의 상세한 설명으로 더욱 명백해질 것이다.

[21] 이에 앞서, 본 명세서 및 청구범위에 사용된 용어나 단어는 통상적이고, 사전적인 의미로 해석되어서는 아니 되며, 발명자가 그 자신의 발명을 가장 최선의 방법으로 설명하기 위해 용어의 개념을 적절하게 정의할 수 있다는 원칙에 입각하여 본 발명의 기술적 사상에 부합되는 의미와 개념으로

해석되어야만 한다.

발명의 효과

[22] 본 발명의 일실시예에 따른 연합학습 시스템은 다수의 로컬 그룹과 같은 로컬 계층 및 로컬 그룹 각각의 마스터 노드와 중앙 서버로 이루어진 글로벌 계층으로 이루어진 계층구조를 갖고 업데이트 횟수를 줄임으로써, 학습에 필요한 계산 및 비용을 절감하고 발생 가능한 보안 위험성을 최소화할 수 있는 효과가 있다.

[23] 본 발명의 다른 실시예에 따른 연합학습 제어방법은 특징 세트(C)의 정보를 이용하여 부적합 노드들을 배제하면서 다수의 로컬 그룹을 생성하므로, 신뢰성을 향상 유지시켜 정보 노출로 인한 보안 위험을 최소화하면서 효율적인 연합학습을 수행할 수 있는 효과가 있다.

도면의 간단한 설명

[24] 도 1은 본 발명의 일실시예에 따른 연합학습 시스템의 구성도.

[25] 도 2는 본 발명의 일실시예에 따른 연합학습 시스템을 구성하는 임의의 로컬 그룹의 구성도.

[26] 도 3은 본 발명의 다른 실시예에 따른 연합학습 제어방법을 설명하기 위한 순서도.

[27] 도 4는 본 발명의 다른 실시예에 따른 연합학습 제어방법을 나타낸 소스코드의 예시도.

발명의 실시를 위한 최선의 형태

[28] 본 발명의 목적, 특정한 장점들 및 신규한 특징들은 첨부된 도면들과 연관되는 이하의 상세한 설명과 바람직한 실시예로부터 더욱 명백해질 것이다. 본 명세서에서 각 도면의 구성요소들에 참조번호를 부가함에 있어서, 동일한 구성요소들에 한해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 번호를 가지도록 하고 있음에 유의하여야 한다. 또한, 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 또한, 본 발명을 설명함에 있어서, 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명은 생략한다.

[29] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 상세히 설명하기로 한다. 도 1은 본 발명의 일실시예에 따른 연합학습 시스템의 구성도이고, 도 2는 본 발명의 일실시예에 따른 연합학습 시스템을 구성하는 임의의 로컬 그룹의 구성도이다.

[30] 본 발명의 일실시예에 따른 연합학습 시스템은 도 1에 도시된 바와 같이 중앙 서버(100)와 다수의 로컬 그룹(200,300,400)을 포함하고, 다수의 로컬 그룹(200,300,400) 각각은 하나의 마스터 노드(Node)와 다수의 노드를 포함하여 구성됩니다. 여기서, 노드는 신경망을 갖는 기기로서 예컨대 IoT(Internet of

Things) 기기, 다른 서버, 스마트 폰 등을 포함할 수 있다.

[31] 중앙 서버(100)는 연합학습을 위해 특징 세트(C)의 정보를 이용하여 다수의 로컬 그룹(200,300,400)을 형성하고, 다수의 로컬 그룹(200,300,400) 각각에서 마스터 노드를 지정할 수 있다. 이때, 중앙 서버(100)는 특징 세트(C)의 정보를 이용한 조건에 부합하지 않는 부적합 노드들(501,502,503,504,505)을 연합학습을 위한 그룹에서 배제할 수 있다. 이렇게 부적합 노드들(501,502,503,504,505)을 배제하고 신뢰성을 갖는 로컬 그룹(200,300,400)을 이용하여 연합학습을 수행하므로, 데이터 희소성 및 데이터 불균형으로 인한 non-iid(non-independent and identically distributed) 문제를 개선하여 연합학습의 신뢰성과 성능을 개선할 수 있다.

[32] 다수의 로컬 그룹(200,300,400) 각각은 대표적으로 도 2에 도시된 바와 같이 하나의 마스터 노드(201), 마스터 노드(201)에 연결된 다수의 노드(202,203,204,205,206,207,208,209) 및 마스터 노드(201)에 연결된 참여 DB(participation DB: 210)를 포함하여 구성된다.

[33] 마스터 노드(201)는 중앙 서버(100)가 특징 세트(C)의 정보를 이용하여 지정된 구성으로, 그룹을 이루는 다수의 노드(202,203,204,205,206,207,208,209) 각각에 대한 특징 세트(C)의 정보 또는 다수의 노드(202,203,204,205,206,207,208,209) 각각에서 수행한 학습 결과를 참여 DB(210)에 저장하고, 중앙 서버(100)의 요청신호에 따라 특징 세트(C)의 정보 또는 수행한 학습 결과를 전송할 수 있다.

[34] 참여 DB(210)는 다수의 로컬 그룹(200,300,400)을 형성하는 과정에서 중앙 서버(100) 또는 마스터 노드에 의해 지정되어, 마스터 노드(201)에 의해 다수의 노드(202,203,204,205,206,207,208,209) 각각에 대해 새로 갱신되는 특징 세트(C)의 정보 또는 다수의 노드(202,203,204,205,206,207,208,209) 각각에서 수행한 학습 결과를 저장할 수 있다.

[35] 이렇게 그룹을 이루는 다수의 로컬 그룹(200,300,400)에 대해, 중앙 서버(100)는 다수의 노드 각각에 대해 새로 갱신되는 특징 세트(C)의 정보를 이용하여 그룹 내의 노드를 배제시킬 수 있어서, 신뢰성을 향상 유지시켜 정보 노출로 인한 보안 위험을 최소화하면서 글로벌 모델 생성과 같은 효율적인 연합학습을 이룰수 있다.

[36] 이에 따라 본 발명의 일실시예에 따른 연합학습 시스템은 다수의 로컬 그룹(200,300,400)과 같은 로컬 계층 및 로컬 그룹(200,300,400) 각각의 마스터 노드와 중앙 서버(100)로 이루어진 글로벌 계층으로 이루어진 계층구조를 갖고 업데이트 횟수를 줄임으로써, 학습에 필요한 계산 및 비용을 절감하고 발생 가능한 보안 위험성을 최소화할 수 있다.

[37]

[38] 이하, 본 발명의 다른 실시예에 따른 연합학습 제어방법에 대해 도 3과 도 4를 참조하여 설명한다. 도 3은 본 발명의 다른 실시예에 따른 연합학습 제어방법을 설명하기 위한 순서도이고, 도 4는 본 발명의 다른 실시예에 따른 연합학습

제어방법을 나타낸 소스코드의 예시도이다.

[39] 본 발명의 다른 실시예에 따른 연합학습 제어방법은 먼저 중앙서버(100)가 연합학습에 참여할 노드들에게 특징 세트(C)의 정보를 요청한다(S310).

[40] 구체적으로, 중앙서버(100)는 연합학습에 참여하고자하는 노드들에게 특징 세트(C)의 정보를 요청하는 신호를 전송할 수 있다.

[41] 이러한 특징 세트(C)의 정보를 요청하는 신호를 수신한 노드들 각각은 특징 세트(C)의 정보를 생성하여 중앙서버(100)로 전달한다.

[42] 이때, 특징 세트(C)의 정보는 노드들 각각의 특성을 나타낸 정보로서, 아래의 [수학식 1]과 같이 나타낼 수 있다.

[43] [수학식 1]

[44]

$$C=\{T,E,A,P,Q,D\}$$

[45] 이러한 특징 세트(C)의 정보를 구성하는 파라미터는 아래의 [표 1]에 기재된 바와 같이 정의될 수 있다.

[46] [표1]

특징 세트(C)의 파라미터	정의
T	신뢰도 점수 (Trust score)
E	수행 능력 (Execution capacity)
A	가용성 (Availability)
P	학습 참여 유무 (Participation in training)
Q	로컬 데이터품질 (Quality of local dataset)
D	디바이스 정보 (Vector having devices information)

[47] 신뢰도 점수(T)는 다른 노드 또는 다른 서버에 의해 결정이 되고, 초기에는 모든 노드들이 예컨대 0.5의 점수를 가질 수 있다. 이러한 신뢰도 점수(T)는 반복적인 프로세스를 통해 마스터 노드(201)에 의해 갱신되어 참여 DB(210)에 저장될 수 있다. 이러한 신뢰도 점수(T)가 낮은 노드는 훈련 과정에서 로컬 그룹 내의 노드들 간의 높은 신뢰도를 유지하기 위해 탈퇴할 수 있다.

[48] 이러한 신뢰도 점수(T)는 아래의 [수학식 2]와 같이 나타낼 수 있고, 마스터 노드(201)에 의해 참여 DB(210)에 저장될 수 있다.

[49] [수학식 2]

[50]

$$T=f(B,RB)=w_1 \times B+w_2 \times RB$$

[51] 여기서, B는 노드의 행동특성수치이고, RB는 추천 점수이며, w_1은 B의 중요도에 따른 가중치이며, w_2는 RB의 중요도에 따른 가중치이다.

[52] 노드의 행동특성수치(B)는 특징 세트(C)의 정보에서 신뢰도 점수(T), 수행능력(E), 참여유무(P), 가용성(A) 등의 정보를 이용하여 결정된다. 즉, 노드의 행동특성수치(B)는 아래의 [수학식 3]과 같은 관계식으로 정규화하여 연산할 수 있다.

[53] [수학식 3]

[54]

$$B = (t^s + e^s + a^s + PF^s) / n$$

[55] 여기서, t^s는 노드의 신뢰도 점수(T)를 정규화한 점수이고, e^s는 노드의 수행능력(E)을 정규화한 점수이며, a^s는 노드의 가용성(A)을 정규화한 점수이며, PF^s는 노드의 참여빈도(PF)를 정규화한 점수이며, n은 B값을 계산하기 위한 특성의 개수로서 여기서는 4를 의미한다. 또한, 노드의 참여빈도(PF)는 학습 과정 동안 마스터 노드에 의해 저장되고 업데이트되는 각 노드의 참여 빈도이며 초기값은 모든 노드에서 0이다.

[56] 추천 점수(RB)는 다른 노드로부터 추천받은 정도를 나타낸 것으로, 아래의 [수학식 4]와 같은 관계식으로 나타낼 수 있다.

[57] [수학식 4]

[58]

$$RB = B_{avg} = \left(\sum_{i=1}^{m} B_i\right) / m$$

[59] 여기서, B_i는 주변 노드의 행동특성수치이고, m은 주변 노드의 개수를 나타낸다.

[60] 수행 능력(E)은 주어진 학습의 처리 능력을 나타낸 값으로, 예컨대 전산처리 속도, 메모리 용량, 통신속도 등의 가용 가능한 전산 및 네트워크 자원을 종합적으로 고려하여 계산한다.

[61] 가용성(A)은 클라이언트가 연합학습 프로세스에 참여하고자 하는 시간을 의미한다.

[62] 학습 참여 유무(P)는 각 노드가 연합학습에 참여하는지 여부를 나타낸 값으로 0 또는 1의 값을 갖는다.

[63] 로컬 데이터품질(Q)은 데이터 클래스별 표본 수를 의미한다. 여러 클래스가 있는 경우 조화 평균값 등의 평균값 계산법을 사용하여 전체 클래스의 데이터품질 값을 계산할 수 있다.

[64] 디바이스 정보(D)는 각 노드의 IP주소, MAC주소, 프로토콜, 위치 등의 정보를 포함한다.

[65]

[66] 이렇게 구성된 특징 세트(C)의 정보를 중앙서버(100)가 연합학습에 참여할 노드들로부터 수신함에 따라, 중앙서버(100)는 노드들중에서 임시의 마스터 노드를 지정한다(S320).

[67] 구체적으로, 중앙서버(100)가 수신한 특징 세트(C)의 정보 중 신뢰도 점수(T),

수행능력(E), 참여유무(P) 및 가용성(A)의 정보를 이용하여 다른 노드보다 상대적으로 높은 값을 갖는 노드를 임시의 마스터 노드로 지정할 수 있다.

[68] 임시의 마스터 노드를 지정한 후, 중앙서버(100)는 수신한 특징 세트(C)의 정보를 이용하여 마스터 노드와 가장 가까운 설정된 개수의 노드들을 선별한다(S330).

[69] 즉, 중앙서버(100)는 디바이스 정보(D)의 위치 정보를 이용하여 지정된 마스터 노드로부터 가장 가까운 노드들을 설정된 개수로 선별할 수 있어서, 예컨대 아래의 [수학식 5]를 이용하여 노드의 위치(x^i)와 지정된 마스터 노드의 위치(μ_j) 사이의 거리 제곱의 합을 사용하여 가장 가까운 로컬 그룹에 할당되어 선별될 수 있다.

[70] [수학식 5]

[71]

$$w_{ik} = \begin{cases} 1 & \text{if } k = \operatorname{argmin}_j \left\| x^i - \mu_j \right\|^2 \\ 0 & \text{otherwise} \end{cases}$$

[72] 여기서, w_{ik}는 거리변수이고, x^i는 노드의 위치이며, μ_j는 마스터 노드의 위치이다.

[73] [수학식 6]

[74]

$$J = \sum_{i=1}^{m} \sum_{k=1}^{K} w_{ik} \left\| x^i - \mu_k \right\|^2$$

[75] 여기서, m은 노드의 개수이고, k는 그룹의 개수이며, x^i는 노드의 위치이며, μ_K는 마스터 노드의 위치이다.

[76] 물론, 상술한 [수학식 6]의 그룹화 함수(J) 이외에 다양한 그룹화 함수를 포함한 알고리즘으로 다수의 로컬 그룹(200,300,400)을 생성할 수 있다.

[77] 이때, 중앙서버(100)는 각 마스터 노드를 다시 지정할 수 있어서, 아래의 [수학식 7]을 이용하여 각 로컬 그룹의 마스터 노드를 재조정할 수 있다.

[78] [수학식 7]

[79]

$$\mu_k = \frac{\sum_{i=1}^{m} w_{ik} x^i}{\sum_{i=1}^{m} w_{ik}}$$

[80] 여기서, μ_K는 마스터 노드의 위치이고, m은 노드의 개수이고, w_{ik}는 거리변수이며, k는 그룹의 개수이며, x^i는 노드의 위치이다.

[81] 이렇게 다수의 로컬 그룹(200,300,400)을 생성하는 과정에서 중앙 서버(100) 또는 마스터 노드가 참여 DB(210)를 지정할 수 있다.

[82] 다수의 로컬 그룹(200,300,400)을 생성한 후, 중앙서버(100)는 각 마스터 노드를 통해 각 그룹을 구성하는 노드로부터 개인정보 보호 수준 및 데이터 공유 방식에 관한 합의를 포함한 연합학습 정책정보를 수신한다(S350).

[83] 이러한 연합학습 정책정보를 수신함에 따라, 다수의 로컬 그룹(200,300,400)과 중앙서버(100)는 연합 학습을 수행하고, 로컬 그룹(200,300,400) 각각의 마스터 노드는 로컬 그룹을 구성하는 다른 노드들로부터 취합한 학습 결과를 중앙서버(100)로 전송한다.

[84] 이와 같은 과정의 본 발명의 다른 실시예에 따른 연합학습 제어방법은 특징 세트(C)의 정보를 이용하여 부적합 노드들을 배제하면서 다수의 로컬 그룹을 생성하므로, 신뢰성을 향상 유지시켜 정보 노출로 인한 보안 위험을 최소화하면서 효율적인 연합학습을 수행할 수 있다.

[85]

[86] 본 발명의 기술사상은 상기 바람직한 실시예에 따라 구체적으로 기술되었으나, 전술한 실시예들은 그 설명을 위한 것이며, 그 제한을 위한 것이 아님을 주의하여야 한다.

[87] 또한, 본 발명의 기술분야의 통상의 전문가라면 본 발명의 기술사상의 범위 내에서 다양한 실시가 가능함을 이해할 수 있을 것이다.

[88] [부호의 설명]

[89] 100: 중앙 서버 200,300,400: 로컬 그룹

[90] 201: 마스터 노드

[91] 202,203,204,205,206,207,208,209: 노드

[92] 210 참여 DB

청구범위

[청구항 1] 적어도 하나의 중앙 서버와 다수의 로컬 그룹을 포함하고,
상기 다수의 로컬 그룹 각각은 하나의 마스터 노드(Node)와 다수의 노드를 포함하여 구성되며,
상기 다수의 로컬 그룹은 상기 중앙 서버가 연합학습을 위한 특징 세트(C)의 정보를 이용하여 형성하는 것을 특징으로 하는 연합학습 시스템.

[청구항 2] 제 1 항에 있어서,
상기 다수의 로컬 그룹 각각은 상기 마스터 노드에 연결된 참여 DB(participation DB)를 더 포함하는 것을 특징으로 하는 연합학습 시스템.

[청구항 3] 제 1 항에 있어서,
상기 특징 세트(C)의 정보는 신뢰도 점수(T), 수행능력(E), 가용성(A), 참여유무(P), 로컬 데이터품질(Q) 및 디바이스 정보(D) 중 어느 하나를 포함하는 것을 특징으로 하는 연합학습 시스템.

[청구항 4] (ㄱ) 중앙서버가 연합학습에 참여할 다수의 노드에게 특징 세트(C)의 정보를 요청하는 단계;
(ㄴ) 상기 중앙서버가 상기 특징 세트(C)의 정보를 이용하여 상기 다수의 노드중에서 임시의 마스터 노드를 지정하는 단계;
(ㄷ) 상기 중앙서버가 상기 마스터 노드와 상기 마스터 노드에 인접한 노드들로 이루어진 다수의 로컬 그룹을 생성하는 단계; 및
(ㄹ) 상기 중앙서버는 상기 마스터 노드를 통해 상기 로컬 그룹을 구성하는 노드로부터 연합학습 정책정보를 수신하는 단계;
를 포함하는 연합학습 제어방법.

[청구항 5] 제 4 항에 있어서,
상기 (ㄷ) 단계에서 다수의 로컬 그룹 각각은 상기 마스터 노드에 연결된 참여 DB(participation DB)를 더 포함하는 것을 특징으로 하는 연합학습 제어방법.

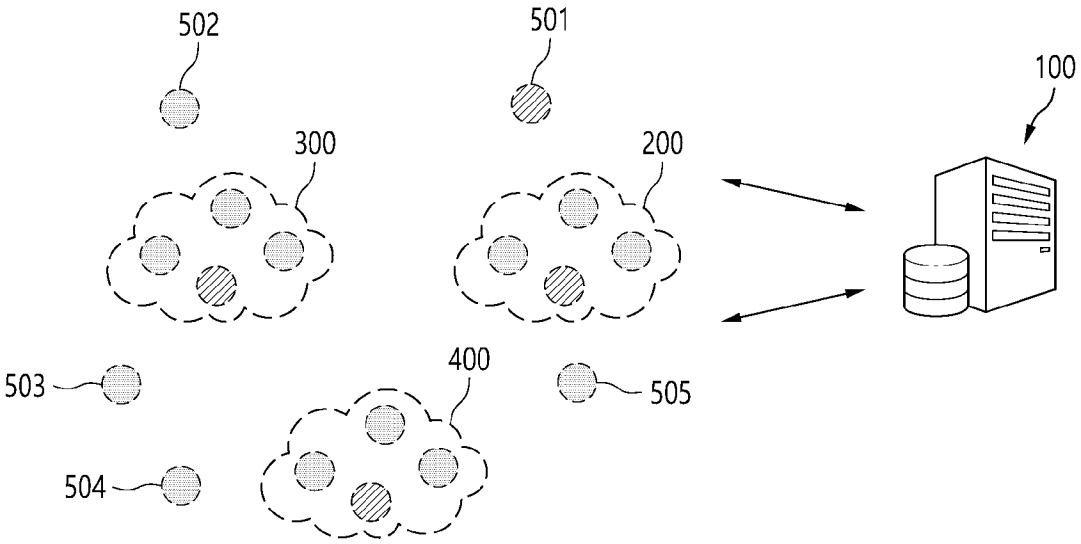
[청구항 6] 제 4 항에 있어서,
상기 특징 세트(C)의 정보는 신뢰도 점수(T), 수행능력(E), 가용성(A), 참여유무(P), 로컬 데이터품질(Q) 및 디바이스 정보(D) 중 어느 하나를 포함하는 것을 특징으로 하는 연합학습 제어방법.

[청구항 7] 제 6 항에 있어서,
상기 신뢰도 점수(T)는 상기 다수의 노드 각각의 행동특성수치(B) 및 추천 점수(RB)에 의해 결정되는 것을 특징으로 하는 연합학습 제어방법.

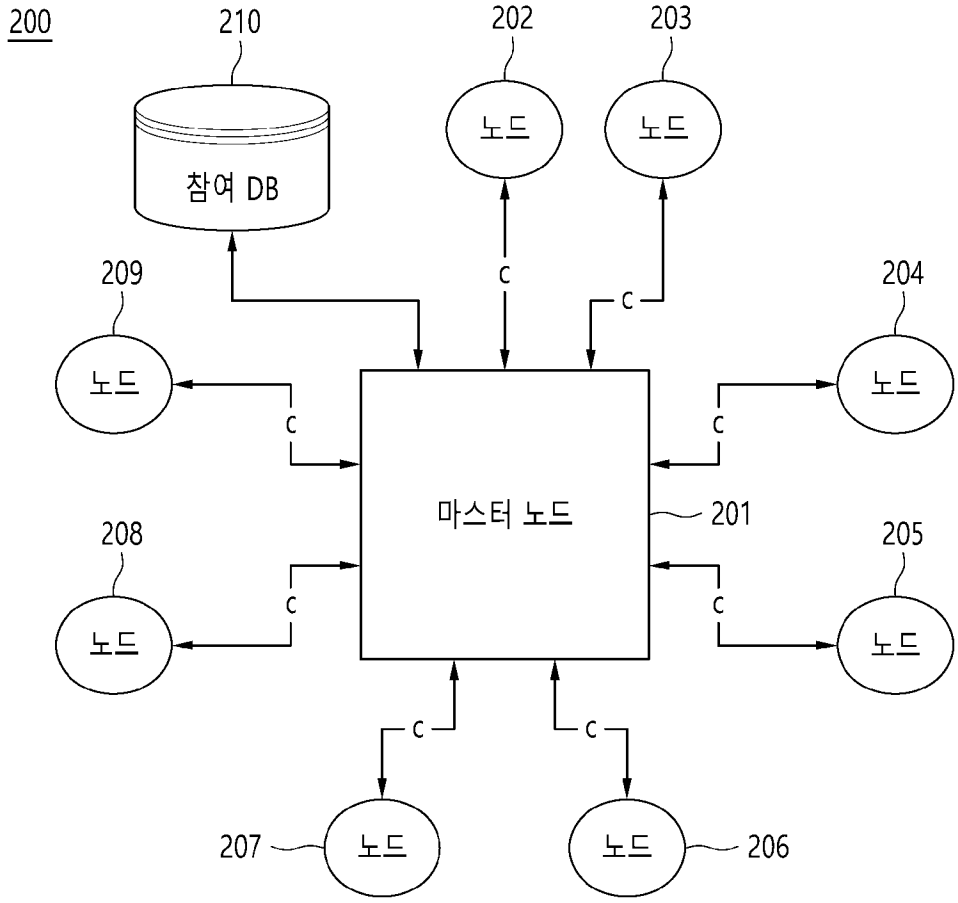
[청구항 8] 제 6 항에 있어서,
상기 (ㄴ)단계는 상기 신뢰도 점수(T), 수행능력(E), 참여유무(P) 및 가용성(A)의 정보를 이용하여 상기 임시의 마스터 노드를 지정하는 것을

특징으로 하는 연합학습 제어방법.

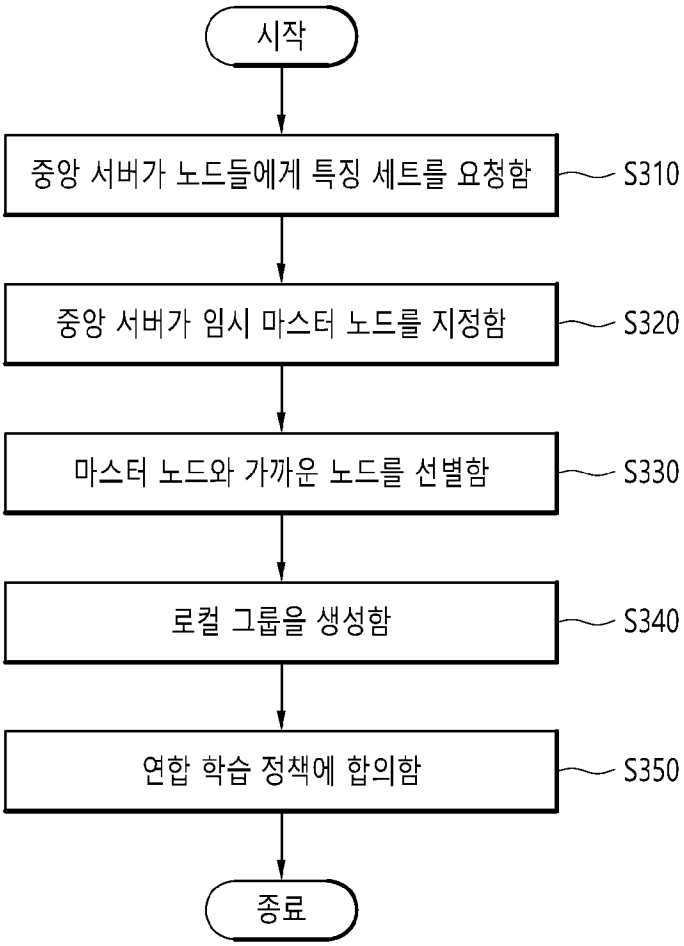
[도1]


502
501
100
300
200
503
400
505
504

[도2]


200
210
202
203
참여 DB
노드
노드
209
204
노드
노드
c
c
c
c
마스터 노드
201
208
205
노드
노드
c
c
c
c
207
노드
노드
206

[도3]


시작
중앙 서버가 노드들에게 특징 세트를 요청함
S310
중앙 서버가 임시 마스터 노드를 지정함
S320
마스터 노드와 가까운 노드를 선별함
S330
로컬 그룹을 생성함
S340
연합 학습 정책에 합의함
S350
종료

[도4]

$N, |K|, TT, t_l, U$ **w** (T)

Function CreateTrustedGroup ( ) ($N, C = \{\}$) :

    / / Using Kmeans or any other clustering K groups will form

    $J = \sum_{i=1}^{m} \sum_{k=1}^{K} w_{ik} \left\| x^i - \mu_k \right\|^2$

    for $Node\ in\ N$ **do**

        / / Decide Group number for each Node

        GroupInfor [$Node$] ← MasterNode = $Cluster_i$ [$Centroid$], Group = $Cluster_i$

    end

    return GroupInfo (G)

initialization **w** (0), C ← { } ;

for $Node\ in\ N$ **do**

    $C = \{\}$ ← GetNodeCharacteristics ($Node$)

end

G ← CreateTrustedGroup (N, C = { })

/ / Send initial Global model to Groups

$[\mathbf{w}_i^k(0)]_{i \in G} \leftarrow \mathbf{w}(0)$

/ / Global Training Using Updates counts

for $u \leftarrow U$ **do**

    / / Local training using allocated t_l

    for $i \leftarrow \in K$ ($in\ parallel$) **do**

        if t_l **then**

            $F^k(\mathbf{w}) \triangleq \sum_{i \in N^k} \frac{|\mathrm{D}_i^k|}{|\mathrm{D}^k|} F_i^k(\mathbf{w})$

        else

            Submit the local updates

        end

    end

    / / Global Aggregation for round u given that t_l is over

    if $u \leq U\ and\ t_l == O$ **then**

        $F(\mathbf{w}) \triangleq \sum_{k \in K} \frac{|\mathrm{D}^k|}{|\mathrm{D}|} F^k(\mathbf{w}), F^k(\mathbf{w}) \triangleq \sum_{i \in N^k} \frac{|\mathrm{D}_i^k|}{|\mathrm{D}^k|} F_i^k(\mathbf{w})$

    end

end

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2023/000064

A. CLASSIFICATION OF SUBJECT MATTER

G06N 20/20(2019.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06N 20/20(2019.01); G06F 16/215(2019.01); G06F 16/242(2019.01); G06F 9/50(2006.01); G06N 3/04(2006.01); G06N 3/08(2006.01); G06N 5/04(2006.01); H04L 12/24(2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models: IPC as above
Japanese utility models and applications for utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & keywords: 연합 학습(federated learning), 로컬 그룹(local group), 중앙 서버(central server), 마스터 노드(master node), 특징 세트(characteristic set)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2021-008675 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)) 21 January 2021 (2021-01-21) See page 5, line 33 - page 6, line 6 and page 7, line 14 - page 8, line 37; and figures 1-2.	1-3
Y		4-8
Y	CN 112636989 A (AGRICULTURAL BANK OF CHINA) 09 April 2021 (2021-04-09) See paragraphs [0066] and [0068].	4-8
A	US 2021-0406782 A1 (TIESET, INC.) 30 December 2021 (2021-12-30) See paragraphs [0118]-[0119]; and claim 1.	1-8
A	KR 10-2021-0153884 A (LINE PLUS CORPORATION) 20 December 2021 (2021-12-20) See paragraphs [0046]-[0048].	1-8

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 March 2023	**30 March 2023**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office **Government Complex-Daejeon Building 4, 189 Cheongsa-ro, Seo-gu, Daejeon 35208**	
Facsimile No. **+82-42-481-8578**	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2023/000064

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 112181971 A (HUAQIAO UNIVERSITY et al.) 05 January 2021 (2021-01-05) See claim 1.	1-8

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2023/000064

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO 2021-008675 A1	21 January 2021	None	
CN 112636989 A	09 April 2021	CN 112636989 B	27 December 2022
US 2021-0406782 A1	30 December 2021	WO 2022-005937 A1	06 January 2022
KR 10-2021-0153884 A	20 December 2021	CN 113807495 A	17 December 2021
		JP 2021-197181 A	27 December 2021
		US 2021-0390152 A1	16 December 2021
CN 112181971 A	05 January 2021	CN 112181971 B	01 November 2022

국 제 조 사 보 고 서

국제출원번호
PCT/KR2023/000064

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06N 20/20(2019.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06N 20/20(2019.01); G06F 16/215(2019.01); G06F 16/242(2019.01); G06F 9/50(2006.01); G06N 3/04(2006.01); G06N 3/08(2006.01); G06N 5/04(2006.01); H04L 12/24(2006.01)

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 연합 학습(federated learning), 로컬 그룹(local group), 중앙 서버(central server), 마스터 노드(master node), 특징 세트(characteristic set)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	WO 2021-008675 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)) 2021.01.21 페이지 5, 라인 33 - 페이지 6, 라인 6; 페이지 7, 라인 14 - 페이지 8, 라인 37; 및 도면 1-2	1-3
Y		4-8
Y	CN 112636989 A (AGRICULTURAL BANK OF CHINA) 2021.04.09 단락 [0066], [0068]	4-8
A	US 2021-0406782 A1 (TIESET, INC.) 2021.12.30 단락 [0118]-[0119]; 및 청구항 1	1-8
A	KR 10-2021-0153884 A (라인플러스 주식회사) 2021.12.20 단락 [0046]-[0048]	1-8
A	CN 112181971 A (HUAQIAO UNIVERSITY 등) 2021.01.05 청구항 1	1-8

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☑ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"D" 본 국제출원에서 출원인이 인용한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2023년03월30일(30.03.2023)	**2023년03월30일(30.03.2023)**

ISA/KR의 명칭 및 우편주소	심사관
대한민국 특허청 **(35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)**	**양정록**
팩스 번호 **+82-42-481-8578**	전화번호 **+82-42-481-5709**

서식 PCT/ISA/210 (두 번째 용지) (2022년 7월)

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2023/000064

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
WO 2021-008675 A1	2021/01/21	없음	
CN 112636989 A	2021/04/09	CN 112636989 B	2022/12/27
US 2021-0406782 A1	2021/12/30	WO 2022-005937 A1	2022/01/06
KR 10-2021-0153884 A	2021/12/20	CN 113807495 A	2021/12/17
		JP 2021-197181 A	2021/12/27
		US 2021-0390152 A1	2021/12/16
CN 112181971 A	2021/01/05	CN 112181971 B	2022/11/01