Soft Computing (2023) 27:9941–9954
https://doi.org/10.1007/s00500-023-08330-6

FOCUS

Securing health care data through blockchain enabled collaborative machine learning

C. U. Om Kumar[1] · Sudhakaran Gajendran[2] · V. Balaji[3] · A. Nhaveen[3] · S. Sai Balakrishnan[3]

Accepted: 25 April 2023 / Published online: 23 May 2023

Abstract

Transferring of data in machine learning from one party to another party is one of the issues that has been in existence since the development of technology. Health care data collection using machine learning techniques can lead to privacy issues which cause disturbances among the parties and reduces the possibility to work with either of the parties. Since centralized way of information transfer between two parties can be limited and risky as they are connected using machine learning, this factor motivated us to use the decentralized way where there is no connection but model transfer between both parties will be in process through a federated way. The purpose of this research is to investigate a model transfer between a user and the client(s) in an organization using federated learning techniques and reward the client(s) for their efforts with tokens accordingly using blockchain technology. In this research, the user shares a model to organizations that are willing to volunteer their service to provide help to the user. The model is trained and transferred among the user and the clients in the organizations in a privacy preserving way. In this research, we found that the process of model transfer between user and the volunteered organizations works completely fine with the help of federated learning techniques and the client(s) is/are rewarded with tokens for their efforts. We used the COVID-19 dataset to test the federation process, which yielded individual results of 88% for contributor a, 85% for contributor b, and 74% for contributor c. When using the FedAvg algorithm, we were able to achieve a total accuracy of 82%.

Keywords COVID-19 · CT scan images · Federated learning · Blockchain · VGG-16 · AlexNet · Inception (V3)

1 Introduction

Collecting data for the purpose of training machine learning model is one of the primary step in the machine learning process. The predictions made by machine learning systems can be pretty much the data on which it is been trained. We're working with digital assets for all of our data and models. When you share a data source with someone, you're essentially handing it over to them and trusting them to keep it secure while they're on the task (Om Kumar et al. 2013, 2014).

Without a doubt, data is a company's most valuable resource. We dwell on data, where businesses place a high value on sharing, analysing, and gathering data on their users and stakeholders, particularly from social media (Rawat et al. 2022). Clarity in how organizations obtain authorization to preserve private data, adhere to their privacy laws, and organize the data obtained is critical to establishing confidence with clients who regard security as a primary priority (Om Kumar and Sathia Bhama 2019, 2021; Om Kumar et al. 2022). Data management for compliance with regulations is perhaps much more critical. Lack of compliance with regulatory obligations regarding how a company gathers, maintains, and manages individual data might result in a hefty penalty (McMahan and Ramage 2017). If the organization is hacked or malware is used, the ramifications in cost of lower profits and loss of client trust may be significantly greater.

✉ C. U. Om Kumar
cuomkumar@gmail.com

[1] School of Computer Science and Engineering, Vellore Institute of Technology, Chennai Campus, Chennai, India

[2] School of Electronics Engineering, Vellore Institute of Technology, Chennai Campus, Chennai, India

[3] Department of Computer Science and Engineering, SRM Easwari Engineering College, Chennai, Tamil Nadu, India

In today's data driven world, the ultimate significance of an organization is derived from the data it collects from its clients, which implies that the data is a valuable resource that should be safeguarded and preserved. Organizations must provide clarity by discussing whatever data they gather, for any purposes or objectives, how the data is being processed, etc. in order to preserve data and ensure trust (Benhar et al. 2020).

It can also be thought of as a multi-stakeholder computation. In a machine learning context, multiple entities will want to work together. One entity may own training data while providing a machine learning server, whereas another entity may own inference data. In this situation, the inference could be performed by a model that belongs to someone else. As a result, trust issues will play a significant role in such complicated situations. Real-world datasets are usually inadequate, inconsistent, and devoid of specific traits or patterns. They're also likely to be full of mistakes. As a result, they're processed into structure that the machine learning algorithm can use to build the model once they've been collected.

Differential privacy (Dwork 2011) method allows to collect personal data while ensuring that the output can't be linked to the presence or absence of any particular individual in the dataset. An algorithm is differentially private if an observer looking at the output can't tell whether a specific individual's data was used in the computation. To safeguard the individual privacy, a random noise is generated using a selected distribution, causing the true response to be perturbed and the result with noise to be returned back to the user (Li et al. 2022).

Manual and automatic data cleaning techniques are used to remove data that has been erroneously added or categorised. Most ML frameworks feature techniques and APIs for balancing missing data in data imputations (Chollet 2017). (1) Attributing missing values with median, mean standard deviation, and k-nearest neighbours (k-NN) of the data in the specified field is a common technique (Choudhury et al. 2020). (2) SVM algorithms are directed learning methods that undergo data analytics for regression and classification problems. (3) Decision tree employs a branching strategy to show every conceivable choice result. So, every node shows a study on a single value, to every path representing the result of that study. (4) Clustering which is a process of gathering comparable sets of data together. It may be used to divide data into clusters and conduct a pattern and analyse it on every dataset (Domadiya and Rao 2021; Hamza et al. 2020).

Neural networks (Gajendran et al. 2020, 2023) which are a set of algorithms which replicate the cognitive activities in order to identify patterns in large datasets and it extends to different domains. Convolution neural network consists of layers that are minimal specifics and are handled by the training stage, whereas higher-level characteristics are handled by the upcoming levels (Howard et al. 2017).

Homomorphic encryption (Huang et al. 2017; Bos et al. 2014) plays a role when it is conceivable to use this technology to do machine learning on encrypted data that remains encrypted throughout. This method permits computation on cypher texts, resulting in an encrypted result that, when decoded, equals the result of the operations conducted on the plaintext.

The extra function of 'dot get' accepts an argument named 'Epsilon', which allows us to set the size of our privacy budget. Every data science project has a privacy budget, which is determined by the level of trust and type of relationship you have with the data owner. Secure multiparty computation algorithm which illustrates that numerous persons may able to combine their inputs to compute a function without disclosing their inputs to one another, implying that multiple people can share ownership of a number. So, in this technique, we'll encrypt some value and distribute it among shareholders, with the original encrypted value being unknown and hidden due to the encryption.

In federated learning (FL), heterogeneous data is frequently collected. The raw data of each client neither stored locally nor being transferred. Analysts do not have access to per-client messages; therefore, data is taken from client data for quick (Weng et al. 2019) aggregation.

Differential privacy is a strategy in which a randomised process is considered differentially private if changing one input element results in only a little change in the output distribution. This means that no judgments can be drawn regarding whether or not a particular sample was used in the learning process. A popular strategy for (Zhao et al. 2019a) gradient-based learning systems is to use differential privacy by randomly alarming the intermediate output (e.g., using Gaussian noise) at each iteration. Of fact, there is an inherent trade-off between adopting differential privacy and reaching a high level of model accuracy, because adding more noise increases privacy while decreasing accuracy. The use of FedAvg which is federated averaging algorithm involving training multiple clients in a distributed manner to maintain the efficiency of communication.

FL divides privacy into two main categories: local privacy and global privacy (Jamil and Kim 2021). Changes made in the model at every round must be private to all third parties to maintain global privacy (Jena 2021). Other hand local privacy ensures that the updates be kept protected from the server as well. On the server, data reduction takes place. Over sampling is a technique for correcting bias or imbalance in a dataset by adding extra observations/ samples to the under-represented classes using methods such as repetition, bootstrapping, or the synthetic minority over-sampling technique (SMOTE). When merging different datasets to create a huge corpus, data integration can help overcome the shortcomings of a single dataset. The dataset size influences the memory and processing required for iterations during training, which is called data normalisation.

As applied to aggregations, the principle of data minimization includes the goal of gathering the required data for the particular computation also known as focused collection, limiting access to data, processing individuals' data as quick as possible, and discarding both collected and processed data as soon as possible. To put it another way, data minimization entails limiting access to data to the minimum number of people possible, which is frequently achieved through security mechanisms such as encryption at transit and rest, access-control lists, secure multiparty computation, and trusted execution environments.

Our privacy rights have been compromised by technology. The majority of what individuals or businesses do today fall into the public domain. Personal and organisational data, behaviours, preferences, and actions are monitored, stored, and used by third parties. The collecting, organisation, and selling of our personal data is at the heart of many new business models. Even if an individual opts out of social networking networks, technology has made it possible to correlate data back to them.

Blockchain technology has the ability to mitigate the consequences of this erosion of privacy while still allowing for the release of personal data when it is necessary (Salah et al. 2019). A user may, for example, retain personal information on a blockchain and temporarily disclose portions of it in order to get services. Bitcoin and other blockchain-based digital currencies have shown that using a peer-to-peer decentralised network and a public ledger, reliable and transparency computation is achievable (Krizhevsky et al. 2012; Yin et al. 2021).

Consensus algorithm are methods through which all clients in a blockchain network achieve a confirmation on the current state of the shared network (Li et al. 2020). Consensus methods improve stability of the network and create confidence amongst anonymous peers in a decentralised manner. Proof of work which is a type of cryptography evidence wherein a participant shows to others that they have invested a specified quantity of computing work (Li et al. 2021). Proof of stake which is a type of blockchain agreement method that selects stakeholders based on one's bitcoin assets.

Federated learning allows decentralised privacy protection and prevents single point failure, by combining blockchain with federated learning (Hao et al. 2020). In addition, blockchain could offer federated learning participants benefits (Qi et al. 2021).

Poisoning attacks can be avoided because a novel blockchain system with a non-tempering feature replaces the central authority. Because poisoning attacks are no longer a threat, the protection mechanism is strengthened even further.

High efficiency is the result of two fundamental traits working together. The first, federated learning, necessitates merely the sharing of training updates. The other one is that only the pointer is saved on the blockchain, while the accompanying data is stored in a distributed hash table off-chain.

2 Motivation

- In the past year, we experienced a vast number of changes due to the pandemic situation. The lack of resources in the healthcare industry was quite evident during this time.
- We have unrestricted access to data in our daily lives (usually) to train a machine learning model. This method is acceptable as long as data privacy is not an issue.
- However, if we need to work on sensitive data such as health and if they refuse to share due to data privacy laws, we're stuck.

This work aims to contribute.

- The model/data used in the existing systems is not anonymized and are fragmented in nature, we are using the decentralized server where the model undergoing decentralization is refined using FL techniques.
- There are situations where the third-party organizations have trust issues for sharing their data. So, we introduce blockchain technology where we reward the organization(s) who volunteer themselves so that the bond between the respective organization increases.

The manuscript is organised as follows: Sect. 1 is an introduction that explains the basic knowledge about the system's fundamentals. Section 2 is a literature review that expands on the research works on existing systems. Section 3 is the system proposal where the system architecture, functional architecture and requirements of the system are explained. Section 4 describes various test scenarios for the modules described by the proposed system, as well as the proposed system's performance analysis. Section 5 includes the conclusion, which summarizes the performance and efficiency of the proposed system which provides improved results and future work in the proposed system.

3 Literature survey

FL shields users from disclosing their personal information while collaboratively training the global model for a range of practical uses. However, there are numerous opportunities for hostile clients to undermine FL's security. Blockchain can be used as a viable remedy to address these problems. Blockchain technology can be used to store ML/DL models and model parameters, enhancing data security and enabling FL decentralisation. FL can also be used to improve blockchain technology in a number of ways, for as by increasing consensus effectiveness. Additionally, by utilising blockchain, local learning model updates on mobile devices may be transferred and confirmed. Immutability, authenticity, distribution, transparency, and decentralisation are just a few of the major characteristics of blockchain.

Qiang et al. (2021) have proposed a system which involves defending the leakage of privacy using CNN in edge devices via BNN where their prosed system uses binary neural networks (BNNs) and convolutional neural networks (CNNs) to collect the data encrypt it before storing it to the cloud and then use it for training and testing without the need for decryption. Their system could lead to risk since they are stored in one place before encrypting. Hu et al. (2020) proposed a personalized federated learning with differential privacy approach which is Effective to user heterogeneity and provides good privacy for user data using iterative search technique. But since the devices are heterogeneous the training process is very complex and challenging in this method. In order to protect the privacy of data, Rahman et al. (2020) have suggested a system that uses data science and machine learning algorithms such as homomorphic encryption and dimension reduction. The proposed system is designed to instil confidence in consumers that their personal information will not be exploited and that data privacy will be protected via machine learning. This system is only used for certain diseases and health issues. Shaham et al. (2021) presented a machine learning approach for the purpose of publishing the location of data in a privacy-preserving manner. Their approach uses k-means algorithms with clustering, alignment, generalization mechanisms. They proposed a technique to build MLA, which is a machine learning-based anonymization framework that secures users' privacy while releasing geographical itinerary datasets. In this system the MLA framework uses a centralized server in which the time is consumed for training and distributing the model.

Tanwar et al. (2020) have proposed a methodology by adopting machine learning techniques to develop smart applications based on blockchain. This methodology uses the consensus algorithm, secure hash algorithm (SHA). The goal of this methodology is to create combination of machine learning and blockchain which are smart application-based improvements that are much resistant to casualties such as smart cities, healthcare, Smart Grid (SG), Unmanned Aerial Vehicle (UAV) but it appears that the performance is hampered by an increase in chain and a high demand for internet bandwidth. Wang et al. (2019) proposed a mechanism for adjusting privacy based on the distribution of data in datasets. As a result, service quality has improved, federal transmission and storage efficiency has improved, and data submitted by each customer learning training has been protected. However, when applying sparse differential gradient to improve transmission efficiency, the model's accuracy drops by 0.03%.

Shayan et al. (2018) proposed decentralized federated learning via mutual knowledge transfer which uses heterogeneous data instead of homogeneous data. When compared to baseline approaches, this has a greater global classification accuracy after a set of number of cycles. But more theoretical analysis for this method needs to be conducted for better performance. Simonyan and Zisserman (2014) proposed a method which offers higher model performance when compared to differential for different datasets, experimental setups, and privacy budgets using logistic regression. But it is found that when differential privacy is used, the performance degradation in federated learning is much more severe. Srivastava et al. (2021) prosed a framework called PPSF which is a privacy-preserving and secure framework for IoT driven smart cities using machine learning and blockchain. This framework uses (PCA), which is principal component analysis technique, (ePoW) enhanced Proof of Work algorithm, LightGBM. PPSF is a smart blockchain framework in which blockchain combines with machine learning to preserve security and privacy in smart cities driven under IoT. The presented PPSF framework was shown to be slightly less than peer privacy-preserving intrusion detection approaches after undergoing multiple studies.

Szegedy et al. (2016) proposed a method for federated learning that is decentralised, reliable, and safe without the use of a centralised model coordinator. This effectively prevents data poisoning threats and enhances model update privacy protection. However, the proposed model's convergence rate is slower than that of the SAE model. Toyoda et al. (2020) proposed a method for implementing layout with a current blockchain technique and rewarding workers with cryptocurrency for adhering to the protocols. However, this solution does not use an open network of blockchain to implement design. Shahbazi and Byun (2022) prosed a system on blockchain-based event detection and by using machine learning and natural language processing to verify trust among individuals using Naive Bayes, logistic regression, XGBoost techniques. The prosed system's main purpose is to develop a system to automatically map crises and catastrophes with the assistance of different relief organizations. In this system due to lack emergency aid facilities, the recovery process in other calamities could delay. Sun et al. (2019) prosed a system for publishing a medical data model through differential privacy. Their prosed system uses algorithms like Differentially Private Mini Batch (DPMB), Mini Batch Gradient Descent (MBGD) algorithm, Back Propagation (BP) algorithm and gradient descent algorithm. This tends to provide good privacy and assurances when it comes to publishing and training data. This system uses only a limited number of datasets and accuracy is reduced when different datasets used simultaneously. Zhou et al. (2019b) have proposed a system which includes heterogeneous networks based on ML techniques to improve the efficiency of communication over decentralized networks using Stochastic Gradient Descent (SGD) algorithm, Communication policy generation algorithm. They proposed NetMax, a communication-efficient decentralised technique for accelerating distributive machine learning across heterogeneous networks. Their system fails to work in the presence of a main server which leads to issues in data privacy.

Healthcare data security and privacy present significant challenges. Protecting sensitive information is a basic aspect of privacy. The rising volume of medical data that is becoming a crucial component of patient treatment has led to attacks on healthcare data. Outside adversaries are often kept at bay by authentication and encryption mechanisms, but the real threat comes from hostile insider behaviour, which leads to attacks like eavesdropping, replay attacks, denial of service attacks, and others.

The current systems for protecting privacy are insufficient to guarantee the complete security of healthcare data. On the other hand, an internal attack, which is substantially worse than an exterior attack, is affecting the majority of the medical records stored on the cloud server. Additionally, as medical data involves sensitive patient information, privacy is a crucial buzzword in the medical system. The privacy concern for each patient differs depending on the data connected to them. How to maintain appropriate privacy without information loss is crucial.

FL is a decentralised strategy that gives numerous network nodes strong, tailored data that is also privacy-aware. With better performance and privacy protection, it offers a lot of potential in many applications. While simultaneously maintaining robust local learning in the local devices, it uses distributed data for training. Although standard FL provides many benefits, it can also lead to substantial communication delays and the failure of a single server that aggregates the learning. Additionally, an adversary node might upload an erroneous model, which could interfere with the FL system's learning process. In order to solve some of the limitations like privacy preservation, the blockchain framework, with its built-in capabilities like traceability, immutability, and transparency, can be connected with FL.

4 Proposed system

The user/data analyst uploads a model that is required from other organizations to the DWeb (Decentralized Web). The purpose of using the DWeb is because it is connected to a decentralized network i.e. Blockchain. It is then connected to the server which is the PySyft federated server. The uploaded model immediately triggers an escrow smart contract by using the Ethereum blockchain where the transaction begins for organizations. The model is distributed among the organizations by the PySyft federated framework. The shared model is then received by the clients/contributors in the respective organizations that are willing to participate and contribute their service to the user/data analyst. The contributors in the organizations train the model at their end using their own data. For aggregation, the trained model is returned or sent to the decentralised server/PySyft federated server. The user/data analyst receives the aggregated model. Simultaneously, the amount to be paid is calculated in the metaverse wallet, which is used to make digital payments. The aggregated model can only be downloaded and accessed once the transaction has been completed by the user/data analyst. Three main modules make up our proposed system.

The first one is a WebApp, where an analyst can send the model to the hospitals to train on their data in my case, COVID CT scan dataset is used as an example. The second is an actual learning protocol: we employ Federated Learning with a potential extension of Differential Privacy in order to keep the data secure. Federated learning alone is not secure even though it eliminates the need for data transfer by using the model transfer technique to train the model on the client-side, there is still direct interaction between the user and the client which makes the connection vulnerable. To avoid this, we are using blockchain as the third component: transfers are performed by blockchain, and each client shares how much they have contributed to the training ground and how to reward each hospital for the work that they did.

In Sect. 4 experimental analysis of this report, we go over the tools we used to create our proposed system in detail.

4.1 Smart contract

Solidity is the programming language that we used for creating Ethereum-based smart contracts. due to the lack of floating-point in the Ethereum Virtual Machine 128-bit integers with a numerator of 64-bit and the 64-bit denominator are used in the client-side part of the system, the Ethereum Virtual Machine simply lacks multidimensional arrays with dynamic sizes, hence the weights are stored in a flattened array of the same 128-bit integers for the federated learning update step.

4.2 Federated averaging

Federated Averaging (FedAvg) is a simplified general form of FedSGD. The logic behind generalization is that averaging the gradient is strictly similar to averaging the weights of the model considering all the local nodes start from the same initialization FedAvg does not degrade the performance of the averaged model i.e. federated average allows multiple training cycles on the nodes and exchange the updated weights without much complexity. The operation of Federated averaging is represented in Fig. 1: Architecture of the BLOCKFED.

The following steps are used to carry out this algorithm.

1. The global model is synchronously delivered to a chosen subset of Federation members (known as clients/contributors).
2. Using its local data, each client computes an updated model.
3. The server receives model updates from each selected contributor.
4. The server combines these models using FedAvg to create a more accurate global model

4.3 Private Ethereum blockchain network

In blockchain custom data cannot be stored hence Ethereum blockchain network with the smart contract is used. Proof of authority, which will allow us to store custom data on blockchain blocks and the miner to run the code that can change the data. Miner nodes are nodes in the blockchain network which is run by the participants. The smart contract method is triggered when the miners receive a request to execute the smart contract, which is then retrieved from the blockchain, executed and the result is stored. Everyone must agree on which value to be saved, which is accomplished through proof of work. However, as the system grows, it takes longer and longer, which is undesirable in our scenario, hence we use proof of authority which allows the system on which value to be accepted in a determined amount of time that is set.

4.4 Federated learning using Ethereum blockchain

Federated learning helps contributors to run a computation on their own device and data in a secure way, rather than the traditional way of sharing data to the server. Here the model is updated from local training, which allows the multiple contributors to training a model together. The uploaded model is being sent to all contributors at the start of the training process via the Ethereum blockchain network for a single training session. Then the contributors start training these models on their data locally on their devices, after the training phase a smart contract is then executed to return the updated models to the Ethereum blockchain network.

Finally, using the federated averaging algorithm, all the contributor's models are merged into the weights and then they are averaged this process is known as federated averaging, the data points from the local model are used to assign which weight is to be updated from each contributors model.

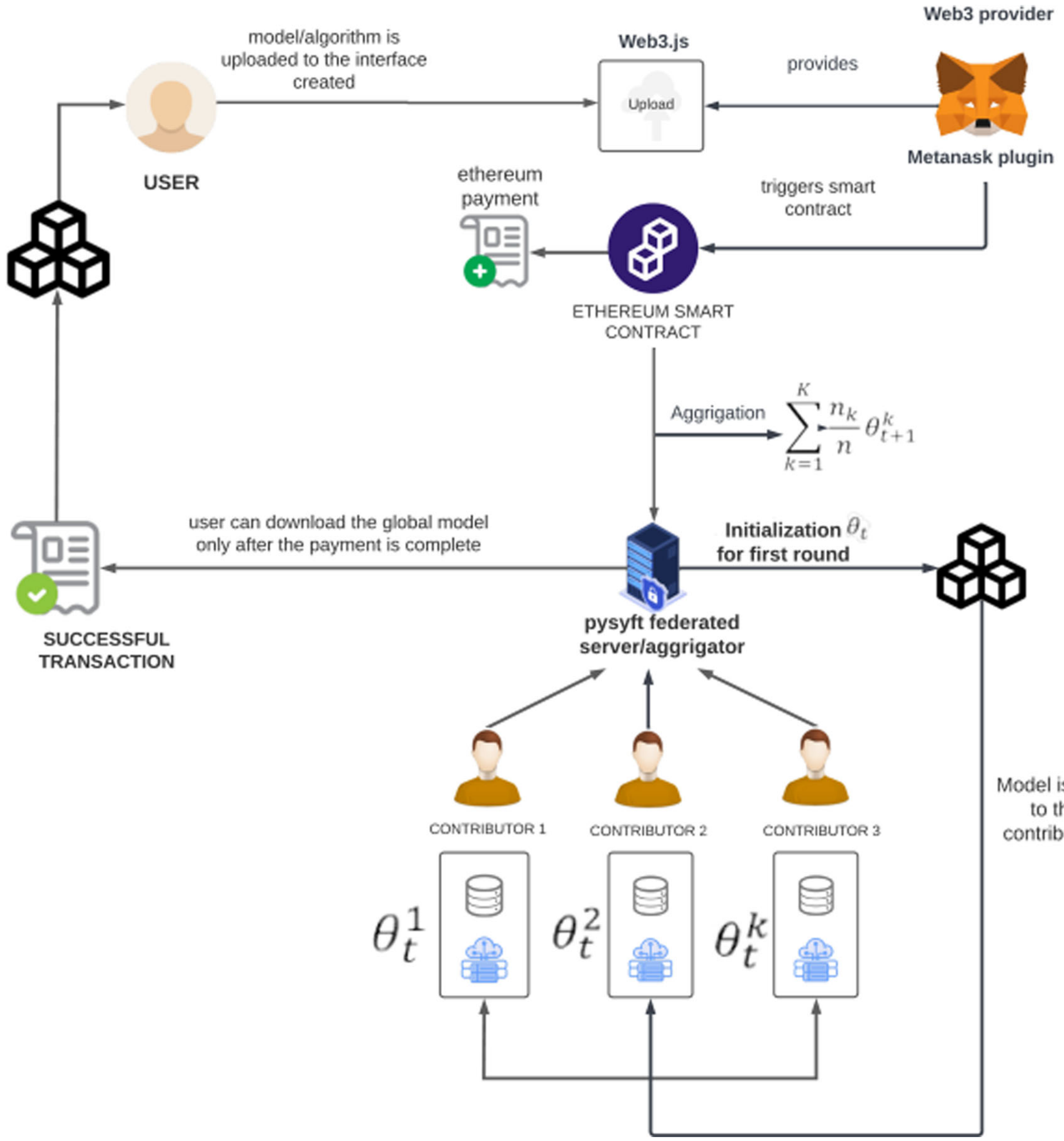
4.5 BLOCKFED using Dweb

The architecture of the proposed Dweb application, which is built using the react and flask web frameworks, is shown in Fig. 2. We need an indirect way to connect the web app because the current available technique does not allow web applications to be built with blockchain from the ground up. Metamask acts as a bridge between the web application and the blockchain, allowing users (data analysts) to interact with clients (hospitals) via the blockchain.

The webpage in our proposed system is built with React and includes the web3.js JavaScript library as well as other web3 dependencies, allowing the user/data analyst to interact with the Ethereum Blockchain created with the Ganache Tool. This is then linked to the Metamask wallet, allowing data transfer and other operations. θ represents the global model parameters, nk represents data size of contributors k, K represents number of contributors and t represents rounds of communication. We utilise updated model parameters after initialising global model parameters at the start of the communication.

4.6 Calculating data contribution

Each time Hospital 1 (X), Hospital 2 (Y) and Hospital 3 (Z) perform a round of training, they are given a number of tokens.



Web3 provider
model/algorithm is uploaded to the interface created
Web3.js
provides
Upload
USER
Metanask plugin
ethereum payment
triggers smart contract
ETHEREUM SMART CONTRACT
Aggrigation $\sum_{k=1}^{K} \frac{n_k}{n} \theta_{t+1}^{k}$
user can download the global model only after the payment is complete
Initialization θ_t for first round
SUCCESSFUL TRANSACTION
pysyft federated server/aggrigator
Model is sent to the contributors
CONTRIBUTOR 1
CONTRIBUTOR 2
CONTRIBUTOR 3
θ_t^1
θ_t^2
θ_t^k

Fig. 1 Architecture of the BLOCKFED

$$\text{Num tokens} = (\text{Test loss before} - \text{test loss after}) \times 1018$$

X, Y and Z have each registered their Ethereum addresses with the server, and the smart contract keeps track of their respective token counts.

Once data analyst/scientist downloads the model and releases her funds, X Y and Z may each withdraw the following amount of Ether from the escrow contract:

$$\text{Withdrawable funds} = \text{Analyst deposit} \times \text{Num tokens}/\text{Total tokens}$$

The major benefit of federated learning and Blockchain in our proposed system is that it prevents data leakage by keeping data on the device without the need for data transfer or pooling, and it allows us to collaboratively train on real-world data. While the Ethereum Blockchain is used to achieve a high level of security because the smart contract is immutable, to anonymize and increase trust between data analysts and contributors, and finally to reward contributors on the same blockchain network for their contribution,

5 Experimental analysis

5.1 Tools and framework

5.1.1 Truffle framework

Truffle suite also known as Truffle which is an development environment based on the Ethereum Blockchain.

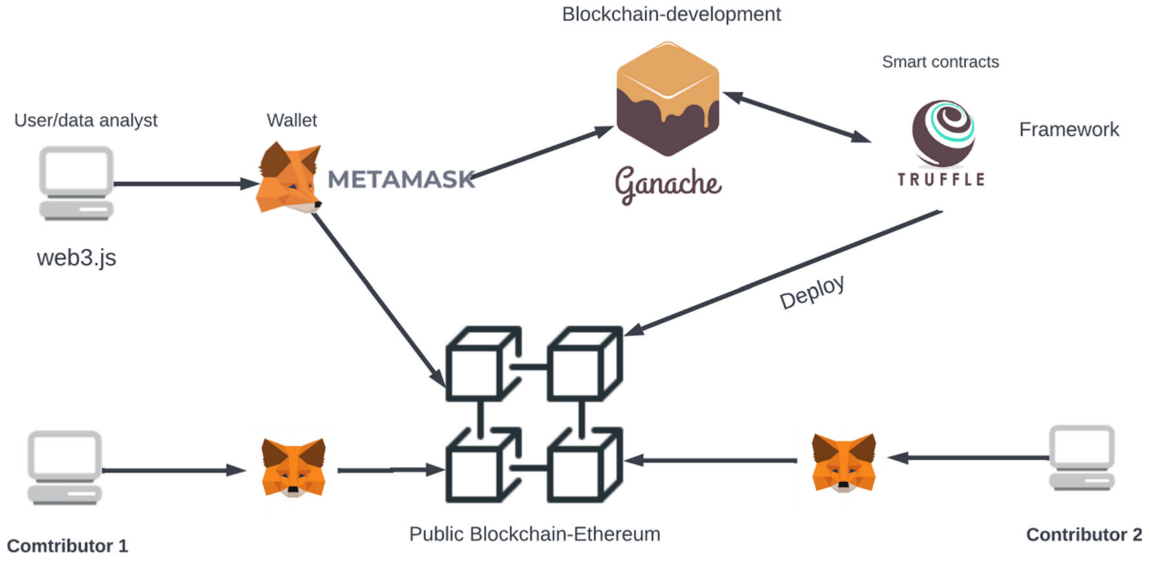


Fig. 2 Decentralized web (Dweb) architecture of the developed model

Truffle is a one-stop shop for DApp development (Distributed Applications): Creating a front-end for DApps, compiling contracts, deploying contracts, injecting contracts into a web app, and testing contracts.

5.1.2 Ganache

Ganache is a Truffle Suite application that lets users create their own Ethereum blockchain on their computer. We were given ten accounts, each containing 100 Ethers, as part of this tool, which greatly aided us in testing our smart contract and simulating different users who use our application.

5.1.3 MetaMask

MetaMask is a cryptocurrency wallet that can be installed as a browser extension on Google Chrome and Mozilla Firefox. Through the use of this tool, we can interact with the different networks of the blockchain from the client side via a web browser, this is done by creating a account in Metamask by using Ganache account private key, using this users perform Ethereum transactions.

5.2 COVID-19 dataset

We know that artificial intelligence (AI) had a respectable reputation in the field medicine and science. AI can assist medical professionals to improve the accuracy of detection of disease, potentially saving lives. The data availability and privacy issues that come with collecting real-world data are currently the most significant challenge faced by current methods. Without a large amount of relevant and useful data, AI will not be able to progress. We gathered data of COVID-19 CT (Yang et al. 2020) from three different hospitals of 34,000 slices for this research. This dataset includes unenhanced chest CT scans from over 1000 individuals who had COVID-19 infections that had been verified. The age range of the patients who received CT imaging was 6–89 years, with a mean age of 47.18, 16.32 (mean standard deviation) years. 60.9% of the population was male and 39.1% was female.

Figure 3 represents some 2D slices from the COVID-19 dataset's CT scans. In addition, Fig. 4 shows a selection of 3D samples.

Each row corresponds to a different patient sample. The first three columns are the 3-dimensional volume's, *XZ*, *XY* and *YX* planes. To simulate a real-world scenario, dataset images are distributed randomly in a non-IID manner, i.e., all CT scans are unique, and CT scans for different patients have a different number of slices.

5.3 Metrics for evaluation

In this work, in order to evaluate the performance of the proposed method, the evaluation measures such as the precision, sensitivity (recall), and specificity is used as shown in below equations.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{1}$$

$$\text{Recall or Sensitivity} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{2}$$

$$\text{Specificity} = \frac{\text{TN}}{\text{TN} + \text{FP}} \tag{3}$$

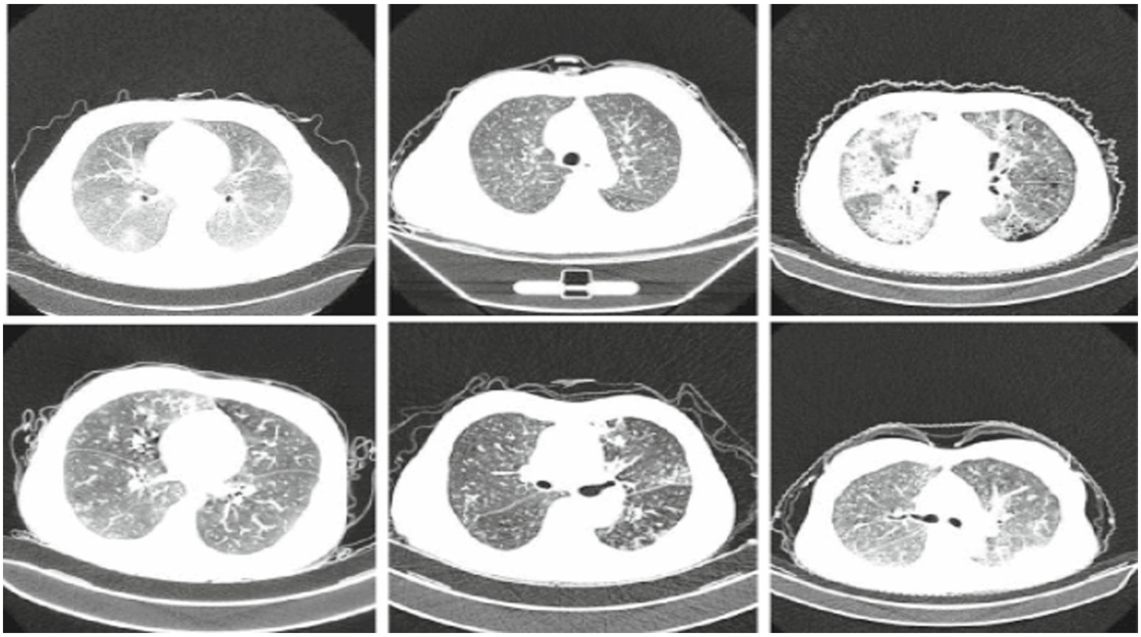


Fig. 3 Samples of CC-19 dataset containing 2D slices of CT scan

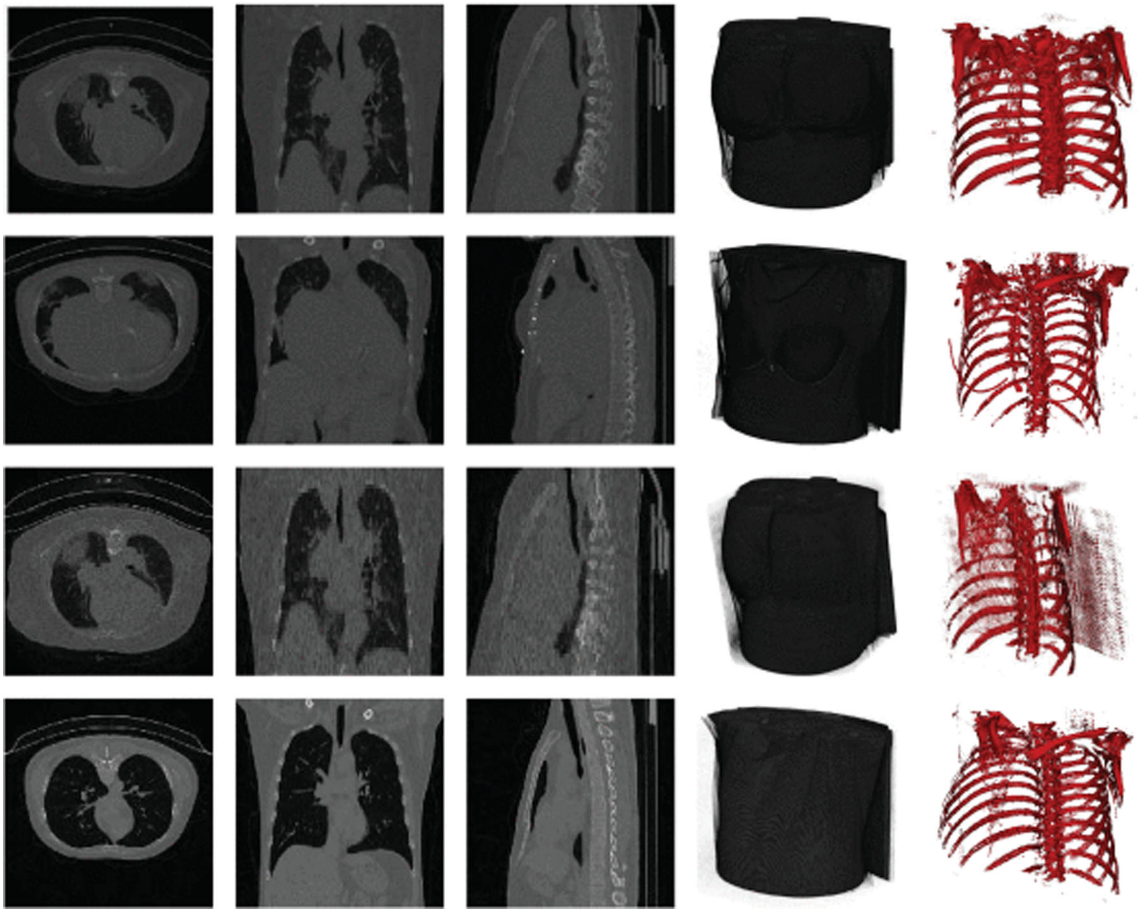


Fig. 4 A selection of samples from the COVID-19 dataset are shown in this diagram

The notations used in the equations are true positive (TP), true negative (TN), false negative (FN), and false positive (FP). Precision is the ratio of number of true positive assessment and number of classified positive assessments. Sensitivity is the ratio of number of true positive assessment and number of all positive assessments. Specificity is the ratio of true negative assessment and number of all negative assessments. Specificity and sensitivity are important factors to be consider in our proposed federated learning model; in our case they refer to capability of the models to distinguish between subjects with and without COVID-19 disease.

Table 1 Our model employs a three-layer Neural Network that was trained in a federated learning manner, combining multiple models from various contributors to achieve a precision of 0.83, a sensitivity of 0.837, and a specificity of 0.004, which is a very low percentage of negative when compared to other deep learning models.

5.4 Comparison using benchmark methods

We conducted experiments using various models such as VGG-16, AlexNet, Inception (V3) to compare the performance of the various models as shown in Table 1.

When compared to the recall and accuracy of other popular models, the accuracy of our BLOCKFED is unaffected and our model obtained similar results to that of VGGI, Alexnet and ResNet models as shown in Figs. 5 and 6. Do to the simulation of the real-world non-i.i.d data scenario by randomly distributing the collected data across contributors before training, the obtained result varies each time the test is run. We achieved a high level of data privacy and security throughout the process due to the incorporation of Blockchain and federated learning.

5.5 BLOCKFED security analysis

To simulate that the dataset was compiled from different contributors and evaluate the performance of federated learning i.e. (model transfer and aggregation), the dataset is distributed at random among three hospitals. In this system, three hospitals data is trained on federated learning manner. The individual evaluated accuracy is shown in Fig. 7a, classification performance of the trained model changes when the hospitals or contributors were increased.

Figure 7b shows the loss of individual contributors, as we can see in Fig. 7a, the samples that are compiled from multiple hospitals hence the result are not the same, hence the model's classification accuracy changes. Accuracy of the BLOCKFED model depends on the number of samples. The same applies for the loss. The pysyft aggregator then aggregates all the locally trained models gathered from the contributors after training process. The run time of different collaborators is shown in Fig. 7c.

We compare our BLOCKFED with another local model with the same dataset as shown in Figs. 6 and 7. The compared models are trained on the complete dataset in IID manner and our model learns from the contributors by aggregating the individual trained models into one global model. Figure 7a and b indicates that the accuracy increases when data contributors iteractions are increasing. However, using blockchain and federated learning on Dweb will not influence the precision but accomplish privacy.

Differences-privacy it is a principled approach which allows us to gain knowledge from the provided data while making sure these results do not allow individuals to distinguish or reidentify the data.

Trust The blockchain's decentralized trust mechanism (smart contract) allows automation according to a set of

Table 1 Comparing performance of well-known deep learning networks to our NN-based BLOCKFED

Feature extraction	Precision	Sensitivity or recall	Specificity
ResNet-50 (V2)	0.830	0.867	0.166
DenseNet-121	0.832	0.903	0.113
DenseNet-169	0.83	0.88	0.126
DenseNet-201	0.829	0.844	0.152
Resnet-152 (V2)	0.828	0.931	0.134
Inception	0.829	0.83	0.159
AlexNet	0.83	0.83	0.190
MobileNet	0.83	0.913	0.089
MobileNet (V2)	0.828	0.873	0.118
ResNet-50	0.833	0.85.9	0.249
VGGI16	0.82	0.829	0.157
VGG19	0.827	0.86	0.128
Xception(V1)	0.83	0.89	0.11
BLOCKFED using 3 NN	0.830	0.837	0.004

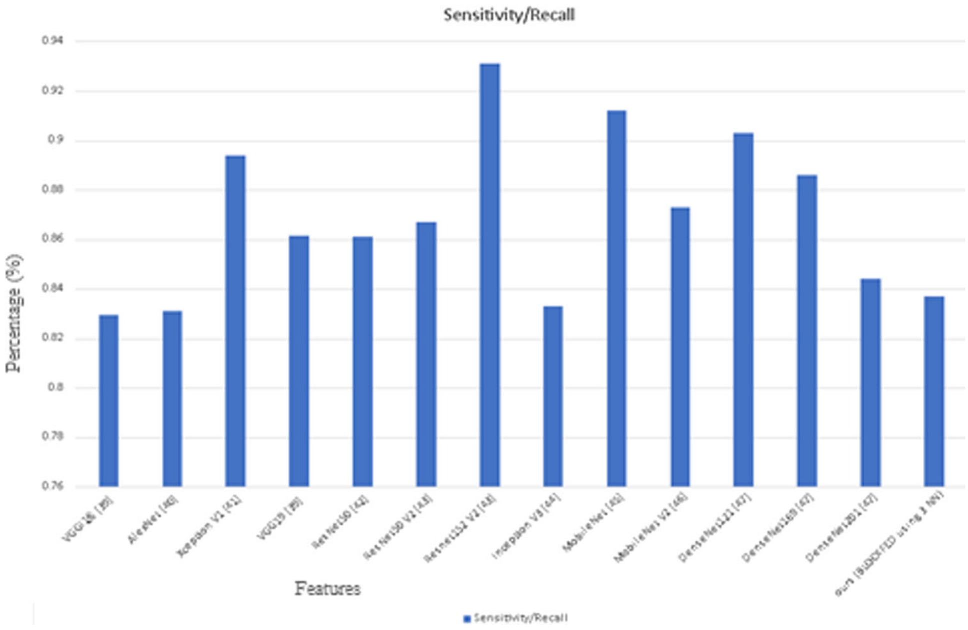


Fig. 5 Sensitivity/recall of the models

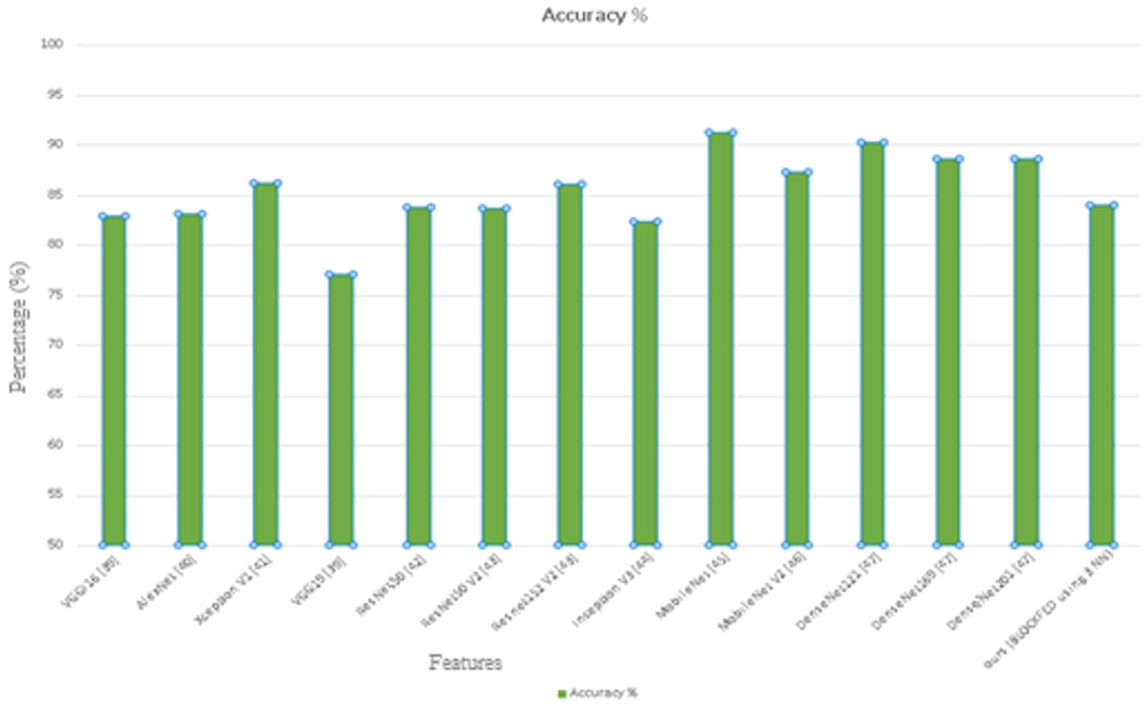


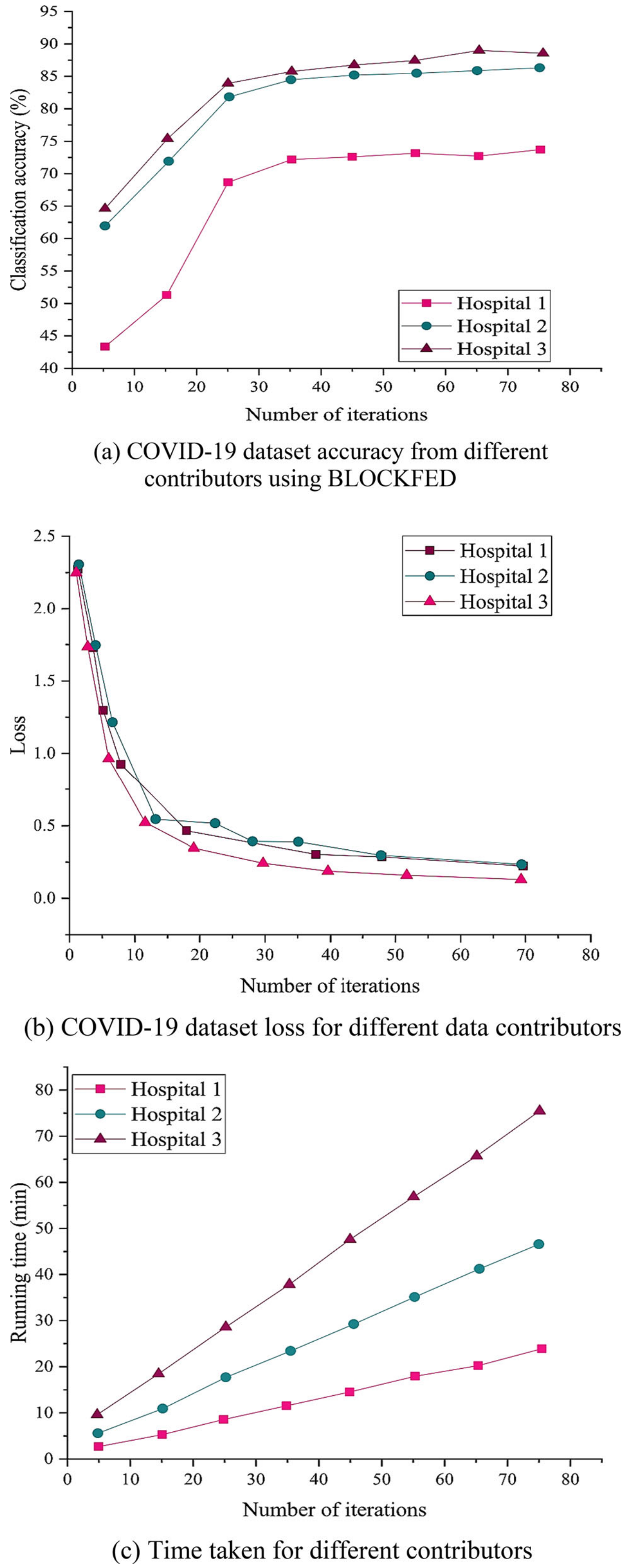
Fig. 6 Accuracy

rules, which improves data security. The blockchain technology assure that data is precise, reliable and can't be fiddled with.

Data security contributors have complete control over the information they provide. With the owner's signature, the owner has the authority to change the data only before compiling the smart contract.

5.6 Computational cost

The proposed system BLOCKFED is compared to a centralised network. The cumulative cost rises as the number of contributors or iterations rises due to the increased load of using blockchain and federated learning, as shown in Fig. 8a and b.



(a) COVID-19 dataset accuracy from different contributors using BLOCKFED

(b) COVID-19 dataset loss for different data contributors

(c) Time taken for different contributors

Fig. 7 **a** COVID-19 dataset accuracy from different contributors using BLOCKFED. **b** COVID-19 dataset loss for different data contributors. **c** Time taken for different contributors

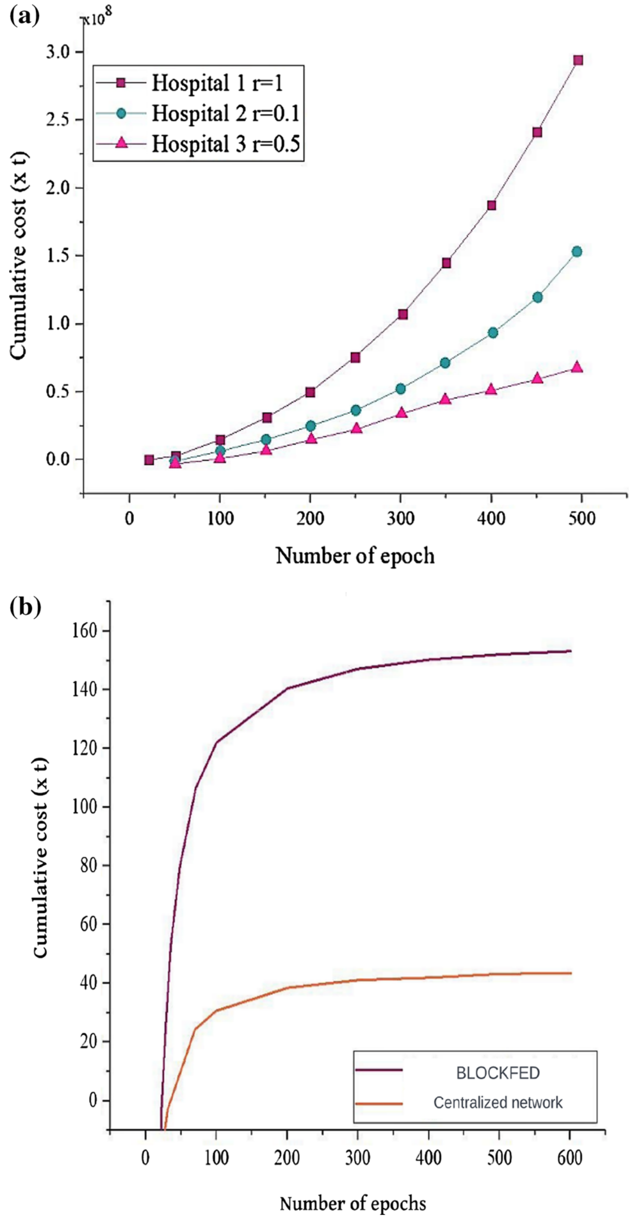


Fig. 8 Proposed BLOCKFED learning cost comparison

The centralized network, on the other hand, has a low cumulative cost by sacrificing security and privacy, as shown in Fig. 8b. By combining Ethereum blockchain and federated learning technique on a decentralized web platform, we were able to train a COVID-19 dataset using 3-layer neural network in a distributed way without sharing the user data and compromising on privacy, when aggregated using the FedAvg algorithm we achieved better precision to that of other models.

6 Conclusion

In this paper, we propose a novel framework that runs on top of Dweb and makes use of blockchain technology, in which multiple contributors work together to train COVID-19 data to achieve the global model and are rewarded with Ethereum tokens for their efforts. Multiple study was done on various deep learning models for training and testing the datasets. By utilising the Ethereum blockchain for decentralisation and the model transfer technique to avoid data collection, the proposed model is highly secure and protects contributors' privacy. The COVID-19 federation process increased each contributor's outcomes, with 0.88% for contributor A, 0.85% for contributor B, and 0.74% for contributor C. Using the FedAvg algorithm, we were also able to achieve a total accuracy of 0.82%. Currently, this effort depends on the efficacy of the protocol used to combine FL and Blockchain in order to provide end device privacy. However, by developing a trust model based on blockchain and having a relatively new consensus method for supporting FL nodes, this restriction of just relying on the protocol will be addressed. The project's future focus will be on finding ways and methods to upload multiple models at the same time to the DWeb. It may also include concentrating on methods for reducing the time required for the model to be trained and since our project does not focus on the contributors' work and progress, creating a frontend for them is something that can be done in the future.

Author contributions CUOK: Conceptualization, reviewing and editing, investigation. GS: Data curation, supervision. VB: Writing, original draft preparation, validation. AN: Visualization, methodology. SSB: Reviewing and editing.

Funding Not applicable.

Data availability The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

Code availability Not applicable.

Declarations

Conflict of interests We hereby declare that there are no conflicts of interest.

References

Benhar H, Idri A, Fernández-Alemán JL (2020) Data preprocessing for heart disease classification: a systematic literature review. Comput Methods Programs Biomed 195:105635

Bos JW, Lauter K, Naehrig M (2014) Private predictive analysis on encrypted medical data. J Biomed Inform 50:234–243

Chollet F (2017) Xception: deep learning with depthwise separable convolutions. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp 1251–1258

Choudhury O, Gkoulalas-Divanis A, Salonidis T, Sylla I, Park Y, Hsu G, Das A (2020) Anonymizing data for privacy-preserving federated learning. arXiv preprint https://arxiv.org/abs/:2002.09096

Domadiya N, Rao UP (2021) Improving healthcare services using source anonymous scheme with privacy preserving distributed healthcare data collection and mining. Computing 103(1):155–177

Dwork C (2011) Differential privacy. In: Encyclopedia of cryptography and security. Springer, Boston, pp 338–340

Gajendran S, Manjula D, Sugumaran V (2020) Character level and word level embedding with bidirectional LSTM—dynamic recurrent neural network for biomedical named entity recognition from literature. J Biomed Inform 112:103609. https://doi.org/10.1016/j.jbi.2020.103609

Gajendran S, Manjula D, Sugumaran V, Hema R (2023) Extraction of knowledge graph of Covid-19 through mining of unstructured biomedical corpora. Comput Biol Chem 102:107808. https://doi.org/10.1016/j.compbiolchem.2022.107808

Hamza R, Yan Z, Muhammad K, Bellavista P, Titouna F (2020) A privacy-preserving cryptosystem for IoT E-healthcare. Inf Sci 527:493–510

Hao M, Li H, Luo X, Xu G, Yang H, Liu S (2020) Efficient and privacy-enhanced federated learning for industrial artificial intelligence. IEEE Trans Ind Inform 16(10):6532–6542. https://doi.org/10.1109/TII.2019.2945367

Howard AG, Zhu M, Chen B, Kalenichenko B, Wang W, Weyand T, Andreetto M, Adam H (2017) Mobilenets: efficient convolutional neural networks for mobile vision applications. arXiv preprint https://arxiv.org/abs/1704.04861

Hu R, Guo Y, Li H, Pei Q, Gong Y (2020) Personalized federated learning with differential privacy. IEEE Internet Things J 7(10):9530–9539

Huang G, Liu Z, Van Der Maaten L, Weinberger KQ (2017) Densely connected convolutional networks. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp 4700–4708

Jamil F, Kim D (2021) An ensemble of a prediction and learning mechanism for improving accuracy of anomaly detection in network intrusion environments. Sustainability 13(18):10057

Jena MD et al (2021) Ensuring data privacy using machine learning for responsible data science. In: Intelligent data engineering and analytics. Springer, Singapore, pp 507–514

Krizhevsky A, Sutskever I, Hinton GE (2012) Imagenet classification with deep convolutional neural networks. In: Advances in neural information processing systems 25

Li Z, Liu J, Hao J, Wang H, Xian M (2020) CrowdSFL: a secure crowd computing framework based on blockchain and federated learning. Electronics 9(5):773

Li J, Meng Y, Ma L, Du S, Zhu H, Pei Q, Shen X (2021) A federated learning based privacy-preserving smart healthcare system. IEEE Trans Ind Inform 18(3):2021–2031

Li C, Li G, Varshney PK (2022) Decentralized federated learning via mutual knowledge transfer. IEEE Internet Things J 9(2):1136–1147. https://doi.org/10.1109/JIOT.2021.3078543

McMahan B, Ramage D (2017) Federated learning: collaborative machine learning without centralized training data. Google Res Blog, vol 3

Om Kumar CU, Sathia Bhama PRK (2019) Detecting and confronting flash attacks from IoT botnets. J Supercomput 75:8312–8338

Om Kumar CU, Sathia Bhama PRK (2021) Efficient ensemble to combat flash attacks. Comput Int. https://doi.org/10.1111/coin.12488

Om Kumar CU, Tejaswi K, Bhargavi P (2013) A distributed cloud-prevents attacks and preserves user privacy. In: 2013 15th International conference on advanced computing technologies (ICACT). IEEE

Om Kumar CU, Kishore S, Geetha A (2014) Debugging using MD5 process firewall. In: 2014 International conference on contemporary computing and informatics (IC3I). IEEE

Om Kumar CU et al (2022) Effective intrusion detection system for IoT using optimized capsule auto encoder model. Concurr Comput Pract Exp 34(13):e6918

Qi Y, Hossain MS, Nie J, Li X (2021) Privacy-preserving blockchain-based federated learning for traffic flow prediction. Future Gener Comput Syst 117:328–337

Qiang W, Liu R, Jin H (2021) Defending CNN against privacy leakage in edge computing via binary neural networks. Future Gener Comput Syst 125:460–470

Rahman SA, Tout H, Ould-Slimane H, Mourad A, Talhi C, Guizani M (2020) A survey on federated learning: the journey from centralized to distributed on-site learning and beyond. IEEE Internet Things J 8:5476–5497

Rawat R et al (2022) Malevolent information crawling mechanism for forming structured illegal organisations in hidden networks. Int J Cyber Warf Terror (IJCWT) 12(1):1–14

Salah K, Rehman MHU, Nizamuddin N, Al-Fuqaha A (2019) Blockchain for AI: review and open research challenges. IEEE Access 7:10127–10149

Shaham S, Ding M, Liu B, Dang S, Lin Z, Li J (2021) Privacy preserving location data publishing: a machine learning approach. IEEE Trans Knowl Data Eng 33(9):3270–3283. https://doi.org/10.1109/TKDE.2020.2964658

Shahbazi Z, Byun Y-C (2022) Blockchain-based event detection and trust verification using natural language processing and machine learning. IEEE Access 10:5790–5800. https://doi.org/10.1109/ACCESS.2020.3139586

Shayan M, Fung C, Yoon CJ, Beschastnikh I (2018) Biscotti: a ledger for private and secure peer-to-peer machine learning. arXiv preprint https://arxiv.org/abs/1811.09904

Simonyan K, Zisserman A (2014) Very deep convolutional networks for large-scale image recognition. arXiv preprint https://arxiv.org/abs/1409.1556

Srivastava GPG, Tripathi R, Gadekallu TR, Xiong NN (2021) PPSF: a privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. IEEE Trans Netw Sci Eng 8(3):2326–2341

Sun Z, Wang Y, Shu M, Liu R, Zhao H (2019) Differential privacy for data and model publishing of medical data. IEEE Access 7:152103–152114. https://doi.org/10.1109/ACCESS.2019.2947295

Szegedy C, Vanhoucke V, Ioffe S, Shlens J, Wojna Z (2016) Rethinking the inception architecture for computer vision. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp 2818–2826

Tanwar S, Bhatia Q, Patel P, Kumari A, Singh PK, Hong W-C (2020) Machine learning adoption in blockchain-based smart applications: the challenges, and a way forward. IEEE Access 8:474–488. https://doi.org/10.1109/ACCESS.2020.2961372

Toyoda K, Zhao J, Zhang ANS, Mathiopoulos PT (2020) Blockchain-enabled federated learning with mechanism design. IEEE Access 8:219744–219756

Wang S, Tuor T, Salonidis T et al (2019) Adaptive federated learning in resource constrained edge computing systems. IEEE J Sel Areas Commun 37(6):1205–1221

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 Trans Dependable Secure Computer 18:2438–2455

Yang X et al (2020) COVID-CT-dataset: a CT scan dataset about COVID-19. arXiv https://doi.org/10.48550/arXiv.2003.13865

Yin L, Feng J, Xun H, Sun Z, Cheng X (2021) A privacy-preserving federated learning for multiparty data sharing in social IoTs. IEEE Trans Netw Sci Eng 8(3):2706–2718. https://doi.org/10.1109/TNSE.2021.3074185

Zhao J, Chen Y, Zhang W (2019a) Differential privacy preservation in deep learning: challenges, opportunities and solutions. IEEE Access 7:48901–48911

Zhao Y, Yu Y, Li Y, Han G, Du X (2019b) Machine learning based privacy-preserving fair data trading in big data market. Inf Sci 478:449–460

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.