The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 24, No. 2, pp.191-196, Apr. 30, 2024. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2024.24.2.191
JIIBC 2024-2-28

이더리움 네트워크 기반의 연합학습

Federated Learning Based on Ethereum Network

황승연*, 김정준**

Seung-Yeon Hwang*, Jeong-Joon Kim**

요 약 최근 여러 기업과 연구기관들이 IoT 장비에서 수집되는 다양한 데이터를 분석하고 실제 응용 서비스를 통해 제공하기 위한 지능형 IoT 기술에 관한 연구가 활발히 진행되고 있다. 하지만 IoT 기기에서 수집되는 데이터들을 연구 및 개발에 사용하기 위해 데이터를 송수신하는 과정에서 개인정보유출과 같은 보안상의 이슈가 발생할 수 있다. 그리고 여러 IoT 기기에서 수집되는 데이터가 증가할수록 데이터 관리에 어려움이 존재하며 데이터를 이동하는 데 큰 비용과 시간이 소요된다. 따라서 본 논문에서는 다양한 기기로 이루어진 연합학습 환경에서 보안상의 이슈와 비효율성을 개선하기 위해 신뢰성이 보장된 이더리움 네트워크 기반의 연합학습 시스템을 개발하고자 한다.

Abstract Recently, research on intelligent IoT technology has been actively conducted by various companies and research institutes to analyze various data collected from IoT devices and provide it through actual application services. However, security issues such as personal information leakage may arise in the process of transmitting and receiving data to use data collected from IoT devices for research and development. In addition, as data collected from multiple IoT devices increases, data management difficulties exist, and data movement is costly and time consuming. Therefore, in this paper, we intend to develop an Ethereum network-based federated learning system with guaranteed reliability to improve security issues and inefficiencies in a federated learning environment composed of various devices.

Key Words : Ethereum Network, Federated Learning, IPFS, Smart Contract

Ⅰ. 서 론

전 세계적으로 새로운 서비스 창출과 개발을 위해 사람, 사물, 공간 등을 서로 밀접하게 연결하여 통신하기 위한 IoT 기술에 대한 수요가 증가하고 있다. 여러 기업과 연구소에서는 이러한 기기들의 단순 연결을 통한 데이터 수집을 넘어 수집된 데이터를 분석하고 실제 응용 서비스를 통해 제공할 수 있는 지능형 IoT 기술에 주목하고 있다. 하지만 이러한 IoT 디바이스는 사이버 공격에 쉽게 노출되며 보안 취약성과 개인정보 유출과 같은 심각한 보안 문제가 존재한다[1-2]. 그리고 여러 IoT 기기에서 수집한 데이터를 딥러닝을 비롯한 인공지능 기술에 접목하기 위해서는 데이터 서버에 취합하여 저장하는 과정이 필수적이다. 하지만 데이터 이동으로 발생하는 디

*준회원, 안양대학교 컴퓨터공학과
**정회원, 안양대학교 소프트웨어학과
접수일자 2024년 2월 2일, 수정완료 2024년 3월 2일
게재확정일자 2024년 4월 5일

Received: 2 February, 2024 / Revised: 2 March, 2024 / Accepted: 5 April, 2024
**Corresponding Author: jjkim@anyang.ac.kr
Dept. ICT Convergence Engineering at Anyang University, Korea

스크 I/O 시간은 데이터의 양에 따라 증가하며 데이터의 양이 많아질수록 심각한 지연시간을 발생시킨다. 그리고 데이터 서버에 저장된 대용량의 빅데이터를 관리하는 과정에서 중복 데이터와 데이터 손실이 발생할 수 있으므로 데이터 관리를 위한 솔루션 등을 추가로 도입해야 하는 어려움이 있다[3].

따라서 본 연구에서는 개인정보보호를 비롯한 여러 보안상의 이슈를 해결하기 위해 탈중앙화 블록체인 네트워크인 이더리움 네트워크를 활용한다. 그리고 각 IoT 기기에서 바로 학습하고 학습된 모델의 가중치를 이용하여 기존 모델의 가중치를 업데이트하는 연합학습 기법을 도입한다. 각 노드에서 학습한 모델을 이용하여 기존 모델의 가중치를 업데이트하는 과정에서 각 모델을 공유하기 위해 P2P(Peer to Peer) 방식의 분산파일시스템인 IPFS를 활용한다. 즉, 다양한 기기로 이루어진 연합학습 환경에서 보안상의 이슈와 데이터 이동에서 발생하는 지연을 최소화하며 신뢰성이 보장된 이더리움 네트워크 기반의 연합학습 시스템을 개발하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 제안한 이더리움 네트워크 기반의 연합학습 시스템 개발과 관련된 기술을 설명한다. 3장에서는 제안한 시스템을 개발하기 위한 환경과 시스템 아키텍처에 대해 설명한다. 4장에서는 이더리움 네트워크에서 연합학습한 모델과 단일 노드에서 학습한 모델의 성능 평가 결과 비교 설명한다. 5장에서는 연구에 대한 결론과 향후 연구 방향에 대해 제시한다.

Ⅱ. 관련 기술

1. 연합학습(Federated Learning)

연합학습은 구글에서 제안한 기법으로 개인 모바일 기기에 저장된 데이터를 이용하여 인공지능 모델 학습을 수행하는 기법이다. 다수의 개별 디바이스에 저장된 데이터를 이용하여 인공지능 모델을 학습하고(로컬 모델) 학습된 파라미터를 중앙 서버로 전송한다. 중앙 서버에서는 파라미터를 통합하기 위한 알고리즘을 이용하여 로컬 모델들을 더 우수한 하나의 모델(글로벌 모델)을 생성한다. 그리고 생성된 글로벌 모델을 개별 디바이스에 전송하는 과정을 반복한다[4]. 이러한 연합학습은 중앙 서버에 구축된 빅데이터를 이용하는 것이 아니라 데이터가 개인 디바이스에서만 이용되기 때문에 정보보호 측면에서도 안전하다. 따라서 이러한 연합학습은 개인정보에 민감한 의료분야에서 활용하기 위해 활발하게 연구가 진행되고 있다[5]. 최근에는 NVIDIA, Intel에서 의료기관과 현업을 통해 연합학습을 위한 플랫폼을 개발하고 있다.

2. IPFS(Interplanetary File System)

IPFS는 모든 컴퓨터를 연결하고자 하는 분산된 P2P 파일 시스템이다. 서버의 연결이 차단되면 치명적인 결과를 낳는 Server-Client 방식과 달리 IPFS에서는 몇몇 노드들의 연결이 끊어지더라도 안정적으로 유지할 수 있다. 대용량의 파일을 빠르고 효율적으로 공유할 수 있으며 파일들의 중복 여부도 알 수 있기 때문에 저장소를 효율적으로 사용할 수 있다. IPFS에 저장되는 파일은 여러 개의 블록으로 이루어져 있으며 각 블록은 고유한 해시(hash)를 갖는다. 사용자는 파일에 할당된 해시 값을 이용하여 원하는 파일을 다운로드할 수 있다[6-7].

3. 이더리움 네트워크(Ethereum Network)

이더리움은 2013년에 처음 제안된 후 2015년에 공개되었으며 비트코인 다음으로 큰 규모의 암호화폐로 성장하였다. 이더리움은 타 블록체인과 다르게 단순히 암호화폐만 주고받는 것이 아니라 스마트 컨트랙트(smart contract)를 접목하여 DApp(Decentralized App) 개발을 위한 프로그래밍이 가능하다. 이러한 DApp을 이용하여 다양한 문제를 해결하고 서비스를 제공하기 위해 분야를 막론하곤 전 세계적으로 수천 개의 프로젝트가 진행 중이다[8-9]. 이더리움은 P2P 네트워크에 연결된 모든 노드가 같은 역할과 기능을 수행하는 완전 분산형 P2P 토폴로지로 구성된다. 중앙 서버를 이용하지 않고 노드 간에 직접 통신하기 때문에 정보가 위변조 되거나 해킹에 노출될 수 있는 위험을 제거할 수 있으므로 대부분의 블록체인 네트워크들은 P2P 방식을 사용하고 있다.

Ⅲ. 연구내용

1. 개발환경

본 논문에서 제안한 이더리움 네트워크 기반의 연합학습 시스템은 Vmware를 이용하여 3대의 가상머신을 생성하였으며 Geth[10]를 이용하여 프라이빗 이더리움 네트워크를 구성하였다. 각 노드는 Ubuntu 20.04 버전의 운영체제 환경에서 개발하였으며 각 로컬노드의 딥러닝 시스템은 Tensorflow Keras를 이용하여 개발하였다. 각

노드에서 학습된 로컬 및 글로벌 모델은 IPFS를 이용하여 저장하였다. 각 노드 간에 로컬 모델과 글로벌 모델 공유를 위한 스마트 컨트랙트는 Remix IDE에서 솔리디티를 이용하여 개발하였다.

2. 이더리움 네트워크 기반 연합학습 시스템

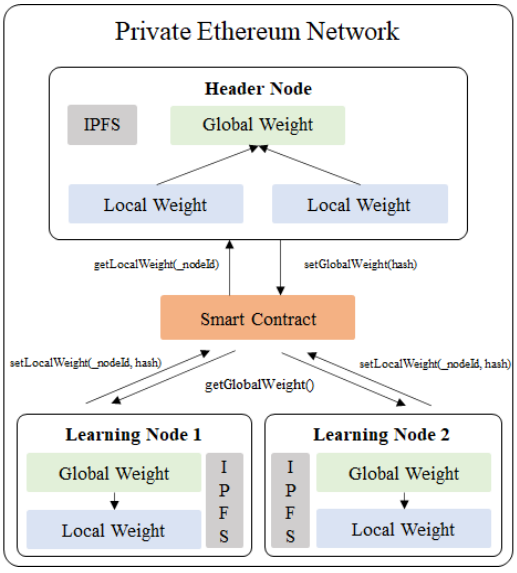

그림 1. 이더리움 네트워크 기반의 연합학습 시스템 아키텍처
Fig. 1. Federated Learning System Architecture Based on Ethereum Network

그림 1은 본 논문에서 제안한 이더리움 네트워크 기반의 연합학습 시스템 아키텍처를 나타내며 실험 성능 평가를 위해 하나의 헤더 노드와 두 대의 학습 노드로 이루어진 프라이빗 이더리움 네트워크를 구성하였다. 그리고 모든 노드에서는 학습 모델 공유를 위해 IPFS 데몬이 실행 중이며 헤더 노드와 학습 노드를 제외한 다른 사용자와 공유하지 않기 위해 IPFS 프라이빗 네트워크를 구성하였다. 그림 2는 IPFS 데몬의 실행 화면을 나타낸다.

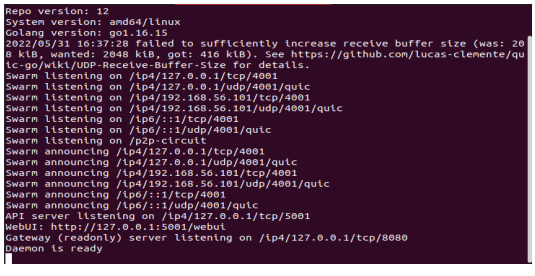

그림 2. IPFS 데몬 실행 화면
Fig. 2. IPFS daemon execution screen

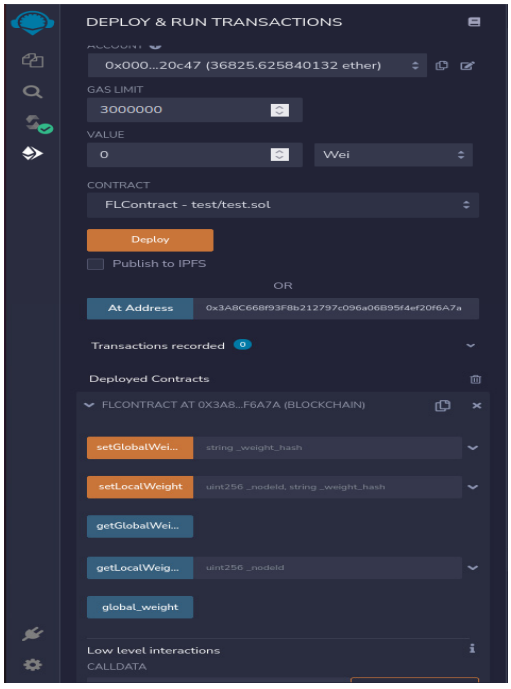

그림 3. 학습 모델 공유를 위한 스마트 컨트랙트
Fig. 3. Smart Contracts for Local and Global Model Sharing

표 1. 스마트 컨트랙트 함수의 입력 및 출력
Table 1. Inputs and Outputs of Smart Contract Functions

함수명	입력	출력
setLocalWeight	nodeId, hash	-
getLocalWeight	nodeId	hash
setGlobalWeight	hash	-
getGlobalWeight	-	hash

헤더 노드는 각 학습 노드에서 도출된 로컬 모델의 학습 가중치를 하나의 글로벌 모델로 통합하는 역할을 하며 각 로컬 모델의 가중치 값의 평균을 구하여 하나의 글로벌 모델을 생성한다. 학습 노드에서는 헤더 노드에서 생성한 글로벌 모델을 이용하여 새로운 로컬 모델을 생성한다. 헤더 노드와 학습 노드는 스마트 컨트랙트의 기능을 이용하여 모델 데이터를 서로 주고받을 수 있다. 스마트 컨트랙트에는 학습 노드에서 생성된 로컬 모델을 저장하기 위한 setLocalWeight() 함수, 헤더 노드에서 각 로컬 모델을 가져오기 위한 getLocalWeight() 함수, 헤더 노드에서 생성된 글로벌 모델을 저장하기 위한 setGlobalWeight() 함수, 학습 노드에서 글로벌 모델을 가져오기 위한 getGlobalWeight() 함수가 포함되어 있

다. setLocalWeight() 함수는 로컬 모델을 저장한 노드의 ID와 IPFS에 저장된 로컬 모델 파일의 해시 값을 입력으로 받는다. getLocalWeight() 함수는 학습 노드의 ID를 입력으로 받고 해당 노드가 저장한 로컬 모델 파일의 해시 값을 출력한다. setGlobalWeight() 함수는 헤더 노드가 IPFS에 저장한 글로벌 모델 파일의 해시 값을 입력으로 받는다. getGlobalWeight() 함수는 별도의 입력을 받지 않으며 IPFS에 저장된 글로벌 모델 파일의 해시 값을 출력한다. 그림 3은 remix에서 구현된 스마트 컨트랙트를 나타내며 각 함수의 입·출력 값을 표 1에 정리하였다.

각 학습 노드에서 로컬 모델 생성을 위해 간단한 CNN(Convolutional Neural Network) 모델을 구현하였으며 아키텍처는 그림 4와 같다.

```
Model: "sequential"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
conv2d (Conv2D)              (None, 28, 28, 32)        320
_________________________________________________________________
max_pooling2d (MaxPooling2D) (None, 14, 14, 32)        0
_________________________________________________________________
conv2d_1 (Conv2D)            (None, 14, 14, 64)        18496
_________________________________________________________________
max_pooling2d_1 (MaxPooling2 (None, 7, 7, 64)          0
_________________________________________________________________
conv2d_2 (Conv2D)            (None, 7, 7, 128)         73856
_________________________________________________________________
max_pooling2d_2 (MaxPooling2 (None, 4, 4, 128)         0
_________________________________________________________________
flatten (Flatten)            (None, 2048)              0
_________________________________________________________________
dense (Dense)                (None, 256)               524544
_________________________________________________________________
dropout (Dropout)            (None, 256)               0
_________________________________________________________________
dense_1 (Dense)              (None, 10)                2570
=================================================================
Total params: 619,786
Trainable params: 619,786
Non-trainable params: 0
```

그림 4. 실험 성능 평가를 위한 신경망 아키텍처
Fig. 4. Neural Network Architecture for Experimental Performance Assessment

학습 모델의 완전연결계층(Fully-Connected Layer)에서는 과적합을 방지하기 위해 Dropout을 추가하였고 가장 마지막 레이어에서는 분류를 위해 Softmax 활성화 함수를 사용하였다.

Ⅳ. 실험 및 결과

1. 데이터셋

본 논문에서 제안한 이더리움 네트워크 기반 연합학습 시스템의 실험 성능 평가를 위해 벤치마크 데이터셋 중 하나인 MNIST[11] 데이터 셋을 사용하였다. MNIST 데이터 셋은 0부터 9까지 총 10개의 클래스로 구성된 숫자 손글씨 이미지를 포함하고 있으며 6만 장의 훈련 데이터셋과 1만 장의 테스트 데이터셋으로 이루어져 있다. 각 이미지는 28×28 픽셀 사이즈로 고정되어 있으며 흑백으로 되어있다. 그림 5는 MNIST 데이터 셋의 샘플 이미지를 나타낸다.

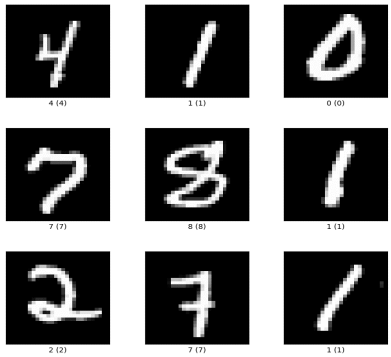

그림 5. MNIST 데이터셋 샘플
Fig. 5. MNIST Dataset Sample

2. 실험 성능 평가

본 논문에서는 이더리움 네트워크 기반의 연합학습 시스템으로 학습한 모델의 정확도와 단일 노드에서 학습한 모델의 정확도를 비교하여 제안한 기법의 실효성을 검증한다. 연합학습 시스템의 경우 각 학습 노드의 로컬 에폭(epoch)과 글로벌 에폭을 5로 설정하였으며 학습률(Learning rate)는 0.001로 설정하였다. 모델의 빠른 수렴을 위해 Adam 옵티마이저(Optimizer)를 사용하였으며 손실 함수는 categorical crossentropy를 사용하였다. 그리고 총 6만 장의 훈련 데이터를 3만 장씩 나누어 각 학습 노드를 학습하였다. 단일 노드에서 학습한 경우에는 6만 장의 훈련 데이터 셋을 모두 이용하였고 에폭을 25로 설정하였으며 기타 하이퍼파라미터는 연합학습 시스템과 똑같이 설정하였다.

글로벌 에폭마다 측정한 각 학습 노드의 정확도는 표 2와 같으며 단일 노드에서 학습한 노드의 정확도는 표 3과 같다.

표 2. 글로벌 에폭당 각 학습 노드의 정확도
Table 2. Accuracy of each learning node per global epoch

글로벌 에폭	학습 노드 1	학습 노드 2
1	98.91%	99.10%
2	99.30%	99.27%
3	99.38%	99.24%
4	99.43%	99.38%
5	99.39%	99.41%

표 3. 에폭당 단일 노드의 정확도
Table 3. Accuracy of a single node per epoch

에폭	정확도
1	98.77%
2	99.05%
3	99.32%
4	99.20%
5	99.24%
6	99.42%
7	99.30%
8	99.36%
9	99.35%
10	99.38%
11	99.45%
12	99.42%
13	99.44%
14	99.45%
15	99.49%
16	99.53%
17	99.47%
18	99.49%
19	99.49%
20	99.49%
21	99.49%
22	99.49%
23	99.48%
24	99.48%
25	99.48%

연합학습 시스템의 헤더 노드에서 생성된 최종 글로벌 모델의 정확도는 99.46%로 측정되었다. 실험 성능 평가의 결과를 통해 연합학습 시스템의 각 학습 노드의 로컬 모델의 경우 단일 노드에서 학습한 모델보다 약간의 성능 저하를 확인할 수 있었지만 무시할 수 있는 정도의 성능 저하로 판단된다. 최종 글로벌 모델과 단일 노드에서 학습한 모델의 경우 비슷한 성능을 달성한 것을 확인할 수 있었다.

V. 결 론

본 연구에서는 데이터 이동으로 인해 발생할 수 있는 보안상의 이슈와 지연시간을 최소화하기 위한 신뢰성이 보장된 이더리움 네트워크 기반의 연합학습 시스템을 개발하였다. 4장의 실험 성능 평가를 통해 제안한 기법의 실효성을 검증하였다. 따라서 이더리움 네트워크 기반의 연합학습 시스템을 의료나 금융 등과 같은 분야에서 활용한다면 보안 문제를 해결하면서 인공지능 기반의 기술을 접목할 수 있을 것으로 기대된다. 향후 연구에는 연합학습 시스템의 모든 학습 노드가 학습이 완료되지 않아도 개별적으로 글로벌 모델을 업데이트할 수 있도록 하여 학습 과정에서 발생하는 지연을 최소화할 수 있는 시스템을 개발하고자 한다. 그리고 동일한 학습 모델이 아닌 서로 다른 학습 모델 간의 앙상블을 통해 연합학습 할 수 있는 방법을 적용한다면 더 고성능을 달성할 수 있을 것으로 기대된다.

References

[1] Howon Kim, Shinwook Heo, Wontae Kang, Sanghyun Lee, Jinjae Lee, Larasati Harashta Tatimma, “Hardware based security technology for reinforcing IoT security”, Communications of the Korean Institute of Information Scientists and Engineers, Vol. 38, No. 9, pp. 25-32.

[2] Hyungbin Kim, Yongho Kim, Cheolwoo You, Hyunhee Park, “Efficient Distributed Clustering Algorithm for Large-Scale Federated Learning”, The Journal of Korean Institute of Communications and Information Sciences, Vol. 47, No. 1, pp. 198-205, 2022.
DOI: http://doi.org/10.7840/kics.2022.47.1.198

[3] June-Beom Park, Jong-Sou Park, “An Implementation of Federated Learning based on Blockchain”, The Journal of Bigdata, Vol. 5, No. 1, pp. 89-96, 2020.
DOI: https://doi.org/10.36498/kbigdt.2020.5.1.89

[4] Kyoungchan Won, Sukjae Jeong, “Design and Effect Analysis of Confederation Interface for ROK-US Combined Exercises”, Journal of the Korea Academia-Industrial cooperation Society, Vol. 19, No. 12, pp. 498-506, 2018.
DOI: https://doi.org/10.5762/KAIS.2018.19.12.498

[5] Geun-Hyeong Lee, Soo-Yong Shin, “Federated Learning on Clinical Benchmark Data: Performance Assessment”, J Med Internet Res 2020, Vol. 22, No. 10, 2020.
DOI: https://doi.org/10.2196/20891

[6] Seounghan Song, Suntae kim, Jung-Hoon Shin, Jeong-Hyu Lee, “Recovery Phrase Management Scheme for Public Blockchain Wallets based on OTP”, Vol. 20, No. 1, pp. 35-44, 2020.
DOI: https://doi.org/10.7236/JIIBC.2020.20.1.35

[7] N. Courtois, P. Emirdag, F.Valsorda, “Private key recovery combination attacks: On extreme fragility of popular Bitcoin key management, wallet and cold storage solutions in presence of poor RNG events”, Cryptology ePrint Archive, 2014.

[8] Soon-Gohn Kim, “A Study on the Blockchain 2.0 Ethereum Platform Analysis for DApp Development”, The Journal of Korea Institute of Information, Electronics, and Communication Technology, Vol. 11, No. 6, pp. 718-723, 2018.
DOI: https://doi.org/10.17661/jkiiect.2018.11.6.718

[9] Kwang-Man KO, et al., “Decentralized Consensus on Internet of Things: Review, Taxonomy, Open Research

Issues", IEEE Access, Vol. 6, pp. 1513-1524, 2018.

[10] Geth, https://geth.ethereum.org/

[11] Y. LeCun, L. Bottou, Y. Bengio, P. Haffner. "Gradient-based learning applied to document recognition", Proceedings of the IEEE, Vol. 86, No. 11, pp. 2278-2324, 1998.

저 자 소 개

황 승 연(준회원)

• Seung-Yeon Hwang received his BS in Department of Computer Science at Korea Polytechnic University in 2019. He is currently studying MS in Department of Computer Science at Anyang University. His research interests include Database System, Big Data, Data Analysis, Machine Learning, etc.

김 정 준(정회원)

• Jeong Joon Kim received his BS and MS in Computer Science at Konkuk University in 2003 and 2005, respectively. In 2010, he received his PhD in at Konkuk University. He is currently a professor at the department of Computer Science at Anyang University. His research interests include Database Systems, Big Data, Semantic Web, Geographic Information Systems (GIS) and Ubiquitous Sensor Network (USN), etc.

※ 이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2022R1F1A1062953).