

Deepfake detection and medical image authentication via a blockchain-integrated deep learning framework

Keshavmurthy Shankar Krupa¹, Kiran Chandrappa²

¹Department of Computer Science and Engineering (IoT and Cybersecurity including Blockchain), B.M.S College of Engineering affiliated to Visvesvaraya Technological University, Belagavi, India

²Department of Information Science and Engineering, Global Academy of Technology affiliated to Visvesvaraya Technological University, Belagavi, India

Article Info

Article history:

Received Sep 23, 2025

Revised Jul 30, 2026

Accepted Aug 12, 2026

Keywords:

Adversarial attack

Blockchain

Decentralized storage

Hybrid deep learning

Medical deepfake detection

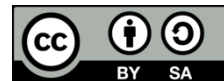
Medical image authenticity

Smart contracts

ABSTRACT

The recent advances in deepfake technologies have increased the risk of adversarial attacks on clinical content. The existing schemes towards image repositories are mostly designed considering a centralized system to store and verify medical images. However, they are susceptible to tampering and data breaches. This paper presents a blockchain-integrated deep learning (DL) framework for a secure and verifiable medical image authentication process. The first stage presents Efficient-vision-transformer (ViT), a hybrid learning model designed based on the joint approach of a convolutional EfficientNet model and vision transformers for detecting deepfake images. The second stage adopts a blockchain approach where the verified real images are subjected to hash computation and then stored on decentralized storage nodes using the interplanetary file system (IPFS). The experimental results showed an impressive detection accuracy of 99% by Efficient-ViT, and it is robust against various adversarial attacks. The blockchain module further ensures tamper-proofing, transparency, and long-term data integrity.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Keshavmurthy Shankar Krupa

Department of Computer Science and Engineering (IoT and Cybersecurity, including Blockchain)

B.M.S. College of Engineering affiliated to Visvesvaraya Technological University

Basavanagudi, Bengaluru, Karnataka 560019, India

Email: krupaks.csi@bmsce.ac.in

1. INTRODUCTION

Recent years have witnessed the potential of deep learning (DL) in many real-world applications, and in the context of the medical sector, it has improved the ability to analyze and interpret medical images, but it has also introduced new security challenges [1]. The recent developments in generative adversarial networks (GANs) and various image generation technologies enabled the generation of very realistic deepfake images that can mislead clinicians and medical experts, which can lead to compromised patient safety and erode confidence in the healthcare system [2], [3]. Meanwhile, the majority of modern solutions for managing medical images use centralized storage, thus exposing sensitive data to any manipulations, attacks, and security vulnerabilities [4]. Even though DL has become a widespread technology for detecting deepfakes, it does not ensure complete cybersecurity [5]. Hence, recent research works in the literature focus on combining DL with the technology of blockchain and decentralized storage [6], [7]. The adoption of decentralized data storage systems such as interplanetary file system (IPFS) that use multiple nodes to store data and make it free from any centralized control, thereby minimizing the chances of single-point failure [8]. However, creating a robust deepfake detection solution is difficult because most of them are vulnerable to adversarial attacks that may be created by the use of image processing attacks or using DL models [9].

Another challenge that emerges from the integration of deepfake detection systems with decentralization is the higher latency and operational costs. In addition, handling of large medical data or high-dimensional medical images in a decentralized manner is another challenge as it requires efficient protocols and data accessibility mechanisms [10].

From the perspective of related work, several research studies have been suggested to offer a robust countermeasure to deepfakes, but limited work has been done in the context of medical deepfakes. The work carried out by Karaköse *et al.* [11] applied a DL on knee X-ray and lung computed tomography (CT) datasets after preprocessing and augmentation, although results on CT scans were inconsistent due to the modality-specific limitations of the approach. Hsu *et al.* [12] developed a transformer-based predictive model incorporating adaptive prompt adjustment to address manipulation in the images. Waqas *et al.* [13] employed synthetic image generation using attention-enhanced generative models, which is effective but requires high computational resources. Ding *et al.* [14] suggested a dual-channel framework to mitigate adversarial perturbations in facial image-based biometric authentication applications. Mitra *et al.* [15] presented a proof-of-concept identity authentication system for smart cities by integrating encrypted cloud storage with a local verification scheme. Duan *et al.* [16] tried to address the detector generalization problem and presented a self-forgery adversarial training strategy to improve robustness against unseen manipulations. The deepfake detection approach using a multimodal approach is suggested by Shang *et al.* [17] for healthcare videos circulated on social media platforms. The research carried out by Xu *et al.* [18] utilized frequency and boundary enhancement blocks in the segmentation networks in order to enhance the detection of the tampered image region. A GAN based predictive model is developed by Zhang *et al.* [19] for facial edits generation. The study towards adopting a blockchain-based solution is seen in Lamas and Carames [20], where authors have combined SHA-256 hashing with blockchain immutability. Similarly, authors [21], [22] emphasized provenance tracing using ethereum and hyperledger fabric, respectively, towards offering proof-of-authenticity. Anitha *et al.* [23] used the Byzantine agreement protocol from Algorand to detect fraudulent users. Another work towards investigating regulatory policies associated with deepfakes in political and pornographic contexts is considered by Okolie [24], where the authors have identified and highlighted critical shortcomings of existing regulation policies. The use of blockchain to ensure security of medical records is seen in the study of Omar *et al.* [25], where integration of ethereum smart contracts with IPFS is carried out for clinical trials, while Madine *et al.* [26] suggested a blockchain-based framework for personal health records to enhance traceability and optimize user control. In a similar way, Mastoi *et al.* [27] used blockchain and watermarking for provenance and Heidari *et al.* [28] used blockchain and federated learning for deepfake detection and to ensure privacy in heterogeneous data.

The identified research gap is that existing studies mainly focus on either deepfake detection or secure storage, whereas an end-to-end framework integrating detection, storage, verification, and retrieval within a single system is still lacking. Another issue identified is that many DL based approaches either lack scalability due to computational overhead or show limited generalization in adversarial scenarios. On the other hand, existing blockchain-based frameworks are often found to be mostly theoretical, as much focus is given on domains outside clinical imaging, and very few works have integrated these two paradigms into a unified system for medical image authentication.

The proposed system aims to present a blockchain-integrated DL framework for deepfake detection and decentralized medical imaging authentication. The proposed study presents a hybrid DL approach for modelling a defensive deepfake detector based on a joint approach of EfficientNet and vision-transformer (ViT). Another contribution made is the incorporation of blockchain technology as a supporting infrastructure that ensures all activities related to deepfake detection are traceable, tamper-evident, and verifiable. The core and novel contribution of the proposed research work is highlighted as follows viz. i) development of a hybrid DL model by integrating EfficientNet for feature extraction with ViT for contextual learning to improve deepfake pattern extraction from input medical images; ii) incorporation of an advanced adversarial training strategy to make the model robustness against evolving forgery techniques and unseen deepfake manipulations; and iii) adoption of blockchain and smart contracts towards achieving secure, decentralized, and tamper-proof framework.

2. METHOD

The prime aim of the proposed research work is to develop an efficient framework using advanced predictive model with blockchain technology to combat deepfake attacks in medical imaging. The proposed methodology involves secure storage, metadata logging with tamper-proof, and decentralized image classification using ethereum and IPFS. Unlike conventional approaches, the proposed model facilitates both maximized detection accuracy as well as data integrity with end-to-end security in authenticating medical images. Figure 1 illustrates a schematic architecture of the proposed model, which consists of four main

modules viz. i) image preprocessing and deepfake detection, ii) adversarial training, iii) decentralized storage through IPFS, and iv) blockchain-based verification. The modelling and implementation of the proposed system are carried out in an integrated manner and are highly synchronous to operate together to preserve the authenticity and integrity of medical images.

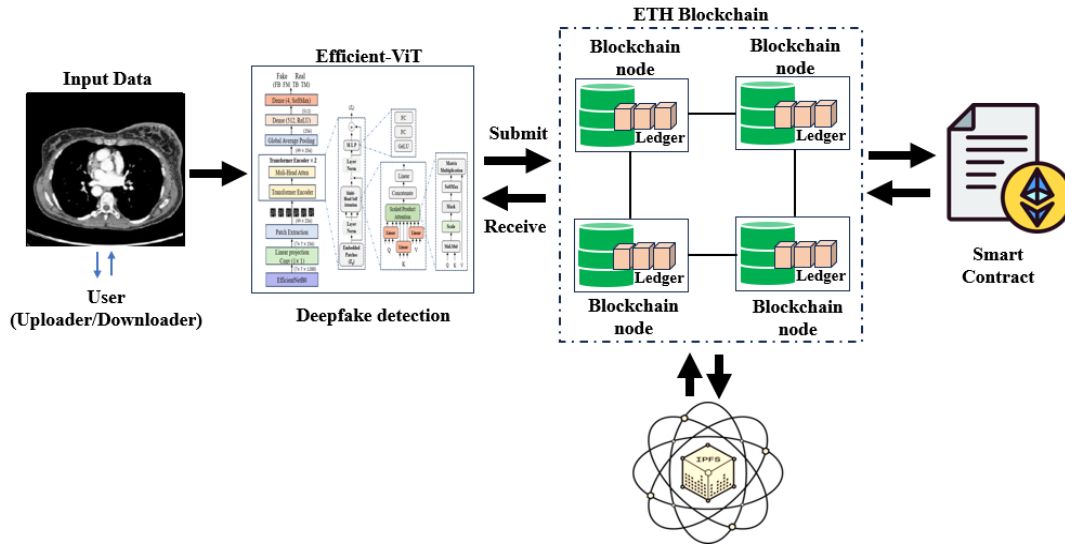


Figure 1. The workflow of the proposed system

The input to the proposed system is the medical images uploaded by a user, such as a doctor, radiologist, or medical researcher. The proposed hybrid model, Efficient-ViT deepfake detector, then verifies it to ensure the medical image is real or tampered with. The Efficient-ViT model extracts spatial and contextual features to classify the image as either authentic or deepfake. Afterwards, a hash function using the SHA-256 algorithm is calculated for those images that have been classified as authentic. The generated hash value serves as the digital signature of the image for later verification. The next process involves uploading authentic medical images to the IPFS network, where the images are divided into many chunks and stored on different computing nodes which further provides a content identifier (CID) for every file. As the CID depends on the content of the file, any change in the image will give rise to a different CID. To reduce the storage burden of the blockchain while ensuring that the image is verifiable, CID, hash of the image, detection outcome, timestamp, and uploader identity are saved onto the ethereum blockchain through the use of Solidity smart contracts. Once the metadata is uploaded on the blockchain, it becomes immutable and cannot be altered or removed. In order to retrieve the image, the CID saved in the blockchain is used to access the image from IPFS nodes. In case of matching hashes, it shows that the image is authentic, and in case if it mismatches then it is flagged as potential tampering of images. This authentication process will ensure that the end-to-end image integrity is maintained and transparency is achieved, which helps clinicians and other stakeholders authenticate medical images.

2.1. Hybrid Efficient-ViT detection

This module of the proposed system utilizes a hybrid learning model based on the integration of Efficient and ViT to detect whether the input medical images are authentic or deepfake. Firstly, the input images are resized to 224×224 pixels and then processed using a Gaussian filter to eliminate image noise, followed by intensity normalization to scale the pixel values within a standard range. After preprocessing, the images are subjected to the proposed Efficient-ViT hybrid model, which combines EfficientNet for multi-scale spatial feature extraction and the ViT model for capturing global contextual relationships through self-attention mechanisms [29]. Once classification is complete, each image is assigned an authenticity label along with a SHA-256 cryptographic hash, which serves as a unique digital fingerprint for later verification. To ensure robustness of the proposed deepfake detection model, an adversarial training strategy is integrated into the hybrid model, as deepfake generation methods continue to evolve and often bypass conventional detectors. In this process, manipulated images with latent or unnoticeable perturbations are generated and included during training. This process makes the model learn from a wider range of forgeries to further strengthen its ability to generalize across unseen manipulations. As a result, the detection model becomes less

vulnerable to adversarial attacks and performs reliably under dynamic conditions. Algorithm 1 illustrates the procedure adopted in deepfake detection in medical images.

Algorithm 1. Image preprocessing and deepfake detection

Input: Medical image dataset $D = \{I_1, I_2, \dots, I_n\}$
Output: Authenticity labels $L = \{l_1, l_2, \dots, l_n\}$, Image hashes $H = \{h_1, h_2, \dots, h_n\}$

1. For each image $I_i \in D$:
 - # Preprocessing Phase
 - 3. Resize I_i to fixed resolution $R \times R$
 - 4. Apply Gaussian filtering to reduce noise
 - 5. Normalize pixel values of I_i to range $[0, 1]$
 - # Deepfake Detection Phase
 - 9. Divide I_i into patches $P_i = \{p_1, p_2, \dots, p_k\}$
 - 10. Embed each patch into feature vectors E_i using the Efficient-ViT embedding layer
 - 11. Apply multi-head self-attention to extract contextual features F_i
 - 12. Feed F_i through transformer layers for representation learning
 - 13. Predict authenticity label $l_i = \text{classify}(F_i)$
 - # Hash Generation
 - 16. Compute the SHA-256 hash h_i for I_i
 - 17. Store (I_i, l_i, h_i) for further blockchain logging
18. Return L, H

2.2. Decentralized storage with interplanetary file system

The storage of the medical data on centralized storage often vulnerable to security risks like unauthorized access, alterations, and single points of failure. In order to mitigate such issues, the proposed framework incorporates the IPFS, which is a peer-to-peer distributed storage system that ensures a decentralized storage mechanism which is immutable, and scalable [30]. The complete implementation procedure is discussed in Algorithm 2. The implementation of IPFS preserves the immutability of medical images and allows verifying information while meeting privacy requirements for medical applications. Once an image is verified by the detection module, it is stored securely in the IPFS network. During this process, the image is divided into smaller data chunks and distributed across multiple peer nodes.

Algorithm 2. Decentralized storage using IPFS and blockchain

Input: D' (Verified image), L (Authenticity Label) and H (Image hash)
Output: CID and T (Transaction Id)

Steps

1. For each verified Image $I_i \in D'$
 - # IPFS Upload Phase
 - 2. Upload I_i to the IPFS network
 - 3. Generate CID
 - $cid_i = H(I_i)$, where $H = \text{SHA-256 hashing}$
 - 4. Store cid_i locally for blockchain logging
 - # Blockchain Logging Phase
 - 5. Prepare metadata packet M_i containing:
 - $M_i = \{cid_i, h_i, l_i, ts_i\}$, where ts_i is the current timestamp.
 - 6. Call the Ethereum smart contract.
 - $t_i = SC.\text{store}(cid_i, h_i, l_i, ts_i)$
 - 7. Save t_i for future verification
 - 8. Return the sets CID and T

End

A unique CID is generated using SHA-256 hashing, which serves as a reference for retrieval and verification, and any change in the original image leads to a different CID, thereby allowing instant detection of tampering. To ensure better scalability features, the system does not store full image data on the blockchain. Instead, only the CID and related metadata, such as the hash, authenticity label, timestamp, and uploader identity, are recorded using ethereum smart contracts. This record storage approach reduces on-chain storage requirements, thereby preserving traceability and auditability.

2.3. Blockchain-based verification

This module of the proposed system is developed using ethereum blockchain [31] which is responsible for securely recording the metadata associated with each input medical image. This module also contains a smart contract developed in Solidity to store essential information, such as SHA-256 hash, CID, classification result, timestamp, and uploader identity. Once all this information is recorded on ethereum blockchain, it is impossible to delete or change it. Here, the smart contract acts as a secure and transparent ledger for validating the authenticity of medical images. After an image is successfully classified and stored

in IPFS, the corresponding metadata is submitted as a blockchain transaction. The smart contract stores the received data permanently on the blockchain and triggers an event after successfully storing the data. In the verification process, an authorized user retrieves the metadata stored in the blockchain and the stored hash value is then compared with the new hash value generated for the image. If both hash values are the same, the image will be considered legitimate; otherwise, it will be considered tampered. The process adopted for integrating blockchain and smart contracts is discussed in Algorithm 3.

Algorithm 3. Blockchain and smart contract integration

Input: CID from IPFS, SHA-256 hash, deepfake detection result, uploader address

Output: Immutable blockchain record for medical image authenticity

1. Initiate the verification process after successful deepfake detection and IPFS upload.
2. Collect metadata: {CID, image-hash, detection-result, uploader-address, and timestamp}.
3. Initiate a transaction to the deployed Ethereum smart contract.
4. Execute the adding record:
 - Pass metadata as arguments.
 - Store data immutably on the blockchain ledger.
5. Generate an event RecordAdded to confirm successful logging.
6. Verify authenticity:
 - Retrieve stored metadata.
 - Compare the stored image-hash with a newly computed hash.
 - If hashes match → Image is authentic; otherwise → Tampering detected.

End of process

2.4. Use case scenario

To demonstrate the real-world applicability of the proposed system, this section presents a use case scenario from a healthcare environment where medical images must be securely stored, verified, and retrieved with guaranteed authenticity. The scenario involves interactions between medical professionals, such as doctors and radiologists, and the system through a web or desktop interface. The process starts with a user uploader or downloader, such as a doctor, radiologist, or patient, who accesses the web or desktop interface to upload a medical image. This interface acts as the primary entry point for interacting with the system and initiates the verification workflow. The image is uploaded; the system generates a cryptographic hash as a unique digital fingerprint for the image, ensuring that even the slightest alteration in the file would result in a completely different hash value. The hashed image is then analyzed using the Efficient-ViT deepfake detection model. The model processes the medical image to determine its authenticity. If the image is uploaded successfully, it is stored on IPFS and generates a CID, which acts as a secure and permanent reference to the image's location within the decentralized storage network. Instead of storing the entire image on the blockchain, the system stores essential metadata using a smart contract deployed on the local ethereum blockchain and the stored metadata is linked with a local database for quick retrieval and indexing. Using this CID, the original image is fetched from IPFS, and the hash is recomputed to ensure its integrity. If the recomputed hash matches the one stored on the blockchain, the image is verified as authentic. Figure 2 highlights the taxonomy diagram summarizing the proposed system, which is based on the adopted use-case scenario.

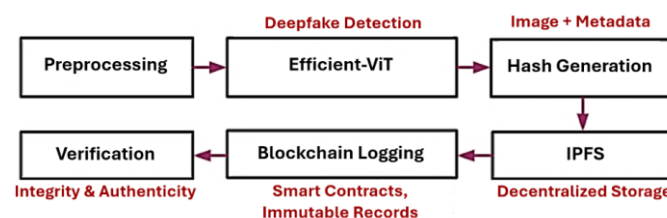


Figure 2. Taxonomy diagram of proposed study

3. RESULTS AND DISCUSSION

All experiments were conducted in Python using the Anaconda environment on a Windows 11 system equipped with 16 GB RAM and an NVIDIA GPU with 6 GB VRAM. The DL model used EfficientNetB0, pretrained on ImageNet, as the backbone for feature extraction. The network architecture included a patch conversion layer using Conv2D with 256 filters, followed by two transformer blocks with four attention heads and a feed-forward network (FFN) of size 128. The classifier head consisted of a dense

layer with 512 rectified linear unit (ReLU) units, a dropout layer with a rate of 0.2, and a final softmax layer for classification. The model was trained using categorical cross-entropy loss and the Adam optimizer. The batch size considered was 32; regularization was applied using dropout along with batch normalization to avoid overfitting and improve generalization. The training of the predictive model was carried out for 30 epochs. The implementation of the blockchain module was done via Ganache framework, where simulation of the local Ethereum network was carried out and wallet management was achieved using MetaMask. Smart contracts were written in Solidity and compiled using an open-source. The connection between the DL model, IPFS, and blockchain was made using Web3 technology. The input medical images which are confirmed as genuine, were stored in IPFS, while associated metadata were permanently recorded on the blockchain. The validation of the proposed framework is done on the deepfake CT dataset [32], which consist of both genuine and manipulated CT images created using the CT-GAN model through addition and removal of lung nodules. The experimental process is done on total of 4,800 images, out of which 3,600 images were used for training, 400 images for validation, and 800 images for testing. The performance of the proposed framework is analyzed considering various performance parameters such as accuracy, F1-score, latency, and gas price evaluated under both normal and adversarial conditions.

3.1. Performance analysis of the Efficient-ViT model for deepfake detection

Figure 3 presents a visual comparison of the original medical image and its adversarially modified versions to evaluate the robustness of the proposed Efficient-ViT framework. Figure 3(a) shows the original medical image without any form of perturbation and represents the baseline input to the system. Figure 3(b) shows the same image after the application of the fast gradient sign method (FGSM) adversarial attack, which introduces targeted noise patterns to influence the classification outcome. Figure 3(c) shows the image influenced by the projected gradient descent (PGD) attack [33], where stronger and iterative perturbations are applied to further challenge the model prediction process.

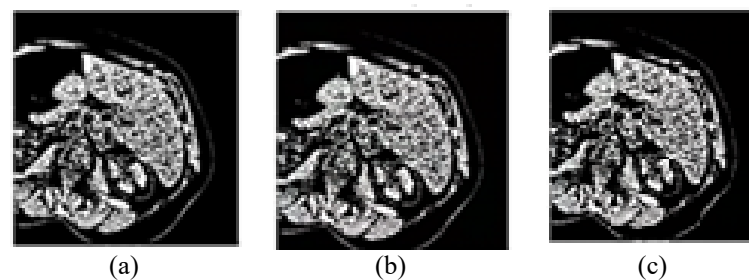


Figure 3. Visual outcomes of the model showing (a) original image, (b) image influenced with FGSM attack, and (c) image influenced with PGD attack

From the visual analysis, it can be observed that perturbations introduced in Figures 3(b) and 3(c) create noticeable distortions that allow the modified images to be identified as different from the original through the human visual system. Such perturbations create a challenge for systems that are trained only for disease recognition without adversarial awareness. However, the experimental outcomes show that the proposed Efficient-ViT model maintains correct class labels with higher confidence scores even under adversarial conditions. This behaviour confirms that the model remains reliable for clinical image authentication and resists manipulation attempts effectively. In addition, the performance evaluation against the PGD attack highlights the ability of the proposed model to handle stronger and iterative noise patterns. The results show that accurate predictions are retained for all four classes, which further confirms the resilience of the Efficient-ViT framework against advanced adversarial manipulation strategies. Table 1 presents quantified numerical outcomes for assessing the overall classification performance of the proposed model for different evaluation scenarios. It can be seen that, on the original test set, the model achieved 99% accuracy, with macro-averaged precision, recall, and F1-scores also reaching 99%. Under the synthetic test set generated by the stable diffusion model, the performance dropped slightly to 98% accuracy, with macro precision, recall, and F1-score of 97%. However, this performance degradation is considerable, as the proposed method still maintains an acceptable range of accuracy and F1-score. Similar analysis can also be made of the other test cases, which suggests that the Efficient-ViT hybrid model maintains high detection reliability for dynamic conditions and highlights its suitability for secure medical image authentication in real-world scenarios.

Table 1. Performance of the proposed Efficient-ViT model under dynamic adversarial test scenarios

Test scenario	Accuracy	Macro precision	Macro recall	Macro F1-score
Original test set	0.99	0.99	0.99	0.99
Synthetic test set (stable diffusion)	0.98	0.97	0.97	0.97
PGD adversarial test set	0.98	0.98	0.98	0.98
FGSM adversarial test set	0.99	0.99	0.99	0.99

3.2. Performance analysis of blockchain model

The logging latency of the suggested blockchain-based system was compared against a traditional centralized database to determine the performance in terms of system execution time. The obtained outcome reported in Table 2 shows that the centralized database takes approximately 0.03 seconds to execute every transaction. However, the proposed blockchain-based system takes about 1.7 - 2.3 seconds to execute every transaction owing to consensus validation, transaction confirmation, and execution of smart contracts. Despite extra execution time taken by blockchain, it offers immutable and tamper-resistant data recording.

Table 2. Latency comparison between centralized database and the blockchain framework

Number of logs	Centralized DB latency (s)	Blockchain latency (s)
100	0.0298	1.6722
300	0.0270	1.6999
500	0.0283	2.2868
700	0.0461	2.1453
900	0.0389	1.8514

The performance analysis in terms of gas usage is conducted to estimate the execution costs of blockchain transactions in the ethereum virtual machine (EVM). The obtained average gas usage is presented in Table 3 for various volumes of transactions. It can be seen from the results that smaller amounts of transactions (100 logs) had higher gas usage per transaction compared to larger amounts (200 logs) due to batch processing benefits. However, gas usage variability grew with the growth of transaction amount due to smart contracts' execution complexity.

Table 3. Average gas usage for blockchain transactions

Transactions	Average gas used
100	33,281
200	30,762
300	40,013
400	46,625
500	40,821

The performance of the proposed methodology is also assessed in terms of retrieval time for images based on the size of files. As illustrated in Figure 4, the initial retrieval time for bigger images (5 - 10 MB) was higher as the information needed to be accessed from the distributed IPFS nodes. However, the subsequent retrieval was faster since the data was stored locally. The outcome findings suggest that, even though the process of decentralization leads to additional time in the first access, later access will be more efficient, and such a tendency is positive in the medical context.

3.3. Comparison with other deepfake detection models

The theoretical comparison of the proposed framework has been done with respect to the existing deepfake detection algorithms to provide a contextual assessment of its applicability and performance. Table 4 highlights the comparison that emphasizes multiple attributes necessary to gauge the performance of all models. The overall outcome of the observation in this table shows that Efficient-ViT offers prominent advantages in contrast to transformer-only models, ResNet, and CT-GAN on the same medical image dataset.

The outcome shown in the above tabulated data shows the extent of potential associated with transformer architectures balances with that of convolution networks for accomplishing better deepfake detection in medical images. Different from CT-GAN [34], which essentially emphasizes synthesis of an image rather than identification, the proposed transformer model is developed towards classification, while it exhibits improved resiliency against adversarial intruders via adversarial training and hybrid design. A moderate range of robustness with a potential baseline of CNN is provided by ResNet, where the capability to encapsulate long-range dependencies. A potential attention mechanism is facilitated by transformer-only

models; however, it is usually associated with reduced optimization and maximized computational cost. It is also seen that the proposed model distinctly combines blockchain technology towards tamper-proof and secure logging towards metadata detection. Therefore, the adopted structure of the proposed model offers more suitability towards real-world and secure authentication of medical images.

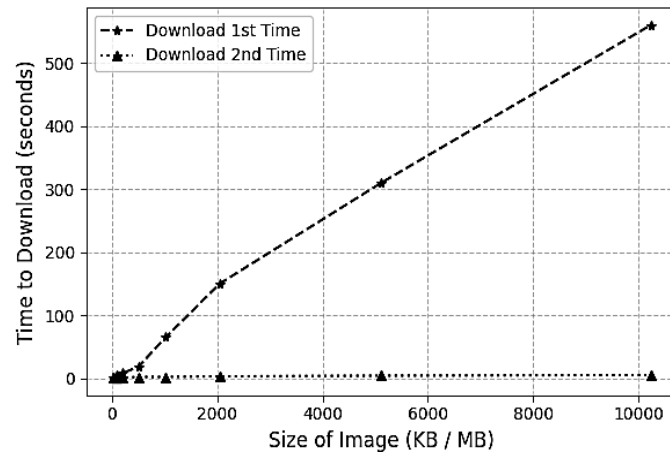


Figure 4. Analysis of download time versus image size

Table 4. Theoretical benchmarking of Efficient-ViT against prior deepfake detection models

Attribute	Efficient-ViT	CT-GAN	ResNet	Transformer-only
Architecture type	Hybrid CNN with transformer	Image synthesis using GAN	Deep network using CNN	Pure transformer model
Feature extraction	EfficientNetB0 backbone with transformer blocks	Fake images for augmentation generated by GAN	Deep residual CNN layers	Multi-head self-attention
Robustness to adversarial attacks	High	Low to moderate	Moderate	Moderate to high
Computational complexity	Moderate	High	Moderate	High
Interpretability	Moderate	Low	Moderate	Moderate
Integration with blockchain	Fully integrated	Not typically integrated	Rarely integrated	Rarely integrated
Suitability for medical imaging	High	Moderate	High	Moderate

4. CONCLUSION

This research study presented an integrated framework based on the joint approach of DL based predictive model and a blockchain technique to tackle deepfakes in medical images. A hybrid Efficient-ViT model is developed using an adversarial training approach, which improved its robustness against unseen or adversarially generated deepfakes. Blockchain technology is used to store the image metadata in an immutable ledger so that records cannot be modified, and it also supports verification and auditability. In addition, IPFS is utilized to store the actual medical images in a decentralized manner. The experimental results showed that the framework can detect deepfake medical images as well as authenticate them using blockchain. Nevertheless, the integration of blockchain added an extra layer of computational complexity and transaction latency to the framework. In the future, the proposed framework will be extended to enhance computational efficiency and reduce the cost of blockchain transactions and storage. Also, it will be optimized to support multiple medical imaging modalities and deploy federated learning into the framework.

FUNDING INFORMATION

The authors state no funding is involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Keshavmurthy Shankar Krupa	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Kiran Chandrappa		✓				✓		✓	✓	✓	✓	✓		

C : ConceptualizationI : InvestigationVi : Visualization

M : MethodologyR : ResourcesSu : Supervision

So : SoftwareD : Data CurationP : Project administration

Va : ValidationO : Writing - Original DraftFu : Funding acquisition

Fo : Formal analysisE : Writing - Review & Editing

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, [KSK], upon reasonable request.

REFERENCES

[1] M. Li, Y. Jiang, Y. Zhang, and H. Zhu, "Medical image analysis using deep learning algorithms," *Frontiers in Public Health*, vol. 11, Nov. 2023, doi: 10.3389/fpubh.2023.1273253.

[2] R. Babaei, S. Cheng, R. Duan, and S. Zhao, "Generative artificial intelligence and the evolving challenge of deepfake detection: a systematic analysis," *Journal of Sensor and Actuator Networks*, vol. 14, no. 1, Feb. 2025, doi: 10.3390/jsan14010017.

[3] K. Kazuhiro *et al.*, "Generative adversarial networks for the creation of realistic artificial brain magnetic resonance images," *Tomography*, vol. 4, no. 4, pp. 159–163, Dec. 2018, doi: 10.18383/j.tom.2018.00042.

[4] M. Eichelberg, K. Kleber, and M. Kämmerer, "Cybersecurity in PACS and medical imaging: an overview," *Journal of Digital Imaging*, vol. 33, no. 6, pp. 1527–1542, Dec. 2020, doi: 10.1007/s10278-020-00393-3.

[5] G. Petmezas, V. Vanian, K. Konstantoudakis, E. E. I. Almaloglou, and D. Zarpalas, "Video deepfake detection using a hybrid CNN-LSTM-Transformer model for identity verification," *Multimedia Tools and Applications*, vol. 84, no. 33, pp. 40617–40636, Mar. 2025, doi: 10.1007/s11042-024-20548-6.

[6] N. Choi and H. Kim, "DDS: deepfake detection system through collective intelligence and deep-learning model in blockchain environment," *Applied Sciences*, vol. 13, no. 4, Feb. 2023, doi: 10.3390/app13042122.

[7] M. B. E. Islam, M. Haseeb, H. Batool, N. Ahtasham, and Z. Muhammad, "AI threats to politics, elections, and democracy: a blockchain-based deepfake authenticity verification framework," *Blockchains*, vol. 2, no. 4, pp. 458–481, Nov. 2024, doi: 10.3390/blockchains2040020.

[8] S. Kumar, A. K. Bharti, and R. Amin, "Decentralized secure storage of medical records using blockchain and IPFS: A comparative analysis with future directions," *Security and Privacy*, vol. 4, no. 5, Sep. 2021, doi: 10.1002/spy2.162.

[9] A. A. Khan, A. A. Laghari, S. A. Inam, S. Ullah, M. Shahzad, and D. Syed, "A survey on multimedia-enabled deepfake detection: state-of-the-art tools and techniques, emerging trends, current challenges; limitations, and future directions," *Discover Computing*, vol. 28, no. 1, Apr. 2025, doi: 10.1007/s10791-025-09550-0.

[10] S. Xu, X. Yang, and Z. Xie, "The future of misinformation control: integrating advanced algorithms and blockchain for effective Deepfake detection," *Peer-to-Peer Networking and Applications*, vol. 18, no. 4, Jul. 2025, doi: 10.1007/s12083-025-02048-y.

[11] M. Karaköse, H. Yetiş, and M. Çeçen, "A new approach for effective medical deepfake detection in medical images," *IEEE Access*, vol. 12, pp. 52205–52214, 2024, doi: 10.1109/ACCESS.2024.3386644.

[12] C.-C. Hsu, M.-Y. Tsai, and C.-M. Yu, "Securing healthcare data integrity: deepfake detection using autonomous AI approaches," *IEEE Journal of Biomedical and Health Informatics*, pp. 1–13, 2025, doi: 10.1109/JBHI.2025.3586963.

[13] N. Waqas, S. I. Safie, K. A. Kadir, S. Khan, and M. H. Kaka Khel, "Deepfake image synthesis for data augmentation," *IEEE Access*, vol. 10, pp. 80847–80857, 2022, doi: 10.1109/ACCESS.2022.3193668.

[14] F. Ding *et al.*, "Securing facial bioinformation by eliminating adversarial perturbations," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 5, pp. 6682–6691, May 2023, doi: 10.1109/TII.2022.3201572.

[15] A. Mitra, D. Bigioi, S. P. Mohanty, P. Corcoran, and E. Kougianos, "iFace 1.1: a proof-of-concept of a facial authentication based digital ID for smart cities," *IEEE Access*, vol. 10, pp. 71791–71804, 2022, doi: 10.1109/ACCESS.2022.3187686.

[16] H. Duan *et al.*, "Adversarial samples generated by self-forgery for face forgery detection," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 7, no. 3, pp. 432–443, Jul. 2025, doi: 10.1109/TBIOM.2025.3529026.

[17] L. Shang, Y. Zhang, Y. Deng, and D. Wang, "MultiTec: a data-driven multimodal short video detection framework for healthcare misinformation on TikTok," *IEEE Transactions on Big Data*, vol. 11, no. 5, pp. 2471–2488, Oct. 2025, doi: 10.1109/TBDATA.2025.3533919.

[18] X. Xu, W. Lv, W. Wang, Y. Zhang, and J. Chen, "Empowering semantic segmentation with selective frequency enhancement and attention mechanism for tampering detection," *IEEE Transactions on Artificial Intelligence*, vol. 5, no. 6, pp. 3270–3283, Jun. 2024, doi: 10.1109/TAI.2023.3347178.

[19] L. Zhang, X. Pan, H. Yang, and L. Li, "On Open-Set, high-fidelity and identity-specific face transformation," *IEEE Access*, vol. 8, pp. 224643–224653, 2020, doi: 10.1109/ACCESS.2020.3044187.

[20] P. F.-Lamas and T. M. F.-Carames, "Fake news, disinformation, and deepfakes: leveraging distributed ledger technologies and blockchain to combat digital deception and counterfeit reality," *IT Professional*, vol. 22, no. 2, pp. 53–59, Mar. 2020, doi: 10.1109/MITP.2020.2977589.

- [21] H. R. Hasan and K. Salah, "Combating deepfake videos using blockchain and smart contracts," *IEEE Access*, vol. 7, pp. 41596–41606, 2019, doi: 10.1109/ACCESS.2019.2905689.
- [22] C. C. K. Chan, V. Kumar, S. Delaney, and M. Gochoo, "Combating deepfakes: multi-LSTM and blockchain as proof of authenticity for digital media," in *2020 IEEE/ITU International Conference on Artificial Intelligence for Good (AI4G)*, IEEE, 2020, pp. 55–62, doi: 10.1109/AI4G50087.2020.9311067.
- [23] S. Anitha, N. Anitha, N. Ashok, T. Daranya, B. Nandhini, and V. Chandrasekaran, "Detection of deepfakes in financial transactions using algorand blockchain consensus mechanism," in *Proceedings of International Conference on Network Security and Blockchain Technology (ICNSBT 2023)*, 2024, pp. 173–183, doi: 10.1007/978-981-99-4433-0_15.
- [24] C. Okolie, "Artificial intelligence-altered videos (deepfakes), image-based sexual abuse, and data privacy concerns," *Journal of International Women's Studies*, vol. 25, no. 2, 2023.
- [25] I. A. Omar, R. Jayaraman, K. Salah, M. C. E. Simsekler, I. Yaqoob, and S. Ellahham, "Ensuring protocol compliance and data transparency in clinical trials using Blockchain smart contracts," *BMC Medical Research Methodology*, vol. 20, no. 1, Dec. 2020, doi: 10.1186/s12874-020-01109-5.
- [26] M. M. Madine *et al.*, "Blockchain for giving patients control over their medical records," *IEEE Access*, vol. 8, pp. 193102–193115, 2020, doi: 10.1109/ACCESS.2020.3032553.
- [27] Q.-A. Mastoi *et al.*, "Enhancing deepfake content detection through blockchain technology," *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 6, 2025, doi: 10.14569/IJACSA.2025.0160607.
- [28] A. Heidari, N. J. Navimipour, H. Dag, S. Talebi, and M. Unal, "A novel blockchain-based deepfake detection method using federated and deep learning models," *Cognitive Computation*, vol. 16, no. 3, pp. 1073–1091, May 2024, doi: 10.1007/s12559-024-10255-7.
- [29] M. Hayat, N. Ahmad, A. Nasir and Z. A. Tariq, "Hybrid deep learning efficientNetV2 and vision transformer (EffNetV2-ViT) model for breast cancer histopathological image classification," in *IEEE Access*, vol. 12, pp. 184119–184131, 2024, doi: 10.1109/ACCESS.2024.3503413.
- [30] M. B. Saif, S. Migliorini, and F. Spoto, "Efficient and secure distributed data storage and retrieval using interplanetary file system and blockchain," *Future Internet*, vol. 16, no. 3, 2024, doi: 10.3390/fi16030098.
- [31] A. Urquhart, "Under the hood of the ethereum blockchain," *Finance Research Letters*, vol. 47, 2022, doi: 10.1016/j.frl.2021.102628.
- [29] "Deepfakes: medical image tamper detection," UC Irvine Machine Learning Repository, 2020, doi: 10.24432/C5J318.
- [33] Z. Zhu, Y. Zhang, A. Ye, X. Wang, C. Wang, and T. Zhu, "Adaptive reinforcement learning based projected gradient descent attack," *The Journal of Supercomputing*, vol. 82, no. 10, 2026, doi: 10.1007/s11227-026-08687-z.
- [34] R. Patole and G. Dhopavkar, "CT-GAN: a cross-modal transformer GAN for superior multi-modal MRI-based Alzheimer's disease detection," *2025 International Conference on Sustainability, Innovation & Technology (ICSIT)*, 2025, pp. 1–7, doi: 10.1109/ICSIT65336.2025.11293880.

BIOGRAPHIES OF AUTHORS



Prof. Keshavmurthy Shankar Krupa     is currently serving as an assistant professor in the Department of Computer Science and Engineering at BMS College of Engineering, Bengaluru, India. She received her Bachelor of Engineering and Master of Technology degrees in Computer Science and Engineering from Visvesvaraya Technological University, Belagavi, Karnataka, India. Her research interests include artificial intelligence and machine learning (AI/ML), cybersecurity, internet of things (IoT), and blockchain technology. She has presented her work at several international conferences and published in peer-reviewed journals. She can be contacted at email: krupaks.csi@bmsce.ac.in.



Dr. Kiran Chandrappa     is currently serving as professor and head of the Department of Information Science and Engineering at Global Academy of Technology, Bengaluru, India. He received his Bachelor of Engineering from Kuvempu University, Master of Technology degree from Visvesvaraya Technological University, Belagavi, and Ph.D. from Jain University, Bengaluru, Karnataka, India. His research interests include computer vision, image processing, AI ML, and blockchain technology. He has contributed to the academic community by publishing articles at various international conferences and peer-reviewed journals. He can be contacted at email: kiranchandrappa@gmail.com.