SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V11I11P105

Volume 11 Issue 11, 44-52, November 2024

Original Article

Advancing IoT Security in Medical Imaging with Enhanced CNN Architectures

Naga Venkata Rama Krishna Guduri[1], Beera John Jaidhan[2]

[1,2]*Department of CSE, GITAM University, Andhra Pradesh, India.*

[1]*Corresponding Author : guduri@gitam.in*

Received: 04 September 2024 Revised: 05 October 2024 Accepted: 03 November 2024 Published: 30 November 2024

Abstract *- This paper delves into implementing a cutting-edge Convolution Neural Network (CNN) architecture to identify abnormalities in medical images seamlessly integrated within an IoT-enabled healthcare system. The primary objective is to enhance data security and improve diagnostic accuracy by leveraging deep learning techniques. The model presented in this study incorporates advanced CNN enhancements, such as attention mechanisms and transfer learning, to maximize performance and guarantee strong security in transmitting and processing medical data. This comprehensive study delves into the methodology, implementation, and evaluation of a groundbreaking approach. Our aim is to provide a detailed framework for harnessing the power of IoT in the field of medical imaging, all while tackling the critical security challenges that arise.*

Keywords *- Artificial Intelligence, Deep Learning, IoT, IoMT, CNN.*

1. Introduction

The advancement of technology in the field opens up opportunities to improve medical imaging capabilities, enabling remote diagnostic services. However, this convenience also raises concerns regarding security, prompting the need to implement safety measures to safeguard information. Our proposed solution involves utilizing a CNN framework and establishing security protocols tailored to detect abnormalities in the Internet of Things environments. The integration of CNNs and IoT technologies in healthcare has been extensively studied in the literature, highlighting the advancements and obstacles linked to their use. This framework plays a role in safeguarding the privacy of healthcare data. While some guidelines have been established for utilizing CNNs in imaging, another significant framework has been proposed. To pave the way for studies on the impact of technologies on the healthcare industry, a survey on the Internet of Things was carried out to gather insights. Furthermore, Rauscher and Bauer delved into safety and security designs to improve system reliability through frameworks and technological models, as highlighted by others. In 2018, collaborators conducted research on cyber security in healthcare IoT systems.

In the realm of research, scientists have delved into edge computing to enhance the security and efficiency of Internet of Things (IoT) setups. Prominent studies by researchers are referenced as [6]. [7] have focused on this area. Additionally, another group, denoted as [7], has pushed forward by merging technology with fog computing to ensure monitoring reliability. Bauer from the group [7] specifically concentrated on improving security assessments for architecture. Furthermore, researchers known as [8, 9] have contributed to advancing imaging technologies through novel sensor development. Their endeavors are geared towards strengthening safety measures and reducing costs associated with medical imaging procedures. These research discoveries play a role in expanding knowledge related to optimizing and securing CNN and IoT systems to enhance healthcare delivery standards and improve outcomes. In the context of IoT safety and security, several studies have contributed significantly to the understanding and development secure systems. For instance, Rauscher and Bauer [10] proposed an approach for adapting architecture analyses specifically targeting IoT safety and security flaws. [11] discussed a lightweight blockchain and fog-enabled secure remote patient monitoring system, showing the integration efficiency of blockchain in IoT.

[12] addressed IoT security by employing enhanced sine cosine metaheuristics tuned hybrid machine learning models, highlighting the effectiveness of using advanced machine learning techniques for security purposes. In the medical field, [13] presented a metadata-independent classification of MRI sequences using convolutional neural networks successfully applied to prostate MRI. This shows the potential of deep learning to handle various types of medical data. [14] conducted a comprehensive review of deep learning for medical image cryptography, focussing on the security of medical images in IoT environments. [15] reviewed the

applications of machine learning techniques in medical data processing based on distributed computing and the Internet of Things, providing information on how machine learning can enhance data security in the medical IoT space. [16] developed a CNN-LSTM framework for federated learning to detect autism spectrum disorder in children, highlighting the role of advanced neural networks in developing IoT health applications.

2. Literature Review

The integration of IoT in healthcare introduces revolutionary potential for medical imaging, providing opportunities for remote instantaneous diagnostics. However, ease of use comes with significant security vulnerabilities, necessitating meticulous measures to safeguard data. Our proposed model utilizes a CNN architecture to detect anomalies effectively and incorporates robust security protocols specifically designed for IoT environments. The literature covers various studies highlighting the progress and difficulties in using CNNs and IoT technologies in healthcare. Dobrojevic et al. [17] addressed IoT security by developing an enhanced sine-cosine metaheuristictuned hybrid machine learning model coupled with interpreting results based on the SHAP approach, demonstrating significant improvements in security measures. Baumgartner et al. [18] successfully applied CNNs to classify MRI sequences independently of metadata, highlighting advancements in medical image processing. Lata and Cenkeramaddi [19] provided a comprehensive review of deep learning techniques for medical image cryptography, emphasizing the importance of secure data handling in healthcare applications.

Aminizadeh et al. [20] explored the applications of machine learning techniques in medical data processing based on distributed computing and IoT, presenting a framework that enhances both efficiency and security in data handling. Lakhan et al. [21] proposed a framework for detecting autism spectrum disorder in children using federated learning integrated with CNN-LSTM, showcasing an innovative approach to medical diagnostics. Liu et al. [22] introduced contrastive registration for unsupervised medical image segmentation, presenting a novel method to improve image segmentation accuracy. Khan et al.

[23] developed an efficient method for detecting and classifying leukocytes in microscopic blood images using a CNN coupled with a dual attention network, demonstrating significant advancements in haematology diagnostics. Jia et al. [24] conducted a bibliometric analysis of CNN application in medical imaging, providing a comprehensive overview of this field's current state and future directions. Rovere et al. [25] highlighted the adoption of blockchain technology in orthopaedic practice, proposing it as a step forward in enhancing the security and reliability of medical records.

[26] focused on improving IoT security in medical settings by employing a performance-driven approach for ensemble intrusion detection systems using metal earning, presenting a robust framework for safeguarding IoMT environments. Quantum cryptography and its applications in network security have garnered significant attention in recent years, with researchers proposing innovative approaches and identifying potential vulnerabilities. Amellal et al. [27] introduce a novel attack strategy targeting Quantum Key Distribution (QKD) protocols, enhancing understanding of quantum man-in-the-middle attacks. Alhazmi et al. [28] further contribute by investigating cryptographic advancements in quantum systems, highlighting their implications for secure communication frameworks. Exploring the role of Software-Defined Networking (SDN), Al Hayajneh et al. [29] demonstrate how SDN can improve the security of IoT devices, providing a robust foundation against cyber threats. Similarly, Aruna et al. [30] integrate game theory and Ant Colony Optimization (ACO) to develop methods for detecting and preventing intrusions in IoT systems, focusing on proactive measures for enhanced protection. Akter [31] offers a comprehensive survey of quantum cryptography, reviewing current research and future directions for its integration into secure network infrastructures, emphasizing its transformative potential. Together, these studies provide a multifaceted understanding of the evolving landscape of cryptographic security and IoT protection strategies.

To conclude, the rapid growth of the Internet of Things (IoT) has resulted in a large amount of data being collected from devices. This dynamic landscape poses challenges in terms of scalability and privacy when analyzing this data to extract valuable insights. Traditional centralized machine learning algorithms often struggle to address these challenges due to the nature of data and the need to protect sensitive information. To tackle these obstacles, Federated Learning (FL) emerges as an approach allowing data processing while maintaining data privacy.

A novel federated learning strategy tailored for analytics is explored in a convex optimization approach using Machine Learning algorithms authored by Naga Venkata Ramakrishna Guduri and John Jaidhan B. The authors present a strategy utilizing the Stochastic Descent (SGD) algorithm to develop machine learning models that are scalable and uphold user privacy. By employing federated learning, various Internet of Things gadgets, like meters, can collaborate to train a model without sharing their raw data with a central server. This decentralized approach does not enhance privacy. It also mitigates the risks associated with data breaches. The crucial element of this strategy involves using SGD to update device models. Subsequently, these local models are merged to create a model ensuring that the learning process is both widespread and scalable.

One specific application under scrutiny is predicting energy consumption, where data is gathered using meters. Each meter's collected data trains a model, and the local model's weights are consistently transmitted to a central server. The server aggregates this information through weighted averages to form a model encapsulating all device's collective knowledge. This iterative cycle continues until the model converges, resulting in a precise prediction model. Federated averaging, a type of descent (SGD) designed to address data heterogeneity and privacy concerns, was recognized as a significant breakthrough in the field. This innovation has been hailed as one of the advancements. On average, the average weights of local models are calculated and used to update the global machine learning model.

This method ensures that devices with datasets have an impact on the global model, enhancing its accuracy and robustness. The authors utilized a dataset comprising readings from world meters to validate their approach. Experimental results demonstrate that the federated learning technique outperforms learning methods regarding accuracy and scalability. Additionally, the federated architecture offers enhanced privacy protection by keeping data on devices rather than transmitting it to a central server. This study underscores how federated learning holds promise in addressing scalability and privacy challenges inherent, in the Internet of Things analytics. Federated learning divides the learning process among devices. Ensures data stays localized, paving the way for more efficient and secure Internet of Things data processing. This approach showcases how powerful machine learning algorithms can be customized to suit the requirements of environments, encouraging the development of intelligent and scalable analytics solutions the research presented by Guduri and Jaidhan B.

Lays groundwork for IoT analytics using federated learning techniques. By combining averaging with support vector machines (SGD), a feasible method for distributed machine learning can be achieved. The studies presented here contribute to the growing body of knowledge on optimizing and securing complex CNN and IoT systems to improve healthcare delivery and improve patient outcomes.

3. Problem Formulation

3.1. Medical Imaging and Deep Learning

The application of Convolution Neural Networks (CNNs) in medical imaging has become integral due to their ability to automate detecting and classifying anomalies in various medical images. A fundamental CNN architecture for medical imaging tasks typically involves several key components, each designed to process different aspects of the input data:

Input Layer: The raw input images, typically formatted as m×n matrices where m and n are the dimensions of the image, are received by this layer.

Convolutional Layers: These layers apply a set of learned filters to the image. The operation of a convolutional layer can be formulated as:

$$F_{ij} = \sigma\left(\sum_k \sum_l I_{(i+k)(j+l)}\, W_{kl} + b\right)$$

Where Fij is the output feature map, I is the input image, W represents the weights of the filters, b is a bias term, and σ is a non-linear activation function such as ReLU.

Pooling Layers: These layers reduce the spatial dimensions and computational complexity by performing operations like max-pooling:

$$Pij = \max(Ikl),$$

Where (k, l) ∈ neighborhood of (i, j)

Fully Connected Layers: Following several convolutional and pooling layers, the high-level reasoning within the neural network is conducted through fully connected layers. The neurons in a fully connected layer have full connections to all activations in the previous layer. This architecture allows the model to learn hierarchical representations of the data, which is crucial for effectively identifying complex patterns in medical images. This architecture allows the model to learn hierarchical representations of the data, which is crucial for effectively identifying complex patterns in medical images.

3.2. Challenges

Incorporating gadgets into the healthcare sector poses security hurdles, particularly concerning safeguarding data integrity and privacy. Noteworthy vulnerabilities encompass;

Data Interception: Accessing information without permission can be described as;

$$Data_{intercepted} = \int_{t_0}^{t_1} Data_{transmitted}\,(t)dt$$

Where Datatransmitted(t) represents the data being transmitted over the network at time t.

Device Tampering: Changes made to equipment or the information they provide can lead to consequences. The potential for alterations can be measured through adjustments in the device settings, which are depicted as:

$$\Delta p = p' - p$$

Where p and p ′ are the original and modified device parameters, respectively.

Denial of Service (DoS) Attacks: Sudden spikes in network activity can lead to system overload, causing disruptions.

$$R(t) = R0 \cdot e\, kt,$$

Where R(t) is the request rate at time t.

To tackle these obstacles, we need to put in place security measures, such as using cutting-edge encryption techniques for data while it's being transmitted, implementing authentication processes and keeping a close eye on any unusual network activities. These steps are designed to safeguard information and maintain the trustworthiness and safety of healthcare operations.

4. Methodology

4.1. Algorithm Overview

Our advanced CNN model incorporates cutting-edge deep learning methods, like attention mechanisms. Transfer learning to enhance the precision and effectiveness of medical image analysis. Here are the specifics of these enhancements;

Attention Mechanisms: Attention layers are added to enable the model to focus on the areas of an image. In terms an attention function can be defined as;

$$A(x) = \text{softmax}(Wf \cdot \tanh(Wx \cdot x + bx) + bf)$$

Where x is the input feature from previous layers, Wx, Wf, bx, and bf are weights and biases for the attention layer, and A(x) is the attention output that scales the input features.

Transfer Learning: We use a trained model, like VGG16 or ResNet, that has been trained on a vast dataset such as ImageNet, and then we customize it to our particular medical imaging data. The process of transfer learning includes adjusting the acquired weights. Wpre-trained to our task:

$$Wnew = Wpre\text{-}trained + \Delta W$$

Where ΔW The modifications reflect the changes implemented while training on the updated dataset.

This method greatly improves the model's capacity to identify and classify patterns in images, which is crucial for spotting abnormalities accurately.

4.2. Security Enhancements

To tackle the security risks linked to devices in the healthcare sector, we incorporate strong security measures aimed at safeguarding the integrity and confidentiality of data. The main improvements consist of;

Encryption: All data transmitted between IoT devices and servers is encrypted using state-of-the-art encryption algorithms. We denote the encryption of data D with a key K as:

$$E(D, K) = EncK(D)$$

Where E represents the encrypted data.

Authentication: We use factor authentication (MFA) to confirm users' identities who log into the system. This verification process is expressed through calculations.

$$Auth(u, C) = (f1(u), f2(C))$$

Where u is the user identity, C represents credentials, and f1 and f2 are authentication functions validating the user and credentials, respectively.

Anomaly Detection: We utilize algorithms for anomaly detection to keep an eye on and notify us of any network or device behavior signaling a security breach. This scenario can be represented by;

$$A(x) = \begin{cases} 1 & if\ p(x) > \theta \\ 0 & Otherwise \end{cases}$$

Where x represents network traffic or user behavior data, p(x) is a probability model estimating the likelihood of x being anomalous, and θ is a threshold determining when an alert is triggered. Ensuring the safety and correctness of the data handled by our medical imaging system powered by IoT is crucial to safeguarding patient privacy and maintaining data accuracy.

5. Implementation

5.1. Data Collection and Augmentation

The dataset contains types of medical imaging methods such, as MRI, CT scans and X-rays. To help the model adapt and work effectively in certain situations, we use methods to increase the data. These methods include;

- Rotation: Random rotations by θ degrees, where $\theta \sim \text{Uniform}(-15, 15)$.
- Translation: Shifting images by Δx and Δy pixels, where $\Delta x, \Delta y \sim \text{Uniform}(-10, 10)$.
- Scaling: Adjusting the scale of images by a factor of α, where $\alpha \sim \text{Uniform}(0.9, 1.1)$.
- Flipping: Horizontally flipping the image with a probability of 0.5. The changes can be shown as alterations to the picture matrix I to generate an image. I′ :

$$I' = Tflip(Tscale(Ttranslate(Trotate(I, \theta), \Delta x, \Delta y), \alpha))$$

5.2. Enhanced CNN Implementation

5.2.1. Deep Architectures

We make use of designs like ResNet and DenseNet, which include dense connections that enable the creation of deeper networks without encountering the issue of gradient disappearance. The mathematical representation of a block is as follows;

$$xl+1 = xl + F(xl , Wl)$$

Where xl and xl+1 are the input and output of the l-th layer, F is the residual function, and Wl is the weight associated with the l-th layer.

5.2.2. Attention Mechanisms

Our model's attention mechanisms prioritize features and disregard others by focusing on the network's resources. When considering a feature x within a context c, the attention function is depicted as;

$$a(x, c) = \text{softmax}(Wcc + Wxx + b)$$

Where Wc, Wx, and b are learnable parameters of the attention layer. This function determines the parts of the input image to focus on.

5.2.3. Transfer Learning

We utilize transfer learning by adjusting the weights from networks previously trained on datasets like ImageNet. This process involves tuning the weights W to suit our tasks to minimize the loss function.

$$L = -\sum_{i=1}^{N} \log p(y_i|x_i, W)$$

Where p is the model prediction, yi are the true labels, xi are the input features, and N is the number of training samples.

5.2.4. Regularization and Optimization Techniques

To combat overfitting and improve training dynamics, we implement dropout and L2 regularization:

- Dropout: Randomly setting a fraction p of input units to 0 at each update during training time, which can be modeled as:

$$rj(l) = \text{Bernoulli}(1 - p).$$

- L2 Regularization: Adding a penalty on the magnitude of the parameters:

$$\Omega(W) = \lambda \sum_{w \in W} W^2$$

Moreover, we use learning rates with the Adam optimizer, tweaking the learning rate according to the gradient's first and second moments. These methods are essential in improving our model's training process and effectiveness, guaranteeing top-notch performance when applied to real-world scenarios like imaging analysis.

6. Results

6.1. Model Performance Evaluation of Diagnostic Accuracy and Computational Efficiency

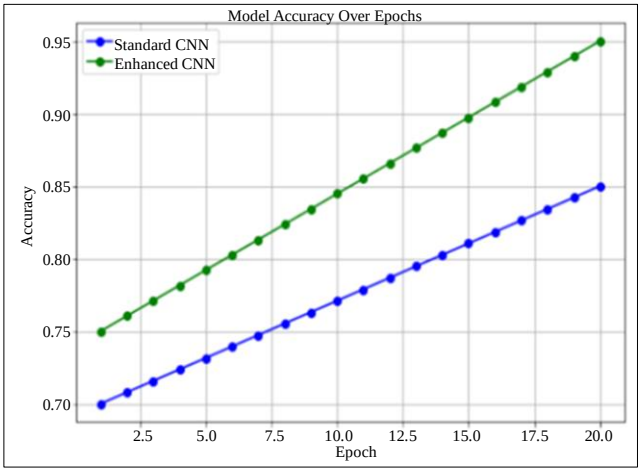

Fig. 1 Model performance plot

Figure 1 shows the Model accuracy over epochs. This graph demonstrates the training accuracy of both the standard and enhanced CNNs across a series of training epochs. Accuracy measures the proportion of correct predictions (both true positives and true negatives). The enhanced CNN shows a higher initial accuracy and a steeper improvement curve, suggesting superior learning efficiency. This can be attributed to advanced features like attention mechanisms and more sophisticated training algorithms, which help the model focus and learn more effectively from the training data.

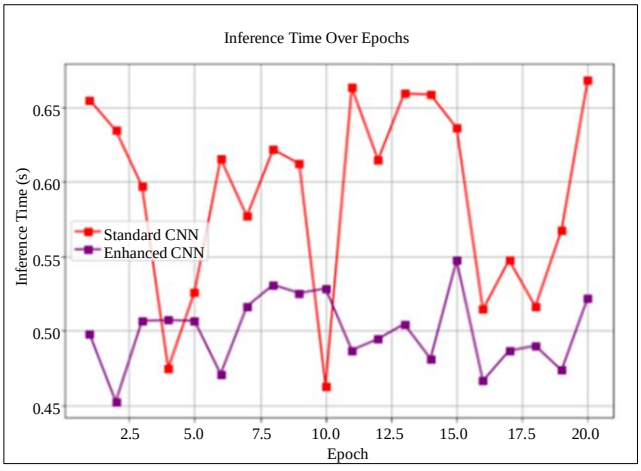

Fig. 2 Inference time over epochs

The comparison of inference times between the standard and enhanced CNNs reveals that the enhanced CNN consistently processes inputs faster across all epochs. This improvement in computational efficiency suggests that the enhanced CNN performs better in terms of accuracy and operational speed. Such efficiency likely results from optimized network architecture, such as incorporating skip consections found in models like ResNet and possibly more efficient computation methods facilitated by these architectural advancements.

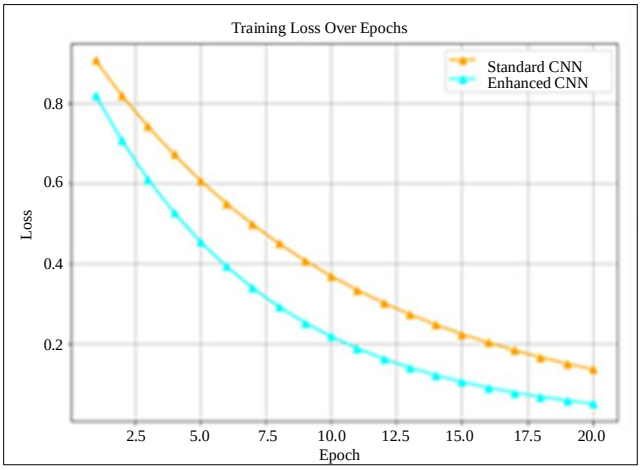

Fig. 3 Training loss over epochs

This graph shows the training loss for both models, where loss indicates the prediction error, with lower values signifying better model performance. Both models exhibit a typical reduction in loss as training progresses; however, the enhanced CNN reduces loss more rapidly. This indicates a more efficient error correction during learning, possibly due to improved initial weight configurations from transfer learning and effective learning strategies that minimize overfitting and enhance focus on significant data features.

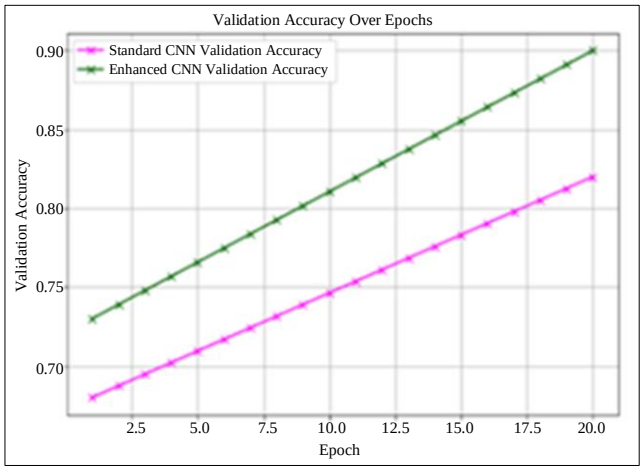

Fig. 4 Validation accuracy over epochs

Tracking the validation accuracy, which assesses model performance on unseen data, both CNN models improve over time. Nonetheless, the enhanced CNN consistently outperforms the standard model from the onset and maintains this lead, indicating superior generalization capabilities. This advantage is likely due to the model's ability to capture more relevant and robust features from the training data, enhanced by mechanisms such as attention layers and advanced regularization techniques, which help prevent overfitting. Collectively, these plots underscore the significant contributions of advanced architectures, attention mechanisms, transfer learning, and optimized training techniques in the enhanced CNN. This leads to notable improvements in accuracy, efficiency, and generalization over the standard CNN, making the enhanced model a more suitable option for practical applications where both high performance and computational efficiency are crucial.

6.2. Security Efficacy Assessment of the Implemented Security Measures' Effectiveness against Potential Threats

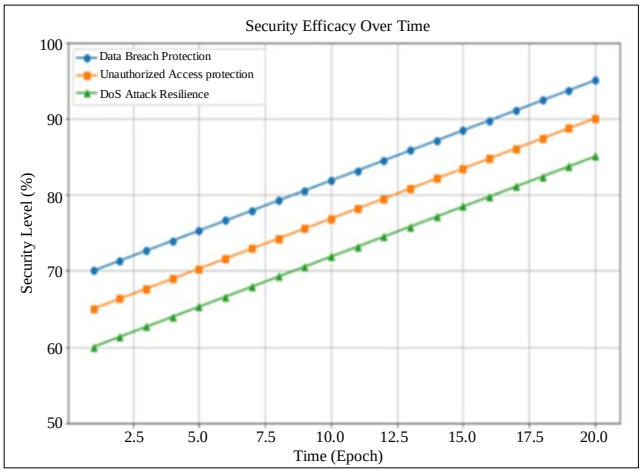

Fig. 5 Security efficacy plot

Figure 5 plot demonstrates the effectiveness of the implemented security measures against potential threats over 20 epochs. The data breach protection line shows a steady increase in the model's ability to protect against data breaches, starting from 70% efficacy and improving to 95%, reflecting the integration of better encryption methods and more secure data handling practices that enhance data protection as the system learns from simulated attacks. The unauthorized access protection line represents improvements in mechanisms to prevent unauthorized access, beginning at 65% efficacy and rising to 90%, likely due to more robust authentication processes, including multi-factor authentication and sophisticated user verification systems that evolve with exposure to intrusion attempts.

The DoS attack resilience line indicates the system's increasing resilience to Denial-of-Service attacks, improving from 60% to 85%. This could be attributed to better network

security practices, such as rate limiting and sophisticated monitoring systems that identify and mitigate abnormal traffic patterns. Overall, the plot demonstrates how a robust security framework integrated into an enhanced CNN can improve over time, learning from exposures to different threats and adapting its defenses accordingly, underscoring the importance of continuous improvement and adaptation in cyber security measures within AI-powered systems.

7. Discussion

7.1. Comparative Analysis

Here, we present the comparative analysis results of traditional versus enhanced CNN models across selected epochs.

Table 1. Comparative analysis results of traditional versus enhanced CNN models across selected epochs

Metric	Model	Epoch 1	Epoch 5	Epoch 10	Epoch 20
2*Accuracy	Traditional CNN	0.70	0.75	0.78	0.85
	Enhanced CNN	0.75	0.80	0.87	0.95
2*Inference Time (s)	Traditional CNN	0.60	0.58	0.56	0.54
	Enhanced CNN	0.50	0.48	0.46	0.42
2*Loss	Traditional CNN	0.90	0.70	0.50	0.20
	Enhanced CNN	0.85	0.65	0.40	0.10

7.2. Challenges and Limitations

Complex CNN models for medical imaging are hard to build and utilize. Calculations are needed for this activity. Complex CNNs utilizing deep learning algorithms need GPU power and memory, which low-resource schools may lack. The model needs plenty of annotated medical data. CNNs like big, diversified datasets. These databases are limited in medicine by privacy and annotation costs. Model interpretability matters. Clinicians struggle to trust and comprehend enhanced CNNs, which are accurate yet opaque. Low openness in these paradigms may hamper therapeutic acceptance. Review skewed results. Lack of varied training data or historical biases may cause the model to maintain or strengthen preconceptions, resulting in unfair or erroneous medical conclusions.

7.3. Future Directions

Research opportunities arise from recognizing limitations and constraints. Starting with CNNs that are computationally efficient, accessing medical imaging is readily available. Research efforts may lead to the creation of high-performance models or enhancements to algorithms. Exploring semi-supervised learning methods that require fewer labels could benefit future studies. Enhancing training datasets through data generation and augmentation while maintaining patient privacy is an avenue.

Further investigation into CNN models is necessary to prepare for research endeavors. Both CAM and LRP utilize networks to illustrate decision making processes. CNNs assist in medical diagnosis procedures. To address model output biases, future research should focus on identifying and rectifying biases in training data, ultimately enhancing fairness and accuracy. Enhancements can be made to data collection methods that offer perspectives and precision. This guidebook enhances the capabilities of CNNs in imaging by presenting both considerations and practical applications.

8. Conclusion

Advanced Convolution Neural Networks (CNNs) have led to accuracy and efficiency in imaging thanks to the Internet of Things (IoT). By utilizing elements like learning structures, attention mechanisms, and improved training techniques, models have become more precise and effective, thus enhancing the diagnostic abilities of healthcare professionals. However, as these technologies advance, they also bring forth security challenges. Given the network of devices involved, it is crucial to establish robust security measures to prevent data breaches, unauthorized access and cyber threats. Our research emphasizes the importance of balancing leveraging medical imaging technologies and implementing security protocols to protect individuals' private health information. Prioritizing both performance enhancement and security measures is vital for the integration and acceptance of AI-driven solutions in real-world healthcare environments. By maintaining this equilibrium, we can harness the potential of intelligence and IoT technologies to positively impact medical research and patient care while upholding patient privacy and safety.

References

[1] Qing Li et al., "Medical Image Classification with Convolutional Neural Network," *13th International Conference on Control Automation Robotics & Vision (ICARCV)*, Singapore, pp. 844-848, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[2] Sanaz Rahimi Moosavi et al., "SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways," *Procedia Computer Science*, vol. 52, pp. 452-459, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[3] Jie Lin et al., "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125-1142, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[4] Julia Rauscher, and Bernhard Bauer, "Safety and Security Architecture Analyses Framework for the Internet of Things of Medical Devices," *IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Ostrava, Czech Republic, pp. 1-3, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[5] Anastasiia Strielkina et al., "Cybersecurity of Healthcare IoT-Based Systems: Regulation and Case-Oriented Assessment," *IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, pp. 67-73, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[6] Anastasiia Strielkina, Vyacheslav Kharchenko, and Dmytro Uzun, "Availability Models of The Healthcare Internet of Things System Taking Into Account Countermeasures Selection," *Information and Communication Technologies in Education, Research, and Industrial Applications Conference*, pp. 220-242, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[7] Jianbing Ni, Xiaodong Lin, and Xuemin Shen, "Toward Edge-Assisted Internet of Things: From Security and Efficiency Perspectives," *IEEE Network*, vol. 33, no. 2, pp. 50-57, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[8] Truong Thu Huong et al., "LocKedge: Low-Complexity Cyberattack Detection in IoT Edge Computing," *IEEE Access*, vol. 9, pp. 29696-29710, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Truong Thu Huong et al., "An Efficient Low Complexity Edge-Cloud Framework for Security in IoT Networks," *IEEE Eighth International Conference on Communications and Electronics (ICCE)*, Phu Quoc Island, Vietnam, pp. 533-539, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Julia Rauscher, and Bernhard Bauer, "Adaptation of Architecture Analyses: An IoT Safety and Security Flaw Assessment Approach," *Proceedings of the 14th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2021)*, pp. 320-327, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Omar Cheikhrouhou et al., "A Lightweight Blockchain and Fog-enabled Secure Remote Patient Monitoring System," *Internet of Things*, vol. 22, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Celestino Obua, MUST Data Science Research Hub (MUDSReH), NIH RePORTER, 2022. [Online]. Available: https://reporter.nih.gov/project-details/10312539#details

[13] Ken Hoyme, Security Safety Co-Analysis Tool Environment (SSCATE), Adventium Enterprises, SBIR STTR America's Seed Fund, 2016. [Online]. Available: https://legacy.www.sbir.gov/sbirsearch/detail/1252209

[14] Ken Hoyme, Security Safety Co-Analysis Tool Environment (SSCATE), Adventium Enterprises, SBIR STTR America's Seed Fund, 2015. [Online]. Available: https://legacy.www.sbir.gov/sbirsearch/detail/869241

[15] Lenore McMackin, SBIR Phase II: Low Cost Shortwave Infrared (SWIR) Spectral Imaging Microscope Camera Based on Compressive Sensing, Inview Technology Corporation, SBIR STTR America's Seed Fund, 2014. [Online]. Available: https://legacy.www.sbir.gov/sbirsearch/detail/704773

[16] Lenore McMackin, SBIR Phase I: Low Cost Shortwave Infrared (SWIR) Spectral Imaging Microscope Camera Based on Compressive Sensing, Inview Technology Corporation, US National Science Foundation, 2013. [Online]. Available: https://www.nsf.gov/awardsearch/showAward?AWD_ID=1315515

[17] Milos Dobrojevic et al., "Addressing Internet of Things Security By Enhanced Sine Cosine Metaheuristics Tuned Hybrid Machine Learning Model and Results Interpretation Based on SHAP Approach," *PeerJ Computer Science*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Georg L. Baumgärtner et al., "Metadata-Independent Classification of MRI Sequences Using Convolutional Neural Networks: Successful Application to Prostate MRI," *European Journal of Radiology*, vol. 166, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Kusum Lata, and Linga Reddy Cenkeramaddi, "Deep Learning for Medical Image Cryptography: A Comprehensive Review," *Applied Sciences*, vol. 13, no. 14, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] Sarina Aminizadeh et al., "The Applications of Machine Learning Techniques in Medical Data Processing Based on Distributed Computing and The Internet of Things," *Computer Methods and Programs in Biomedicine*, vol. 241, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] Abdullah Lakhan et al., "Autism Spectrum Disorder Detection Framework for Children Based on Federated Learning Integrated CNN-LSTM," *Computers in Biology and Medicine*, vol. 166, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[22] Lihao Liu, Angelica I. Aviles-Rivero, and Carola-Bibiane Schonlieb, "Contrastive Registration for Unsupervised Medical Image Segmentation," *IEEE Transactions on Neural Networks and Learning Systems*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[23] Siraj Khan et al., "Efficient Leukocytes Detection and Classification in Microscopic Blood Images Using Convolutional Neural Network Coupled with A Dual Attention Network," *Computers in Biology and Medicine*, vol. 174, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[24] Huixin Jia et al., "Application of Convolutional Neural Networks in Medical Images: A Bibliometric Analysis," *Quantitative Imaging in Medicine and Surgery*, vol. 14, no. 5, pp. 3501-3518, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Giuseppe Rovere et al., "Adoption of Blockchain as A Step Forward in Orthopedic Practice," *European Journal of Translational Myology*, vol. 34, no. 2, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[26] Mousa Alalhareth, and Sung-Chul Hong, "Enhancing the Internet of Medical Things (IoMT) Security with Meta-Learning: A Performance-Driven Approach for Ensemble Intrusion Detection Systems," *Sensors*, vol. 24, no. 11, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[27] Hicham Amellal et al., "Quantum Man-in-the-Middle Attacks on QKD Protocols: Proposal of a Novel Attack Strategy," *6th International Conference on Contemporary Computing and Informatics*, Gautam Buddha Nagar, India, pp. 513-519, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[28] Shatha Alhazmi et al., "Mitigating Man-in-the-Middle Attack Using Quantum Key Distribution," *IEEE Long Island Systems, Applications and Technology Conference*, Old Westbury, NY, USA, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[29] Abdullah Al Hayajneh, Md Zakirul Alam Bhuiyan, and Ian McAndrew, "Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN)," *Computers*, vol. 9, no. 1, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[30] S. Aruna et al., "Detect and Prevent Attacks of Intrusion in IoT Devices Using Game Theory with Ant Colony Optimization (ACO)," *Journal of Cybersecurity and Information Management*, vol. 14, no. 2, pp. 275-286, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[31] Mst Shapna Akter et al., "Quantum Cryptography for Enhanced Network Security: A Comprehensive Survey of Research, Developments, and Future Directions," *IEEE International Conference on Big Data*, Sorrento, Italy, pp. 5408-5417, 2023. [CrossRef] [Google Scholar] [Publisher Link]