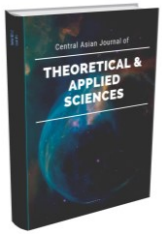

CENTRAL ASIAN JOURNAL OF THEORETICAL AND APPLIED SCIENCE

https://cajotas.centralasianstudies.org/index.php/CAJOTAS

Volume: 07 Issue: 01 | January 2026 ISSN: 2660-5317

Article

A Secure Blockchain-Federated Deep Learning Model for Privacy-Preserving COVID-19 Diagnosis

Zaid Mohammed Mortada[1], Ola Baqer Abdulhadi[2]

1. Department of Postgraduate Studies, University of Kufa, Najaf, Iraq
2. Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq

* Correspondence: zaidm.alhusaini@uokufa.edu.iq

Abstract: Traditional diagnostic techniques have been exposed as having several shortcomings regarding sensitivity, scalability, and data protection due to COVID-19's widespread impact. A centralized training strategy remains hampered by data-sharing limitations, privacy risks, and a lack of trust between medical institutions despite deep learning's potential for accurate disease identification in chest CT imaging. This study presents a federated deep learning framework based on blockchain for privacy-aware diagnosis of COVID-19 via CT scans. A shared model can be trained collaboratively and decentralized, without requiring patients' sensitive information to be exchanged. In addition to homomorphic encryption, model gradients are also encrypted during training to further maintain data confidentiality. To enhance the effectiveness of feature extraction and classification, capsule networks and extreme learning machines are combined in an ensemble learning strategy. In experiments across multiple feature extraction networks, the proposed framework achieves very high recall, reflecting its high ability to detect COVID-19 cases while maintaining reliable precision. Accordingly, the proposed framework offers a practical and reliable solution for large-scale collaborative medical image analysis in pandemic situations that integrates accuracy, privacy preservation, and security.

Received: 5 Nov. 2025
Revised: 25 Nov. 2025
Accepted: 20 Dec. 2025
Published: 26 Jan. 2026

Keywords: Blockchain Technology, COVID-19 Detection, Federated Learning, Privacy-Preserving, Medical Imaging.

1. Introduction

Over a year after the first cases of Coronavirus (COVID-19) were reported, the virus has spread massively and suddenly throughout the world. Thousands of people die from acute respiratory infections caused by Coronavirus [1]. COVID-19 detection remains a high-priority task because of its highly contagious nature. This disease can be diagnosed using swabs taken from the throat and nasopharynx. Sample errors and low viral loads can affect diagnosis accuracy, however. A contrast is the antigen test, which despite its speed has a poor sensitivity. It is also possible to detect infections on patients through radiological studies, such as computed tomography (CT) of the chest and X-rays. A deep

learning model can improve CTs and X-rays to detect different types of infections. To increase the accuracy of deep learning models, a small set of infected samples can be used to train and improve them. Despite the lack of training data, sensitivity and accuracy remain difficult to predict. This problem can be solved best through federated learning. A key component of federated learning is the collection of models from different sources and their collaboration over a decentralized network [2]. Even so, health care centers lack privacy-preserving strategies that prevent the sharing of such confidential data [3].

Author [4] proposed a distributed model to ensure privacy by allowing users to share gradients. The methodology, however, could be exploited by passive attackers [5]. The author developed a privacy-preserving gradient aggregation framework based on the federated learning global model [6]. A author of [7] proposed threshold secret sharing schemes as well as homomorphic encryption (HE). In terms of authenticity, the shared model cannot provide any assurance. Moreover, there is still a trust issue between different sources, resulting in poor data quality and model training. There have been several successful applications of deep learning in healthcare. However, there is still a distrust issue between different sources, which leads to poor data quality [8]. Using deep learning, Covid-19 has been diagnosed with promising results. Covid-19 uses radiological imaging as a primary diagnostic tool. The CT scan characteristics of Covid-19 patients (visual symptoms) are similar to those of those with early ground-glass opacity and late lung consolidation. Moreover, the lungs have a more peripheral distribution and a rounded shape. In patients with viral pneumonia, CT scans are similar to those taken by those with other infections or inflammatory diseases of the lungs. Consequently, radiologists distinguish viral pneumonias from Covid19 infections. Furthermore, advanced technologies could automate Covid19 detection without compromising user privacy or security.

It may not represent the whole population to segment the health information by hospital systems. In biomedicine, federated learning has shown to be a promising strategy. The limitations of limited training data and restricted data sharing can be overcome with federated learning [9]. With multi-system federated learning, patient data is shared to ensure more accurate results. Any party who has been granted permission to view and audit blockchain records can take advantage of its transparency. Any blockchain record falls under this category [10]. The healthcare sector is showing a lot of interest in blockchain technology, along with cryptocurrencies. The Bitcoin digital currency uses blockchains to store transaction information. Decentralization, transparency, integrity, and traceability are all advantages of blockchain technology, which was first used in 2008. The blockchain technology's supporters contend that it provides a secure means of managing data files by using an immutable, decentralized ledger. These cutting-edge technologies can be applied to a significant number of applications, including health care. Among the top ten technologies recommended by the European Parliamentary Research Service for combatting Covid-19 problems is blockchain. Blockchain technology could enable secure, imputable monitoring of disease outbreaks to combat COVID-19.

2. Related Work

COVID-19 and other chest diseases are classified using machine learning, deep learning, and fuzzy logic. In his study [11], Author evaluated all of the latest medical imaging analytics techniques, including prediction, electronic therapy, stage classification, and virtual monitoring. SVMs, DTs, KNNs, and ANNs are supervised learning classifiers used in medical imaging to detect chest diseases. As well as being vital for worldwide data transfers, the BCT is also crucial for accessing medical records through a dispersed network of blocks. According to the author, modern medical images are transmitted via a technology that has recently become popular in the medical industry [11]. Author [12]

proposed a decentralized FL architecture called Block FL, which stands for blockchain federated learning by federating its reach, avoided single points of failure. Based on the results of local training, devices can access public networks [13]. Gradient recording and reward can be scaled by establishing a systematic library of off-chain recordings.

In a recent study [14], automated FL was shown to improve local ML model quality and productivity using neural architecture search (NAS) and federated neural architecture search (FedNAS). When using local ML models in a federated environment, the default configuration did not perform well for clients without unique IDs (also known as non-IIDs). An FL chain is an openly verified, centralized, and highly trustworthy FL ecosystem, presented in [15]. Through the use of BCT, FL chains can be implemented without a central FL coordinator. As a result of the author, a FL approach was proposed for patients with COVID-19 [16]. CXR photographs of abnormal patients can be used to train neural networks that can be used to recommend an electronic therapy based on the recommendations of the neural network. A big data set cannot be used with the predictor developed because of its limitations. Medical imaging is made easier with PriMIA, a free and open-source software framework [17]. Based on FL, it categorizes pediatric radiology from a variety of sources. As part of PriMIA, DCNN uses a trained pediatric CXR image collection to classify cardiac illness stages. DCNN is trained using a gradient-based model to detect chest infections at an early stage. An assessment of the quality of the research was conducted according to the PRISMA guidelines [18]. A PRISMA-compliant literature review ensures high levels of transparency and rigor. The systematic review process contributes to systematic review process because it reduces bias, improves reporting quality, and contributes to medical research. Artificial intelligence, deep learning, transfer learning, and federated learning were included in the search, as were Coronavirus, COVID-19, and artificial intelligence, deep learning, and transfer learning. COVID-19 has clinical, epidemiological, and basic science components that have been overlooked. From different publishers and preprints, we obtained a total of 11,700 papers about how DL and FL are applied to COVID-19.

By combining federated learning with blockchain technology, trustable AI systems can be built. The Author [19] proposes federated artificial intelligence based on blockchains and Proof-of-Work consensus. According to the authors [20], a blockchain-based peer-to-peer machine learning process could operate completely decentralized. Using novel mining methods and blockchain-based federated learning processes, we have developed a new framework for secure COVID-19 data analytics. An algorithm for global aggregation that uses blockchain technology can protect against malicious devices, according to the author [21]. Multi-edge servers implement a fault-tolerant consensus protocol that prevents malicious servers from manipulating model data. With drones and blockchains, federated learning enables secure accumulation through two-stage authentication, as well as differential privacy protections [22].

3. Proposed Methodology

The system model will be analyzed after an overview of deep learning, federated learning, homomorphic encryption, and blockchain-based federated learning.

3.1 Deep Learning

Figure 1 shows how the deep learning models are trained using feed forward and back propagation algorithms. X and w represent the input and parameter vectors, respectively, in the feed forward function defined as $(x; w) = y^{-}$. Each instance of $(x_i; y_i)$ uses $D = (x_i; y_i); i \in I$ as its training dataset. A loss function is represented by l, while a training dataset is represented by $L(D; w) = \frac{1}{|D|}\sum_{(x_i; y_i)\in S} l\left(y_i, f(X_i, W)\right)$. Backpropagation was carried out using stochastic gradient descent (SGD).

$$W^{t+1} \leftarrow W^t - \eta^{\Delta} w^L(D^t, W^t) \quad (1)$$

In the case of hyperparameters, η is the learning rate, and η is the iteration vector. In Equation 1, the standard training procedure for one hospital or user is shown using D^tas the training dataset.

3.2 Federated Learning

Developing a shared model for healthcare could be easier with federated learning. Additionally, federated learning allows hospitals to collect data from a variety of sources without compromising privacy. By federating learning, resources (such as memory and power) are reduced, and training quality is improved. Through federated learning, the model is learned collaboratively and shared among machines. $u \in U$ users have private datasets $D_u \subseteq D$. In the following equation, $D^t = U_{u\epsilon U} D_u^t$ with SGD is represented as a mini-batch dataset

$$w^{t+1} \leftarrow w^t - \eta \frac{\sum_{u\epsilon u} \nabla w^L(D_u^t, w^t)}{|U|} \quad (2)$$

The local model is shared by each user to the blockchain distributed ledger so that it can be trained to be shared globally. Updates to the global model are uploaded by hospitals and users.

$$F_i(w) = \frac{1}{|D_i|} \sum_{j \in D_i} F_i(w, a_i, b_i) \quad (3)$$

The weights of data must be minimized using a global loss function $F_i(w, a_i, b_i)$ when there is more than one device or hospital with dataset D [23]. Calculate the difference between $F_i(w, a_i, b_i)$ and its estimated value based on the global model function of $F(w)$

$$F(w) = \frac{1}{|M_I|} \sum_{i \in I} u_i . F_i(w) = \frac{1}{|M_I|} \sum_{i \in I} \sum_{j \in D_i} u_i . \frac{f_i(w, a_i, b_i)}{|D_i|} \quad (4)$$

The number of individual hospitals is represented by i and (a_i, b_i) respectively in a hospital dataset model [28]. We aim to improve the accuracy of the model by minimizing the loss function iteratively. Consider the loss function as follows:

$$Q(w, t) = \begin{matrix} \arg minF(w) \\ i \in I, t \leq T \end{matrix} \quad (5)$$

$$\Pr(w_i \in R_d) \leq \exp(\in) Pr(w_i' \in \mathbb{R}_d) \quad (6)$$

$$\sum_{i=1}^{t} \Delta t(i) \leq \min(T_1, T_2, .., T_n) \quad (7)$$

In this example, $\Pr(w_i \in R_d) \leq \exp(\in) Pr(w_i' \in \mathbb{R}_d)$ stands for the confidentiality of the users [24] and $(T_1, T_2, .., T_n)$ $\Delta t(i)$,. The time taken for each iteration.

3.3 Cryptography Based on Homomorphism

Using cryptographic homomorphism, encrypted data (cipher text) can be calculated without decryption. Decryption results in the new encrypted data matching the unencrypted data's result. As a solution, we utilized the BGV [25] encryption scheme, which takes a large amount of noise as input and outputs unencrypted data. Further, there is a key-switching procedure that text-encrypts data. For readers, you can find details about the encryption scheme here [26]. The gradients [27] were therefore encrypted using homomorphic encryption for sharing in the blockchain network. Previously, the gradients were encrypted and shared to a centralized server [28]. Blockchain networks that are distributed are not considered. Blockchain databases solve a cost-effective problem. In this way, we encrypt the local model and train it to the global model using homomorphic encryption.

Before tensor encryption, some mini-batch datasets have matrices Z with a size of $S * T$, and private key matrices with a size of $S * S$

$$\begin{bmatrix} \emptyset_{11}\emptyset_{12}\cdots\emptyset_{1S} \\ \emptyset_{21}\emptyset_{22}\cdots\emptyset_{2S} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ \emptyset_{S1}\emptyset_{S2}\cdots\emptyset_{SS} \end{bmatrix} \tag{8}$$

Mini-batch datasets can only be shared by users/participants

$$\begin{bmatrix} \mathbb{Z}_{(1)} \\ \mathbb{Z}_{(2)} \\ \vdots \\ \mathbb{Z}_{(S)} \end{bmatrix} \begin{bmatrix} \emptyset_{11}\emptyset_{12}\cdots\emptyset_{1S} \\ \emptyset_{21}\emptyset_{22}\cdots\emptyset_{2S} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ \emptyset_{S1}\emptyset_{S2}\cdots\emptyset_{SS} \end{bmatrix} \otimes \begin{bmatrix} Z_{(1)} \\ Z_{(2)} \\ \vdots \\ Z_{(N)} \end{bmatrix} \tag{9}$$

A blockchain's vector data is shown by $Z(i)$. An operator displays the product of two cipher texts.

$$\mathbb{Z}_{(1)} = \emptyset_{i1} Z_{(1)} + \emptyset_{i2} Z_{(2)} + \cdots + \emptyset_{iN} Z_{(S)} \tag{10}$$

Thus, the linear transformation maintains low rank functionality. Homomorphic encryption with a private key can be seen in functions $\emptyset_{ij} \in [0;\ 1)$, and $\sum_{j=1} \psi_{i,j} = 1$.

3.4 Blockchain-Enabled Federated Learning

Gathering data from multiple sources is crucial to training the best AI model for industry 4.0 without compromising user privacy. The global AI model is therefore updated using federated learning and blockchain technology. Data models from local and global sources can be aggregated using blockchain technology.

A smart contract updates models and uploads weights. Decentralization and enhanced security are achieved through the integration of blockchain technology and federated learning in this proposed architecture. Furthermore, decentralization makes the model more accurate and prevents poisoning attacks. Federated learning still has some issues, including insufficient incentives and poisoning attacks. Thus, some researchers develop the blockchain from a federated learning perspective [29], [30]. Similarly, design a technique to protect privacy. In previous studies, the encryption technique was not included with the gradient sharing of blockchain models, which created a major problem. Gradient aggregation using directed acyclic graphs and Proof-of-Work consensus algorithms is presented in the paper. Moreover, the work is entirely decentralized, and the privacy of the users is not compromised in any way.

3.4.1 Data Normalization

Using the technique described in [30], the proposed study normalizes the data. Since the data is heterogeneous, the proposed federated learning models require strong normalization methods. A CT scan image is normalized by adjusting both its signal and its spatial characteristics. Medical practices commonly use two types of windows in CT scans because of the Hounsfield units (HU). Using this window size, equation 1 calculates the normalized value.

$$Onormalized = \frac{o - WL}{WW} \tag{11}$$

An image with a normalized intensity is called Normalized, and an image with an original intensity is called O. An experiment has been conducted using [0.01, 0.5] as the lower bound window size.

3.4.2 Spatial Normalization Technique

Using CT scan images of various dimensions and resolutions, spatial normalization is adopted. CT scan images are always 332 x 332 x 512 mm3 in resolution according to CT scan protocol [30]. A standardization process involves converting all datasets and images into federated learning-compatible formats. As a result, it improves learning and performance.

3.4.3 Model Training Using Ensemble Capsules

A strong feature extraction layer and classification mechanism have made deep learning popular over the past few years. To classify images, convolutional neural networks (CNNs) have become increasingly popular. In feature-space CNNs, spatial relationships between features are not taken into account, which can increase computation complexity and affect the performance of the classifier. Through the combination of capsule networks and extreme learning machines (ELMs), it improves classification accuracy and diagnosis.

The COVID-19 is better predicted using ELM instead of traditional dense classification layers based on a capsule network that extracts strong feature maps.

3.4.4 Capsule Networks

As a solution, a capsule network with 50 layers (convolutional layer (1), hidden layer (2), primary cap (3), and direct cap (4)) was used to overcome the limitation. Capsule networks use normalized input images as inputs. A two-phase process is involved.

- Entity's likelihood of existing.
- Parameters used to instantiate entities.

Equation (12) encodes the spatial relationship between low-level and high-level features by means of input vectors "s" and weight matrices "W" and "U".

$$B(i.j) = W - (i,j)U(i,j) * S_j \tag{12}$$

Using equation (13), we can calculate the capsule "D" based on the sum of weighted input vectors

$$S(j) = \sum_j B(i,j) * D(j) \tag{13}$$

In equation (14) nonlinearity is accounted for by squashing.

$$B(i,j) = W_{i,j}U(i,j) * S_j \tag{14}$$

As the test results are analyzed, it is gradually adjusted to ensure that low-level capsules are distributed evenly between high-level capsules.

3.5 Federated Learning for Global Training

The following sections provide detailed information on how multiple hospitals can share data decentralized. The proposed model allows hospitals to share their models without compromising privacy, and the models are aggregated using federated learning. Hospitals are represented by H, and datasets are represented by d. In a federated model, ensemble learning is viewed as a global model M where weights W are distributed randomly among hospitals.

Using blockchain technology, a collaborative framework can train and share knowledge [31]. Within the hospital's federated learning model, local and global weights are integrated [32]. As a starting point, CT scan data from multiple sources are gathered into a local model and normalized accordingly. In an ensemble capsule network, the data and images are normalized and segmented to identify a COVID-19 suspect. Blockchain networks are used to distribute local model weights for global models.

The number of hospitals is represented by d, which represents the total dataset including both training and testing datasets.

$$D_i^{train} = \left\{\left(A_{i,j}^{train}, B_{i,j}^{train}\right)\right\} Wherej = 1toN - train\ data \tag{15}$$

As shown in equation 16, testing data is also represented as follows:

$$D_{i,j}^{test} = \left\{\left(A_{i,j}^{train}, B_{i,j}^{train}\right)\right\} Wherej = 1toN - train\ data \tag{16}$$

A global model is therefore trained using the dataset presented in equation 10.

$$D(i) = D_i^{train}\ UD_i^{test} \tag{17}$$

A heterogeneous group of hospitals collects the $D(i)$ data, so the distribution of data remains unequal. ELM weights W are distributed among hospitals in every round of

communication. In the blockchain network, hospitals create local models based on weights obtained and stored. Each round, new weights are loaded into the blockchain network. Equation (18) determines how weights should be updated mathematically.

$$\eta = w^i - w^l \tag{18}$$

Suppose w^i and w^1 are global and local weights, respectively. As a last step, the ELM-based deep learning algorithm is developed by aggregating all the local models in the blockchain.

3.6 Blockchain-Based Data Retrieval Process

In a block chain network, each hospital provides the data (local models) as a transaction [33]. Data retrieval from the nodes is based on two parameters, namely distance (d) and hospital identification (ID). Hospitals are assigned unique IDs based on their distance from each other. Blockchains maintain log tables to store unique hospital IDs. Hospitals in the neighbourhood are identified by their unique IDs, which are used to retrieve the data.

A hospital is represented mathematically by an X, which represents the different communities in which it is located. Equation (19) gives the expression for neighbourhood distance between nodes

$$d\big(A(i), A(j)\big) = \sum\nolimits_{p,1,\epsilon} \{A(i)UA(j) - A(i)nA(j)\}$$
$$Attributes\ of\ the\ Nodes / \sum\nolimits_{p,1,\epsilon} \{A(i)UA(j)\} * \tag{19}$$
$$Attributes\ of\ Nodes * \log\big(A(i), A(j)\big)$$

Hospitals $A_{(i)}$ and $A_{(j)}$are the unique IDs of i^{th} and j^{th} two neighbouring hospitals

The sharing of data between requester and source hospitals requires a high level of security. A hospital can only share learned models with requesters instead of sharing the entire data set. Federated data is used for the consensus algorithm, which allows hospitals to communicate with one another. Blockchain nodes store the data of providers and requesters.

4. Result and Discussion

The table presents a comparison of precision across various feature extraction networks. Results show that AlexNet and ResNet50 deliver the highest precision score of 0.833, indicating a slightly stronger ability to correctly identify positive samples with fewer false alarms. DenseNet121 (0.832) and DenseNet169 (0.831) also perform well, benefiting from their dense feature propagation and efficient information reuse. In contrast, traditional architectures such as VGG16 (0.8269) and VGG19 (0.827) exhibit marginally lower precision, suggesting reduced discriminative power compared with deeper or more refined models. Lightweight networks like MobileNet and MobileNetV2 maintain consistent precision values in the range of 0.828–0.830, highlighting their effectiveness in achieving reliable performance with lower computational cost. Overall, the proposed model attains a precision of 0.83, closely matching the performance of leading architectures and demonstrating its capability to provide dependable and robust predictions.

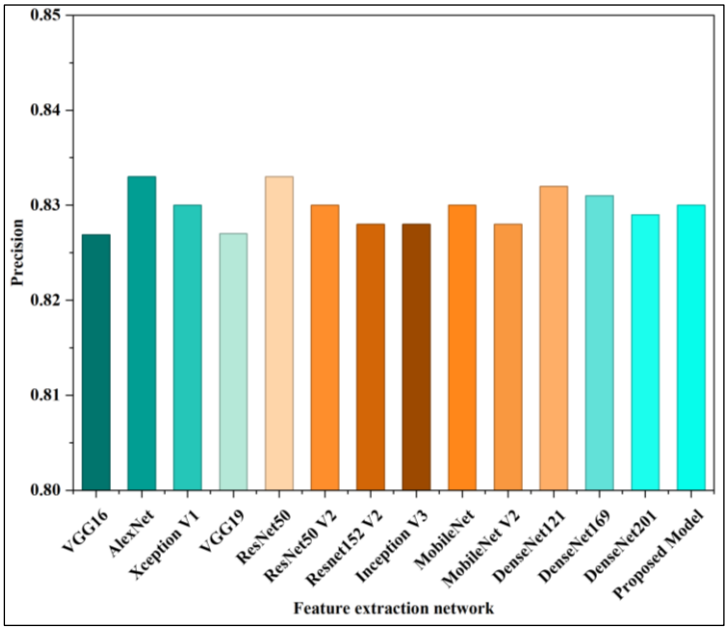

Figure 1: Precision Comparison of Different Feature Extraction Networks.

Figure 2 summarizes the recall performance of different feature extraction networks, highlighting their ability to correctly identify positive cases. Among the conventional models, MobileNet (0.912) and DenseNet121 (0.903) achieve the highest recall, demonstrating strong sensitivity in capturing relevant features. Xception V1 (0.894) and DenseNet169 (0.886) also show robust performance, indicating effective representation learning. In contrast, ResNet50 (0.771) records the lowest recall, suggesting a higher rate of missed detections. Classical architectures such as VGG16 (0.8294) and VGG19 (0.8616) deliver moderate recall values, reflecting stable but less optimized sensitivity. Notably, the proposed model achieves a recall of 0.987, significantly outperforming all baseline networks, which confirms its superior capability to detect positive instances with minimal false negatives.

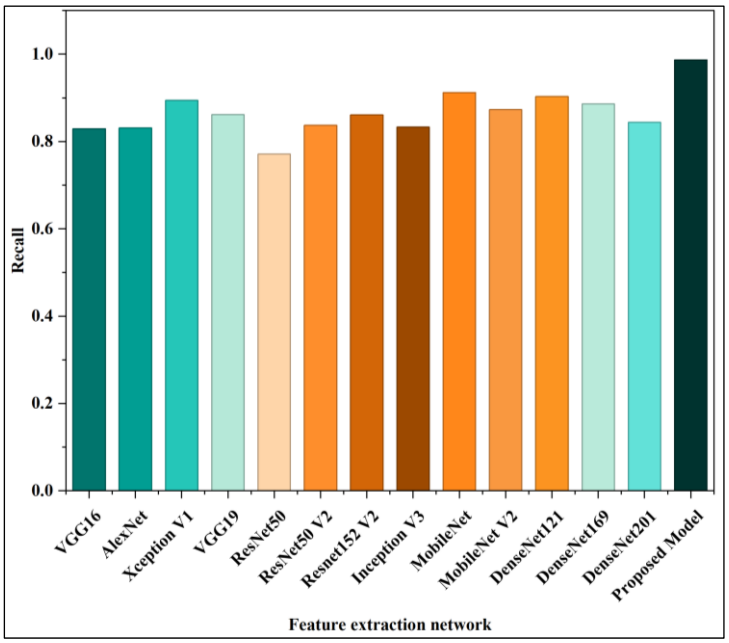

Figure 2: Recall Comparison of Different Feature Extraction Networks.

Figure 3 compares the specificity performance of different feature extraction networks, reflecting their ability to correctly identify negative cases. Among the baseline models, ResNet50 achieves the highest specificity value of 0.249, indicating a stronger capability to reduce false positives compared with other networks. AlexNet (0.191) and ResNet50 V2 (0.166) also show relatively better specificity, while architectures such as VGG16 (0.1561), Inception V3 (0.159), and DenseNet201 (0.152) demonstrate moderate performance. Lightweight models, particularly MobileNet (0.089), exhibit lower specificity, suggesting a higher tendency to misclassify negative samples. Notably, the proposed model records a very low specificity of 0.004, which indicates that it is highly biased toward identifying positive cases. This behavior aligns with its exceptionally high recall, emphasizing sensitivity over specificity and making it more suitable for applications where minimizing missed detections is prioritized over false alarms.

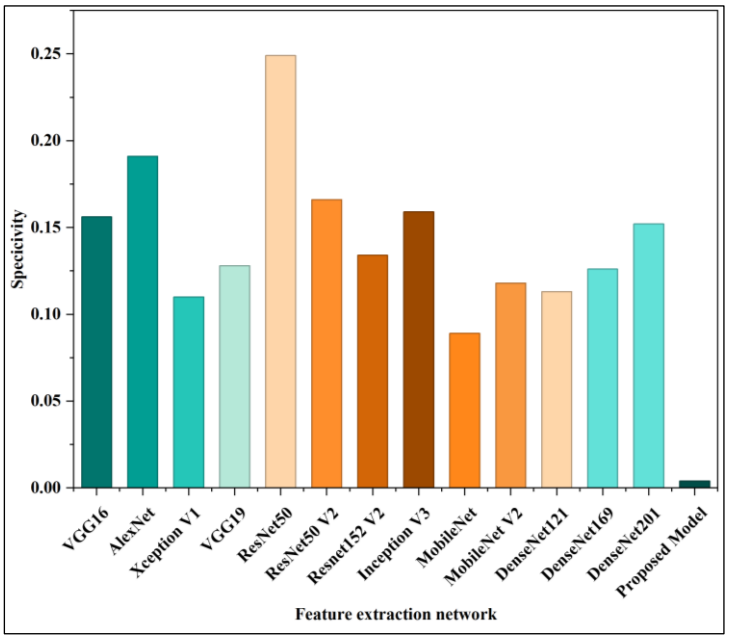

Figure 3: Networks for Feature Extraction: Comparison of Specificity.

According to Figure 4, different feature extraction networks perform differently in terms of accuracy. VGG16 achieves the highest accuracy of 0.8281, indicating strong overall classification capability among the evaluated models. ResNet50 (0.6735) also performs relatively well, benefiting from residual learning that supports stable feature representation. Most other deep architectures, including AlexNet, Inception V3, and ResNet50 V2, attain moderate accuracy values around 0.59–0.60, reflecting balanced but less optimal performance. Lightweight and densely connected models such as MobileNet, DenseNet121, and DenseNet169 show comparatively lower accuracy, suggesting limitations in capturing discriminative global features for this task. The proposed model records an accuracy of 0.4628, which is lower than the baseline networks; however, this outcome is consistent with its design emphasis on maximizing recall, indicating a deliberate trade-off where sensitivity is prioritized over overall accuracy.

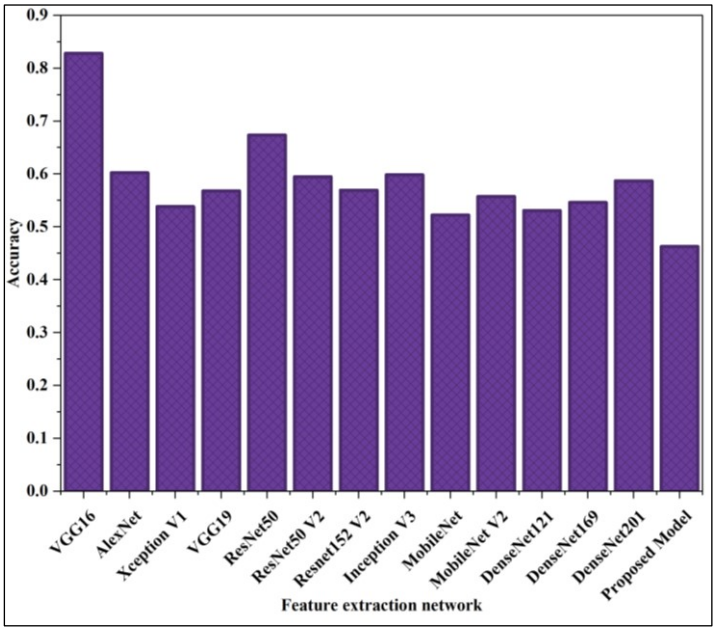

Figure 4: Accuracy Comparison of Different Feature Extraction Networks.

5. Conclusion

In this study, a blockchain-federated deep learning framework was developed to detect COVID-19 from chest CT images. A multi-hospital diagnostic model can be jointly developed by integrating federated learning, blockchain infrastructure, and homomorphic encryption. A capsule-based ensemble architecture improves feature extraction and classification by capturing spatial relationships within medical images effectively. Based on experimental results, the proposed model achieves notably higher recall than conventional deep learning methods, which emphasizes its ability to reduce missed detections of COVID-19. Despite a trade-off between sensitivity and specificity, this approach aligns well with clinical screening requirements that require reliable identification early in the process. The proposed framework offers a scalable, privacy-preserving, and trustworthy framework for collaborative medical diagnosis, as well as providing a solid foundation for future intelligent healthcare systems that depend on secure inter institutional cooperation.

REFERENCES

1. S. Verma *et al.*, "An automated face mask detection system using transfer learning based neural network to preventing viral infection," *Expert Systems*, vol. 41, no. 3, p. e13507, Mar. 2024, doi: 10.1111/exsy.13507.
2. P. Rani, J. Kumar, S. Singh, P. Dey, and L. H. Jasim, "Decoding the Aspects of Intelligent Traffic Management," in *Artificial Intelligence Technologies for Smart and Sustainable Urban Transportation*, 1st ed., P. Raj, S. Yadav, M. K. Mishra, S. P. Yadav, and V. H. C. Albuquerque, Eds., Wiley, 2025, pp. 287–300. doi: 10.1002/9781394346776.ch17.
3. P. Rani, R. Kumar, A. Singh, J. Jagtap, and M. Almusawi, "Testifying the Criticality of the Internet of Things (IoT), 5G and AI: A Perfect Combination for Battery Management," in *Artificial Intelligence Technologies for Smart and Sustainable Urban Transportation*, 1st ed., P. Raj, S. Yadav, M. K. Mishra, S. P. Yadav, and V. H. C. Albuquerque, Eds., Wiley, 2025, pp. 71–87. doi: 10.1002/9781394346776.ch5.
4. R. Shokri and V. Shmatikov, "Privacy-Preserving Deep Learning," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, Denver Colorado USA: ACM, Oct. 2015, pp. 1310–1321. doi: 10.1145/2810103.2813687.

5. M. Majeed, M. Ashfaq, P. Rani, A. Hussain, and M. Azam Zia, "AI-Driven Anomaly Detection and Traffic Management in Software-Defined IoT Networks for Smart Agriculture," *Trans Emerging Tel Tech*, vol. 36, no. 12, p. e70301, Dec. 2025, doi: 10.1002/ett.70301.
6. K. Bonawitz *et al.*, "Practical Secure Aggregation for Privacy-Preserving Machine Learning," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, Dallas Texas USA: ACM, Oct. 2017, pp. 1175–1191. doi: 10.1145/3133956.3133982.
7. X. Zhang, S. Ji, H. Wang, and T. Wang, "Private, Yet Practical, Multiparty Deep Learning," in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, Atlanta, GA, USA: IEEE, Jun. 2017, pp. 1442–1452. doi: 10.1109/ICDCS.2017.215.
8. S. K. Lo *et al.*, "Blockchain-based Trustworthy Federated Learning Architecture," 2021, *arXiv*. doi: 10.48550/ARXIV.2108.06912.
9. X. Sun, A. Bommert, F. Pfisterer, J. Rähenfürher, M. Lang, and B. Bischl, "High Dimensional Restrictive Federated Model Selection with Multi-objective Bayesian Optimization over Shifted Distributions," in *Intelligent Systems and Applications*, vol. 1037, Y. Bi, R. Bhatia, and S. Kapoor, Eds., in Advances in Intelligent Systems and Computing, vol. 1037. , Cham: Springer International Publishing, 2020, pp. 629–647. doi: 10.1007/978-3-030-29516-5_48.
10. M. Ali, H. Karimipour, and M. Tariq, "Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges," *Computers & Security*, vol. 108, p. 102355, Sep. 2021, doi: 10.1016/j.cose.2021.102355.
11. S. M. and V. K. Chattu, "A Review of Artificial Intelligence, Big Data, and Blockchain Technology Applications in Medicine and Global Health," *BDCC*, vol. 5, no. 3, p. 41, Sep. 2021, doi: 10.3390/bdcc5030041.
12. R. Rehyadd and P. Rani, "Sign-Based Encryption-Enabled Reliable Data Communication for Mobile Ad Hoc Networks," in *2025 International Conference on Next Generation of Green Information and Emerging Technologies (GIET)*, Gunupur, India: IEEE, Aug. 2025, pp. 1–7. doi: 10.1109/GIET65294.2025.11234764.
13. I. Martinez, S. Francis, and A. S. Hafid, "Record and Reward Federated Learning Contributions with Blockchain," in *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, Guilin, China: IEEE, Oct. 2019, pp. 50–57. doi: 10.1109/CyberC.2019.00018.
14. C. He, E. Mushtaq, J. Ding, and S. Avestimehr, "Fednas: Federated deep learning via neural architecture search," 2021, Accessed: Dec. 23, 2025. [Online]. Available: https://openreview.net/forum?id=1OHZX4YDqhT
15. X. Bao, C. Su, Y. Xiong, W. Huang, and Y. Hu, "FLChain: A Blockchain for Auditable Federated Learning with Trust and Incentive," in *2019 5th International Conference on Big Data Computing and Communications (BIGCOM)*, QingDao, China: IEEE, Aug. 2019, pp. 151–159. doi: 10.1109/BIGCOM.2019.00030.
16. F. M. Salman, S. S. Abu-Naser, E. Alajrami, B. S. Abu-Nasser, and B. A. Alashqar, "Covid-19 detection using artificial intelligence," 2020, Accessed: Dec. 23, 2025. [Online]. Available: https://www.academia.edu/download/76845282/IJAER200304.pdf
17. G. Kaissis *et al.*, "End-to-end privacy preserving deep learning on multi-institutional medical imaging," *Nat Mach Intell*, vol. 3, no. 6, pp. 473–484, May 2021, doi: 10.1038/s42256-021-00337-8.
18. M. R. H. Mondal, S. Bharati, and P. Podder, "Diagnosis of COVID-19 Using Machine Learning and Deep Learning: A Review," *CMIR*, vol. 17, no. 12, pp. 1403–1418, Dec. 2021, doi: 10.2174/1573405617666210713113439.
19. Y. Qu *et al.*, "Decentralized Privacy Using Blockchain-Enabled Federated Learning in Fog Computing," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5171–5183, Jun. 2020, doi: 10.1109/JIOT.2020.2977383.
20. M. Shayan, C. Fung, C. J. M. Yoon, and I. Beschastnikh, "Biscotti: A Blockchain System for Private and Secure Federated Learning," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 7, pp. 1513–1525, Jul. 2021, doi: 10.1109/TPDS.2020.3044223.
21. Z. Yang, Y. Shi, Y. Zhou, Z. Wang, and K. Yang, "Trustworthy Federated Learning via Blockchain," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 92–109, Jan. 2023, doi: 10.1109/JIOT.2022.3201117.

22. A. Islam, A. Al Amin, and S. Y. Shin, "FBI: A Federated Learning-Based Blockchain-Embedded Data Accumulation Scheme Using Drones for Internet of Things," *IEEE Wireless Commun. Lett.*, vol. 11, no. 5, pp. 972–976, May 2022, doi: 10.1109/LWC.2022.3151873.
23. H. Zhu and Y. Jin, "Multi-Objective Evolutionary Federated Learning," *IEEE Trans. Neural Netw. Learning Syst.*, vol. 31, no. 4, pp. 1310–1322, Apr. 2020, doi: 10.1109/TNNLS.2019.2919699.
24. Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Differentially Private Asynchronous Federated Learning for Mobile Edge Computing in Urban Informatics," *IEEE Trans. Ind. Inf.*, vol. 16, no. 3, pp. 2134–2143, Mar. 2020, doi: 10.1109/TII.2019.2942179.
25. Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) Fully Homomorphic Encryption without Bootstrapping," *ACM Trans. Comput. Theory*, vol. 6, no. 3, pp. 1–36, Jul. 2014, doi: 10.1145/2633600.
26. Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) Fully Homomorphic Encryption without Bootstrapping," *ACM Trans. Comput. Theory*, vol. 6, no. 3, pp. 1–36, Jul. 2014, doi: 10.1145/2633600.
27. L. T. Phong, Y. Aono, T. Hayashi, L. Wang, and S. Moriai, "Privacy-Preserving Deep Learning via Additively Homomorphic Encryption," *IEEE Trans.Inform.Forensic Secur.*, vol. 13, no. 5, pp. 1333–1345, May 2018, doi: 10.1109/TIFS.2017.2787987.
28. H. Li, D. Liu, Y. Dai, T. H. Luan, and S. Yu, "Personalized Search Over Encrypted Data With Efficient and Secure Updates in Mobile Clouds," *IEEE Trans. Emerg. Topics Comput.*, vol. 6, no. 1, pp. 97–109, Jan. 2018, doi: 10.1109/TETC.2015.2511457.
29. Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain Empowered Asynchronous Federated Learning for Secure Data Sharing in Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4298–4311, Apr. 2020, doi: 10.1109/TVT.2020.2973651.
30. Y. Qu *et al.*, "Decentralized Privacy Using Blockchain-Enabled Federated Learning in Fog Computing," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5171–5183, Jun. 2020, doi: 10.1109/JIOT.2020.2977383.
31. Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated Machine Learning: Concept and Applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, Mar. 2019, doi: 10.1145/3298981.
32. R. Durga and E. Poovammal, "Federated Learning Model for Healthchain System," in *2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, Kedah, Malaysia: IEEE, Dec. 2021, pp. 1–6. doi: 10.1109/ICRAIE52900.2021.9703948.
33. S. A. Latif *et al.*, "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems," *Computer Communications*, vol. 181, pp. 274–283, Jan. 2022, doi: 10.1016/j.comcom.2021.09.029.