High-Confidence Computing 5 (2025) 100302

Contents lists available at ScienceDirect

High-Confidence Computing

journal homepage: www.sciencedirect.com/journal/high-confidence-computing

Research article

FedViTBloc: Secure and privacy-enhanced medical image analysis with federated vision transformer and blockchain

Gabriel Chukwunonso Amaizu [a,b], Akshita Maradapu Vera Venkata Sai [a,*], Sanjay Bhardwaj [b], Dong-Seong Kim [b], Madhuri Siddula [c], Yingshu Li [d]

[a] Digital Twin Research Group, Department of Computer and Information Sciences, Towson University, Towson 21252, USA
[b] IT Convergence Engineering, Kumoh National Institute of Technology, Gumi 39177, South Korea
[c] Department of Computer Science, North Carolina Agricultural and Technical University, Greensboro 27411, USA
[d] Department of Computer Science, Georgia State University, Atlanta 30303, USA

ARTICLE INFO

Article history:
Received 1 December 2024
Revised 21 January 2025
Accepted 31 January 2025
Available online 15 February 2025

Keywords:
AI
Blockchain
Decentralized
Federated Learning
Medical images
Machine Learning
ViT

ABSTRACT

The increasing prevalence of cancer necessitates advanced methodologies for early detection and diagnosis. Early intervention is crucial for improving patient outcomes and reducing the overall burden on healthcare systems. Traditional centralized methods of medical image analysis pose significant risks to patient privacy and data security, as they require the aggregation of sensitive information in a single location. Furthermore, these methods often suffer from limitations related to data diversity and scalability, hindering the development of universally robust diagnostic models. Recent advancements in machine learning, particularly deep learning, have shown promise in enhancing medical image analysis. However, the need to access large and diverse datasets for training these models introduces challenges in maintaining patient confidentiality and adhering to strict data protection regulations. This paper introduces FedViTBloc, a secure and privacy-enhanced framework for medical image analysis utilizing Federated Learning (FL) combined with Vision Transformers (ViT) and blockchain technology. The proposed system ensures patient data privacy and security through fully homomorphic encryption and differential privacy techniques. By employing a decentralized FL approach, multiple medical institutions can collaboratively train a robust deep-learning model without sharing raw data. Blockchain integration further enhances the security and trustworthiness of the FL process by managing client registration and ensuring secure onboarding of participants. Experimental results demonstrate the effectiveness of FedViTBloc in medical image analysis while maintaining stringent privacy standards, achieving 67% accuracy and reducing loss below 2 across 10 clients, ensuring scalability and robustness.

1. Introduction

According to the World Health Organization (WHO), cancer is a broad collection of diseases that can begin in practically any organ or tissue of the body. These diseases are brought on when abnormal cells grow out of control, cross their normal boundaries to infect nearby body parts, and/or spread to other organs [1]. Cancer was responsible for almost 22% of deaths from noncommunicable diseases (NCDs) between 2000 and 2016, and it has become the leading cause of premature death in high-income countries [2].

Cancer of the skin is by far the most common of all cancers. Some major types of sin cancer include melanoma, squamous cell carcinoma, basal cell carcinoma, Merkel cell carcinoma, and sebaceous carcinoma [3]. Melanoma accounts for only about 1% of skin cancers but causes a large majority of skin cancer-related deaths. Moreover, it is estimated that about 28,120 men and 39,490 women in the United States will be diagnosed with melanoma in 2023 of which 5,420 men and 2570 women of those diagnosed are expected to die [4]. Skin cancer is one of the leading types of cancer in terms of new cases and mortality for both males and females of the 20 world regions surveyed in 2020 [5].

Due to the steady and continuous depletion of the ozone layer, the amount of hazardous ultraviolet (UV) radiation making its way to the earth's surface is on the rise. These UV rays are one major cause of melanoma as they can cause enormous damage to the DNA on skin cells and cause those cells to not function effectively leading to them becoming cancerous cells [6]. This phenomenon is referred to as acquired gene mutations, where the gene changes occur over a person's lifetime as opposed to inherited gene mutation where the affected cells are passed from parent to offspring [4].

* Corresponding author.
E-mail address: amaradapuveravenkatasai@towson.edu (A.M.V.V. Sai).

https://doi.org/10.1016/j.hcc.2025.100302

Experts have come to the conclusion that the early detection of cancer often opens the door to more treatment options. Moreover, it can help prevent the further spread of cancer and thus reduce the mortality rate associated with cancers [7]. However, the traditional means of cancer detection involving lesion inspections by physicians using their naked eyes followed by dermoscopy for skin lesion pattern analysis solely depends on the physician's skills, and often lesions on the skin look similar, thus it is hard to detect cancers early using this technique.

In recent analyses by medical experts, it has been unequivocally established that timely cancer detection significantly broadens the scope of available therapeutic interventions. Additionally, early detection plays a crucial role in curbing the progression of cancer, thereby mitigating mortality rates associated with malignancies [7]. Nevertheless, the conventional approach to cancer detection, reliant on visual inspection of lesions by physicians, followed by dermoscopy for skin lesion pattern analysis, heavily relies on the skill and expertise of the medical practitioner. Given the inherent resemblance of certain skin lesions, this method proves inadequate for achieving early cancer detection [7,8]. Moreover, the manual procedure for skin cancer inspection is prone to time consumption and susceptible to potential human errors during the diagnostic process.

While medical imaging advancements have improved cancer detection, they have also raised significant privacy concerns. Medical images often contain sensitive patient information, and centralized storage or sharing can risk data breaches and unauthorized access. Ensuring privacy and security in medical image analysis is vital to maintaining patient trust and complying with government regulations [9].

1.1. Research motivations

1. **Preserving Patient Privacy**: The primary motivation is to address the critical concern of preserving patient privacy in medical image analysis.
2. **Enhancing Data Security**: Another key motivation is to enhance the security of sensitive medical data.
3. **Enabling Collaborative Research**: The paper seeks to facilitate collaborative medical research while respecting data privacy.
4. **Early Skin Cancer Detection**: One of the specific application areas and motivations for the paper is to improve early skin cancer detection through medical image analysis.

1.2. Research contributions

The major contributions of this work include:

1. The use of Vision Transformer models in a federated learning setting for medical image analysis. This integration allows multiple clients (medical institutions) to collaboratively train a powerful deep-learning model without sharing raw data, thus preserving data privacy.
2. Proposed a hybrid privacy-preserving technique that involves fully homomorphic encryption (FHE) and differential privacy. FHE encrypts the model updates sent from clients to the server. This ensures that the updates are kept confidential during transmission. At the server, a differential privacy mechanism is applied to aggregate the encrypted model updates. This technique involves the addition of noise to the aggregated updates, preserving the privacy of individual client contributions.
3. This paper implements blockchain technology for client registration, ensuring secure and trusted onboarding of participants in the federated learning process. Each client's identity and credentials are securely recorded on the blockchain, preventing unauthorized access and ensuring that only trusted and authenticated clients can participate in the collaborative training. This blockchain-based client management enhances the overall security and trustworthiness of the federated learning system for medical image analysis.

The organization of the paper is as follows: Section 2 reviews related works and background studies. Section 3 outlines the proposed system model. Section 4 details the experimental setup and analyzes the results of the proposed scheme. Finally some future research directions were introduced in Section 5, and Section 6 concludes the paper.

2. Related works & background study

Over the years, a wide array of technologies and approaches have been employed for the diagnosis of skin lesions. However, it is worth noting that many of these approaches have prioritized achieving accurate diagnoses without adequate consideration for client privacy. Conversely, some methodologies have taken into account the critical aspect of client privacy alongside diagnostic accuracy. In the following section, we provide an overview of select technologies and methodologies utilized in the detection of skin cancer.

2.1. Federated learning in medical images

The escalating generation of data across diverse sources has prompted the emergence of Federated Learning, a novel approach to machine learning. Unlike traditional centralized methods, Federated Learning enables collaborative model training without centralizing raw data. It leverages local data storage and processing, allowing individual entities to refine a shared model through iterative updates while safeguarding data privacy [10]. Federated Learning has notably surged in popularity within the health sector. The sensitive nature of patient data and the demand for advanced machine learning models have driven its adoption. This approach addresses challenges in sharing medical data due to privacy and regulatory concerns, offering collaborative model training while ensuring data security [11–13]. Authors in [14] presented a comprehensive review of FL approaches used in medical image analysis.

An intelligent federated ML-based dermoscopy was proposed in [15]. The authors built a dermoscopic device that would enable clinicians to better diagnose skin tumors. It was named adaptive because the authors claimed it was capable of classifying new skin tumors even after deployment through its continuous learning process. The FL consisted of a previously proposed cloud-based ensemble CNN. Experimental results show a skin lesion classification accuracy of 95% using the ISIC dataset. In [16], privacy-preserving FL for skin cancer diagnosis was proposed. The authors aimed to break down data silos and demonstrate the collaborative nature of AI. They used a CNN model of two blocks with each block consisting of a convolutional layer, a ReLU layer, and a max pooling layer. Moreover, 5 edge devices were used for experimental, and the model trained for 50 epochs showed an accuracy of 90% which was lower than the 95% recorded without using FL. However, the drop in loss was justified by the improvement in data privacy. Custom FL is introduced in [17], with the aim of client models in FL to better avoid the negative influence introduced in the global model by other clients. In this

approach, each client trains its own model while the FL model is mainly used as a feature extractor that guides the training of each client model. Each client node first splits its network into a feature extractor and a task-specific head, then trains and updates its personalized network iteratively prior to sending the update to the server for aggregation. Experiments were carried out using the HAM10000 dataset with varying numbers of clients and results compared with other methods. AN accuracy of 79% was the highest recorded for this scheme.

While FL has shown great improvements in the classification of skin cancer, it is still plaque with some challenges such as poisoning and byzantine attacks. A poisoning attack occurs when a client's local training data or model is tampered with or polluted thereby affecting the security of the FL system. Whereas a byzantine attack occurs when multiple clients collude to attack a distributed learning environment [18].

2.2. Vision transformers in medical images

The Vision Transformer (ViT) stands as a revolutionary neural architecture that has transformed computer vision by leveraging self-attention mechanisms from natural language processing and applying them to image data. ViT deconstructs images into fixed-size patches, embedding them linearly before directing them through a transformer encoder [19,20]. This innovative approach eliminates the necessity for manually designed convolutional neural networks and instead allows for end-to-end learning of image features. By enabling interactions among patches in both directions, ViT captures extensive dependencies, enhancing its ability to model the broader context of images. ViT's remarkable success has not only expanded the frontiers of image classification but has also sparked progress in diverse computer vision tasks, ushering in fresh prospects for AI research and practical applications [21,22].

Authors in [23] proposed a two-tier architecture for the effective classification of skin cancer. The first tier consists of data augmentation methods aimed at increasing the number of samples in the HAM10000 dataset. Whereas in the second tier, the authors leveraged the prowess of medical vision transformers (MVT) used in medical image analysis to develop an MVT-based model for skin cancer classification. A large ViT model was used with an MLP head attached to the ViT output. An accuracy of 96%, sensitivity of 96%, f1-measure of 97%, and precision of 96% were recorded. A novel ViT model for skin cancer classification was presented in [24]. The approach relied on transfer learning by using a pre-trained ViT model and fine-tuning it with the HAM10000 dataset. Fine-tuning was done by adding at the end of the transformer encoder block, a classification block consisting of a flattened layer, and two batch normalizations separated by a dense layer with GeLU activation. The experiment achieved a 94% accuracy, outperforming all compared methods. Similarly in [25], a pre-trained ViT fine-tuned with an MLP on the HAM10000 was used. However, a contrastive learning approach was introduced. Contrastive learning uses a contrastive loss function to reduce the similarity of samples belonging to the same class and maximize the similarity of samples in different classes. This model had an accuracy of 94%.

2.3. Blockchain & FHE in medical images

Blockchain is a distributed ledger system and has seen rapid adoption since the release of the Bitcoin white paper in 2012. It is a chain of blocks that holds data as digital signatures in a decentralized and distributed manner. The major features and strengths of blockchain are its immutability, transparency, and decentralized nature [26]. In the health sector, blockchain has been deployed for medical data access [27], and drug tracing among others [28]. Using FHEs, blockchain networks, when deployed in the health sector, help to provide an additional layer of data security.

Authors in [29] proposed a framework that used blockchain and DL for skin cancer classification. Blockchain was used in storing the medical images of patients while an optimal DL model was used for the training and classification of the images. Although blockchain and AI have consistently been used together [30], there exists very little attention paid to using them for the classification of skin cancer.

3. System model

This section introduces a novel framework for classifying skin lesions. The proposed framework proficiently distinguishes between cancerous and non-cancerous lesions. Moreover, it is designed to mitigate the risk of private or sensitive client data leakage. The system protects sensitive medical images and metadata, including patient identifiers and diagnostic information. A compromise in this data could lead to unauthorized access, misuse, or breaches of patient confidentiality, resulting in legal, ethical, and operational repercussions for healthcare providers.

The process begins with each client (hospital institution) submitting a request to join the blockchain network, referred to as the registration stage. Upon completion of client registration, the client receives the global model and commences training with its local data. Local training utilizes a pre-trained ViT model that has been adapted for classification tasks. Following a few training epochs, the client is prepared to transmit its updates to the server. By employing FHE, the model updates are encrypted to ensure confidentiality before transmission to the server. To safeguard the client's identity, differential privacy is employed by introducing a level of noise during the aggregation of encrypted model updates on the server. While FHE secures the transmission of model updates, Differential Privacy (DP) obfuscates individual contributions during aggregation by introducing controlled noise. For instance, updates from a hospital's local model are encrypted, ensuring unreadability during transmission. At the server, DP adds small random noise (e.g., ± 0.01) to aggregated updates, such as modifying a value of 0.65 to 0.64 or 0.66. This dual-layer approach ensures end-to-end privacy, addressing potential inference attacks while enabling collaborative model training.

Fig. 1 presents a visual representation of the proposed scheme, which consists of eight (8) distinct steps, each of which is elaborated upon below:

1. The client initiates the process by sending a join request to the blockchain network.
2. The network evaluates the request, accepting it only if the specified conditions are satisfied.
3. Subsequently, the server dispatches a global model to the registered client.
4. The client commences its training procedure, utilizing its local data in conjunction with the modified ViT model.
5. Upon completion of training, the model updates are subjected to encryption.
6. The encrypted updates are transmitted to the server.
7. An algorithm for differential privacy (DP) is established.
8. The model aggregation process is executed using the DP mechanism defined in step 7.
9. Steps 3 through 8 are iteratively repeated as needed.

This schematic representation delineates the core sequence of actions within the proposed scheme. The algorithm and symbolic notations for the proposed scheme are both given in Algorithm 1 and Table 1 respectively.

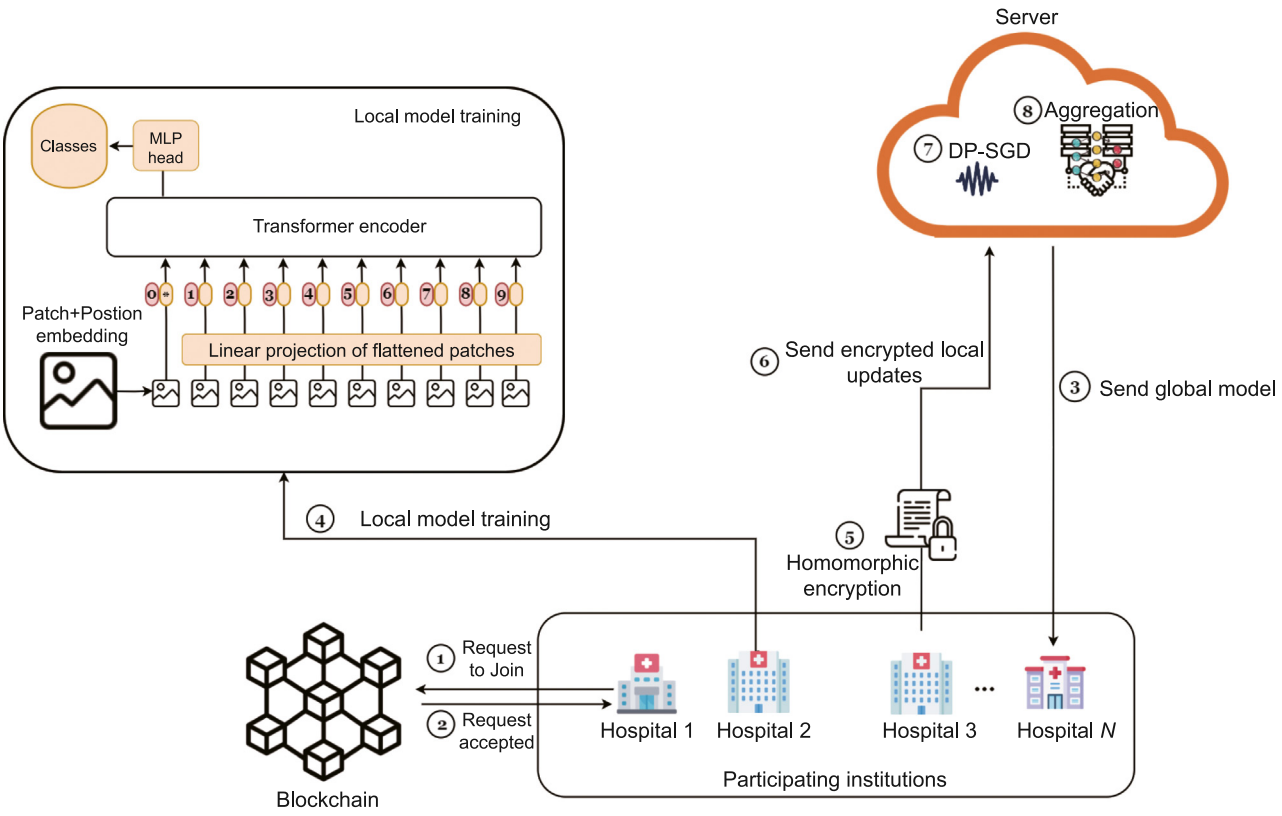

Fig. 1. Architecture of the FedViTBloc framework.

Table 1
Notation summary.

Symbol	Description
C	Number of clients
T	Number of training rounds
$w^{(t)}$	Global model weights at round t
$w_i^{(t)}$	Local model weights of client i at round t
$\tilde{w}_i^{(t)}$	Encrypted local model weights of client i at round t
Enc()	Encryption operation
$\oplus, \otimes$	Homomorphic addition and scalar multiplication operations
$\mathcal{N}(0, \sigma^2)$	Gaussian noise for Differential Privacy
$\tilde{\eta}$	Encrypted noise for DP

3.1. Federated learning architecture

This paper employs a Federated Learning (FL) architecture, wherein multiple clients contribute to the training of a model. In FL, clients collaboratively train a model under the coordination of a central server while maintaining decentralized control over their training data. FL typically encompasses three (3) key steps: (1) The server dispatches the initial model to each client device. (2) Each device trains its model using its local data, without sharing it with other devices. (3) The server collects and aggregates the locally trained models from all participating clients using Federated Averaging (FedAvg). FedAvg computes a weighted average of the model parameters based on the size of the local datasets at each client, ensuring efficient and accurate aggregation across heterogeneous data distributions [10].

Despite the absence of direct data exchange between the server and clients, there is a potential risk posed by malicious actors who could analyze the parameters trained and uploaded by clients, potentially revealing sensitive client information and data [31]. Additionally, there is the concern that these updates from clients could be intercepted and tampered with before reaching the server [18]. Hence, it is evident that data security and client privacy remain significant challenges within the FL framework. These issues will be addressed in subsequent subsections. In this paper, each client represents a hospital institution, and the FL system can accommodate any number of clients meeting specific minimum requirements.

3.2. Blockchain

In federated learning, participants may include organizations, individuals, or devices, each with specific access requirements and permissions. Smart contracts, as self-executing agreements on a blockchain, provide an automated and tamper-resistant means of enforcing access control. When a participant seeks to join a federated learning network or contribute data to the collaborative model, a smart contract deployed on the blockchain can facilitate access control checks. Although all clients can use the global model for inference, not all clients can be allowed to contribute to the global model training. The smart contract can verify the eligibility of a participant based on predefined rules and conditions encoded within the contract.

This paper introduces the utilization of a smart contract for access control by defining a function for client registration. To participate in training, a client must initially invoke the "register" method on the smart contract and possess a specified minimum amount of training data before being granted access. Additionally, the smart contract defines a reward distribution model, automatically computing and disbursing rewards to participants based on the size of their contributed data. Participants who contribute a substantial volume of data are eligible for rewards. To facilitate a client's participation, they must provide their name (hospital name) during the registration process. Upon approval, a unique blockchain address is allocated to the client. Subsequently, this assigned address serves as the client's means of interaction

Algorithm 1 Privacy-Preserving Federated Learning

Input:

- C: Number of participating clients
- $\mathcal{D}_i$: Local dataset of client i ($i \in \{1, 2, \ldots, C\}$)
- T: Number of training rounds
- w_0: Initial global model weights
- ϵ: Privacy budget for Differential Privacy
- $\mathcal{E}$: Homomorphic encryption scheme (encryption Enc(), homomorphic operations $\oplus$, $\otimes$)

Initialization: Server initializes global model weights w_0.
Server shares Enc(w_0) (encrypted global model) with all clients $\{C_1, C_2, \ldots, C_C\}$.
for $t = 1$ to T **do**
  for each client i in parallel **do**
    Model Training: Client i decrypts Enc($w^{(t)}$) to obtain $w^{(t)}$.
    Train local model using dataset $\mathcal{D}_i$, resulting in updated weights $w_i^{(t)}$.
    Encryption: Client encrypts local weights: $\tilde{w}_i^{(t)} = \text{Enc}(w_i^{(t)})$.
    Client sends $\tilde{w}_i^{(t)}$ to the server.
  end for
  Aggregation at Server:
  Perform homomorphic aggregation:

$$\tilde{w}^{(t+1)} = \frac{1}{C} \bigoplus_{i=1}^{C} \tilde{w}_i^{(t)}$$

  Add Differential Privacy:
  Server adds noise calibrated to the privacy budget ϵ:

$$\tilde{\eta} = \text{Enc}(\eta), \quad \eta \sim \mathcal{N}(0, \sigma^2), \quad \sigma = \Delta f / \epsilon$$

  where Δf is the sensitivity of the aggregation function.

$$\tilde{w}^{(t+1)} = \tilde{w}^{(t+1)} \oplus \tilde{\eta}$$

  Server shares $\tilde{w}^{(t+1)}$ with all clients.
end for
Output: Final encrypted global model $\tilde{w}_T$.

with the Federated Learning (FL) architecture on all future occasions as no two clients can have the same address. The use of smart contracts ensures fairness, transparency, and immediate compensation, reducing the need for centralized intervention.

3.3. Modified vision transformer

Transformers, originally rooted in self-attention mechanisms and initially applied in natural language processing, have found extensive utility in various computer vision tasks, consistently outperforming other deep neural networks such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) [21]. A key concept underlying Vision Transformer (ViT) models involves segmenting input images into fixed-size patches, which are then processed through a transformer-based architecture. This approach enables the extraction of comprehensive global and intricate local features from the image [20].

In this study, we incorporate a pre-trained vit model, notable for its moderate layer count, attention heads, and associated parameters. With a patch size of 16 and the ability to handle 224×224 images, this model has exhibited proficiency on the ImageNet dataset. Therefore, we perform fine-tuning to adapt it for skin lesion classification. To achieve this, we introduce a custom classification head, which is connected to the end of the ViT model. This classification head consists of a series of connected layers. A pictorial structure of the ViT model can be seen in Fig. 2.

The initial layer unflattens the 1D array inherited from the previous layer, resulting in a 4D array, which is then passed through a convolutional layer. The output from the convolutional layer undergoes max-pooling before being flattened and subsequently passed through a fully connected layer that includes two hidden layers. Finally, the output layer is responsible for categorizing the input into one of seven distinct classes of skin lesions. This custom classifier effectively processes the ViT model outputs, ultimately providing predictions for skin lesion types.

3.4. Security & privacy-preserving techniques

As mentioned earlier, Federated Learning (FL) is susceptible to security and privacy vulnerabilities, particularly during the upload of model updates from clients to the server and during the aggregation of these updates on the server [31]. In this paper, we present methods to enhance the security of model updates before they are uploaded to the server. Additionally, we employ a privacy-preserving aggregation technique to safeguard client privacy during the aggregation process.

3.4.1. Secure model updates

In contrast to conventional encryption methods, which rely on the exchange of public or private keys for decryption prior to computation, FHE enables computations to be performed directly on encrypted data without the need for decryption. This paper incorporates FHE in FL to ensure secure transfer and processing of model updates from clients to the server. Using PySyft, a Python library for privacy-preserving machine learning, each client's local model parameters are encrypted before being transmitted. Once the encrypted updates reach the server, operations such as aggregation and global model updates are executed directly on the encrypted data, maintaining data confidentiality throughout the federated learning process. This ensures that sensitive client information remains secure while enabling collaborative training.

3.4.2. Differential privacy aggregation

During FL training, it is important to preserve the privacy of individual client and their contributions. FL inherently aims to protect the privacy of individual participants' data. However, even in FL, there can be risks of information leakage or inference attacks. Differential Privacy (DP) adds an additional layer of privacy protection by making it mathematically challenging for an attacker to determine whether a specific individual's data was used in the model training or to extract sensitive information about an individual from the model's output [32,33]. Moreover, medical institutions will be more willing to participate in FL collaborations if they know their data will be treated with strong privacy guarantees.

One approach to enhancing utility while maintaining privacy is through the management of a privacy budget. The privacy budget is a finite and predetermined amount of privacy protection, typically denoted as epsilon (ϵ). The selection of ϵ is a pivotal decision in the context of DP. A smaller ϵ corresponds to a more stringent privacy guarantee, signifying stronger privacy protection. Conversely, a larger ϵ implies a weaker privacy guarantee, allowing for a higher potential for information leakage [34]. Following the application of DP, model aggregation takes place on the server before the aggregated model is transmitted to the participating clients.

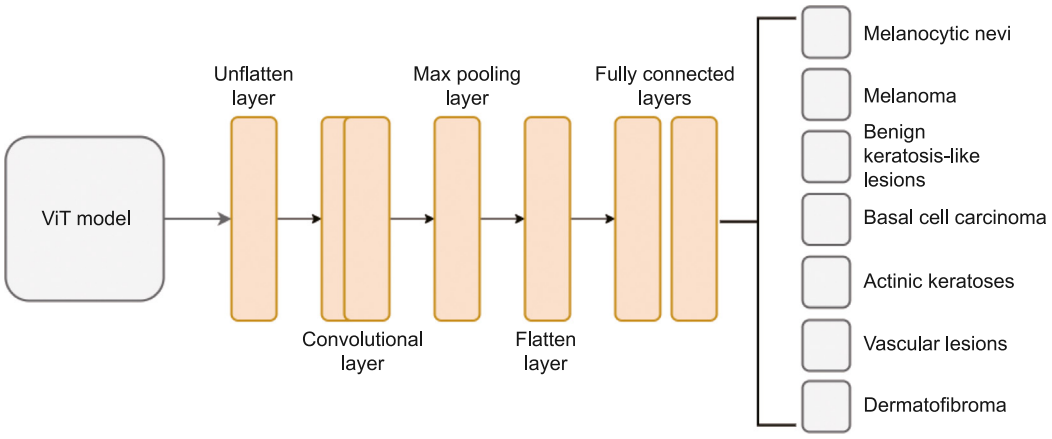

Fig. 2. Modified vision transformer.

In this work, we have incorporated Opacus, a library designed for integrating Differential Privacy (DP) into PyTorch models [35]. Furthermore, we have explored various noise levels to strike a balance between achieving better privacy and maintaining acceptable data utility.

3.5. System complexity

The complexity of FedVitBloc algorithm can be analyzed in three primary aspects, client-side computation, server-side computation, and communication overhead.

3.5.1. Client-side computation complexity

The training complexity depends on the size of the local dataset ($|\mathcal{D}_i|$), the model architecture, and the number of epochs (E). If the model has M parameters, the training complexity is approximately $O(E \cdot |\mathcal{D}_i| \cdot M)$. FHE is applied to the model updates after training. Encrypting each parameter incurs a cost of $O(\log M)$, so for M parameters, the total complexity of encryption is: $O(M \cdot \log M)$. Each client sends its encrypted model updates to the server. If the model has M parameters, the communication cost per client is $O(M)$.

3.5.2. Server-side computation complexity

Aggregating the encrypted updates from C clients involves homomorphic addition and scalar multiplication. For M parameters per client, the aggregation complexity is $O(C \cdot M)$. The server adds noise calibrated to the privacy budget ϵ. Noise generation is typically independent of M, so this operation has negligible complexity compared to aggregation $O(1)$.

3.5.3. Communication overhead

Communication overhead is incurred during the exchange of model updates between clients and the server. Each client sends its encrypted model updates of size M to the server. For C clients, the total communication cost is $O(C \cdot M)$. The server sends the aggregated encrypted global model of size M back to all clients, adding another $O(C \cdot M)$. The total communication overhead per round is: $O(C \cdot M)$.

3.5.4. Total complexity per round

Combining all components, the total complexity per round (T rounds) is:

$$O\left(T \cdot \left(E \cdot |\mathcal{D}_i| \cdot M + M \cdot \log M + 2C \cdot M\right)\right)$$

4. Experiments

This section encompasses a comprehensive account of the experimental procedures conducted in this research, the technologies employed, and a subsequent discussion of the obtained results.

4.1. Experimental setup

The experimental setup employed an Ubuntu operating system equipped with three NVIDIA GeForce RTX 3090 GPUs. For the different components of the proposed scheme, three distinct files were utilized:

1. **server.py**: This file is responsible for defining the server configuration and handling model aggregation.
2. **client.py**: Within this file, functionalities for client training and testing are implemented. Additionally, it contains functions for communicating with the smart contract to verify client registration and manage reward assignments.
3. **client_registration.sol**: This smart contract is a prerequisite for clients to register before participating in the training process. It maintains a record of client addresses and enforces the reward system.

As previously mentioned, our implementation leveraged PySyft for FHE and Opacus for Differential Privacy (DP) on model parameters, primarily within the *client.py* component. In the context of blockchain implementation, we utilized Ganache, a local blockchain network, to facilitate our experiments. Ganache sets up a private blockchain network that runs on a local machine, allowing one to create and manipulate accounts, mine blocks, and deploy smart contracts in a controlled environment. It generates a set of test accounts with predefined addresses and private keys. These accounts were used as client accounts for testing the proposed scheme. The federated learning architecture is built using the Flower [36] framework.

4.2. Dataset

The "HAM10000" dataset is a collection of dermatoscopic images of common pigmented skin lesions, designed for use in machine learning and artificial intelligence research, particularly in the field of dermatology and medical image analysis. It consists

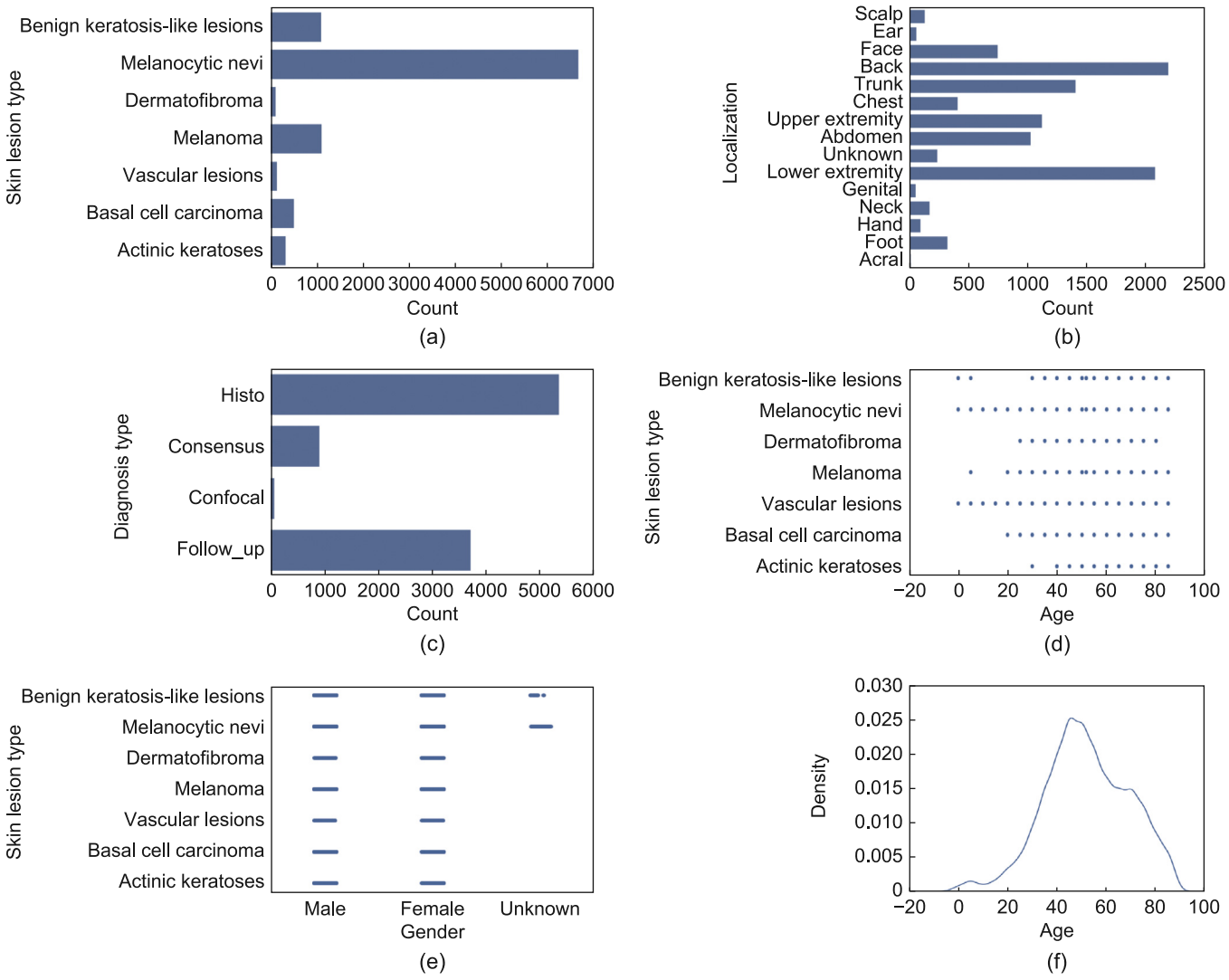

Fig. 3. Insight into the HAM10000 dataset. (a) Distribution of skin lesion type. (b) Distribution of lesion localization. (c) Diagnosis type distribution. (d) Age distribution across skin lesion types. (e) Gender-based distribution of skin lesion types. (f) Age distribution.

of 10,015 clinical images of pigmented lesions, which include various types of skin conditions such as melanoma, nevus, seborrheic keratosis, and more. These images are accompanied by metadata, including diagnostic information and patient details, making it a valuable resource for training and testing machine learning models to detect skin cancer and other skin disorders [37]. An insight into the dataset is presented in Fig. 3.

In Fig. 3a, it is evident that Melanocytic nevi constitute the majority of samples, with approximately 6700 instances, followed by benign keratosis-like lesions with around 1000 samples. Fig. 3b highlights that skin lesions are primarily localized on the back (approximately 2100 samples), trunk (approximately 2000 samples), and lower extremities (approximately 1200 samples). The dataset predominantly uses histopathology as the diagnostic method, with nearly 5000 cases, followed by medical follow-ups at approximately 4000 cases, as shown in Fig. 3c. Fig. 3d illustrates that Melanocytic nevi span all age groups, while basal cell carcinoma predominantly affects patients aged 60 and above. Gender-wise, as depicted in Fig. 3e, most lesion types are evenly distributed, with actinic keratoses showing a higher prevalence in males. Finally, Fig. 3f reveals that the majority of skin lesions occur in adults aged 30 to 80, with density peaks around ages 20 and 60.

4.3. Experimental results

4.3.1. Accuracy & loss

The efficacy of the proposed approach is meticulously scrutinized through a comprehensive analysis of accuracy, defined as the proportion of correct predictions made by the model out of the total number of examples. Fig. 4 vividly illustrates the accuracy trends for five distinct clients (Clients 1 to 5) as the number of epochs increases. Initially, the accuracy for all clients starts at approximately 50% but experiences consistent improvements as training progresses. By epoch 20, the accuracy for all clients shows a significant jump, with Client 1 achieving approximately 67%, Client 2 reaching 65%, and Client 3, Client 4, and Client 5 stabilizing around 62%–64%. Despite some fluctuations in earlier epochs, the accuracy converges for all clients between 65% and 67% by epoch 50, showcasing uniform performance across the client spectrum. This exponential growth in accuracy underscores the robustness and effectiveness of the proposed approach across multiple clients. The observations substantiate the approach's potential to consistently enhance accuracy metrics with prolonged training, reinforcing its impact and suitability for diverse client scenarios.

Likewise, a parallel behavior is discerned among Clients 6 to 10, as elucidated in Fig. 5. The accuracy for these clients starts at

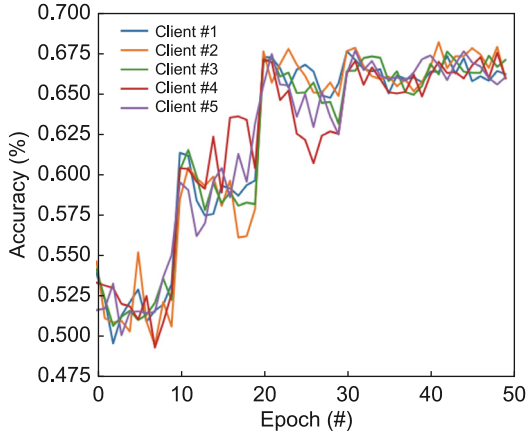

Fig. 4. Accuracy trends for clients 1 to 5 over increasing epochs.

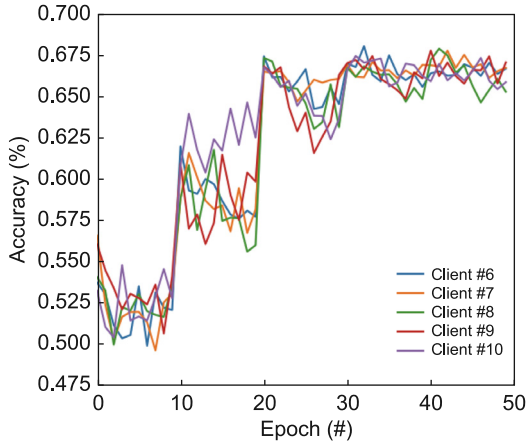

Fig. 5. Accuracy trends for clients 6 to 10 over increasing epochs.

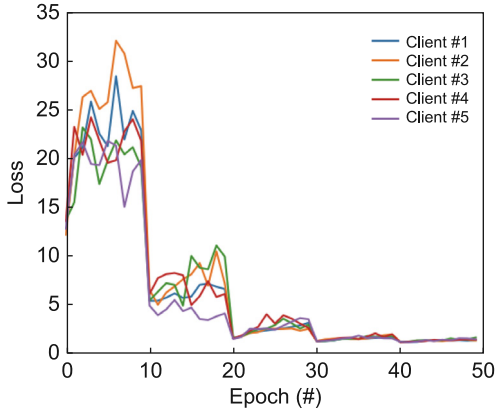

Fig. 6. Loss reduction for clients 1–5 over training epochs.

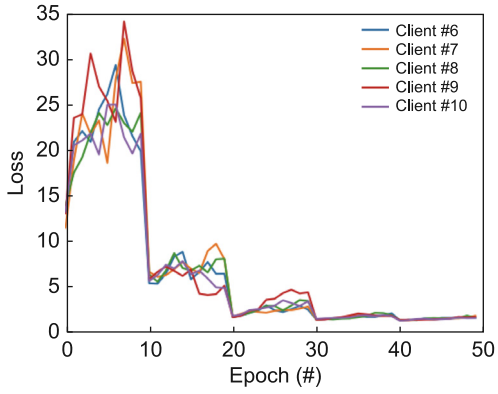

Fig. 7. Loss reduction for clients 6–10 over training epochs.

approximately 50% in the initial epochs, with some variability. A notable improvement is observed around epoch 20, where Client 6 achieves an accuracy of approximately 67%, while Clients 7, 8, 9, and 10 reach accuracies between 64% and 66%. By epoch 50, all clients converge with accuracies stabilizing between 65% and 67%, mirroring the trend observed in Clients 1 to 5. This consistent pattern of accuracy improvement with an increasing number of epochs underscores the robust and generalizable nature of the proposed approach. The uniformity in accuracy trends across multiple client groups highlights the adaptability and scalability of the approach, substantiating its efficacy in diverse client scenarios. This further reaffirms the reliability and broad applicability of the proposed method in optimizing accuracy across a wide client spectrum.

Loss refers to the measure of error between the predicted class probabilities and the actual class labels. The behavior of the proposed approach is also analyzed for Clients 1 to 5 for loss, as depicted in Fig. 6. Initially, the loss for all clients is high, with values exceeding 20, and Client 2 peaking at over 30 within the first few epochs. However, a significant reduction in loss is observed around epoch 10, where all clients show a sharp decrease, with loss values dropping below 5. By epoch 20, the loss values for all clients converge, stabilizing between 0 and 2, and remain consistent through to epoch 50. This consistent trend highlights the effectiveness of the proposed approach in minimizing loss over successive epochs across various clients. The substantial reduction in loss signifies the approach's ability to refine and optimize model parameters, contributing to enhanced performance and convergence. The observed uniformity in loss reduction across multiple clients underscores the reliability and versatility of the proposed approach, substantiating its applicability and effectiveness in diverse client scenarios.

Similarly, the behavior is observed for Clients 6 to 10 in terms of loss, as illustrated in Fig. 7. Initially, the loss for all clients is high, exceeding 20 for most clients and peaking at over 35 for Client 7 within the first few epochs. A sharp reduction in loss occurs around epoch 10, where all clients drop their loss values below 5. By epoch 20, the loss for all clients stabilizes, with values consistently falling between 0 and 2, and this trend persists through to epoch 50.

This consistent and noticeable exponential decrease in loss emphasizes the robustness and effectiveness of the proposed approach in minimizing loss across a diverse range of clients. The substantial reduction in loss signifies the approach's ability to adapt and optimize model parameters for improved convergence and overall performance. This consistent behavior further supports the generalizability and reliability of the proposed approach, indicating its potential to yield favorable outcomes across different sets of clients.

Likewise, we observe a consistent trend in the accuracy of the proposed approach concerning epsilon, as illustrated in Fig. 8. At lower epsilon values (e.g. $\epsilon = 20$), accuracy starts at approximately 50%. As epsilon increases, a notable improvement in accuracy is observed, with accuracy reaching around 60% at $\epsilon = 30$ Beyond this, the accuracy continues to improve steadily, peaking at approximately 67% when ϵ exceeds 40. This observation emphasizes the positive association between epsilon values

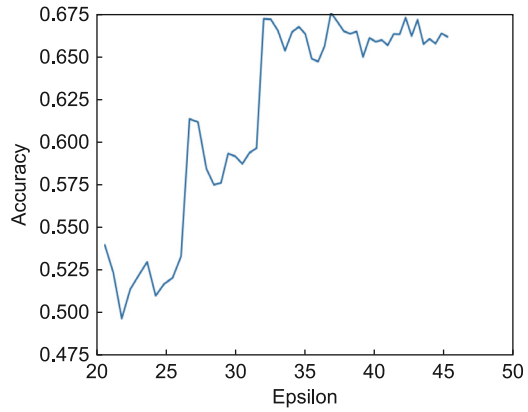

Fig. 8. Relationship between epsilon values and model accuracy.

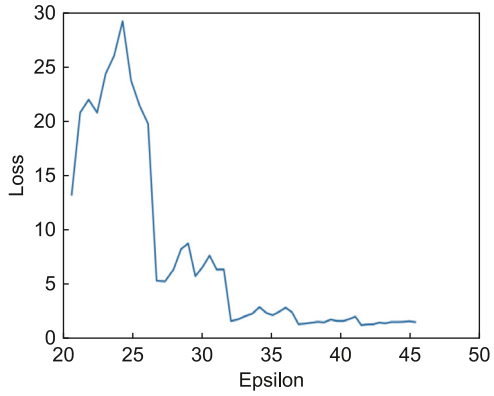

Fig. 9. Relationship between epsilon values and model loss.

and the accuracy attained by the proposed approach. The trend highlights the adaptability and responsiveness of the approach to variations in epsilon, demonstrating its capacity to optimize accuracy in accordance with the specified constraints. This steadfast and positive connection between epsilon and accuracy serves to underscore the effectiveness and versatility of the proposed approach across diverse epsilon scenarios.

In a parallel manner, the trend is evident for the loss incurred by the proposed approach concerning epsilon, as illustrated in Fig. 9. At lower epsilon values (e.g. $\epsilon = 20$), the loss is initially high, exceeding 20 and peaking at nearly 30. As epsilon increases, a significant reduction in loss is observed. Around $\epsilon = 30$, the loss decreases sharply to values below 5. Beyond $\epsilon = 35$, the loss stabilizes, maintaining consistent values close to 2 across higher epsilon values.

This observation emphasizes the inverse correlation between epsilon values and the incurred loss by the proposed approach. The trend underscores the adaptability and responsiveness of the approach to variations in epsilon, demonstrating its capacity to optimize loss based on the specified constraints. This consistent and negative relationship between epsilon and loss further highlights the efficacy and versatility of the proposed approach across different epsilon scenarios, providing valuable insights into its performance under varying privacy considerations.

The Table 2 encapsulates crucial metrics across multiple evaluation rounds for the proposed approach. Each row corresponds to a distinct round, providing insights into the model's evolving performance. The "Accuracy (%)" column reveals the percentage of correct predictions, showcasing a modest improvement from 69.0602% in Round 1 to 70.357% in Round 2. The "Loss" metric, reflecting the disparity between predicted and actual values,

Table 2
Evaluation metrics across multiple rounds. This table provides a comprehensive overview of key performance metrics (accuracy, loss, and epsilon) for the proposed FedViTBloc approach over different evaluation rounds.

Round	Accuracy (%)	Loss	Epsilon (ϵ)
1	69.0602	1.29843	28.1379
2	70.3570	1.29780	40.1070

slightly decreases from 1.29843 to 1.2978, indicating improved model precision. Epsilon (ϵ), a parameter influencing privacy levels in federated learning, is highlighted in the table. In Round 1, an epsilon value of 28.1379 is employed, and it increases to 40.1070 in Round 2. The chosen epsilon values signify the delicate balance between privacy preservation and model accuracy, where higher epsilon values prioritize enhanced privacy at the potential expense of accuracy. This table provides a comprehensive snapshot of the model's performance dynamics, privacy considerations, and the nuanced trade-offs inherent in federated learning evaluations.

4.4. Smart contract

Blockchain is leveraged in this work to enhance security through its decentralized architecture, effectively eliminating a single point of failure. Nonetheless, smart contracts are recognized as potential sources of security vulnerabilities within the blockchain ecosystem. To mitigate such vulnerabilities and safeguard user data and privacy, we have rigorously examined our smart contract using SOlidCheck [38]. The analysis yielded an impeccable result, with a security score of 100%, as depicted in Fig. 10. This outcome underscores the robustness of our system against vulnerabilities, ensuring data privacy.

The deployment details of the smart contract are presented in Fig. 11. The deployment cost and gas cost amounted to 0.002280652875 ETH and 675749 units, respectively.

Additionally, Fig. 12 provides a limited screenshot of the server.py and client.py terminal outputs. In the server.py command line output (the first terminal in the figure), it is evident that two out of five clients were sampled in the first round, with the results successfully received, indicating no failures. In the client.py output (the remaining five terminals), client training is initiated only when the isRegistered flag is set to True. Initially, the flag is False; upon invocation of the smart contract, the client is registered, and training commences.

5. Future work

While the proposed FedViTBloc framework demonstrates significant advancements in privacy-preserving medical image analysis, there are several directions for future research to enhance its capabilities.FHE introduces computational overhead that can limit scalability in real-world applications. Future work will explore optimizing FHE implementations to improve efficiency while maintaining strong privacy guarantees.

Also, the increased complexity introduced by privacy-preserving techniques, such as FHE and DP, can negatively impact model accuracy. Future work will focus on optimizing the trade-off between system complexity and model performance by fine-tuning hyperparameters, improving aggregation methods, and exploring privacy-enhancing algorithms with lower computational overhead. The blockchain component ensures secure client registration and participation. However, the scalability and energy consumption of the blockchain need to be optimized. Future work will explore energy-efficient consensus mechanisms and sharding techniques to enhance the blockchain's performance.

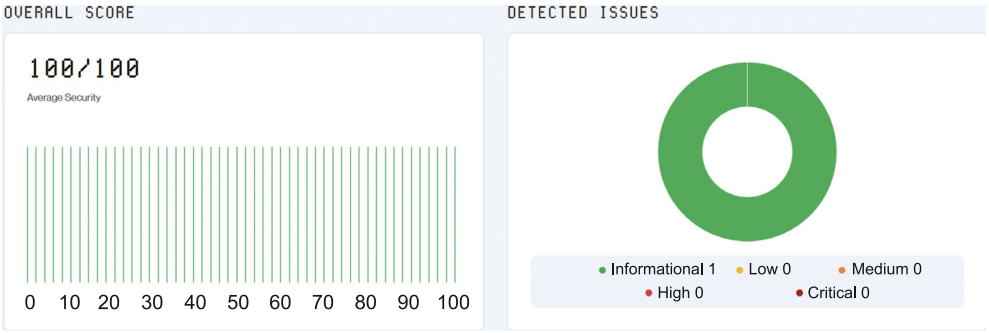

Fig. 10. Security evaluation of the smart contract using SolidCheck.

```
s16@ICT: ~/sc/test
File  Edit  View  Search  Terminal  Help

Compiling your contracts...
===========================
> Everything is up to date, there is nothing to compile.


Starting migrations...
======================
> Network name:    'development'
> Network id:      5777
> Block gas limit: 6721975 (0x6691b7)


01_deploy_contracts.js
======================

   Replacing 'ClientRegistration'
   ------------------------------
   > transaction hash:    0xcd207e8fc9a33e6395fe68719567959f8b16e139241e1dc271e4d48a9d7165f7
   > Blocks: 0            Seconds: 0
   > contract address:    0xf88d4c8135e184A26EACc7d6570e23A778331dfE
   > block number:        1
   > block timestamp:     1720748305
   > account:             0xA0E7507a4a5Ddcb9A6C820dBc587Fd270e9D3765
   > balance:             99.997719347125
   > gas used:            675749 (0xa4fa5)
   > gas price:           3.375 gwei
   > value sent:          0 ETH
   > total cost:          0.002280652875 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:      0.002280652875 ETH

Summary
=======
> Total deployments:   1
> Final cost:          0.002280652875 ETH


s16@ICT:~/sc/test$
```

Fig. 11. Console output showing the deployment of the ClientRegistration smart contract on the blockchain network using the Truffle framework. Key details include the transaction hash, contract address, block number, gas used, and the total deployment cost in Ethereum, indicating a successful setup for secure client registration.

6. Conclusion

The rising incidence of cancer calls for advanced techniques for early detection and diagnosis. Early intervention is essential for improving patient outcomes and alleviating the overall strain on healthcare systems. Traditional centralized approaches to medical image analysis pose significant risks to patient privacy and data security, as they necessitate the collection of sensitive information in a single location. Additionally, these methods often face challenges related to data diversity and scalability, which impede the development of universally robust diagnostic models. Recent advancements in machine learning, particularly deep learning, have shown potential in enhancing medical image analysis. However, the requirement to access large and diverse datasets for training these models presents challenges in preserving patient confidentiality and complying with strict data protection regulations. In this study, we proposed FedViTBloc, a novel framework that integrates Federated Learning, Vision Transformers, and blockchain technology to enhance the security and privacy of medical image analysis. Our approach addresses critical issues related to patient data privacy and security while enabling collaborative research among medical institutions. The experimental results on the HAM10000 dataset validate the efficacy of our framework in accurately classifying skin lesions, showcasing its potential for early cancer detection. The incorporation of FHE and differential privacy ensures that sensitive data remains secure throughout the training process. Additionally, blockchain technology provides a secure mechanism for client registration and participation, further strengthening the trustworthiness of the system. FedViTBloc represents a significant advancement in the field of medical image analysis, offering a scalable and secure solution for real-world applications. Future work will focus on optimizing the framework and exploring additional privacy-preserving techniques to further enhance data security.

Fig. 12. Terminal Outputs of server.py and client.py Scripts. This screenshot captures the terminal outputs during the federated learning process, demonstrating successful client registration and training, with details on the interactions between the server and clients.

CRediT authorship contribution statement

Gabriel Chukwunonso Amaizu: Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Akshita Maradapu Vera Venkata Sai:** Writing – review & editing, Supervision, Funding acquisition. **Sanjay Bhardwaj:** Supervision, Investigation. **Dong-Seong Kim:** Supervision. **Madhuri Siddula:** Funding acquisition. **Yingshu Li:** Funding acquisition.

Declaration of Generative AI and AI-assisted technologies in the writing process

During the preparation of this work, the authors used chatGPT in order to perform English corrections. After using this tool/service, the authors reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This research was supported by the Ministry of Science and ICT, Korea, under the Grand IT Research Center support program (IITP-2022-2020-0-01612) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation) and Priority Research Centers Program through the National Research Fund (NRF) Korea funded by the Ministry of Education, Science and Technology, South Korea (2018R1A6A1A03024003). This research was also supported in part by National Science Foundation (NSF) of USA (2200673) and the Office of Sponsored Programs & Research Seed Funding Program at Towson University, United States.

References

[1] What is cancer by WHO, 2023, URL https://www.who.int/health-topics/cancer#tab=tab_1. (Accessed 21 July 2023).
[2] World Health Organization, et al., World health statistics 2020, 2020.
[3] Types of skin cancer, American academy of dermatology association, 2023.
[4] Key statistics for melanoma skin cancer, American cancer society, 2023.
[5] Jacques Ferlay, Murielle Colombet, Isabelle Soerjomataram, Donald M Parkin, Marion Piñeros, Ariana Znaor, Freddie Bray, Cancer statistics for the year 2020: An overview, Int. J. Cancer 149 (4) (2021) 778–789.
[6] Marwan Ali Albahar, Skin lesion classification using convolutional neural network with novel regularizer, IEEE Access 7 (2019) 38306–38313, http://dx.doi.org/10.1109/ACCESS.2019.2906241.
[7] Mary K Tripp, Meg Watson, Sophie J Balk, Susan M Swetter, Jeffrey E Gershenwald, State of the science on prevention and screening to reduce melanoma incidence and mortality: The time is now, CA: Cancer J. Clin. 66 (6) (2016) 460–480.
[8] Muhammad Zia Ur Rehman, Fawad Ahmed, Suliman A. Alsuhibany, Sajjad Shaukat Jamal, Muhammad Zulfiqar Ali, Jawad Ahmad, Classification of skin cancer lesions using explainable deep learning, Sensors (ISSN: 1424-8220) 22 (18) (2022) http://dx.doi.org/10.3390/s22186915, URL https://www.mdpi.com/1424-8220/22/18/6915.
[9] Blagoj Ristevski, Ming Chen, Big data analytics in medicine and healthcare, J. Integr. Bioinform. 15 (3) (2018) 20170030, http://dx.doi.org/10.1515/jib-2017-0030.
[10] Chen Zhang, Yu Xie, Hang Bai, Bin Yu, Weihong Li, Yuan Gao, A survey on federated learning, Knowl.-Based Syst. (ISSN: 0950-7051) 216 (2021) 106775, http://dx.doi.org/10.1016/j.knosys.2021.106775, URL https://www.sciencedirect.com/science/article/pii/S0950705121000381.
[11] A. Rahman, M.S. Hossain, G. Muhammad, D. Kundu, T. Debnath, M. Rahman, M.S.I. Khan, P. Tiwari, S.S. Band, Federated learning-based AI approaches in smart healthcare: concepts, taxonomies, challenges and open issues, Clust. Comput. (2022) 1–41, http://dx.doi.org/10.1007/s10586-022-03658-4, Epub ahead of print.
[12] Ashish Rauniyar, Desta Haileselassie Hagos, Debesh Jha, Jan Erik Håkegård, Ulas Bagci, Danda B. Rawat, Vladimir Vlassov, Federated learning for medical applications: A taxonomy, current trends, challenges, and future research directions, 2022, arXiv:2208.03392.
[13] Fengpan Zhao, Yan Huang, Akshita Maradapu Vera Venkata Sai, Yubao Wu, A cluster-based solution to achieve fairness in federated learning, in: 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking, ISPA/BDCloud/SocialCom/SustainCom, 2020, pp. 875–882, http://dx.doi.org/10.1109/ISPA-BDCloud-SocialCom-SustainCom51426.2020.00135.
[14] Md Fahimuzzman Sohan, Anas Basalamah, A systematic review on federated learning in medical image analysis, IEEE Access 11 (2023) 28628–28644, http://dx.doi.org/10.1109/ACCESS.2023.3260027.

[15] Manzoor Ahmed Hashmani, Syed Muslim Jameel, Syed Sajjad Hussain Rizvi, Saurabh Shukla, An adaptive federated machine learning-based intelligent system for skin disease detection: A step toward an intelligent dermoscopy device, Appl. Sci. (ISSN: 2076-3417) 11 (5) (2021) 2145, http://dx.doi.org/10.3390/app11052145.

[16] Yifan Li, Yuechen He, Yufei Fu, Sizhe Shan, Privacy preserved federated learning for skin cancer diagnosis, in: 2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications, ICPECA, 2023, pp. 27–33, http://dx.doi.org/10.1109/ICPECA56706.2023.10075862.

[17] Jeffry Wicaksana, Zengqiang Yan, Xin Yang, Yang Liu, Lixin Fan, Kwang-Ting Cheng, Customized federated learning for multi-source decentralized medical image classification, IEEE J. Biomed. Health Inform. 26 (11) (2022) 5596–5607, http://dx.doi.org/10.1109/JBHI.2022.3198440.

[18] Jie Wen, Zhixia Zhang, Yang Lan, Zhihua Cui, Jianghui Cai, Wensheng Zhang, A survey on federated learning: challenges and applications, Int. J. Mach. Learn. Cybern. (ISSN: 1868-808X) 14 (2) (2023) 513–535, http://dx.doi.org/10.1007/s13042-022-01647-y, URL https://doi.org/10.1007/s13042-022-01647-y.

[19] Shengju Qian, Yi Zhu, Wenbo Li, Mu Li, Jiaya Jia, What Makes for Good Tokenizers in Vision Transformer? IEEE Trans. Pattern Anal. Mach. Intell. (2022) 1–13, http://dx.doi.org/10.1109/TPAMI.2022.3231442.

[20] Jie Ma, Yalong Bai, Bineng Zhong, Wei Zhang, Ting Yao, Tao Mei, Visualizing and Understanding Patch Interactions in Vision Transformer, IEEE Trans. Neural Netw. Learn. Syst. (2023) 1–10, http://dx.doi.org/10.1109/TNNLS.2023.3270479.

[21] Kai Han, Yunhe Wang, Hanting Chen, Xinghao Chen, Jianyuan Guo, Zhenhua Liu, Yehui Tang, An Xiao, Chunjing Xu, Yixing Xu, Zhaohui Yang, Yiman Zhang, Dacheng Tao, A Survey on Vision Transformer, IEEE Trans. Pattern Anal. Mach. Intell. 45 (1) (2023) 87–110, http://dx.doi.org/10.1109/TPAMI.2022.3152247.

[22] Khalid Al-hammuri, Fayez Gebali, Awos Kanan, Ilamparithi Thirumarai Chelvan, Vision transformer architecture and applications in digital health: a tutorial and survey, Vis. Comput. Ind. Biomed. Art (ISSN: 2524-4442) 6 (1) (2023) 14, http://dx.doi.org/10.1186/s42492-023-00140-9.

[23] Suliman Aladhadh, Majed Alsanea, Mohammed Aloraini, Taimoor Khan, Shabana Habib, Muhammad Islam, An effective skin cancer classification mechanism via medical vision transformer, Sensors (ISSN: 1424-8220) 22 (11) (2022) 4008, http://dx.doi.org/10.3390/s22114008.

[24] Guang Yang, Suhuai Luo, Peter Greer, A novel vision transformer model for skin cancer classification, Neural Process. Lett. (ISSN: 1573-773X) (2023) http://dx.doi.org/10.1007/s11063-023-11204-5.

[25] Chao Xin, Zhifang Liu, Keyu Zhao, Linlin Miao, Yizhao Ma, Xiaoxia Zhu, Qiongyan Zhou, Songting Wang, Lingzhi Li, Feng Yang, Suling Xu, Haijiang Chen, An improved transformer network for skin cancer classification, Comput. Biol. Med. (ISSN: 0010-4825) 149 (2022) 105939, http://dx.doi.org/10.1016/j.compbiomed.2022.105939, URL https://www.sciencedirect.com/science/article/pii/S0010482522006746.

[26] Ahmed Afif Monrat, Olov Schelén, Karl Andersson, A survey of blockchain from the perspectives of applications, challenges, and opportunities, IEEE Access 7 (2019) 117134–117151, http://dx.doi.org/10.1109/ACCESS.2019.2936094.

[27] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, Andrew Lippman, MedRec: Using blockchain for medical data access and permission management, in: 2016 2nd International Conference on Open and Big Data, OBD, 2016, pp. 25–30, http://dx.doi.org/10.1109/OBD.2016.11.

[28] Thomas McGhin, Kim-Kwang Raymond Choo, Charles Zhechao Liu, Debiao He, Blockchain in healthcare applications: Research challenges and opportunities, J. Netw. Comput. Appl. (ISSN: 1084-8045) 135 (2019) 62–75, http://dx.doi.org/10.1016/j.jnca.2019.02.027, URL https://www.sciencedirect.com/science/article/pii/S1084804519300864.

[29] Mengfang Li, Yuanyuan Jiang, Yanzhou Zhang, Haisheng Zhu, Medical image analysis using deep learning algorithms, Front. Public Health (ISSN: 2296-2565) 11 (2023) http://dx.doi.org/10.3389/fpubh.2023.1273253, URL https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2023.1273253.

[30] Khaled Salah, M. Habib Ur Rehman, Nishara Nizamuddin, Ala Al-Fuqaha, Blockchain for AI: Review and open research challenges, IEEE Access 7 (2019) 10127–10149, http://dx.doi.org/10.1109/ACCESS.2018.2890507.

[31] Reza Shokri, Vitaly Shmatikov, Privacy-preserving deep learning, in: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, CCS '15, Association for Computing Machinery, New York, NY, USA, ISBN: 9781450338325, 2015, pp. 1310–1321, http://dx.doi.org/10.1145/2810103.2813687.

[32] Kang Wei, Jun Li, Ming Ding, Chuan Ma, Howard H. Yang, Farhad Farokhi, Shi Jin, Tony Q.S. Quek, H. Vincent Poor, Federated learning with differential privacy: Algorithms and performance analysis, IEEE Trans. Inf. Forensics Secur. 15 (2020) 3454–3469, http://dx.doi.org/10.1109/TIFS.2020.2988575.

[33] Zaobo He, Akshita Maradapu Vera Venkata Sai, Daehee Huang, Hanzhou Zhang, Qilong Han, Differentially private approximate aggregation based on feature selection, J. Comb. Optim. 41 (2021) http://dx.doi.org/10.1007/s10878-020-00666-1.

[34] Amjad Qashlan, Priyadarsi Nanda, Manoranjan Mohanty, Differential privacy model for blockchain based smart home architecture, Future Gener. Comput. Syst. (ISSN: 0167-739X) 150 (2024) 49–63, http://dx.doi.org/10.1016/j.future.2023.08.010.

[35] Opacus AI, 2023, URL https://opacus.ai. (Accessed 21 July 2023).

[36] Flower dev, 2023, URL https://flower.dev/. (Accessed 21 July 2023).

[37] HAM10000 dataset, 2023, URL https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/DBW86T. (Accessed 21 July 2023).

[38] Solid check, 2024, URL https://solidcheck.io/. (Accessed 16 July 2024).