(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2023 년 6 월 29 일 (29.06.2023)

WIPO | PCT

(10) 국제공개번호
WO 2023/120776 A1

(51) 국제특허분류:
G06N 3/04 (2006.01) *G06N 20/20* (2019.01)
G06N 3/08 (2006.01)

(21) 국제출원번호: PCT/KR2021/019745

(22) 국제출원일: 2021 년 12 월 23 일 (23.12.2021)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2021-0186279 2021 년 12 월 23 일 (23.12.2021) KR

(71) 출원인: 경희대학교 산학협력단 (**UNIVERSITY-INDUSTRY COOPERATION GROUP OF KYUNG HEE UNIVERSITY**) [KR/KR]; 17104 경기도 용인시 기흥구 덕영대로 1732, Gyeonggi-do (KR).

(72) 발명자: 홍충선 (**HONG, Choong Seon**); 16941 경기도 용인시 수지구 상현로 30-10, 233-101, Gyeonggi-do (KR). 뉴엔후 낫 민 (**NGUYEN, Huu Nhat Minh**); 17103 경기도 용인시 기흥구 서그내로 16번길 17, 203호, Gyeonggi-do (KR). 레쾅 후이 (**LE, Quang Huy**); 16705 경기도 수원시 영통구 청명남로4번길 21-4, B03호, Gyeonggi-do (KR). 신종훈 (**SHIN, Jong Hoon**); 17098 경기도 용인시 기흥구 덕영대로 1883, 204동 1101호, Gyeonggi-do (KR).

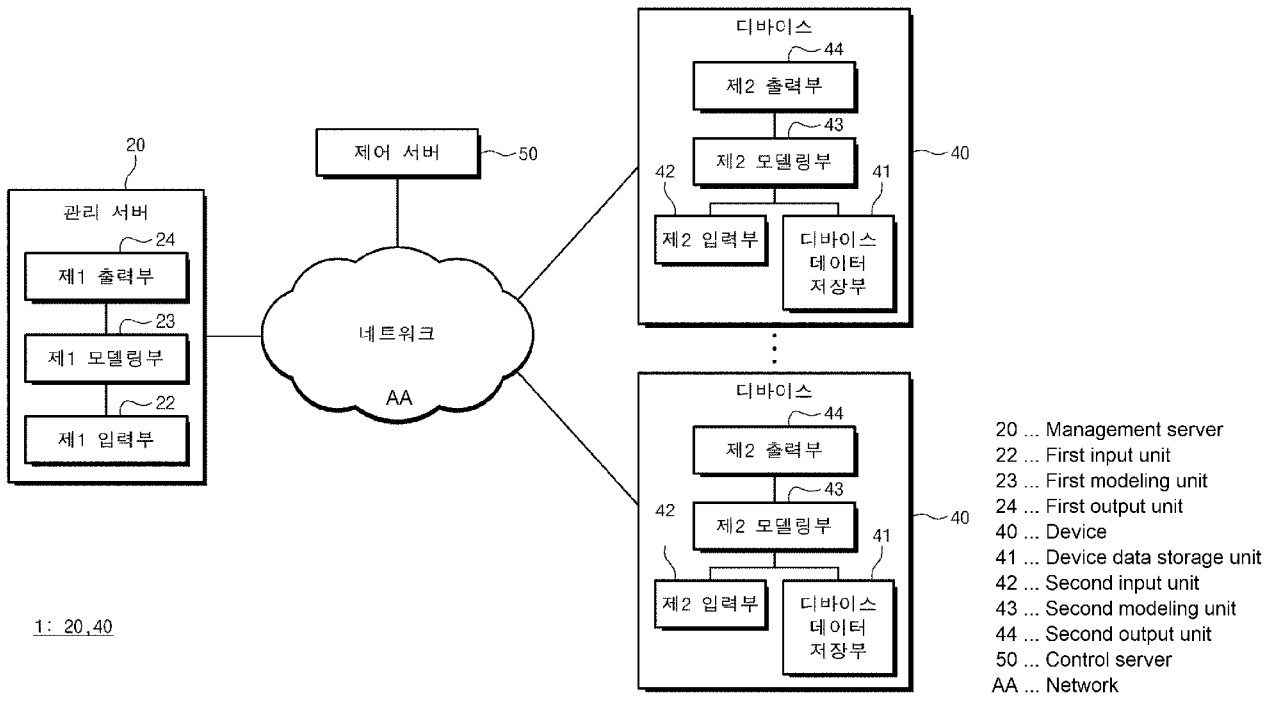
(74) 대리인: 강일신 등 (**KANG, Il Shin** et al.); 06753 서울특별시 서초구 바우뫼로 150, 2층, Seoul (KR).

(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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, 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.

WO 2023/120776 A1

(54) **Title:** DEVICE-TO-DEVICE KNOWLEDGE TRANSMISSION METHOD USING PROXY DATASET IN FEDERATED LEARNING, AND SYSTEM THEREFOR

(54) **발명의 명칭:** 연합학습에서 프록시데이터 세트를 이용한 장치 간 지식 전달 방법 및 그 시스템



1: 20,40

(57) **Abstract:** A device-to-device knowledge transmission method using a proxy dataset in federated learning, according to the present invention, comprises the steps of: downloading proxy data; generating, by a management server, management server output knowledge by machine learning input data by using a first artificial neural network function; generating, by first to nth devices, a plurality of pieces of device output knowledge by machine learning input data by using a second artificial neural network function; and if a preset number of times is reached, stopping the machine learning, transmitting the management server output knowledge to the first to nth devices, and transmitting the plurality of pieces of device output knowledge to the management server.

[다음 쪽 계속]

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, 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, 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))

(57) 요약서: 본 발명인 연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달방법은, 프록시데이터를 다운로드하는 단계, 관리서버에서 제1 인공신경망함수를 이용하여 입력데이터를 기계학습하여 관리서버출력지식을 생성하는 단계, 제1 내지 제n 디바이스에서 제2 인공신경망함수를 이용하여 입력데이터를 기계학습하여 복수의 디바이스출력지식을 생성하는 단계 및 미리 설정된 횟수에 도달한 경우 상기 기계학습을 중단하고 관리서버출력지식을 제1 내지 제n 디바이스에 전송하고 복수의 디바이스출력지식을 관리서버에 전송하는 단계를 포함하는 단계를 포함한다.

명세서

발명의 명칭: 연합학습에서 프록시데이터 세트를 이용한 장치 간 지식 전달 방법 및 그 시스템

기술분야

[1] 본 발명은 연합학습에서 프록시데이터 세트를 이용한 장치 간 지식 전달 방법 및 그 시스템에 관한 것이다.

[2] 본 발명은 과학기술정보통신부의 집단연구지원(R&D)(과제고유번호: 1711135177, 과제번호: 2020R1A4A1018607, 연구과제명: Meta Federated Learning기반 이동엣지 컴퓨팅시스템 핵심구조 개발, 과제관리기관: 한국연구재단, 과제수행기관: 경희대학교(국제캠퍼스) 산학협력단, 연구기간: 2020.07.01.~2023.02.28.) 및 정보통신방속혁신인재양성(R&D)(과제고유번호: 1711139517, 과제번호: 2021-0-02068-001, 연구과제명: 인공지능 혁신 허브 연구개발, 과제관리기관: 정보통신기획평가원, 과제수행기관: 경희대학교(국제캠퍼스) 산학협력단, 연구기간: 2020.07.01.~2025.12.31.)의 일환으로 수행한 연구로부터 도출된 것이다. 한편, 본 발명의 모든 측면에서 한국 정부의 재산 이익은 없다

배경기술

[3] 최근의 모바일 애플리케이션은 사용자의 데이터에 기반하여 AI기반 카메라, 증강확장현실(XR, Extended Reality), 및 지능형비서와 같은 다양한 AI 기능을 구비하고 있다. 다만, 위와 같은 중앙 집중식 머신러닝(ML)을 사용하는 AI기능은 필수적으로 개인정보데이터가 유출될 염려가 있다.

[4] 이에, 개인정보데이터의 유출을 방지할 수 있는 연합학습(FL)에 기반한 머신러닝(ML)을 사용하는 AI기능의 개발이 지속적으로 진행되고 있다.

[5] 그러나, 위와 같은 연합학습(FL)에 기반한 머신러닝을 사용하는 AI기능은 중앙컴퓨팅장치와 다양한 사용자디바이스에서 학습데이터의 이질성이 존재하므로 머신러닝학습의 기능이 저하될 수 있고 결론적으로 머신러닝학습모델의 차이가 발생된다.

[6] 이에, 개인정보데이터의 유출을 방지하는 동시에 중앙컴퓨팅장치와 사용자디바이스에서 머신러닝학습의 성능을 향상시키는 기술이 필요한 실정이다.

발명의 상세한 설명

기술적 과제

[7] 본 발명이 해결하고자 하는 기술적 과제는, 연합학습(FL)에 기반한 머신러닝을 이용하는 AI 학습과정에서 개인정보데이터의 유출을 방지하기 위한 연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달 방법 및 그 시스템에 관한 것이다.

[8] 또한, 본 발명이 해결하고자 하는 기술적 과제는, 연합학습(FL)에 기반한 머신러닝을 이용하는 AI 학습과정에서 통신데이터부하를 최소화시키면서도 머신러닝의 학습기능을 향상시키기 위한 연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달 방법 및 그 시스템에 관한 것이다.

과제 해결 수단

[9] 본 발명의 한 실시예에 따른 연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달 방법은, 프록시데이터를 다운로드하는 단계, 관리서버에서 제1 인공신경망함수를 이용하여 입력데이터를 기계학습하여 관리서버출력지식을 생성하는 단계, 제1 내지 제n 디바이스에서 제2 인공신경망함수를 이용하여 입력데이터를 기계학습하여 복수의 디바이스출력지식을 생성하는 단계 및 미리 설정된 횟수에 도달한 경우 기계학습을 중단하고 관리서버출력지식을 제1 내지 제n 디바이스에 전송하고 복수의 디바이스출력지식을 관리서버에 전송하는 단계를 포함한다.

[10] 또한, 본 발명의 한 실시예에 따른 관리서버에서 제1 인공신경망함수를 이용하여 입력데이터를 기계학습하여 관리서버출력지식을 생성하는 단계는, 제1 내지 제n 디바이스에서 제공된 복수의 제n 디바이스출력지식을 입력받는 단계 및 입력데이터에 기초하여 제1 인공신경망함수에서 생성된 제n 관리서버출력지식 및 프록시데이터에 기초하여 제1 손실함수를 생성하는 단계를 포함한다.

[11] 또한, 본 발명의 한 실시예에 따른 관리서버에서 제1 인공신경망함수를 이용하여 입력데이터를 기계학습하여 관리서버출력지식을 생성하는 단계는, 복수의 제n 디바이스출력지식, 제n 관리서버출력지식, 및 프록시데이터에 기초하여 제1 정규화함수를 생성하는 단계, 제1 손실함수 및 제1 정규화함수에 기초하여 제1 인공신경망함수를 생성하는 단계 및 제1 인공신경망함수에서 입력데이터를 기계학습하고 제n+1 관리서버출력지식을 생성하는 단계를 더 포함한다.

[12] 또한, 본 발명의 한 실시예에 따른 제1 내지 제n 디바이스에서 제2 인공신경망함수를 이용하여 입력데이터를 기계학습하여 복수의 디바이스출력지식을 생성하는 단계는, 관리서버에서 제공된 제n+1 관리서버출력지식을 입력받는 단계, 제1 내지 제n 디바이스 각각에서 생성된 복수의 제n 디바이스개인데이터를 업로드하는 단계 및 입력데이터에 기초하여 생성된 복수의 제n 디바이스출력지식 각각 및 복수의 제n 디바이스개인데이터 각각에 기초하여 복수의 제2 손실함수를 생성하는 단계를 포함한다.

[13] 또한, 본 발명의 한 실시예에 따른 제1 내지 제n 디바이스에서 제2 인공신경망함수를 이용하여 입력데이터를 기계학습하여 복수의 디바이스출력지식을 생성하는 단계는, 복수의 제n 디바이스출력지식 각각, 제n+1 관리서버출력지식, 및 프록시데이터에 기초하여 복수의 제2

정규화함수를 생성하는 단계, 복수의 제2 손실함수 및 복수의 제2 정규화함수에 기초하여 복수의 제2 인공신경망함수를 생성하는 단계 및 복수의 제2 인공신경망함수에 기초하여 입력데이터를 기계학습하고 복수의 제n+1 디바이스출력지식을 생성하는 단계를 더 포함한다.

[14] 또한, 본 발명의 한 실시예에 따른 미리 설정된 횟수에 도달한 경우 기계학습을 중단하고 관리서버출력지식을 제1 내지 제n 디바이스에 전송하고 복수의 디바이스출력지식을 관리서버에 전송하는 단계를 포함하는 단계는, 미리 설정된 횟수에 도달한 경우 제1 인공신경망함수에서 입력데이터의 기계학습을 중단하고 제n+1 관리서버출력지식을 제1 내지 제n 디바이스에 전송하는 단계 및 미리 설정된 횟수에 도달한 경우 제2 인공신경망함수에서 입력데이터의 기계학습을 중단하고 복수의 제n+1 관리디바이스출력지식을 관리서버에 전송하는 단계를 포함한다. 또한, 본 발명의 한 실시예에 따른 연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달시스템은, 프록시데이터 및 제1 인공신경망함수를 이용하여 입력데이터를 기계학습하고 관리서버출력지식을 생성하는 관리서버, 프록시데이터 및 제2 인공신경망함수를 이용하여 입력데이터를 기계학습하고 복수의 디바이스출력지식을 생성하는 제1 내지 제n 디바이스 및 미리 설정된 횟수에 도달한 경우 기계학습을 중단하는 제어서버를 포함한다.

[15] 또한, 본 발명의 한 실시예에 따른 상기 관리서버는, 제1 내지 제n 디바이스에서 복수의 제n 디바이스출력지식을 입력받는 제1 입력부, 입력데이터에 기초하여 제1 인공신경망함수에서 생성된 제n 관리서버출력지식 및 프록시데이터에 기초하여 제1 손실함수를 생성하고 복수의 제n 디바이스출력지식, 제n 관리서버출력지식, 및 프록시데이터에 기초하여 제1 정규화 함수를 생성하고 제1 손실함수 및 제1 정규화 함수에 기초하여 제1 인공신경망함수를 생성하는 제1 모델링부 및 제1 인공신경함수에서 입력데이터를 기계학습한 결과인 제n+1 관리서버출력지식을 제1 내지 제n 디바이스에 출력하는 제1 출력부를 포함한다.

[16] 또한, 본 발명의 한 실시예에 따른 제1 내지 제n 디바이스 각각은, 제n+1 관리서버출력지식을 입력받는 제2 입력부, 미리 저장된 제n 개인의 데이터셋과 프록시 데이터셋으로 학습한 디바이스의 지식 업로드시키는 디바이스 데이터셋 저장부, 입력데이터에 기초하여 생성된 제n 디바이스출력지식 및 미리 저장된 제n 디바이스개인데이터에 기초하여 제2 손실함수를 생성하고 제n 디바이스출력지식, 제n+1 관리서버출력지식, 및 프록시데이터에 기초하여 제2 정규화함수를 생성하고, 제2 손실함수 및 제2 정규화함수에 기초하여 제2 인공신경망함수를 생성하는 제2 모델링부 및 제2 인공신경망함수에 기초하여 입력데이터를 기계학습하고 제n+1 디바이스출력지식을 생성하는 제2 출력부를 포함한다.

[17] 또한, 본 발명의 한 실시예에 따른 제어서버는, 미리 설정된 횟수에 도달한 경우 제1 인공신경망함수에서 입력데이터의 기계학습을 중단하고 제n+1

관리서버출력지식을 제1 내지 제n 디바이스에 전송하고 미리 설정된 횟수에 도달한 경우 제2 인공신경망함수에서 입력데이터의 기계학습을 중단하고 복수의 제n+1 관리디바이스출력지식을 관리서버에 전송하도록 제어한다.

[18] 또한, 본 발명의 한 실시예에 따른 연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달방법을 실행시키는 프로그램이 기록된 컴퓨터로 판된 가능한 비일시적 기록 매체를 포함한다.

발명의 효과

[19] 본 발명에 따른 연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달방법 및 그 시스템은 연합학습(FL)에 기반한 머신러닝을 이용하는 AI 학습과정에서 개인정보데이터의 유출을 방지할 수 있다.

[20] 또한, 본 발명에 따른 연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달방법 및 그 시스템은 연합학습(FL)에 기반한 머신러닝을 이용하는 AI 학습과정에서 통신데이터의 부하를 최소화시키고 학습 속도를 증가시켜 기계학습의 학습기능을 향상시킬 수 있다.

도면의 간단한 설명

[21] 도 1은 본 발명의 한 실시예에 따른 연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달시스템에 관한 도면이다.

[22] 도 2는 본 발명의 한 실시예에 따른 관리서버 및 복수의 디바이스에서 인공신경망함수를 이용하여 머신러닝을 수행하는 과정을 설명하는 도면이다.

[23] 도 3은 본 발명의 한 실시예에 따른 관리서버에서 머신러닝을 수행하는 과정을 설명하는 흐름도이다.

[24] 도 4는 본 발명의 한 실시예에 따른 복수의 디바이스에서 인공신경망함수를 이용하여 머신러닝을 수행하는 과정을 설명하는 흐름도이다.

발명의 실시를 위한 형태

[25] 이하, 첨부한 도면을 참고로 하여 본 발명의 여러 실시 예들에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예들에 한정되지 않는다.

[26] 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 동일 또는 유사한 구성요소에 대해서는 동일한 참조 부호를 붙이도록 한다. 따라서 앞서 설명한 참조 부호는 다른 도면에서도 사용할 수 있다.

[27] 또한, 도면에서 나타난 각 구성의 크기 및 두께는 설명의 편의를 위해 임의로 나타내었으므로, 본 발명이 반드시 도시된 바에 한정되지 않는다. 도면에서 여러 층 및 영역을 명확하게 표현하기 위하여 두께를 과장되게 나타낼 수 있다.

[28] 또한, 설명에서 "동일하다"라고 표현한 것은, "실질적으로 동일하다"는 의미일 수 있다. 즉, 통상의 지식을 가진 자가 동일하다고 납득할 수 있을 정도의

동일함일 수 있다. 그 외의 표현들도 "실질적으로"가 생략된 표현들일 수 있다.

[29] 도 1은 본 발명의 한 실시예에 따른 연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달시스템에 관한 도면이다.

[30] 본 발명의 한 실시예에 따른 연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달시스템(1)은 관리서버(20) 및 복수의 디바이스(40)를 포함할 수 있다.

[31] 관리서버(20)는 제1 입력부(22), 제1 모델링부(23), 및 제1 출력부(24)를 포함할 수 있다.

[32] 제1 입력부(22)는 프록시데이터를 다운로드 할 수 있다. 제1 입력부(22)는 복수의 디바이스(40)에서 기계학습한 결과물인 복수의 디바이스출력지식(g1, ..., gn, 도 2 참고)을 입력 받을 수 있다.

[33] 제1 모델링부(23)는 제1 입력부(22)에서 제공되는 복수의 디바이스출력지식(g1, ..., gn), 프록시데이터, 및 제1 모델링부(23)(또는, 글로벌(전역) 모델)에 미리 저장된 제1 인공신경망함수(ANN(1))에서 기계학습한 결과물인 관리서버출력지식(gs, 도 2 참고)에 기초하여 입력데이터(x1)를 기계학습하기 위한 제1 인공신경망함수(ANN(1))를 재생성할 수 있다.

[34] 구체적으로, 제1 모델링부(23)는 제1 모델링부(23)에 미리 저장된 제1 인공신경망함수(ANN(1))에서 기계학습한 결과물인 관리서버출력지식(gs)과 업로드된 프록시데이터에 기초하여 제1 손실함수를 생성할 수 있다.

[35] 제1 모델링부(23)가 생성하는 제1 손실함수는 다운로드된 프록시데이터와 미리 저장된 제1 인공신경망함수(ANN(1))에서 기계학습한 결과물인 관리서버출력지식(gs)의 차이 값을 함수로 나타낸 것으로서, 지식증류법(KD, Knowledge Distillation)을 이용하여 생성될 수 있다.

[36] 또한, 제1 모델링부(23)는 제1 인공신경망함수(ANN(1))에서 기계학습한 결과물인 관리서버출력지식(gs), 다운로드된 프록시데이터, 및 복수의 디바이스출력지식(g1, ..., gn)에 기초하여 제1 정규화함수를 생성할 수 있다.

[37] 제1 모델링부(23)가 생성하는 제1 정규화함수는 다운로드된 프록시데이터를 기준으로 제1 인공신경망함수(ANN(1))에서 기계학습한 결과물인 관리서버출력지식(gs) 및 복수의 디바이스출력지식(g1, ..., gn) 간의 정규화 값을 함수로 나타낸 것으로서, 쿨백-라이블러 발산(Kullback-Leiber divergence, KLD) 및 Jensen-Shannon divergence 발산 등을 이용하여 생성될 수 있다.

[38] 쿨백-라이블러 발산(Kullback-Leiber divergence, KLD)이란 두개의 확률분포의 차이를 계산하는데 사용되는 함수로서, 이상적인 분포에 대해서 그 분포에 근사하는 다른 분포를 사용해 데이터를 샘플링 한다면 발생할 수 있는 정보 엔트로피의 차이를 의미한다. Jensen-Shannon divergence 발산은 쿨백-라이블러 발산(Kullback-Leiber divergence, KLD)을 거리 개념으로 사용하는 것으로서, 쿨백-라이블러 발산(Kullback-Leiber divergence, KLD)에 기초하여 2개의 정보 엔트로피 차이를 산출하고 평균을 내는 방식을 의미한다.

[39] 제1 모델링부(23)는 제1 손실함수 및 제1 정규화함수에 기초하여 입력데이터(x1)를 기계학습하기 위한 제1 인공신경망함수(ANN(1))를 재생성할 수 있다.

[40] 제1 출력부(24)는 제1 인공신경망함수(ANN(1))에 기초하여 입력데이터(x1)를 기계학습한 결과물인 관리서버출력지식(gs)을 복수의 디바이스(40)에 제공할 수 있다. 제1 출력부(24)에서 출력된 관리서버출력지식(gs)은 네트워크(30)를 통해서 복수의 디바이스(40)에 제공될 수 있다.

[41] 복수의 디바이스(40)는 디바이스데이터저장부(41), 제2 입력부(42), 제2 모델링부(43), 및 제2 출력부(44)를 포함할 수 있다.

[42] 디바이스데이터저장부(41)는 디바이스(40)의 디바이스개인데이터를 저장할 수 있다. 이때, 디바이스개인데이터란 디바이스(40)를 사용하는 사용자의 데이터에 관한 것으로써 이미지, 텍스트, 음성파일 등 다양한 형태에 해당할 수 있다. 복수의 디바이스(40)의 디바이스데이터저장부(41)에 저장된 디바이스개인데이터는 사용자의 데이터에 따라서 서로 다를 수 있다.

[43] 제2 입력부(42)는 프록시데이터를 다운로드할 수 있다. 제2 입력부(42)는 관리서버(20)에서 기계학습한 결과물인 관리서버출력지식(gs)을 입력 받을 수 있다.

[44] 제2 모델링부(43)는 제2 입력부(42)에서 제공되는 관리서버출력지식(gs), 디바이스데이터저장부(41)에서 제공되는 디바이스개인데이터, 및 제2 모델링부(43)에 미리 저장된 제2 인공신경망함수(ANN(2(1), ..., ANN(2(n))에서 기계학습한 결과물인 디바이스출력지식(g1, ..., gn)에 기초하여 입력데이터(x2)를 기계학습하기 위한 제2 인공신경망함수(ANN(2(1), ..., ANN(2(n))를 재생성할 수 있다.

[45] 구체적으로, 제2 모델링부(43)는 디바이스데이터저장부(41)에서 제공되는 디바이스개인데이터와 다운로드된 프록시데이터에 기초하여 제2 손실함수를 생성할 수 있다.

[46] 제2 모델링부(43)가 생성하는 제2 손실함수는 다운로드된 프록시데이터와 디바이스데이터저장부(41)에서 제공되는 디바이스개인데이터의 차이 값을 함수로 나타낸 것으로서, 제1 인공신경망함수와 동일한 지식증류법(KD, Knowledge Distillation)을 이용하여 생성될 수 있다.

[47] 또한, 제2 모델링부(43)는 제2 인공신경망함수(ANN(2(1), ..., ANN(2(n))에서 기계학습한 결과물인 디바이스출력지식(g1, ..., gn), 업로드된 프록시데이터, 및 관리서버(20)에서 제공되는 관리서버출력지식(gs)에 기초하여 제2 정규화함수를 생성할 수 있다.

[48] 제2 모델링부(43)가 생성하는 제2 정규화함수는 다운로드된 프록시데이터를 기준으로 제2 인공신경망함수(ANN(2(1), ..., ANN(2(n))에서 기계학습한 결과물인 디바이스출력지식(g1, ..., gn) 및 관리서버출력지식(gs 간의 정규화 값을 함수로 나타낸 것으로서, 제2 인공신경망함수(ANN(2(1), ..., ANN(2(n))와

동일한 쿨백-라이블러 발산(Kullback-Leiber divergence, KLD) 및 Jensen-Shannon divergence 발산 등을 이용하여 생성될 수 있다.

[49] 제2 모델링부(43)는 제2 손실함수 및 제2 정규화함수에 기초하여 입력데이터(x2)를 기계학습하기 위한 제2 인공신경망함수(ANN(2(1), ..., ANN(2(n))를 재생성할 수 있다.

[50] 제2 출력부(44)는 제2 인공신경망함수(ANN(2(1), ..., ANN(2(n))에 기초하여 입력데이터(x2)를 기계학습한 결과물인 디바이스출력지식(g1, ..., gn)을 관리서버(20)에 제공할 수 있다. 제2 출력부(44)에서 출력된 디바이스출력지식(g1, ..., gn)은 네트워크(30)를 통해서 관리서버(20)에 제공될 수 있다.

[51] 제어서버(50)는 미리 설정된 횟수를 초과하면 제1 인공신경망함수(ANN(1))에서 입력데이터(x1)를 기계학습하는 것을 중단할 수 있다. 제어서버(50)는 미리 설정된 횟수를 초과하면 제2 인공신경망함수(ANN(2(1), ..., ANN(2(n))에서 입력데이터(x2)를 기계학습하는 것을 중단할 수 있다.

[52] 도 2는 본 발명의 한 실시예에 따른 관리서버 및 복수의 디바이스에서 인공신경망함수를 이용하여 머신러닝을 수행하는 과정을 설명하는 도면이다.

[53] 관리서버(20)에 포함된 제1 모델링부(23)가 생성하는 제1 인공신경망함수(ANN(1))는 제1 입력층(IL(1)), 제1 은닉층(HL(1)), 및 제1 출력층(OL(1))로 구성될 수 있다.

[54] 제1 입력층(IL(1))에는 입력데이터(x1)가 인가될 수 있다. 제1 입력층(IL(1))에 인가된 입력데이터(x1)가 제1 은닉층(HL(1))을 통과하면서 관리서버출력값데이터(zs)가 생성될 수 있다. 제1 은닉층(HL(1))을 통해서 생성된 관리서버출력값데이터(zs)는 제1 출력층(OL(1))으로 인가될 수 있다.

[55] 제1 은닉층(HL(1))은 다양한 활성화함수(activation function)에 의해서 구성될 수 있으며, 제1 은닉층(HL(1))에 인가된 입력데이터(x1)는 다양한 활성화함수(activation function)에 의해서 가중치 값이 곱해지고 관리서버출력값데이터(zs)으로 변환될 수 있다.

[56] 이하, 활성화함수(activation function)에 의해서 입력데이터(x1)에 곱해지는 가중치 값을 특성값데이터(또는, es)라 명명한다.

[57] 이때, 관리서버출력값데이터(zs)는 활성화함수(activation function)에 의해서 입력데이터(x1)에 곱해지는 특성값데이터(es)에 대한 정보를 포함하고 있다.

[58] 제1 모델링부(23)의 제1 출력층(OL(1))에서 생성된 관리서버출력값데이터(zs)는 제1 출력부(24)로 인가될 수 있다.

[59] 이때, 제1 출력부(24)는 네트워크(30)를 통해서 특성값데이터(es)에 대한 정보를 포함하는 관리서버출력값데이터(zs)에 기초하여 관리서버출력지식(gs)을 복수의 디바이스(40)에 제공할 수 있다.

[60] 복수의 디바이스(40)에 포함된 제2 모델링부(43)가 생성하는 제2

인공신경망함수(ANN(2(1)), ..., ANN(2(n)))는 제2 입력층(IL(2)), 제2 은닉층(HL(2)), 및 제2 출력층(OL(2))로 구성될 수 있다.

[61] 제2 입력층(IL(2))에는 입력데이터(x2)가 인가될 수 있다. 제2 입력층(IL(2))에 인가된 입력데이터(x2)가 제2 은닉층(HL(2))을 통과하면서 디바이스출력값데이터(z1, ..., zn)가 생성될 수 있다. 제2 은닉층(HL(2))을 통해서 생성된 디바이스출력값데이터(z1, ..., zn)는 제2 출력층(OL(2))으로 인가될 수 있다.

[62] 제2 은닉층(HL(2))은 다양한 활성화함수(activation function)에 의해서 구성될 수 있으며, 제2 은닉층(HL(2))에 인가된 입력데이터(x2)는 다양한 활성화함수(activation function)에 의해 가중치 값이 곱해지고 디바이스출력값데이터(z1, ..., zn)로 변환될 수 있다.

[63] 이하, 복수의 디바이스(40)에서 활성화함수(activation function)에 의해서 입력데이터(x2)에 곱해지는 가중치 값 각각을 특성값데이터(또는, e1, ..., en)라 명명한다.

[64] 이때, 디바이스출력값데이터(또는, z1, ..., zn)는 활성화함수(activation function)에 의해서 입력데이터(x2)에 곱해지는 가중치 값 각각인 특성값데이터(또는, e1, ..., en)에 대한 정보를 포함하고 있다.

[65] 제2 모델링부(43)의 제2 출력층(OL(2))에서 생성되는 복수의 디바이스출력값데이터(z1, ..., zn)는 제2 출력부(44)로 인가될 수 있다.

[66] 이때, 제2 출력부(44)는 네트워크(30)를 통해서 특성값데이터(e1, ..., en)에 대한 정보를 포함하는 복수의 디바이스출력값데이터(z1, ..., zn)에 기초하여 복수의 디바이스출력지식(g1, ..., gn)을 관리서버(20)에 제공할 수 있다.

[67] 도 1 및 도 2를 함께 참고하면, 관리서버(20)는 활성화함수(activation function)에 의해서 입력데이터(x1)에 곱해지는 가중치 값을 특성값데이터(또는, es) 또는 특성값데이터(es)에 대한 정보를 포함하는 디바이스출력값데이터(zs)에 기초하여 관리서버출력지식(gs)를 복수의 디바이스(40)에 제공하므로 통신데이터의 부하를 최소화시켜 통신속도를 증가시킬 수 있다.

[68] 복수의 디바이스(40)는 활성화함수(activation function)에 의해서 입력데이터(x2)에 곱해지는 가중치 값을 특성값데이터(e1, ..., en) 또는 특성값데이터(e1, ..., en)에 대한 정보를 포함하는 복수의 디바이스출력값데이터(z1, ..., zn)에 기초하여 복수의 디바이스출력지식(g1, ..., gn)을 관리서버(20)에 제공하므로 통신데이터의 부하를 최소화시켜 통신속도를 증가시킬 수 있다.

[69] 복수의 디바이스(40)의 제2 모델링부(43)에서 생성된 제2 인공지능신경망(ANN(2(1)), ..., ANN(2(n)))은 복수의 디바이스(40)의 디바이스데이터저장부(41)에서 제공되는 디바이스개인데이터 각각에 기초하여 생성될 수 있으나, 상술한 바와 같이 복수의 디바이스(40)는 관리서버(20)에 특성값데이터(e1, ..., en) 또는 디바이스출력값데이터(z1, ..., zn)만을 전송하므로

디바이스개인데이터는 전송되지 않는다. 이에, 복수의 디바이스(40)에서 사용자의 개인정보데이터는 관리서버(20)에 전송되지 않으므로 개인정보데이터의 유출을 방지할 수 있다.

[70] 복수의 디바이스(40)의 제2 모델링부(43)에서 생성된 제2 인공지능신경망(ANN(2(1)), ..., ANN(2(n)))은 관리서버(20)에서 제공되는 관리서버출력값데이터(zs)에 기초한 관리서버출력지식(gs)에 기반하여 생성되고 관리서버(20)의 제1 모델링부(23)에서 생성되는 제1 인공지능신경망(ANN(1))은 복수의 디바이스(40)에서 제공되는 디바이스출력값데이터(z1, ..., zn)에 기초한 복수의 디바이스출력지식(z1, ..., zn)에 기반하여 생성되므로 관리서버(20)에서 학습되는 학습데이터와 복수의 디바이스(40)에서 학습되는 학습데이터의 이질성이 감소될 수 있어 머신러닝학습의 기능이 증가될 수 있다.

[71] 도 3은 본 발명의 한 실시예에 따른 관리서버에서 머신러닝을 수행하는 과정을 설명하는 흐름도이다.

[72] 단계(S10)에서 프록시데이터를 다운로드할 수 있다.

[73] 구체적으로, 관리서버(20)의 제1 입력부(22)는 프록시데이터를 다운로드 할 수 있다.

[74] 단계(S11)에서 복수의 디바이스에서 제공된 복수의 제n 디바이스출력지식을 입력받을 수 있다.

[75] 구체적으로, 관리서버(20)의 제1 입력부(22)는 복수의 디바이스(40)에서 제2 인공신경망함수(ANN(2(1), ..., ANN(2(n))에 기초하여 생성된 복수의 제n 디바이스출력지식(g1, ..., gn)을 입력받을 수 있다.

[76] 단계(S12)에서 제1 인공신경망함수(ANN(1))를 통해 산출된 제n 관리서버출력지식(gs)과 프록시데이터를 이용하여 제1 손실함수를 생성할 수 있다.

[77] 구체적으로, 관리서버(20)의 제1 모델링부(23)는 제1 인공신경망함수(ANN(1))에서 기계학습한 결과물인 제n 관리서버출력지식(gs)과 업로드된 프록시데이터에 기초하여 제1 손실함수를 생성할 수 있다.

[78] 단계(S13)에서 제1 인공신경망함수(ANN(1))를 통해 산출된 제n 관리서버출력지식(gs), 복수의 제n 디바이스출력지식(g1, ..., gn), 및 프록시데이터를 이용하여 제1 정규화함수를 생성할 수 있다.

[79] 구체적으로, 관리서버(20)의 제1 모델링부(23)는 제1 인공신경망함수(ANN(1))에서 기계학습한 결과물인 제n 관리서버출력지식(gs), 단계(S11)에서 입력받은 복수의 제n 디바이스출력지식(g1, ..., gn), 및 프록시데이터를 이용하여 정규화함수를 생성할 수 있다.

[80] 단계(S14)에서 제1 손실함수 및 제1 정규화함수에 기초하여 제1 인공신경망함수를 재생성할 수 있다.

[81] 구체적으로, 관리서버(20)의 제1 모델링부(23)는 단계(S12)에서 생성된 제1 손실함수 및 단계(S13)에서 생성된 제1 정규화함수에 기초하여 제1 인공신경망함수(ANN(1))를 재생성할 수 있다.

[82] 단계(S15)에서 재생성된 제1 인공신경망함수(ANN(1))에서 입력데이터를 기계학습하고 제n+1 관리서버출력지식(gs)을 생성할 수 있다.

[83] 구체적으로, 관리서버(20)의 제1 모델링부(23)의 제1 입력층(IL(1))에 입력데이터(x1)가 인가될 수 있고 제1 인공신경망함수(ANN(1))를 통해서 제n+1 관리서버출력지식(gs)이 생성될 수 있다.

[84] 단계(S16)에서 제n+1 관리서버출력지식을 복수의 디바이스 각각에 제공할 수 있다.

[85] 구체적으로, 제어서버(50)는 미리 설정된 학습 횟수가 도달한 경우 제1 모델링부(23)에서 기계학습을 중단시키고, 제1 출력부(24)는 제n+1 관리서버출력지식(gs)을 복수의 디바이스(40)의 각각에 제공할 수 있다.

[86] 도 4는 본 발명의 한 실시예에 따른 복수의 디바이스에서 인공신경망함수를 이용하여 머신러닝을 수행하는 과정을 설명하는 흐름도이다.

[87] 단계(S20)에서 프록시데이터를 다운로드할 수 있다.

[88] 구체적으로, 복수의 디바이스(40)의 제2 입력부(42)는 프록시데이터를 다운로드할 수 있다.

[89] 단계(S21)에서 관리서버에서 제공된 제n+1 관리서버출력지식을 입력받을 수 있다.

[90] 구체적으로, 복수의 디바이스(40)의 제2 입력부(42)는 관리서버(20)에서 제공된 제n+1 관리서버출력지식(gs)을 입력받을 수 있다.

[91] 단계(S22)에서 복수의 디바이스에서 생성된 복수의 제n 디바이스개인데이터를 업로드할 수 있다.

[92] 구체적으로, 복수의 디바이스(40)는 디바이스데이터저장부(41)에 저장된 복수의 제n 디바이스개인데이터를 업로드 할 수 있다.

[93] 단계(S23)에서 제2 인공신경망함수를 통해 산출된 복수의 제n 디바이스출력지식 및 복수의 제n 디바이스개인데이터에 기초하여 복수의 제2 손실함수를 생성할 수 있다.

[94] 구체적으로, 복수의 디바이스(40)의 제2 모델링부(43)는 디바이스데이터저장부(41)에서 업로드된 제n 디바이스개인데이터 및 제2 인공신경망함수(ANN(2(1), ..., ANN(2(n))를 통해 산출된 복수의 제n 디바이스출력지식(g1, ..., gn)에 기초하여 복수의 제2 손실함수를 생성할 수 있다.

[95] 예를 들어, 어느 하나의 디바이스(40)의 제2 모델링부(43)는 어느 하나의 디바이스(40)의 디바이스데이터저장부(41)에서 업로드된 제n 디바이스개인데이터 및 어느 하나의 디바이스(40)의 제2 인공신경망함수를 통해 산출된 제n 디바이스출력지식에 기초하여 제2 손실함수를 생성할 수 있다.

[96] 또는, 다른 하나의 디바이스(40)의 제2 모델링부(43)는 다른 하나의

디바이스(40)의 디바이스데이터저장부(41)에서 업로드된 제n 디바이스개인데이터 및 다른 하나의 디바이스(40)의 제2 인공신경망함수를 통해 산출된 제n 디바이스출력지식에 기초하여 제2 손실함수를 생성할 수 있다.

[97] 단계(S25)에서 제2 인공신경망함수를 통해 산출된 복수의 제n 디바이스출력지식, 관리서버에서 제공된 제n+1 관리서버출력지식, 및 프록시데이터를 이용하여 복수의 제2 정규화함수를 생성할 수 있다.

[98] 구체적으로, 복수의 디바이스(40)의 제2 모델링부(43)는 제2 인공신경망함수(ANN(2(1), ..., ANN(2(n))에서 기계학습한 결과물인 제n 디바이스출력지식(g1, ..., gn), 관리서버(20)에서 제공된 제n+1 관리서버출력지식(gs), 및 프록시데이터를 이용하여 정규화함수를 생성할 수 있다.

[99] 단계(S26)에서 제2 손실함수 및 제2 정규화함수에 기초하여 제2 인공신경망함수를 재생성할 수 있다.

[100] 구체적으로, 복수의 디바이스(40)의 제2 모델링부(43)는 단계(24)에서 생성된 제2 손실함수 및 단계(S27)에서 생성된 제2 정규화함수에 기초하여 제2 인공신경망함수(ANN(2(1), ..., ANN(2(n))를 재생성할 수 있다.

[101] 단계(S27)에서 재생성된 제2 인공신경망함수에서 입력데이터를 기계학습하고 복수의 제n+1 디바이스출력지식을 생성할 수 있다.

[102] 구체적으로, 복수의 디바이스(40)의 제2 모델링부(43)의 제2 입력층(IL2(1), ..., IL2(n))에 입력데이터(x2)가 인가될 수 있고, 제2 인공신경망함수(ANN(2(1), ..., ANN(2(n))를 통해서 복수의 제n+1 디바이스출력지식(g1, ..., gn)이 생성될 수 있다.

[103] 단계(S28)에서 복수의 제n+1 디바이스출력지식과 제n+1 관리서버출력지식을 비교할 수 있다.

[104] 구체적으로, 제어서버(50)는 미리 설정된 학습 횟수에 도달한 경우 제2 모델링부(43)에서 기계학습을 중단시키고 제2 출력부(44)는 제n+1 관리서버출력지식을 관리서버(20)에 제공할 수 있다.

[105] 지금까지 참조한 도면과 기재된 발명의 상세한 설명은 단지 본 발명의 예시적인 것으로서, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미 한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

청구범위

[청구항 1] 프록시데이터를 다운로드하는 단계;
관리서버에서 제1 인공신경망함수를 이용하여 입력데이터를 기계학습하여 관리서버출력지식을 생성하는 단계;
제1 내지 제n 디바이스에서 제2 인공신경망함수를 이용하여 상기 입력데이터를 기계학습하여 복수의 디바이스출력지식을 생성하는 단계; 및
미리 설정된 횟수에 도달한 경우 상기 기계학습을 중단하고 상기 관리서버출력지식을 상기 제1 내지 제n 디바이스에 전송하고 상기 복수의 디바이스출력지식을 상기 관리서버에 전송하는 단계를 포함하는,
연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달방법.

[청구항 2] 제1 항에 있어서,
상기 관리서버에서 제1 인공신경망함수를 이용하여 입력데이터를 기계학습하여 관리서버출력지식을 생성하는 단계는,
상기 제1 내지 제n 디바이스에서 제공된 복수의 제n 디바이스출력지식을 입력받는 단계; 및
상기 입력데이터에 기초하여 상기 제1 인공신경망함수에서 생성된 제n 관리서버출력지식 및 상기 프록시데이터에 기초하여 제1 손실함수를 생성하는 단계를 포함하는,
연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달방법.

[청구항 3] 제2 항에 있어서,
상기 관리서버에서 제1 인공신경망함수를 이용하여 입력데이터를 기계학습하여 관리서버출력지식을 생성하는 단계는,
상기 복수의 제n 디바이스출력지식, 상기 제n 관리서버출력지식, 및 상기 프록시데이터에 기초하여 제1 정규화함수를 생성하는 단계;
상기 제1 손실함수 및 상기 제1 정규화함수에 기초하여 상기 제1 인공신경망함수를 생성하는 단계; 및
상기 제1 인공신경망함수에서 상기 입력데이터를 기계학습하고 제n+1 관리서버출력지식을 생성하는 단계를 더 포함하는,
연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달방법.

[청구항 4] 제3 항에 있어서,
상기 제1 내지 제n 디바이스에서 제2 인공신경망함수를 이용하여 상기 입력데이터를 기계학습하여 복수의 디바이스출력지식을 생성하는 단계는,
상기 관리서버에서 제공된 제n+1 관리서버출력지식을 입력받는 단계;
상기 제1 내지 제n 디바이스 각각에서 생성된 복수의 제n 디바이스개인데이터를 업로드하는 단계; 및

상기 입력데이터에 기초하여 생성된 복수의 제n 디바이스출력지식 각각 및 상기 복수의 제n 디바이스개인데이터 각각에 기초하여 복수의 제2 손실함수를 생성하는 단계를 포함하는,
연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달방법.

[청구항 5] 제4 항에 있어서,
상기 제1 내지 제n 디바이스에서 제2 인공신경망함수를 이용하여 상기 입력데이터를 기계학습하여 복수의 디바이스출력지식을 생성하는 단계는,
상기 복수의 제n 디바이스출력지식 각각, 상기 제n+1 관리서버출력지식, 및 상기 프록시데이터에 기초하여 복수의 제2 정규화함수를 생성하는 단계;
상기 복수의 제2 손실함수 및 상기 복수의 제2 정규화함수에 기초하여 복수의 상기 제2 인공신경망함수를 생성하는 단계; 및
상기 복수의 제2 인공신경망함수에 기초하여 상기 입력데이터를 기계학습하고 복수의 제n+1 디바이스출력지식 생성하는 단계를 더 포함하는,
연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달방법.

[청구항 6] 제5 항에 있어서,
미리 설정된 횟수에 도달한 경우 상기 기계학습을 중단하고 상기 관리서버출력지식을 상기 제1 내지 제n 디바이스에 전송하고 상기 복수의 디바이스출력지식을 상기 관리서버에 전송하는 단계를 포함하는 단계는,
상기 미리 설정된 횟수에 도달한 경우 상기 제1 인공신경망함수에서 상기 입력데이터의 기계학습을 중단하고 상기 제n+1 관리서버출력지식을 상기 제1 내지 제n 디바이스에 전송하는 단계; 및
상기 미리 설정된 횟수에 도달한 경우 상기 제2 인공신경망함수에서 상기 입력데이터의 기계학습을 중단하고 상기 복수의 제n+1 관리디바이스출력지식을 상기 관리서버에 전송하는 단계를 포함하는,
연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달방법

[청구항 7] 프록시데이터 및 제1 인공신경망함수를 이용하여 입력데이터를 기계학습하고 관리서버출력지식을 생성하는 관리서버;
상기 프록시데이터 및 제2 인공신경망함수를 이용하여 상기 입력데이터를 기계학습하고 복수의 디바이스출력지식을 생성하는 제1 내지 제n 디바이스; 및
미리 설정된 횟수에 도달한 경우 상기 기계학습을 중단하는 제어서버를 포함하는,
연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달시스템.

[청구항 8] 제7 항에 있어서,

상기 관리서버는,
상기 제1 내지 제n 디바이스에서 복수의 제n 디바이스출력지식을 입력받는 제1 입력부;
상기 입력데이터에 기초하여 상기 제1 인공신경망함수에서 생성된 제n 관리서버출력지식 및 상기 프록시데이터에 기초하여 제1 손실함수를 생성하고
상기 복수의 제n 디바이스출력지식, 상기 제n 관리서버출력지식, 및 상기 프록시데이터에 기초하여 제1 정규화 함수를 생성하고 상기 제1 손실함수 및 상기 제1 정규화 함수에 기초하여 상기 제1 인공신경망함수를 생성하는 제1 모델링부; 및
상기 제1 인공신경함수에서 상기 입력데이터를 기계학습한 결과인 제n+1 관리서버출력지식을 상기 제1 내지 제n 디바이스에 출력하는 제1 출력부를 포함하는,
연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달시스템.

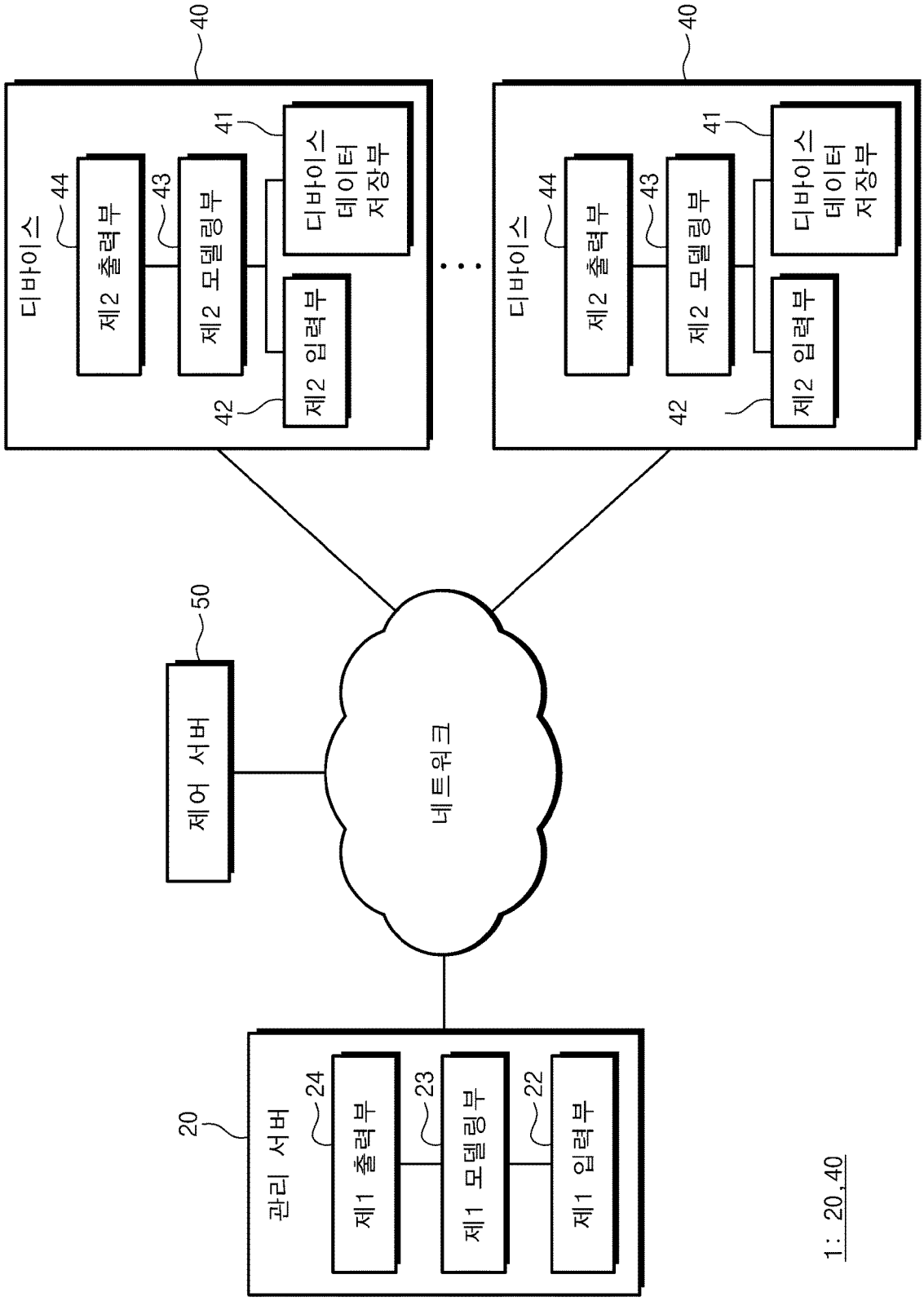
[청구항 9] 제8 항에 있어서,
상기 제1 내지 제n 디바이스 각각은,
상기 제n+1 관리서버출력지식을 입력받는 제2 입력부;
미리 저장된 제n 디바이스개인데이터와 상기 프록시 데이터에 기초하여 상기 기계학습한 상기 복수의 제n 디바이스출력지식을 업로드시키는 디바이스데이터셋저장부;
상기 입력데이터에 기초하여 생성된 제n 디바이스출력지식 및 상기 미리 저장된 제n 디바이스개인데이터에 기초하여 제2 손실함수를 생성하고
상기 제n 디바이스출력지식, 상기 제n+1 관리서버출력지식, 및 상기 프록시데이터에 기초하여 제2 정규화함수를 생성하고, 상기 제2 손실함수 및 상기 제2 정규화함수에 기초하여 상기 제2 인공신경망함수를 생성하는 제2 모델링부; 및
상기 제2 인공신경망함수에 기초하여 상기 입력데이터를 기계학습하고 제n+1 디바이스출력지식을 생성하는 제2 출력부를 포함하는,
연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달시스템.

[청구항 10] 제9 항에 있어서,
상기 제어서버는,
상기 미리 설정된 횟수에 도달한 경우 상기 제1 인공신경망함수에서 상기 입력데이터의 기계학습을 중단하고 상기 제n+1 관리서버출력지식을 상기 제1 내지 제n 디바이스에 전송하고 상기 미리 설정된 횟수에 도달한 경우 상기 제2 인공신경망함수에서 상기 입력데이터의 기계학습을 중단하고 상기 복수의 제n+1 관리디바이스출력지식을 상기 관리서버에 전송하도록 제어하는,
연합학습에서 프록시데이터를 이용한 데이터 전달시스템.

[청구항 11] 제1 항의 연합학습에서 프록시 데이터셋을 이용한 장치 간 지식 전달방법을 실행시키는 프로그램이 기록된 컴퓨터로 판된 가능한 비일시적 기록 매체.

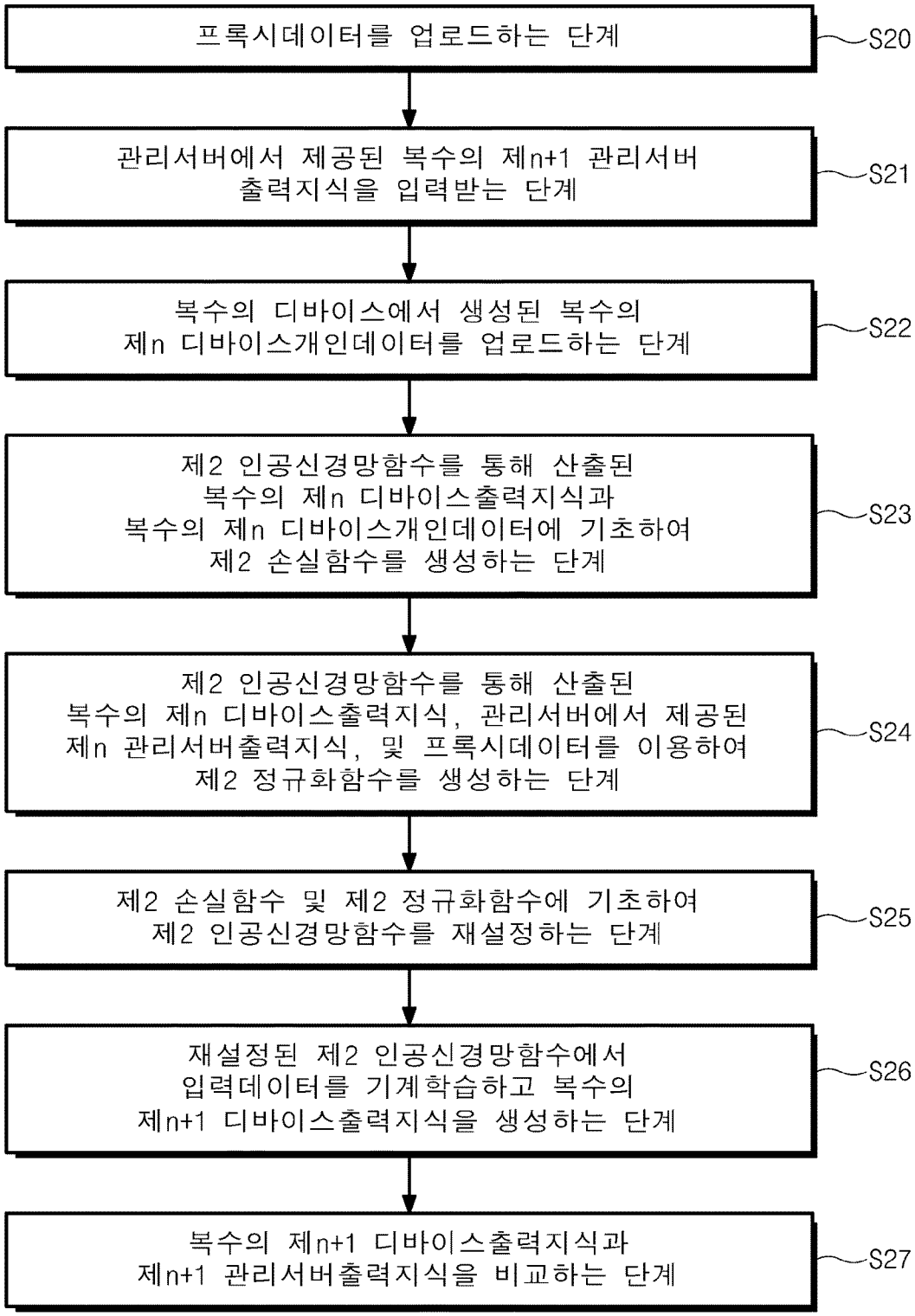
WO 2023/120776 PCT/KR2021/019745

[도1]

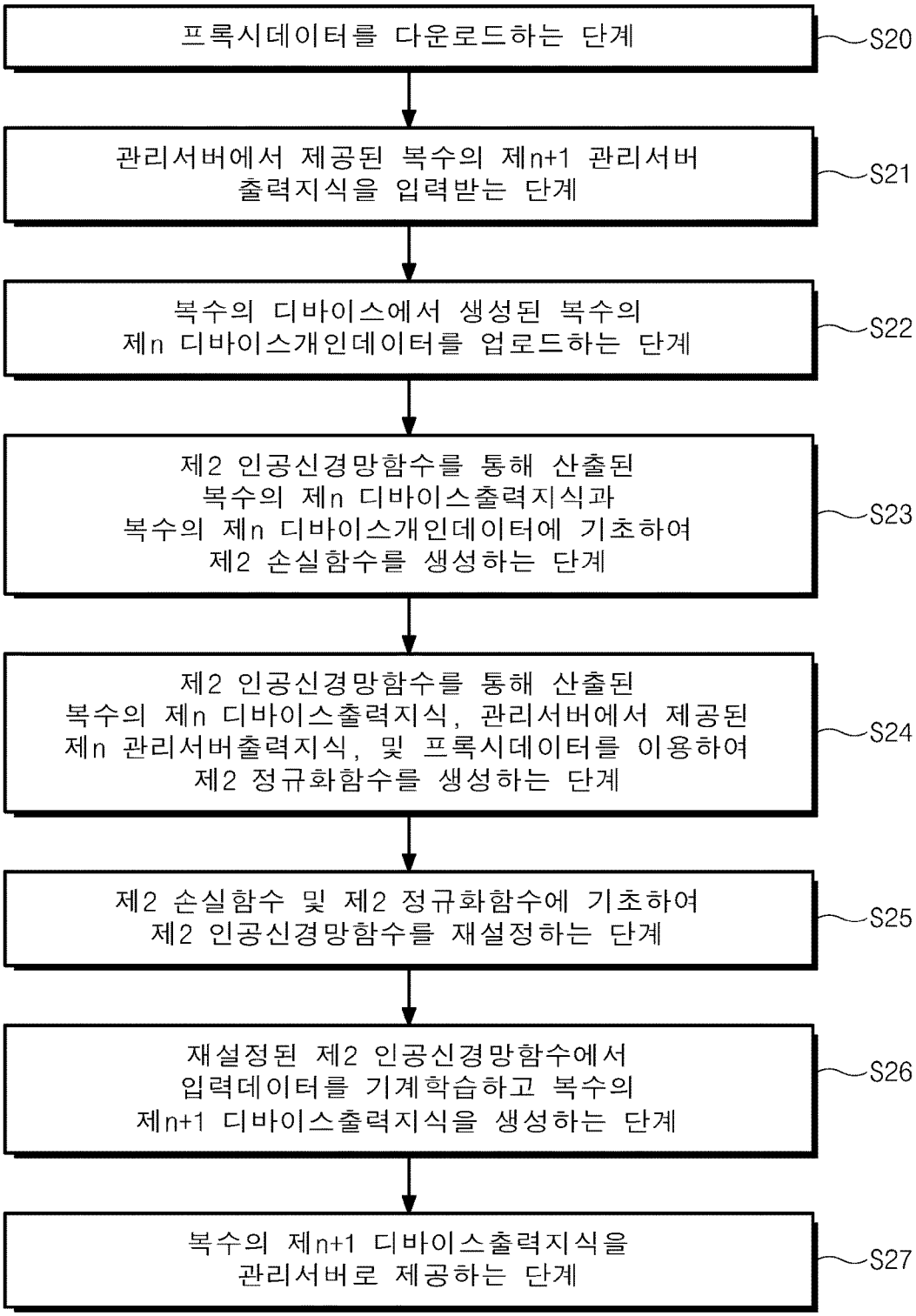


1: 20, 40

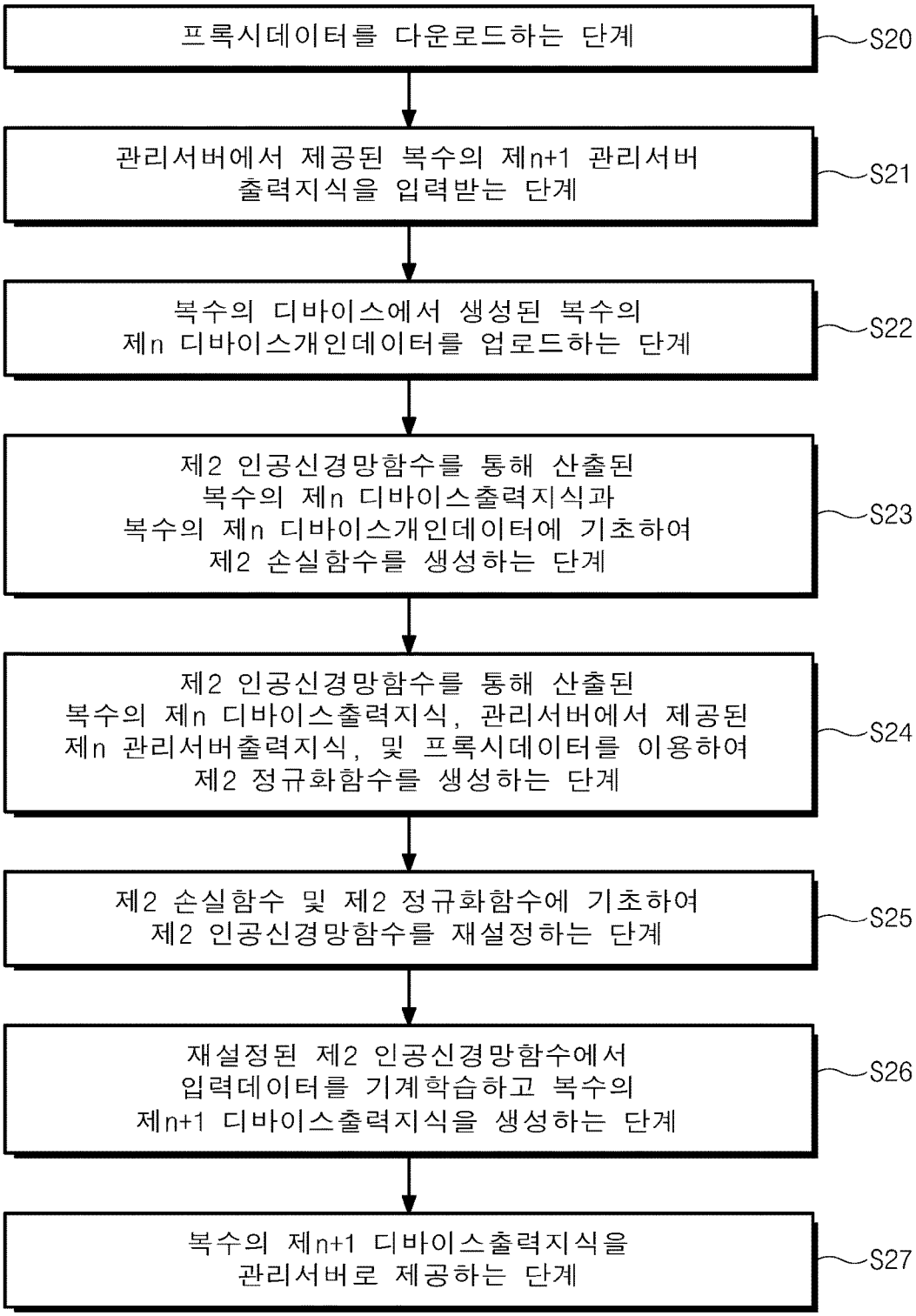
[도2]


프록시데이터를 업로드하는 단계
S20
관리서버에서 제공된 복수의 제n+1 관리서버 출력지식을 입력받는 단계
S21
복수의 디바이스에서 생성된 복수의 제n 디바이스개인데이터를 업로드하는 단계
S22
제2 인공신경망함수를 통해 산출된 복수의 제n 디바이스출력지식과 복수의 제n 디바이스개인데이터에 기초하여 제2 손실함수를 생성하는 단계
S23
제2 인공신경망함수를 통해 산출된 복수의 제n 디바이스출력지식, 관리서버에서 제공된 제n 관리서버출력지식, 및 프록시데이터를 이용하여 제2 정규화함수를 생성하는 단계
S24
제2 손실함수 및 제2 정규화함수에 기초하여 제2 인공신경망함수를 재설정하는 단계
S25
재설정된 제2 인공신경망함수에서 입력데이터를 기계학습하고 복수의 제n+1 디바이스출력지식을 생성하는 단계
S26
복수의 제n+1 디바이스출력지식과 제n+1 관리서버출력지식을 비교하는 단계
S27

[도3]


프록시데이터를 다운로드하는 단계
S20
관리서버에서 제공된 복수의 제n+1 관리서버 출력지식을 입력받는 단계
S21
복수의 디바이스에서 생성된 복수의 제n 디바이스개인데이터를 업로드하는 단계
S22
제2 인공신경망함수를 통해 산출된 복수의 제n 디바이스출력지식과 복수의 제n 디바이스개인데이터에 기초하여 제2 손실함수를 생성하는 단계
S23
제2 인공신경망함수를 통해 산출된 복수의 제n 디바이스출력지식, 관리서버에서 제공된 제n 관리서버출력지식, 및 프록시데이터를 이용하여 제2 정규화함수를 생성하는 단계
S24
제2 손실함수 및 제2 정규화함수에 기초하여 제2 인공신경망함수를 재설정하는 단계
S25
재설정된 제2 인공신경망함수에서 입력데이터를 기계학습하고 복수의 제n+1 디바이스출력지식을 생성하는 단계
S26
복수의 제n+1 디바이스출력지식을 관리서버로 제공하는 단계
S27

[도4]


프록시데이터를 다운로드하는 단계
S20
관리서버에서 제공된 복수의 제n+1 관리서버 출력지식을 입력받는 단계
S21
복수의 디바이스에서 생성된 복수의 제n 디바이스개인데이터를 업로드하는 단계
S22
제2 인공신경망함수를 통해 산출된 복수의 제n 디바이스출력지식과 복수의 제n 디바이스개인데이터에 기초하여 제2 손실함수를 생성하는 단계
S23
제2 인공신경망함수를 통해 산출된 복수의 제n 디바이스출력지식, 관리서버에서 제공된 제n 관리서버출력지식, 및 프록시데이터를 이용하여 제2 정규화함수를 생성하는 단계
S24
제2 손실함수 및 제2 정규화함수에 기초하여 제2 인공신경망함수를 재설정하는 단계
S25
재설정된 제2 인공신경망함수에서 입력데이터를 기계학습하고 복수의 제n+1 디바이스출력지식을 생성하는 단계
S26
복수의 제n+1 디바이스출력지식을 관리서버로 제공하는 단계
S27

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2021/019745

A. CLASSIFICATION OF SUBJECT MATTER

G06N 3/04(2006.01)i; **G06N 3/08**(2006.01)i; **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 3/04(2006.01); G06F 17/10(2006.01); G06N 20/00(2019.01); G06N 20/20(2019.01); G06N 3/08(2006.01); H04L 29/08(2006.01); H04L 65/40(2022.01)

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), 프록시 데이터(proxy data), 훈련(training), 설정(predefined), 횟수(number), 손실 함수(loss function)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2021-0051604 A (SK TELECOM CO., LTD. et al.) 10 May 2021 (2021-05-10) See paragraphs [0027] and [0057]; and claims 1-2 and 6.	1-11
Y	KR 10-2019-0032433 A (NANTOMICS, LLC et al.) 27 March 2019 (2019-03-27) See paragraph [0020]; and claim 1.	1-11
Y	JP 2019-144642 A (NIPPON TELEGRAPH & TELEPHONE) 29 August 2019 (2019-08-29) See claim 1.	2-6,8-10
A	CN 113691594 A (HANGZHOU DIANZI UNIVERSITY) 23 November 2021 (2021-11-23) See claim 1.	1-11
A	US 2021-0365841 A1 (SHALOUDEGI, Kiarash et al.) 25 November 2021 (2021-11-25) See paragraphs [0080]-[0093]; and figure 5.	1-11

☐ 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 August 2022	**31 August 2022**

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
Information on patent family members

International application No.
PCT/KR2021/019745

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
KR 10-2021-0051604 A	10 May 2021	KR 10-2403476 B1	27 May 2022
KR 10-2019-0032433 A	27 March 2019	CA 3031067 A1	25 January 2018
		CN 109716346 A	03 May 2019
		EP 3485436 A1	22 May 2019
		EP 3485436 A4	01 April 2020
		JP 2019-526851 A	19 September 2019
		TW 201812646 A	01 April 2018
		US 2018-0018590 A1	18 January 2018
		WO 2018-017467 A1	25 January 2018
JP 2019-144642 A	29 August 2019	JP 6753874 B2	09 September 2020
		US 2021-0034978 A1	04 February 2021
		WO 2019-159783 A1	22 August 2019
CN 113691594 A	23 November 2021	None	
US 2021-0365841 A1	25 November 2021	WO 2021-233030 A1	25 November 2021

국 제 조 사 보 고 서

국제출원번호
PCT/KR2021/019745

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06N 3/04(2006.01)i; **G06N 3/08**(2006.01)i; **G06N 20/20**(2019.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06N 3/04(2006.01); G06F 17/10(2006.01); G06N 20/00(2019.01); G06N 20/20(2019.01); G06N 3/08(2006.01); H04L 29/08(2006.01); H04L 65/40(2022.01)

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), 프록시 데이터(proxy data), 훈련(training), 설정(predefined), 횟수(number), 손실 함수(loss function)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-2021-0051604 A (에스케이텔레콤 주식회사 등) 2021.05.10 단락 [0027], [0057]; 및 청구항 1-2, 6	1-11
Y	KR 10-2019-0032433 A (난토믹스, 엘엘씨 등) 2019.03.27 단락 [0020]; 및 청구항 1	1-11
Y	JP 2019-144642 A (NIPPON TELEGRAPH & TELEPHONE) 2019.08.29 청구항 1	2-6,8-10
A	CN 113691594 A (HANGZHOU DIANZI UNIVERSITY) 2021.11.23 청구항 1	1-11
A	US 2021-0365841 A1 (KIARASH SHALOUDEGI 등) 2021.11.25 단락 [0080]-[0093]; 및 도면 5	1-11

☐ 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
2022년08월30일(30.08.2022)	**2022년08월31일(31.08.2022)**

ISA/KR의 명칭 및 우편주소

대한민국 특허청
(35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)

팩스 번호 **+82-42-481-8578**

심사관

양정록

전화번호 **+82-42-481-5709**

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2021/019745

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2021-0051604 A	2021/05/10	KR 10-2403476 B1	2022/05/27
KR 10-2019-0032433 A	2019/03/27	CA 3031067 A1	2018/01/25
		CN 109716346 A	2019/05/03
		EP 3485436 A1	2019/05/22
		EP 3485436 A4	2020/04/01
		JP 2019-526851 A	2019/09/19
		TW 201812646 A	2018/04/01
		US 2018-0018590 A1	2018/01/18
		WO 2018-017467 A1	2018/01/25
JP 2019-144642 A	2019/08/29	JP 6753874 B2	2020/09/09
		US 2021-0034978 A1	2021/02/04
		WO 2019-159783 A1	2019/08/22
CN 113691594 A	2021/11/23	없음	
US 2021-0365841 A1	2021/11/25	WO 2021-233030 A1	2021/11/25