Vietnam
VinUniversity

2021 International Blockchain Olympiad

Lam Nguyen Thanh Thao
Nguyen Duy Anh Quan
Nguyen Mai Phuong
Pham Phuoc Minh Quang
Pham Quang Bach
Tran Huong Lan

LifeLink
September 21st, 2021

Table of Contents

Abstract

Our business (LifeLink) offers a Blockchain-based federated learning model that provides a protected, non-compromise healthcare data collaboration platform, where healthcare database owners (i.e. hospitals, clinics, healthcare service providers) and research agencies (i.e. pharmaceutical companies, medical equipment manufacturing companies, health research institutes, AI healthcare companies) can easily be connected to accelerate healthcare innovation. We aim to prevent the risk of individual's privacy leakage and organization's data breach, while maintaining high accuracy in AI application development.

1 Market Problem & Opportunity

1.1 The life-saving impact of Artificial Intelligence (AI) in medical research

AI has powered medical research and the process, from laboratories' bench to bedside, is based on four key principles - the 4 'Ps' of personalized medicine, which are prediction and prevention of disease, more precise diagnoses; targeted and personalized interventions (i.e. therapy/ treatment). (Alonso et al., 2019)

Around the world, AI solutions are increasingly adopted within 69% of healthcare companies (McKinsey & Company, 2020). Its application could potentially create $150 billion in annual savings for the US healthcare economy by 2026 (Accenture, 2019). In Europe, 380,000 to 403,000 lives can potentially be saved with the use of AI annually. (John, 2020)

The Asia Pacific region also witnessed the fastest growth. AI Singapore, for instance, is a national program driven by government-wide partnerships and was granted SGD$35 million in AI research to lower the risk of diabetes, high cholesterol, and high blood pressure progression and complication development. (Burton, 2020)

1.2 From regional to global: the problem of health data privacy

However, the biggest barrier to fostering AI in healthcare is the inability to access a massive amount of sensitive patient data (i.e. medical records, data from mobile or wearable devices, etc.) while preserving their privacy to the absolute extent.

For example, in Hong Kong, the Electronic Health Record Sharing System receives limited acceptance rates from hospitals and private clinics or laboratories, with more than 730,000 patients registered to the system, but only 40,000 patient records are granted access by healthcare professionals (Deloitte, 2020). Similarly, in the G20 countries, especially the US, about 40 percent of hospitals and private doctors are reluctant to use electronic medical record systems due to privacy concerns.

1.3 Current shortcomings of Federated Learning solutions

Currently, a small number of healthcare organizations have resorted to Federated Learning solutions. By training their health data locally and sending the outcomes to a central server, the patient data never leaves their system and thus, there is greater privacy. However, this process has two tremendous drawbacks:

Firstly, via communicating model updates during the training process, these healthcare organizations could reveal sensitive information, either to a third party or to the central server. Other approaches that aim to solve this problem, including Secure Multiparty Computation or Differential Privacy, come with the cost of reduced performance & efficiency. (Abelson et al., 2015)

Secondly, federated learning is subjected to the Byzantine general problem, a scenario in which one or more clients in a federated learning setting will perform a malicious act in an attempt to sabotage the training process. Multiple algorithms, such as Krum or Bulyan, have been proposed to alleviate this problem, but so far none have stood strong against new attacking methods. Without a compelling reason to contribute, a client can simply choose to wreak havoc on the system whenever it feels like it.

With the rise of AI adoption in healthcare, the urgent need for data privacy of patients among healthcare providers, and the inadequacy of current solutions, LifeLink witnesses the significance of building a more reliable, stable and equitable decentralized platform for healthcare data analytics to empower AI in medical research.

2 Our Solution

A blockchain-based platform using Federated Learning to support stable machine learning collaborations between healthcare providers, pharma companies, and AI health companies without centralizing and sharing patient data.

Specifically, task owners and data owners are two main types of participants who can join and benefit from the platform.

2.1 Task Owners

As mentioned above, due to the positive impacts of AI application to healthcare, the demand for access to databases is increasing for both business and research purposes. In this case, we consider task owners as public health researchers, those that want to publish requests to train their federated learning model to healthcare agencies. They are provided access to the following functions to make the process of publishing tasks easier: Workflow management, Access to open datasets. Besides, they can also manage the amount of participating master data as well as the reward level set by the system, which depends on their training goals. For those that want to receive help on Machine Learning and Deep Learning models, we provide AI engineer broker services, in which the system will automatically reach out to companies that provide AI engineers in case researchers need to develop models.

2.2 Data Owners

We define data owners here as organizations, agencies that have healthcare datasets (i.e. Hospitals, clinics, health service providers). When joining the platform, data owners can contribute to global health, and benefit from our reward system. Their work would be training existing models published by task owners locally using their dataset, then sending the results to the platform without revealing any patients' record. Again, to promote participation, we provide an AI algorithm to fastly suggest the tasks which are suitable with their dataset's characteristics. This Client will automatically prepare data, train the given model, and also aggregate the global one. For those who do not have enough resources to train, the system will assign them a computer with full ownership to use to process the information. Note that we do not have any access to the information on that assigned computer, and every data movement between devices will be E2E encrypted using homomorphic encryption.

2.3. Use cases

Patient data for AI in cancer treatment

In 2020, 58.3% of global cancer deaths occured in Asia and by 2025 cases in India are expected to rise by 12% to 1.56 million. In response, a health tech company A is building AI models that support oncologists to develop effective, personalized cancer treatment for their patients. Company A is unable to acquire enough patient data since hospitals are concerned about re-identification risk from several health data leaks. By using LifeLink, Company A can send their AI model to our platform, and the platform will give a signal to a wide-ranging network of healthcare providers to train their patient data locally using this model and send the model outcomes back to Company A. This network includes:

- Hospitals that are specialized in cancer treatment and own clinical data of cancer survivors performing laboratory-based exercise tests post cancer treatment & demographic information.
- Mobile & Wearable devices companies like Fitbit that track changes in cancer survivors and own patient-generated health data (PGHD), including calories, steps taken, sleep efficiency, heart rate variability, body temperature, etc.
- Telehealth companies that obtain patient treatment history

After Company A receives each model outcome from different stakeholders, it will give them a reward through our platform. Our platform will reward each healthcare provider that participates in the project based on the quality of their outcomes.

3 Market

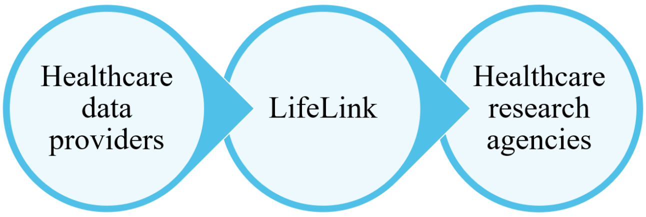
The global AI in healthcare market size is expected to grow from USD 8.23 billion in 2020 and reach USD 194.4 billion by 2030; it is projected to grow at a CAGR of 38.1% during the forecast period. (Allied Market Research, 2021)

- **Top end-user applications:**
  - Patient Data and Risk Analysis
  - Inpatient Care & Hospital Management
  - Medical Imaging & Diagnostic
  - Drug discovery
- **Target customers:** Healthcare organizations in the private sector

4 Partners

Stakeholders are classified into 2 groups:

- Healthcare data providers are those who have a large database of medical records and medical examination results
- Healthcare research agencies are those who want to train their AI models to accelerate precision drug development, transform healthcare product quality or develop treatment and patient outcomes



- Hospitals
- Clinics
- Healthcare service providers
- Wearable technology companies

- Pharmaceutical companies
- Medical equipment manufacturing companies
- Health research institutes
- AI healthcare companies

Fig 1. Overview of our partners

5 Business model

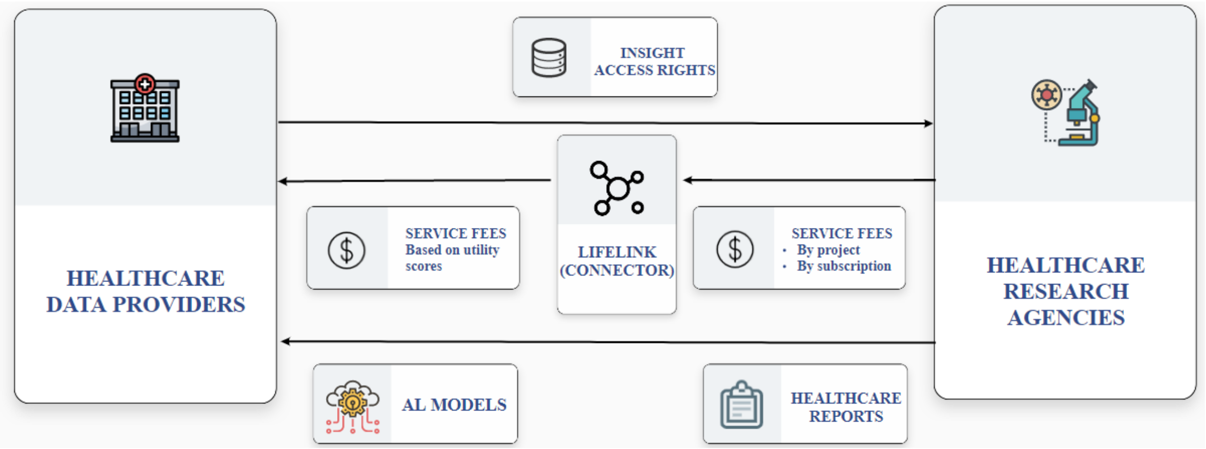


Fig 2. Overview of our business model

- Healthcare research agencies: Pay service fees by project or by monthly subscription
- Healthcare data providers: Receive (1) service fees based on their **utility scores** calculated by LifeLink system, (2) AI models and (3) insight reports from healthcare research agencies
- LifeLink: Receive service fees & profits for platform maintenance

6 Competition

Company	Market	Technology	Weakness
Owkin Connect	United States	Federated Learning only	● Less secure than a decentralized server ● Lack of effective reward system
Rhino Health			
Lynx.MD			
Definitive Healthcare	United States	Centralized data server	● Use publicly available datasets ● Not fully privacy-oriented
Sensyne Health	United Kingdom	Centralized data server	● Collect personal information when a person signs up for their service ● Not fully privacy-oriented
PHEMI Trustworthy Health DataLab	Canada	Cloud-based system	● Require uploading of PII (Personal Identifiable Information) to a big data warehouse ● Not fully privacy-oriented

7 Risks

1. **Potential Business Risks:**

   a. **Competition:**

Data analytics is a highly competitive service with many direct and indirect competitors. Among these competitors are companies that have already established reputation and credibility for themselves.

   b. **Slow platform adoption:**

Some hospitals in developing countries may be resistant to adopt new technology as they lack the needed knowledge and expertise in areas such as AI, Machine Learning, and Blockchain.

   c. **Data-intensive:**

In order for the prediction model to be accurate, there needs to be a high number of data available, and having inadequate data would make the model inaccurate, and thus, diminish the company's credibility.

   d. **Asynchronous data:**

Healthcare data, stored in multiple data formats and systems for every provider, is scattered across tens of thousands of healthcare providers and is rarely accessed by patients directly. As a single patient's data is spread across many health personnel and facilities, it is needed by just as many for care coordination.

2. **Business Risk Mitigation:**

   a. **Competition:**

Our business has the competitive edge over other data analytics businesses because of the high accuracy of our training model due to not having to over-anonymize our data and also that the risk of data re-identification has been considerably mitigated.

b. Slow platform adoption:

We will provide guidelines and training on the process of using the obtained data on the training model so that hospitals without the required expertise would be able to easily and quickly use the model.

c. Data-intensive:

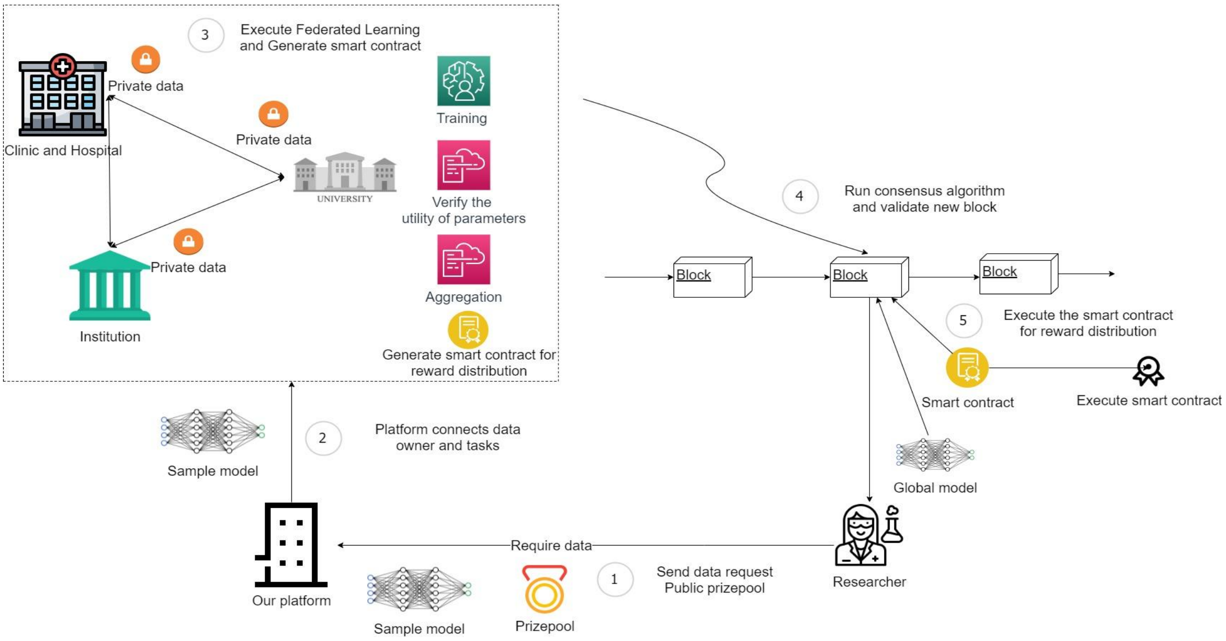
There has always been the demand by hospitals to share data among themselves but they have not been able to due to privacy concerns. With the usage of our model, as mentioned above, the risk of data re-identification has been considerably mitigated.

d. Asynchronous data:

General guidelines on how data should be stored and shared will be shared among hospitals in the same network to make sure that the data shared would be synchronized.

8 Architecture & Governance

The following figure illustrates our solution:



3
Execute Federated Learning and Generate smart contract
Private data
Clinic and Hospital
Private data
UNIVERSITY
Private data
Institution
Training
Verify the utility of parameters
Aggregation
Generate smart contract for reward distribution
4
Run consensus algorithm and validate new block
Block
Block
Block
5
Execute the smart contract for reward distribution
Smart contract
Execute smart contract
Global model
Sample model
2
Platform connects data owner and tasks
Our platform
Require data
Researcher
1
Send data request Public prizepool
Sample model
Prizepool

Fig 3. System Overview

Our solution consists of three main components: **Blockchain, dedicated server**, and **User Client**. The blockchain network is responsible for storing the block ID, reputation score of nodes, and reward-distributed contract for DataOwners based on their weight-utility. The dedicated server, on another hand, will act as the connector between task owners and data owners. Its mission is to introduce tasks to data owners and distribute bonuses based on contracts from the blockchain. Users access our service via either mobile app or website. Once the aggregation phrase is completed, reward will be distributed to participants.

8.1 BlockChain network

The blockchain functions as a platform for secure and indisputable aggregation of intermediate gradients used in federated learning. Our proposed blockchain is based on Hyperledger Sawtooth, a business-grade permissioned blockchain system suitable for cross-silo federated learning.

When data owners join the network, they will be given a number of reputation, represented as tokens. The bootstrapping process of the blockchain happens when a genesis block is created, in which asset statements of each client are recorded and the reputation token is dispersed equally among all participants. Falling in line with the Bitcoin tradition, there will be a fixed number of reputation tokens.

An asset statement contains the statement of ownership (the public key for verification), as well as a set of keywords that can be used as metadata for our own hosted servers to match data owners to task owners.

$$\text{ASSET} = \{\text{pk}, \text{Metadata}\}$$

The reputation token serves two purposes:

- For data owners: The reputation token dictates how much the model update can be trusted. Model updates from data owners who have low reputation can be ignored if the number of trustworthy updates before timeout reaches a predefined threshold (dependent on the training task).
- For validators: The more reputation a validator has, the more likely it is that the validator will get to update the next block.

The server will suggest data owners who have the same metadata to participate in a “village” consisting of validator nodes and the task owner. The data owners will train their data according to hardcoded logic within the Training Chaincode, and when they finish their required number of epochs, they will launch a transaction to the Aggregating Chaincode. Transmission of the parameter updates must be encrypted using an additive homomorphic encryption scheme, i.e. Paillier.

After a specified timeout, validators will start executing the Aggregation Chaincode to aggregate the intermediate parameter updates using FedAVG and calculate shapley values. At this point, Proof-of-Elapsed Time (PoET) will start assigning to each validator a random sleep time, during which time the validator is free to execute other things (e.g. matching other tasks with data owners). Whichever wakes up first will win the block and get to update the global model. Data owners who fail to submit a model in time will have their reputation token removed and given to the block winner.

The randomness is dependent on both the hardware (Intel SGX enclave generator) and the number of reputation token one has:

$$\text{Chance to get the next block} = \text{Num. of reputation token} + \text{random number} \times \text{Village size}$$

Note that a 0 reputation does not necessarily mean the chance for contribution is over. Conversely, the larger the village, the harder it is for a party which had committed wrongdoing to be able to participate in subsequent rounds.

8.2 Dedicated server (platform)

The main mission of our platform is to connect researchers and data owners. The platform will work to manage and provide services to users. Specifically, it will be a stable server for connecting tasks and data owners. Note that, even if this server crashes, the training of the tasks will still take place normally, the server does not participate in the transaction (model) between the two parties but is only the referrer.

8.3 User Client

This will be a type of client application that will, first and foremost, be designed primarily for the web, and then develop on mobile.

- **Task Owner (Researchers):**

- Task Publishing: This interface includes 2 main functions including publishing and canceling tasks. With the publishing function, the task owner must upload the model and input requests. This model will be sent to a dedicated server under SSH protocol to ensure security. Once data owners are involved, the model is transferred to those data owners.
- Workflow management: The job management interface includes a job progress check, including how many rounds have been trained. The loss function, precision, and some other errors are plotted for analysis purposes. The task owner can also manage the number of nodes (the number of participants) and the reward per person.
- Service costs: The system will apply a utility vector-based money mechanism calculated by the nodes in the blockchain. These utility vectors will be calculated by "shapley values" (Wang et al., 2019), one of the methods of measuring the contributions of participants based on the parameters updated. In addition, service or cloud computing costs (in case of use) will be calculated at a reasonable fee.

- **Data Owner (Clinics, Institutions):**

- Tasklist: The Tasklist will be published on our platform. Appropriate tasks can be suggested to Data owners using AI. In particular, the AI will provide an analysis based on the participants and contributions in the previous task.
- Task management: Use cookies to access computer system information (only use locally, do not transmit information). Thereby, the system will provide training time, temperature, device status, and so on to ensure safety and convenience for users.
- Cloud computing service: For those who do not have enough resources to train, the system will assign them a computer with full ownership to use to process the information. Note that we could not get any information from that assigned computer.

9 Value Proposition

Technology	Traditional AI	Federated Learning	Blockchain-based federated learning
Decentralized data (No sharing)		X	X
Decentralized server			X
Incentive			X

Our mission is to enable healthcare institutions to exchange health insights without ever having to betray their patients.

a. No-compromise privacy

Most solutions for crowdsourcing health data stops at being “data banks”: clusters of cloud servers that hospitals must upload their data to in order for companies or research institutions to scrutinize. To do that, many rely on the concept of the data clean room, in which data will be stripped of PII (personally identifiable information) and added noise. This classic tradeoff between privacy and utility is not low-hanging fruit, and might provoke distrust in patients who do not explicitly give consent for their data to be sent somewhere else. Our solution aims to cultivate a healthy collaboration culture, where healthcare companies, hospitals and research institutes can live together in harmony, and privacy, be it the individual or the organization, is respected. No data is ever transferred outside of their home, which also significantly reduces information transfer overhead; this is beneficial in places where the Internet connection is unreliable.

b. Stability and reliability

Having blockchain as the backend to federated learning greatly bolsters the technology’s power to protect the privacy of the individual. Since every client has an indisputable copy of the global model, there is no single point vulnerable to attack, electricity outages, or other unexpected situations. Furthermore, the burden of training the dataset is not on the shoulder of one central server, but is rather spread out over many clients. This BYOL (bring your own lunch) approach ensures that the responsibility of maintaining the system is also decentralized.

10 Distribution/Expansion

We plan to begin our operation in Vietnam, then we would expand to Malaysia and Singapore. After that, we would expand to other countries within the Asia-Pacific region: Thailand, Hong Kong, Taiwan, The Philippines.

The general method behind our expansion is that for each country, we will first target private hospitals because of their higher level of development and investment in technology and infrastructure. This will allow the implementation of our technology much smoother and would yield better results from the higher quality of data provided from them.

Vietnam

When we first begin our operation in Vietnam, we plan to approach VinMec, the most developed private hospital system in Vietnam. VinMec has many hospitals all across the country and thus, the cooperation between our company and VinMec would allow us to demonstrate how we will be able to safely use the data between hospitals for the learning model.

After our partnership with VinMec, we would be able to make a reputation for ourselves, and from then, we would expand to other private hospitals in Vietnam. During the process of working with other private hospitals, we will consider whether cooperation with public hospitals would be feasible as there are concerns with regards whether public hospitals would have the needed expertise to make use of the shared data for the training models.

Malaysia and Singapore

We choose Malaysia and Singapore to be the next target after having successfully operated in Vietnam. This is because among the countries near to Vietnam, they have the highest level of infrastructure and technology in the healthcare industry and this would make it easier for us to promote the usage of our business in the hospitals in Malaysia and Singapore.

For Malaysia, we plan to first partner with private hospitals, and more specifically are Oriental Melaka Straits Medical Centre and Mahkota Medical Centre, both located in the city of Melaka. The rationale behind such a choice is that they are both located in the same city, and thus, data synchronization between them would be easier, allowing for higher accuracy from our learning model.

For Singapore, we plan to partner with Parkway Pantai and Raffles Medical Group as the former is the largest healthcare provider with hospitals in several South East Asia countries, while the latter is one of the largest private healthcare providers in Asia. When we have successfully implemented our technology in these private healthcare providers, we will then expand to both private and public hospitals. The reason for the difference in approach for Singapore compared to other countries is that both the private and public healthcare sector in Singapore are well developed.

America

After operating successfully in Asian market, our ambition is to penetrate into America by cooperating with top American private hospitals. This brings new hope in the global effort to crowdsource health insight, where healthcare models will no longer be limited by inherent biases in race, climate and living standards, among others.

References

Abelson, Reed; Goldstein, Matthew (2015). "Anthem Hacking Points to Security Vulnerability of Healthcare Industry". The New York Times. New York. ISSN 0362-4331. Retrieved 17 February 2015.

Accenture (2019). AI: AN ENGINE FOR GROWTH. https://www.accenture.com/us-en/insight-artificial-intelligence-healthcare%C2%A0

Allied Market Research. (2021). Artificial Intelligence in healthcare market: Global report – 2030. https://www.alliedmarketresearch.com/artificial-intelligence-in-healthcare-market?fbclid=IwAR0CQpNMboBdPaHoXaUMjWytg7ChB0-PNJpoIfqIwX-aoSEu4Jz4n2CSzpU

Alonso, S. G., de la Torre Díez, I., & Zapiraín, B. G. (2019). Predictive, personalized, preventive and participatory (4P) Medicine applied TO telemedicine and Ehealth in the literature. Journal of Medical Systems, 43(5). https://doi.org/10.1007/s10916-019-1279-4

Burton, P. (2020, January 17). *AI in APAC HEALTHCARE: Building the foundations*. PharmaBoardroom. Retrieved September 21, 2021, from https://pharmaboardroom.com/articles/ai-in-apac-healthcare-building-the-foundations/.

Deloitte (2020). The socio-economic impact of AI in healthcare. https://www.medtecheurope.org/wp-content/uploads/2020/10/mte-ai_impact-in-healthcare_oct2020_report.pdf

Johns (2020). How AI could augment medical devices to save lives, money and time. NS Medical Devices. Retrieved September 21, 2021, from https://www.nsmedicaldevices.com/analysis/ai-medical-device-technology/.

Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Zhao, S. (2019). Advances and open problems in federated learning. arXiv preprint arXiv:1912.04977.

McKinsey & Company (2020). Transforming healthcare with AI, The impact on the workforce and organisations. https://eithealth.eu/wp-content/uploads/2020/03/EIT-Health-and-McKinsey_Transforming-Healthcare-with-AI.pdf

Shahani, Aarti (2015). "The Black Market For Stolen Health Care Data : All Tech Considered : NPR". npr.org. Retrieved 17 February 2015.

Wang, G., Dang, C. X., & Zhou, Z. (2019). Measure contribution of participants in federated learning. *2019 IEEE International Conference on Big Data (Big Data)*. https://doi.org/10.1109/bigdata47090.2019.9006179

Weng, J., Weng, J., Zhang, J., Li, M., Zhang, Y., & Luo, W. (2019). Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive. IEEE Transactions on Dependable and Secure Computing.

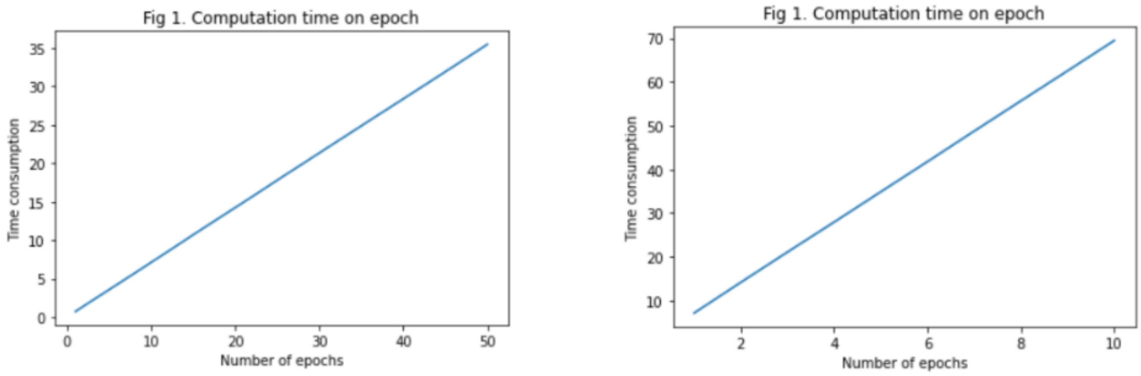
Appendix

In this section, we will introduce the blockchain-based federated learning experiments performed for our proposed method.

The system used in our experiment is Ubuntu 18.04 LTS, the backend used is the GPU version of Pytorch, with the 12GB NVIDIA Tesla K80 GPU acceleration for model calculation.

We simulate a CNN network on the MNIST dataset that includes 30000 datapoints. In this experiment, we simulate 10 clients with 3000 data points each for the federated learning task. This dataset will be used to recognize handwriting digits. In this experiment, we use two 2-D convolutional layers following by 2 linear layers. ReLUs will be used for the activation functions. All the components above will be implemented using Pytorch.

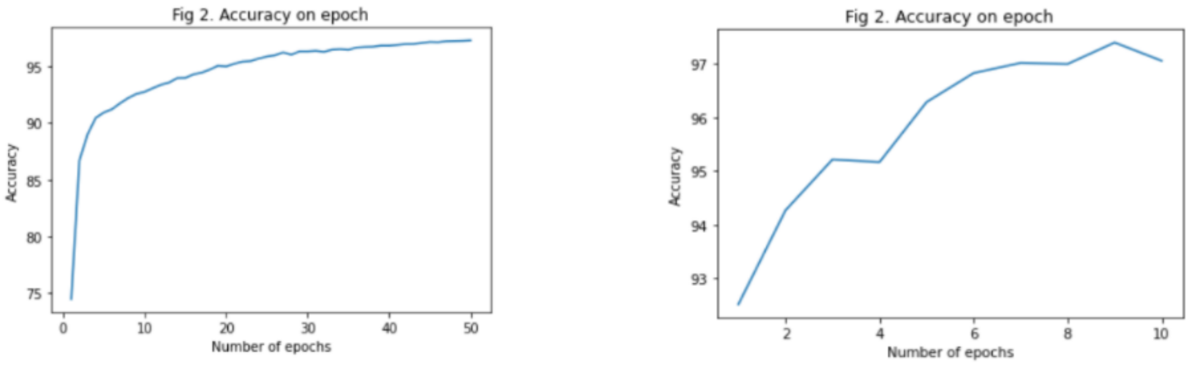
The test set will have 10000 data points completely different from the training dataset for the most objective validation. The following figures illustrate how we could enhance the model efficiency in comparison with the traditional AI model.



Our proposed solution

Traditional AI

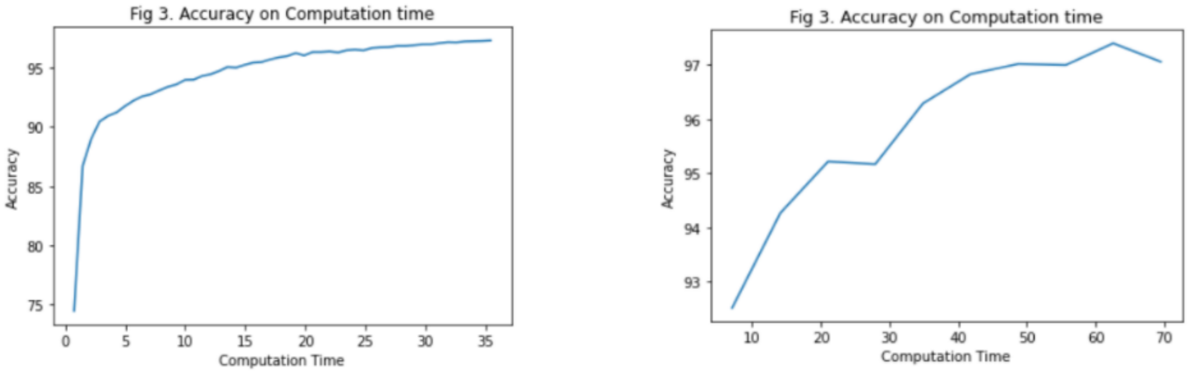
Fig 1. Computation time vs epochs size



Our proposed solution

Traditional AI

Fig 2. Accuracy on epoch



Our proposed

Traditional AI

Fig 3. Accuracy on Computation time

Clearly, it needs more epochs to get to the convergence point compared with the traditional AI. In this experiment, we need approximately 50 epochs to get the accuracy at 97%, whereas 9 epochs are needed in traditional AI. However, the training time for each training epoch in federated learning is much lower than the centralized server. Specifically, the training time for federated learning is just half of the centralized CNN network. In total, 50 epochs took roughly 35 seconds for training, which is a significant drop compared with 70 seconds from the traditional ones. On the other hand, we could see that the aggregated model from local ones could enhance the accuracy a bit (figure 4). This means the local overfitting could be avoided by the influence of other clients.

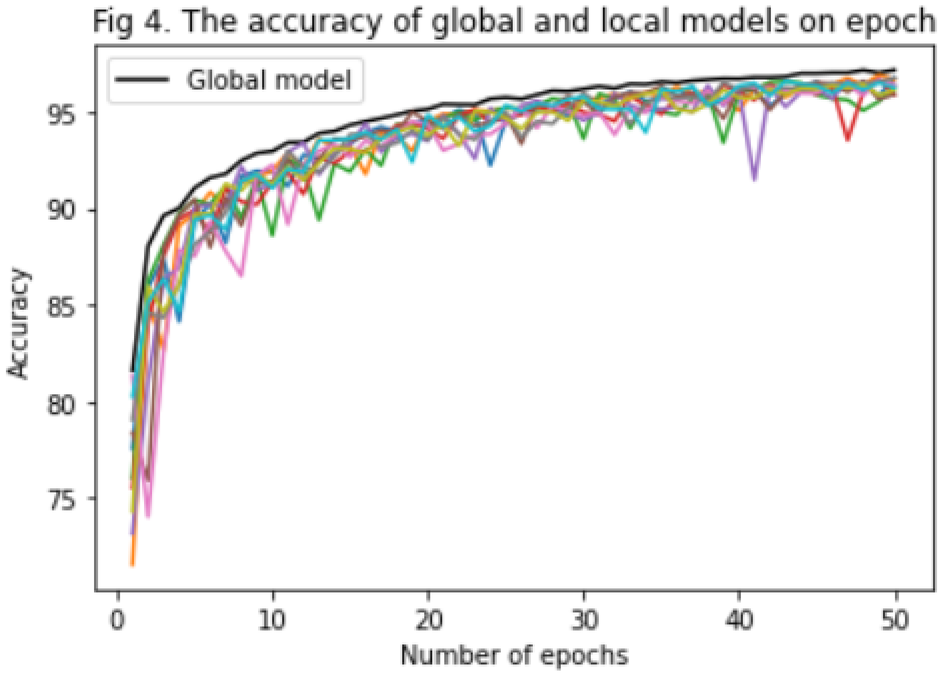


Fig 4. The accuracy of global and local models on epoch