2025 International Conference on Intelligent Communication Networks and Computational Techniques (ICICNCT)

A Hybrid Blockchain and Convolutional Neural Network for Secure Cloud-Assisted Medical Image Analysis

1st Raed Hameed
Department of Computers Techniques Engineering
College of Technical Engineering, The Islamic University
Najaf, Iraq
raedalabedy@iunajaf.edu.iq

2nd Mohan Kumar. T G
Department of Information Science and Engineering
Nitte Meenakshi Institute of Technology, Nitte (Deemed to be University)
Bengaluru, India
mohankumar.tg@nmit.ac.in

3rd Narendra Chennupati
Independent Researcher
Frisco, TX, USA
chennupati.be@gmail.com

4th Preethi Varthini. S
Department of Artificial intelligence and Data Science
Dhanalakshmi Srinivasan College of Engineering and Technology
Mamallapuram, India
preethivarthinis.aids@dscet.ac.in

5th Vinny Kuriakose
Department of Biomedical Engineering
Dhanalakshmi Srinivasan Engineering College
Coimbatore, India
vinnyjijo22@gmail.com

2025 International Conference on Intelligent Communication Networks and Computational Techniques (ICICNCT) | 979-8-3315-8623-2/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICICNCT66124.2025.11232809

***Abstract*—In recent years, securing medical images in the cloud has become essential owing to the rapid accumulation of Computed Tomography (CT), Magnetic Resonance Imaging (MRI), and ultrasound data from hospitals, diagnostic centers, and IoMT-enabled devices. However, the Customizable Unique Node Access (CUNA)-based deep encryption model has limited scalability, verifiable provenance, and lacked advanced analytics for accurate medical interpretation. To overcome these limitations, this research proposes a hybrid Blockchain and Convolutional Neural Network (B-CNN) model for secure cloud-assisted medical image processing. Initially, data is collected from medical imaging devices integrated with hospital information systems and sensors. Preprocessing at the edge nodes then performs normalization of image dimensions, anonymization of patient identifiers, denoising, and metadata generation. Encrypted medical data are stored off-chain, whereas a permissioned blockchain records immutable hashes, access policies, and consent. A CNN–transformer hybrid network extracts spatial features through convolutional layers and global context from transformer encoders and then combines them for accurate classification to enhance scalability, security, diagnostic precision, and trust in cloud healthcare systems. The experimental results demonstrated that the proposed B-CNN model outperformed the existing CUNA model in terms of accuracy (93.23%).**

Keywords—blockchain, cloud healthcare systems, convolutional neural network, medical image processing, secure cloud-assisted.

I. INTRODUCTION

In recent years, the rapid development of digital healthcare and the widespread penetration of medical imaging modalities have generated significant amounts of sensitive clinical data in need of secure storage, efficient processing, and accurate diagnosis reading. Medical imaging modalities include Computed Tomography (CT), Magnetic Resonance Imaging (MRI), ultrasound, X-ray, and digital pathology [1]. With increasing reliance on healthcare cloud infrastructure, healthcare professionals have instant scalable storage. Also, higher levels of performance through High-Performance Computing (HPC) platforms, and numerous Artificial Intelligence (AI) algorithms on cloud infrastructure to assist in analyzing medical images in real time [2]. The embedded security of sensitive patient data in cloud environments and the corresponding challenges in implementing security practices, policies, and governance mandate pressing steeping and scaling in terms of security, privacy, and trusting cloud computing systems to manage sensitive patient data [3]. Medical data are very sensitive in nature and desirable for the potential exploitation of cyber-attackers, especially where there is a high volume of sensitive patient data. Centralized storage in traditional approaches to manage data risk defaults patient data management to a level of non-guarantee, non-auditable, and no trust [4]. Medical data management focused on privacy and accountability is currently constrained to three main approaches: encryption mechanisms, federated learning frameworks, and blockchain-supported audit trials [5]. These approaches offer different levels of privacy-preserving and accountable medical data management, but still provide limited scalability and latency issues, and do not consider the heterogeneous nature of the healthcare system. Neural Networks (NNs) are used effectively to learn spatial features in medical images [6]. The major challenges in acquiring long-range contextual dependencies when developing models for complex diagnostic tasks include analyzing tumor progression and multi-organ disease detection.

Moreover, automatic feature identification and contextual analysis tasks provided by transformer-based architectures have been utilized to perform similar tasks in full-body medical imaging [7]. However, it has been observed that transformer-based architectures require large-scale training data and computing resources, which is a challenge for real-world primary healthcare system implementations. These challenges have motivated researchers to adopt hybrid frameworks incorporating blockchain for decentralized trust management and Deep Learning (DL) for improved diagnostic intelligence [8]. Blockchain provides immutable logging of medical image records, patient consent, and access control, and enables distributed verification without the need for a centralized authority that provides sophisticated discrimination capabilities [9]. State-of-the arts methods includes blockchain-integrated frameworks for electronic health records and medical Internet of Things (IoT) data, but only limited efforts focus on imaging pipelines where both privacy preservation and computational efficiency are critical [10]. Similarly, while transformer hybrid models have outperformed traditional models in diagnosis performance on recent benchmarks, their coupling with security, distributed storage, and access control capabilities has not been explored. This gap motivates future work that is reflected in the proposed actor hub on a blockchain, which combines DL architectures that increase not only classification accuracy and robustness, but also supports security, transparency, and scalability features of blockchain.

The contribution of this research includes:

- The Blockchain and Convolutional Neural Network (B-CNN) framework integrates blockchain with cloud storage, ensuring that medical images are encrypted, immutably logged, and access-controlled through smart contracts for healthcare data sharing.
- Combining a Convolutional Neural Network (CNN) for spatial-local feature extraction and transformers for global contextual reasoning enhances the accuracy of classification in medical image analysis.
- By combining edge preprocessing, off-chain encrypted storage, and blockchain logging, the framework enables efficient, tamper-resistant, and scalable cloud-assisted medical image analysis suitable for real-world healthcare ecosystems.

The rest of this paper is organized as follows: Section 2 establishes the literature review, Section 3 demonstrates the proposed methodology, Section 4 specifies the results of the proposed model with existing models as well as discussion, and Section 5 summarizes the overall conclusion of the research.

II. Literature Reviews

Sun et al. [11] suggested a verifiable compressed and privacy-enhanced sensing reconstruction for cloud medical image processing. Initially, the hierarchical framework integrated Reinforcement Learning (RL) with rule-based control to manage decision-making for autonomous vehicles in multilane environments. The process began by training a Deep RL (DRL) agent to learn the optimal driving speed given a range of traffic conditions. Subsequently, a series of predetermined rule-based policies were applied to the lower-level processes associated with all lane-changing and car-following behaviors, ultimately conditioning the model to comply with safety and traffic laws. Subsequently, the high-level learning elements and rule-based actions were merged to formulate final driving strategies that aimed to balance efficiency with safety. However, reliance on static rule hierarchies reduces flexibility in unexpected or conflicting scenarios, limiting its generalization in highly dynamic traffic conditions.

Kumar et al. [12] demonstrated the development of cloud-assisted classification for the preservation of secure data storage in smart cities. Initially, the model used XGBoost to prioritize the features we collected and to find which features had high relevance or importance, which helped filter out useless parameters, allowing for reduced computing effort. The model then created an Online Extended Belief Rule Base (OEBRB) that was customizable based on incoming information from sensors to constantly adapt to the ever-changing nature of the underwater environment. Finally, an Evidence Reasoning (ER) algorithm was applied to infer the type of fault and produce interpretable diagnostic results. However, the rule base can still grow excessively large in highly complex environments, and clustering-based reduction introduces an additional computational burden.

Ahmad et al. [13] presented a cloud-assisted medical Internet of things (IoT)-based quantum safe multi-factor user authentication protocol. Initially, the model established a hierarchical framework that integrated DRL with rule-based reasoning to handle multilane autonomous driving tasks. This framework first utilizes a high-level decision-making module to determine the vehicle's lane-changing intentions and overall driving strategy. Subsequently, a low-level RL controller was applied to execute the acceleration, braking, and steering commands based on the chosen strategy. Subsequently, a rule-based reasoning layer filters unsafe or illegal actions, ensuring that the vehicle's decisions comply with fundamental traffic rules and safety constraints. However, reliance on static rule hierarchies limits flexibility in handling conflicting rules and unpredictable traffic scenarios, thereby reducing its robustness in highly dynamic environments.

Abdulrahman Alzahrani [14] suggested cloud-centric authentication and developed a provable secure system for e-healthcare. Initially, the model employed a perception module for sensing multiple sources of real-time data from a variety of sources, such as cameras, LiDAR, and radar sensors, to create a representation of the driving environment of an autonomous vehicle. The model then filters these data to generate spatial and temporal features that are useful for capturing vehicles, pedestrians, and obstacles. Next, the model engages a decision-making process, with the extracted features leading to planning and control actions so that the autonomous vehicle can navigate, change lanes, and avoid collisions, even in the presence of dynamic traffic. After this process, the model processes the fused representation through classification layers to predict the final categories of emotion. However, the lack of interpretability and the need for large amounts of labeled training data make it difficult to justify critical decisions and limit its reliability in unseen or rare-edge cases.

Gayathri S and Gowri S [15] introduced Customizable Unique Node Access (CUNA) for privacy preserving medical records storage using deep encryption in cloud environment. Initially, the model independently extracted speech and facial features using convolutional and spectral analysis methods to capture emotional cues from voice and facial expressions. These extracted features were then transformed into intermediate representations and passed through an attention-based fusion network that emphasized the most relevant emotional signals across modalities. Subsequently, the fused representation is processed through classification layers to predict the final emotion categories. However, reliance on deep attention mechanisms is computationally expensive, leading to limited implementation in real-time systems and data-limited environments, as it would not be appropriate.

III. Methodology

This research introduces a secure cloud-assisted medical image analysis B-CNN framework that integrates blockchain to overcome the challenges of privacy, scalability, and diagnostic accuracy. Initially, multimodal medical images and clinical records were gathered from X-rays, CT scans, and MRIs with respect to ethical principles and documentation. In the preprocessing phase, the images are normalized, anonymized, denoised, and tagged with metadata to achieve standardization and readiness for security. A blockchain-based security layer was then applied by employing encryption, off-chain storage, Merkle proofs, and smart contracts to guarantee tamper resistance, consent-driven access, and regulatory compliance. Finally, the CNN–transformer hybrid model combines local spatial feature extraction with global contextual learning, which enables classification. The overall performance of the Blockchain with CNN (B-CNN) model is shown in Figure 1.

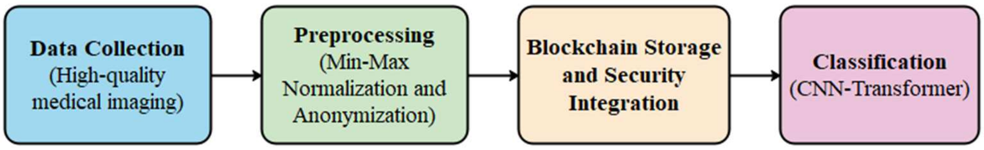

Fig. 1. Block diagram of the proposed B-CNN.

A. Data collection

Initially, data is collected by assembling high-quality medical imaging datasets [15] that have ethical approvals in place and offer a clinical context. Medical imaging is obtained using a wide variety of instruments, including X-ray, CT, MRI, ultrasound, and histopathology, within Picture Archiving and Communication System (PACS) and Digital Imaging and Communications in Medicine (DICOM) servers connected to hospital infrastructure. To ensure the contextual and diagnostic relevance of the images, structured information from Hospital Information Systems (HIS) and Electronic Health Records (EHR) were linked. These included patient demographics, comorbidities, laboratory reports, and diagnostic codes using pseudonymized identifiers to protect patient privacy. Further, data were collected from wearable sensors (ECG, pulse oximetry, and temperature sensors) and environmental logs from the imaging devices to develop a multimodal instrument. Ethical concerns are directly addressed by including backend informed consent mechanisms to collect data digitally logging patient permissions to the research, diagnostic, or data sharing process. These data is categorized with metadata on structural features such as acquisition parameters or timestamps, and then cryptographic hashes are used for the data integrity verification process. Next, the collected data are input into the preprocessing step to secure the cloud-assisted analytical data, which is described in the following step.

B. Preprocessing

The preprocessing stage is a transition from unprocessed multimodal acquisitions to safe cloud-enabled analysis, which ensures that the acquired data are standardized, fully anonymized, denoised, and optimized for downstream modeling. This stage began at edge nodes co-located with imaging devices and hospital gateways, thereby minimizing latency and protecting patient privacy before the data left institutional boundaries. The first operation is the normalization of image dimensions because different modalities generate scans at varying resolutions and matrix sizes to ensure uniform input to the hybrid CNN–transformer network. Then, the images are resized into a fixed matrix using bilinear interpolation for continuous-tone modalities such as MRI and bicubic interpolation for sharper modalities such as X-rays. By considering an image intensity function $I(x,y)$, the normalized pixel intensity at the rescaled coordinates (x',y') is expressed as Equation (1):

$$I'(x',y') = \sum_{i=0}^{1} \sum_{j=0}^{1} w_{ij} \cdot I(x+i, y+j) \qquad (1)$$

where w_{ij} is bilinear interpolation weights, and pixel intensity normalization is then applied to account for the dynamic range inequality over devices, which is often done with min–max normalization. The mathematical representation of the normalization is shown in Equation (2):

$$I_{norm}(x,y) = \frac{I(x,y) - I_{min}}{I_{max} - I_{min}} \qquad (2)$$

where $I_{\min}$ and $I_{\max}$ denote the modality-specific intensity extrema. Then, the anonymization function step is executed to remove any Personally Identifiable Information (PII) from associated clinical metadata and Digital Imaging and Communications in Medicine (DICOM) headers. Patient-reported data are more extensive and contain attributes, such as names, IDs, birth dates, and hospital accession numbers. All identical information is hashed with the same secure one-way function to obtain a pseudonymous token and is stored exactly and immutably on the blockchain, without ever directly reporting sensitive information. If d represents a metadata field, then the anonymized version is $d' = H(d)$, where $H(.)$ signifies a cryptographic hash function. This step ensures compliance with regulations and noise reduction, followed by targeting both acquisition noise and compression artifacts. Gaussian filtering and nonlocal means (NLM) are the primary tools, where Gaussian smoothing uses a convolution kernel, which is denoted by Equation (3):

$$I_{denoise}(x,y) = \sum_{u=-k}^{k} \sum_{v=-k}^{k} G(u,v) \cdot I_{norm}(x-u, y-v) \qquad (3)$$

In the case of MRI and CT data, for which structural fidelity is paramount (to track spatial trajectories), the NLM filtering comparison used a weighted average of the pixels with neighboring pixels of similar texture, which produced a filtering mechanism to reduce random noise while preserving anatomical edges. Metadata generation is incorporated to capture contextual information necessary for blockchain-based indexing and later multimodal learning. Each image was tagged with an acquisition timestamp, modality, resolution, anonymized patient ID, consent flags, and device calibration details. Feature-level descriptors were also generated during preprocessing, including the Histogram of Oriented Gradients (HOG) and wavelet coefficients, which later aided CNN feature extraction by embedding structural priors. Encryption-ready segmentation of files was conducted to further prepare secure storage. Images are partitioned into chunks, each chunk hashed and signed; although full encryption occurred in the subsequent storage stage, chunking ensured that even partial leaks could not reconstruct meaningful medical content. Each chunk hash is computed using Equation (4).

$$h_i = H(C_i) \tag{4}$$

where C_i represents the ith image segment, which is then assembled into a Merkle tree to enable efficient verification of large imaging datasets, providing integrity checks against tampering. Temporal imaging modalities, such as echocardiography, temporal alignment, and frame sampling, were implemented. Redundant frames are dropped using interframe correlation thresholds, where the frame is discarded if $\mathrm{Corr}(F_t, F_{t-1}) > \theta$ is a modality-specific redundancy threshold. Finally, all preprocessed data underwent partitioned into patient-level separation using a blockchain-based layer to avoid leakage.

C. Blockchain Storage and Security Integration

After preprocessing, the medical images and associated metadata entered the blockchain-based security layer, benefitted from decentralized trust, provided tamper-resistance, and exaggerated access control, while ensuring the scalability required by large healthcare datasets. The preprocessed medical images are encrypted and stored off-chain in distributed cloud storage, and only cryptographic fingerprints, consent records, and access policies are committed to the permissioned blockchain ledger. The encryption process ensured that sensitive data could not be accessed, even if off-chain storage was compromised. Each medical image is encrypted using a symmetric key through algorithms such as AES-256, which is defined in Equation (5):

$$C = E_{K_s}(I) \tag{5}$$

Ciphertexts stored in a distributed cloud repository. To allow secure key sharing between authorized stakeholders (clinicians, researchers, or AI services), the symmetric key is further encrypted with the recipient's public key K_{pub} as shown in Equation (6):

$$K_{enc} = E_{K_{pub}}(K_s) \tag{6}$$

Only the intended recipient can retrieve the key using their private key K_{priv}, thereby accessing the decrypted medical image. To record the integrity of off-chain data, the system computed an SHA- 256 hash for each encrypted image file. If an image is segmented into multiple chunks $C_1, C_2, \dots, C_n$, the Merkle tree structure is adopted for a scalable verification. Each chunk produces a hash $h_i = H(C_i)$, and pairs of these hashes are recursively combined, as shown in Equation (7):

$$h_{parent} = H(h_{left} \| h_{right}) \tag{7}$$

Until the Merkle root, h_{root} is obtained, which is written to the blockchain ledger as an immutable proof of integrity. During retrieval, re-hashing the chunks and comparing the recalculated root with the on-chain value confirmed the authenticity without downloading the entire dataset. In addition to integrity, blockchain maintains access policies and patient consent records as a smart contract. When data are added to the blockchain, a transaction is created in the chain that contains: (i) the data hash or Merkle root, (ii) the anonymized Patient ID, (iii) the consent flags, and (iv) the Role-Based Access Control List (RBAC). More formally, if U is a user making an access request with role r, and P is the policy adjacent to the record, then access is only granted if Equation (8) is satisfied.

$$Access(U, I) = \begin{cases} 1 & if\, r \in P.allowed \wedge consent = valid \\ 0 & otherwise \end{cases} \tag{8}$$

This ensured that every access attempt was transparently validated by decentralized logic rather than by a single centralized server. Consensus among blockchain nodes is achieved through a permissioned consensus algorithm such as Practical Byzantine Fault Tolerance (PBFT), chosen for its efficiency in consortium healthcare networks where participants (hospitals, labs, and insurers) are authenticated. In PBFT, each transaction (hash storage, consent update, and access request) passes through a pre-preparation, preparation, and commit phase across the validator nodes. This consensus ensured that once a transaction was written, it became immutable, making retrospective tampering impossible. To further strengthen trust, timestamps on entries into the blockchain created an auditable-time-based sequence of events. For example, each access attempt creates a log entry with a tuple, as shown in Equation (9):

$$Log = (U, I, t, action,\ result,\ sig) \tag{9}$$

Where U denotes the user, I indicates the image identification representation, t signifies the timestamp, action refers to the attempted operation, result is the outcome (either granted or denied), and sig is the digital signature of the validating node. These logs enable full accountability and forensic tracking of every interaction between patient data and hospital management. By separating user identification and action, the system can handle terabytes of imaging data while maintaining the benefits of blockchain immutability. The use of encryption, off-chain storage, cryptographic hash, Merkle proofs, smart contracts with RBAC, and PBFT consensus ensures that the patient data remain confidential, tamper apparent, and provides access to only those parties to obtain access under consent-driven governance. This security layer ensures compliance and builds trust with patients, clinicians, and cloud providers, as well as a secure backbone to operate the hybrid CNN-transformer diagnostic model.

D. CNN-Transformer Hybrid Model for Feature Extraction and Classification

After securing the medical data with blockchain integration, the next critical stage involved designing a hybrid CNN and transformer-based architecture for robust feature extraction and precise classification of medical images. This model was chosen to combine the strengths of CNNs in capturing fine-grained spatial-local features and transformers in modeling global contextual dependencies, thereby addressing the limitations of traditional CNN-only and transformer-only models. The process began by feeding preprocessed and standardized images into CNN convolutional layers. These layers apply several learnable kernels as inputs to learn hierarchical spatial features that resemble edges, textures, and organ structures. If $I(x, y)$

denotes the normalized input image, $K(m,n)$ denotes a convolution filter, and the feature map $F(i,j)$ at position (i,j) is computed as Equation (10):

$$F(i,j) = \sum_m \sum_n I(i+m, j+n) \cdot K(m,n) + b \quad (10)$$

Where b is learnable bias, and having multiple such filters gave us a different diversity of low-level to high-level features, enough to retain features for subtle pathologic markers such as microcalcifications in a mammogram or lesions in the CT scans. To introduce nonlinearity, Rectified Linear Units (ReLU) are applied, which is denoted by Equation (11):

$$f(z) = max(0,z) \quad (11)$$

Then, an adaptive average pooling layer is used to reduce the dimensionality while maintaining the true structure and improving the scalability and efficiency of the model on larger datasets. The CNN backbone produces meaningful spatial embeddings, but medical imaging tasks are also reliant on capturing long-range dependencies (e.g., spatial connectivity of the regions of interest in brain MRIs or tumor spread in lung CTs). As such, the extracted CNN feature maps were flattened as sequences to be input into a transformer encoder. The multi-head self-attention (MHSA) system from the transformer encoder architecture was used to model the relationships among image patches. For each patch embedding x_i, three vectors were calculated: query $Q = x_i W_Q$, key $\mathrm{K} = \mathrm{x_i W_K}$, and value $\mathrm{V} = \mathrm{x_i W_V}$, where $\mathrm{W_Q, W_K, W_V}$ are learnable matrices. The attention weights between patches i and j were calculated using Equation (12):

$$Attention(Q_i, K_j, V_j) = softmax\left(\frac{Q_i K_j^T}{\sqrt{d_k}}\right) V_j \quad (12)$$

Where d_k is the dimension of the key vector, which allows the model to emphasize clinically relevant areas without regard to spatial location. The model captures multiple complementary contextual patterns using a combination of attention heads. The outputs of the MHSA layers are passed into the feed-forward layer with residual connections and layer normalization, which allows for a better gradient flow and increased convergence rate. This hybridization provided both CNN-based local consistency and transformer-based global consistency. Once the transformer stage produces contextualized embeddings, the CNN–transformer fusion is performed by concatenating the CNN feature maps and transformer embeddings into a joint representation vector Z is computed as Equation (13):

$$Z = [F_{CNN} \| F_{Trans}] \quad (13)$$

Where, || denotes concatenation. This fusion step ensures that fine local structures and global dependencies coexist in a learned representation. For classification, Z was passed through fully connected layers, followed by a Softmax classifier to predict diagnostic outcomes. If z is the final representation, the probability of class c is represented by Equation (14).

$$P(y = c \mid z) = \frac{exp(zW_c + b_c)}{\sum_{k=1}^{C} exp(zW_k + b_k)} \quad (14)$$

Where C denotes the number of diagnostic categories, such as healthy, benign anomaly, and malignant tumor. Its integration with blockchain ensures that all model outputs, weights, and decisions can be logged immutably for auditability. The combination of secure storage, ethical governance, and advanced DL has empowered a trustworthy, scalable, and highly accurate system for cloud-assisted medical image processing in healthcare networks. The performance of the proposed B-CNN model is discussed in the following section.

IV. Experimental Results

The experimental results were obtained in a high-performance computing environment to ensure efficient model training and validation. This environment uses multi-core processors such as an Intel i7, at least 16 GiB of random-access memory (RAM), and a GPU such as an NVIDIA GTX 1080 to compute DL training. In particular, the software environment includes Python and DL libraries such as TensorFlow and PyTorch. Secure cloud-assisted medical image analysis framework integrating blockchain and CNN–transformer hybrid model. The system then begins with multimodal data collection, followed by preprocessing steps, such as normalization, anonymization, and denoising. Blockchain ensures encrypted off-chain management, tamper-proof storage, and consent-driven access via smart contracts. The B-CNN model extracts local spatial and global contextual features for diagnostic classification. The evaluation metrics, such as accuracy, precision, recall, and F1-score, are formulated as follows in equation (15-18):

$$Accuracy\ (acc) = \frac{TP+TN}{TP+TN+FP+FN} \quad (15)$$

$$Precision\ (pr) = \frac{TP}{TP+FP} \quad (16)$$

$$Recall\ (re) = \frac{TP}{TP+FN} \quad (17)$$

$$F1 - score = \frac{2 \times pr \times re}{pr + re} \quad (18)$$

Here, TN and TP denote the true negatives and positives, respectively, FN, FP represent the false negatives and false positives, respectively.

A. Performance Analysis

The performance of the proposed B-CNN model was compared with that of various existing methods, such as KNN and SVM, using evaluation metrics. Existing approaches are presented in Table 1.

TABLE I. PERFORMANCE ANALYSIS OF PROPOSED B-CNN.

Performance Models	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
KNN	90.36	84.18	92.69	90.84
SVM	91.72	87.33	93.83	91.59
Proposed B-CNN	93.23	88.95	94.56	92.72

Table 1 presents the performance of the proposed B-CNN framework compared with existing methods. The B-CNN model achieved better results than the conventional approaches, including accuracy (93.23%), precision (88.95%), recall (94.56%), and F1-score (92.72%), outperforming the KNN model in terms of accuracy (90.36%), precision (84.18%), recall (92.69%), and F1- score (90.84%). Similarly, the SVM model had an accuracy of (91.72%), precision (87.33%), recall (93.83%), and F1-score (91.59%), respectively. The proposed B–CNN framework facilitates secure, scalable, and trustworthy cloud-assisted medical-image analysis. Combining blockchain-based integrity and consent management with advanced hybrid DL for accurate diagnostic capabilities in modern digital ecosystems.

B. Comparative Analysis

The proposed B-CNN framework was compared with the existing CUNA [15] model by using comprehensive evaluation metrics. An evaluation of the proposed B-CNN method is presented in Table 2.

TABLE II. COMPARATIVE ANALYSIS OF PROPOSED B-CNN.

Comparative Models	Accuracy (%)
CUNA [15]	92
Proposed B-CNN	93.23

Table 2 shows that the proposed B-CNN framework obtained better results than the existing CUNA [15] model in terms of accuracy (93.23%) respectively. The existing CUNA [15] model obtained minimal results in terms of accuracy (92%), which represent significant improvements in model performance.

C. Discussion

The objective of this research is to design a secure cloud-assisted medical image system using the proposed B-CNN framework. Existing models, such as KNN, SVM, and CUNA [15], have been employed for medical image classification owing to their simplicity and effectiveness in small-scale datasets. However, KNN suffers from a high computational cost during inference, which requires distance calculations, making it unsuitable for real-time cloud-assisted systems. Similarly, SVM establishes strong performance for binary classification but struggles with multiclass and large datasets because of its high training complexity and poor scalability. Moreover, the existing CUNA uses CNNs to model uncertainty; however, it struggles to capture long-range dependencies in complex diagnostic tasks because of its heavy reliance on convolutional layers. To overcome these limitations, the proposed B-CNN model introduces a hybrid transformer architecture that is capable of extracting local features and learning global relationships across a full medical image. Blockchain integration defines immutable logging, decentralized trust, and consumer consent-driven control as components that preserve logging, decentralization, and consumer consent.

V. CONCLUSION

This research presents a secure and intelligent framework for cloud-assisted medical image analysis that integrates blockchain technology with a CNN–transformer hybrid model. Initially, multimodal medical images were collected from hospital PACS, HIS/EHR records, and wearable sensors while ensuring ethical compliance and privacy through pseudonymization. In the preprocessing stage, images are normalized, anonymized, denoised, and prepared with metadata generation and cryptographic segmentation, ensuring both data quality and integrity. Blockchain integration provides decentralized trust, off-chain encrypted storage, immutable logging, and consent-driven smart contract enforcement, thereby guaranteeing security, accountability, and compliance. Finally, the CNN–Transformer hybrid model enabled accurate classification by combining local feature extraction with global contextual modeling. The experimental results demonstrated that the proposed B-CNN achieved the highest accuracy of 93.23% when compared with the existing CUNA model. In the future, this work will be extended by incorporating eXplainable AI (XAI) techniques to enhance clinical interpretability and optimize lightweight CNN–Transformer architectures for edge devices.

REFERENCE

[1] Majhi, M., Pal, A.K., Pradhan, J., Islam, S.H. and Khan, M.K., 2022. Computational intelligence based secure three-party CBIR scheme for medical data for cloud-assisted healthcare applications. Multimedia Tools and Applications, 81(29), pp.41545-41577.

[2] Li, D., Wu, Y., Lü, Q., Zhang, K., Wang, Z. and Wu, J., 2024. Pmir: an efficient privacy-preserving medical images search in cloud-assisted scenario. Neural Computing and Applications, 36(3), pp.1477-1493.

[3] Zhu, D., Zhu, H., Huang, C., Lu, R., Feng, D. and Shen, X., 2023. Efficient and accurate cloud-assisted medical pre-diagnosis with privacy preservation. IEEE Transactions on Dependable and Secure Computing, 21(2), pp.860-875.

[4] Singh, C.E.J. and Jagatheeswari, A., 2023. Secured blind digital certificate and Lamport Merkle cloud assisted medical image sharing using blockchain. Multimedia Tools and Applications, 82(6), pp.9323-9342.

[5] Karthiyayini, S., John Simon Christopher, J., Sheik Arafat, I. and Syed Moomin, F.M.H., 2024. Enhanced Model for Medical Image Data Security Using Machine Learning. SN Computer Science, 5(8), p.1103.

[6] Yang, T., Li, Y., He, J., Liu, Z., Ren, F., Wang, T. and Hou, G., 2024. Secure and traceable multikey image retrieval in cloud-assisted internet of things. IEEE Internet of Things Journal.

[7] Zhu, D., Zhu, H., Wang, X., Lu, R. and Feng, D., 2022. An accurate and privacy-preserving retrieval scheme over outsourced medical images. IEEE Transactions on Services Computing, 16(2), pp.913-926.

[8] Ling, J. and Duan, R., 2025. Privacy preserving technology for data sharing in cloud-assisted internet of medical things. Cluster Computing, 28(7), p.447.

[9] Tang, W., Zhang, X., Gu, D., Huang, C., Xue, J. and Liang, X., 2024. Enabling authorized fine-grained data retrieval over aggregated encrypted medical data in cloud-assisted e-health systems. IEEE Transactions on Cloud Computing.

[10] Mahajan, H.B. and Junnarkar, A.A., 2023. Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing. Multimedia Tools and Applications, 82(28), pp.44335-44358.

[11] Sun, X., Tian, C., Tian, W. and Zhang, Y., 2022. Privacy-enhanced and verifiable compressed sensing reconstruction for medical image processing on the cloud. Ieee Access, 10, pp.18134-18145.

[12] Kumar, A., Khan, S.B., Pandey, S.K., Shankar, A., Maple, C., Mashat, A. and Malibari, A.A., 2023. Development of a cloud-assisted classification technique for the preservation of secure data storage in smart cities. Journal of Cloud Computing, 12(1), p.92.

[13] Ahmad, A. and Jagatheswari, S., 2024. Quantum safe multi-factor user authentication protocol for cloud assisted medical iot. IEEE Access.

[14] Alzahrani, A., 2024. Developing a Provable Secure and Cloud-Centric Authentication Protocol for the e-Healthcare System. IEEE Access.

[15] Gayathri, S. and Gowri, S., 2022. CUNA: A privacy preserving medical records storage in cloud environment using deep encryption. Measurement: Sensors, 24, p.100528.