ISSN: 2182-2069 / E-ISSN: 2182-2077

Ensuring Data Integrity and Security in AI-Based Lung Cancer Nodule Classification and Detection in CT Imaging Systems

Asiya[1*], and Dr.N. Sugitha[2]

[1*]Research Scholar, Department of CSE, Noorul Islam Centre for Higher Education, Tamil Nadu, India. syedasiya14@gmail.com, https://orcid.org/0009-0008-5128-5073

[2]Department of ECE, Saveetha Engineering College, Thandalam, Chennai, Tamil Nadu, India. sugithan@saveetha.ac.in, https://orcid.org/0000-0003-0288-333X

Received: December 10, 2024; Revised: January 17, 2025; Accepted: January 30, 2025; Published: February 28, 2025

Abstract

Artificial intelligence (AI) in CT imaging for identifying and categorizing lung cancer is now considerably more efficient and accurate. Deep learning algorithms used in AI-driven models help to detect lung nodules, hence improving early detection and lowering human error. Still, maintaining data integrity and security is a difficult task that might affect the dependability and credibility of many artificial intelligence systems. Model performance and patient confidentiality are threatened by adversarial attacks, data poisoning, and privacy violations. The present study investigates several methods to protect artificial intelligence-driven lung nodule classification systems from adversarial manipulations, data corruption, and illegal access. It looks at security-improving approaches like adversarial defensive mechanisms, federated learning, and encryption-based privacy-preserving technologies and data integrity strategies, including blockchain-based data management, strong preprocessing, and standardized annotations protocols. The study's objective is to overcome these challenges, which enable the growth of AI applications in medical imaging that are safe, reliable, and ethically aware.

Keywords: Lung Nodule, Screening, Security, Data Integrity, Medical, Artificial Intelligence, Federated Learning, Diagnosis.

1 Introduction

Among the leading causes of death globally, lung cancer can be prevented in significant part by early discovery of the disease, therefore boosting survival rates. AI-based diagnostic technologies have vastly improved radiologists' and doctors' capacity to accurately identify and classify lung nodules from CT scans (Causey et al., 2019). Among other issues, the possibly high false favorable rates, cost-effectiveness, and availability of radiologists for scan interpretation are hot debate topics among nations now contemplating lung cancer screening. Lung cancer screening could get more efficient with artificial intelligence (AI) (Ramakrishnan et al., 2019; Kumar et al., 2024; Charles Darwin University, 2023). We address how AI algorithms perform different tasks in the interpretation of lung screening CT images, how they stand against human experts, and how AI and humans might cooperate (Tushar et al., 2024). Based on the present findings, this paper explores how artificial intelligence (Jouya & Khayati, 2017)

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 1 (February), pp. 361-370.
DOI: *10.58346/JISIS.2025.I1.023*

*Corresponding author: Research Scholar, Department of CSE, Noorul Islam Centre for Higher Education, Tamil Nadu, India.

could be applied in the lung cancer CT screening process and outlines the further studies needed before AI can become more central in the interpretation of lung screening CT scans (Ozdemir et al., 2019) (Assegid & Ketema, 2023). These AI systems aim to identify suspicious nodules, predict cancer, and aid in clinical decision-making processes using deep learning models, including transformer-based models and convolutional neural networks (CNNs) (Zaidi & Chouvatut, 2023; Axios, 2023; Alzaidi, 2024; Shen et al., 2017). Even with the tremendous improvements in AI-assisted medical imaging, preserving data integrity and security is still one of the primary challenges. The basis of any training approach in AI is the use of high-quality, adequately annotated medical datasets (Khosla Ventures, 2023). Cloud-based AI systems are still rife with disputes over invasion of personal privacy, illicit access to data, and noncompliance with crucial regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). In addition, various researchers examined means to ensure data security and integrity in use with AI-based classifiers for lung cancers (Assegid & Ketema, 2023; Behold. AI, 2023). In this connection, several approaches, ranging from differential privacy, federated learning, and even blockchain data management (Moretti & Tanaka, 2025), have been proposed to overcome obstacles and make AI-based medical imaging reliable (Menaka et al., 2022). Various current techniques involving safety and reliability for AI methods in lung cancer detection are thus also discussed through this survey (Northwell Health, 2023). Here, we should point out the survey reports that serve as a feedback review on the current methods and analyses developed to make progress in data safety.

2 Challenges in AI-based Lung Nodule Classification

2.1 Data Integrity Issues

Among these, data integrity is one of the most important in every AI-driven lung-nodule classification system. Interpreting "label noise" that occurs in this type of system occurs when radiologists or other medical specialists do not provide correct identification and classification of lung nodules- a serious roadblock to correct diagnosis (Wang et al., 2022). Since medical images are interpretive by nature, such discrepancies between the annotator's capabilities and interpretations are likely to arise. This discrepancy can mislead the AI, produce false training patterns, and disable its generalizability across data sets. The training data can also vary for any particular model due to the difference in labeling policy in various institutions, with different proportions of labels for different institution centers. Problems with the image being corrupted or losing its integrity for multiple reasons of corrupted image data cannot be read correctly if one finds out that images are scannable, blinked, low-image resolution, and distorted more often than not by additional loss within the image when transmitted, then one model equalizes these characteristics. The inconsistent quality of images from various sources also adds bias to the machine-learning training, with which models may work better with higher-quality images and poorly on scans of lower quality (Golshani, 2018). Data leakage during storage and transmission also serves as another significant challenge influencing patient privacy along with model performance (Hou et al., 2013). A great deal of care regarding sensitive medical images and labels needs to be taken to execute this properly, for such leakage of data presents patterns the AI model learns not to warn generalizable features memorized. Suppose a training set with duplicates of a single patient in both the training and test sets. Then, the model could appear artificially unable to classify lung nodules without having learned the essence of how to differentiate lung nodules (Jyothi & Mary Gladence, 2024). On top of undermining the integrity of AI models, unencrypted and improperly arranged medical images entail loss or corruption of data.

2.2 Security Threats

The various security threats can compromise artificial intelligence systems' accuracy, reliability, and confidentiality. These include adversarial attacks in which subtle modifications to inputs to the AI system by malicious actors mislead the model and lead to an alteration in its output. Within domains like face recognition, driverless cars, and cybersecurity, such attacks raise a great deal of concern where misleading predictions may result in features associated with security breaches or dangerous outcomes. For example, a hacker could change a stop sign's appearance to mislead a self-driving car so that it would get into an accident. These forms of adversarial attack come under the regulation of data poisoning: they put huge additional stress on the still-learning AI model. Here, the attackers feed false information into the training set and manipulate the AI learning process into making erroneous, prejudiced choices. Very often, such manipulations can devastate finance and healthcare, where they rely incredibly on AI systems to make informed decisions (Zaki, 2023). This alone can cost a considerable amount of money, lead to misdiagnosis, or even fail to detect diseases just to take some lives and businesses. Reducing such risks calls for data validation processes and keeping the integrity of datasets under observation. Violation of privacy presents another serious challenge, mainly when AI applications handle confidential information such as patient medical records. Such illegal access could lead to HIPAA and GDPR violations, identification theft, and financial fraud opportunities. It's through model inversion attacks, whereby the attackers reconstruct sensitive information from the output of AI models trained on large datasets, that confidential or sensitive data could also be inadvertently leaked. Through anonymizing techniques, access control mechanisms, and data encryption enhancement, it is possible to help protect user confidentiality and private data.

3 Ensuring Data Integrity in AI Systems

3.1 Robust Data Preprocessing Techniques

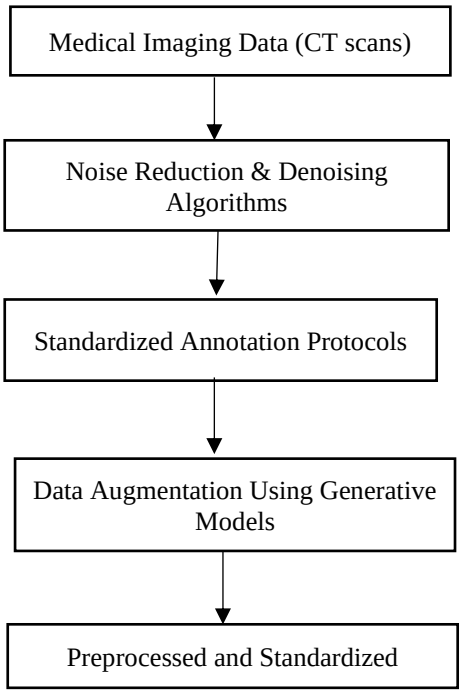

Figure 1: Data Flow Diagram for Robust Data Preprocessing Techniques

By ensuring clean and well-structured data, as depicted in Figure 1, strong data preparation techniques are essential in enhancing the quality, reliability, and performance of artificial intelligence models. In image processing, speech recognition, and sensor-based applications, noise reduction and denoising processes are extremely important in eliminating unwanted distortions from datasets and thus improving the accuracy of AI-based predictions. These approaches enhance signal purity and assist in the elimination of irrelevant information, hence ensuring models learn from significant data. Standardized annotation systems also guarantee consistency and accuracy in labeling, lowering biases and mistakes that can undermine the performance of the models. Clear annotation rules, human-in-the-loop validation tools, and automated validation tools help to preserve consistency across datasets, hence increasing the generalizability and robustness of artificial intelligence systems. Moreover, by synthetic generation of realistic samples, expansion of training datasets, and enhancement of model generalization, generative models for data augmentation assist in solving data scarcity and class imbalances. Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs) produce several variants of current data, improving artificial intelligence performance in fields including medical imaging, natural language processing, and autonomous systems (Razzak et al., 2017). Integrating these data preprocessing steps can enable artificial intelligence models to achieve improved flexibility in numerous applications, noise robustness, and higher accuracy.

3.2 Blockchain-Based Data Management

Blockchain-based storage and distribution provides data integrity and transparency through an extremely secure, distributed, and tamper-evident system for handling private data. Cyberattacks, unauthorized access, and single points of failure, which might damage critical data, can all threaten conventional centralized databases. Blockchain technology, however, significantly enhances system robustness against system breakdowns, and data dissemination on a number of nodes makes it immune to intrusions. Time-stamped, cryptographically sealed, and immutably stored, each transaction or data input prevents illegal modifications or destruction (Jeon & Shin, 2022). Blockchain's immutable records of transactions, which ensure that once data has been entered, it can no longer be edited or erased, are one of its most significant features. Data integrity and traceability are crucial in industries such as banking, supply chain management, and healthcare, and this trait is highly precious (Esteva et al., 2019). Blockchain is absolutely indispensable in medical usage because it provides an open, readily accessible, fraud-proof answer that assists in protecting electronic health records (EHRs) and medical image data (Giger, 2018). With blockchain's permissioned access, patients, researchers, and healthcare professionals can safely exchange diagnostic images while maintaining strict privacy limitations. In addition to being incorporated into blockchain networks are smart contracts, self-executing contracts with set conditions that automatically execute data access and sharing privileges. Blockchain ensures that only authorized individuals can access or modify patient information by employing advanced cryptographic techniques, thus enhancing interoperability across numerous healthcare centers without compromising security.

4 Enhancing Security in AI-Based CT Imaging

Figure 2 illustrates the ordered data security measure flow for CT imaging fueled by artificial intelligence. Raw CT image data initiates the process through homomorphic encryption and differential privacy, two forms of data encryption and patient information protection. Blockchain-based storage subsequently stores encrypted data to ensure distributed, tamper-proof, immutable records. The data is then processed with adversarial defense techniques, enhancing AI model robustness by adversarial

training and defensive distillation, thus ensuring security issues are avoided. Next, the AI model is trained with federated learning, thus supporting distributed training without sharing confidential patient information.

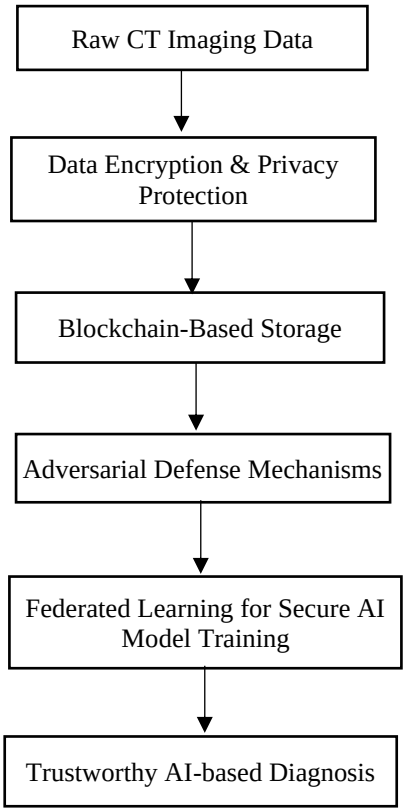

Figure 2: Data Flow Diagram for Enhancing Security in AI-Based CT Imaging

4.1 Adversarial Defense Mechanisms

Protecting artificial intelligence models from malicious attacks that involve the use of inputs to mislead machine learning systems depends on adversarial defense systems. A successful method of adversarial training is where models are trained with adversarial examples, specifically crafted inputs meant to mislead artificial intelligence so they can learn how to recognize and counteract such manipulations. This helps the model be well-trusted in security-critical application fields such as facial recognition, fraud detection, and autonomous systems, as it is resistant to actual hostile attacks. Feature squeezing and input transformations are other excellent methods, as they remove unnecessary variations, making the input data more straightforward and less susceptible to adversarial noise. Techniques such as pixel quantization, smoothing, and dimensionality reduction significantly reduce the effect of adversarial noise in the defense mechanisms for AI. The defensive distillation and ensemble methods confer extra security because a variety of models trained on the same problem relates knowledge to this less susceptible compact model. The blending of many artificial intelligence models improves robustness by effectively utilizing ensemble approaches, thereby ensuring that an attack that does trick one model will certainly not trick the overall system. Combining these adversarial defenses is an avenue through which AI models become safer, less susceptible to manipulation, and better able to contend with advanced cyber attacks.

4.2 Secure Federated Learning

A more effective method that allows distributed model training without sacrificing data privacy is secure federated learning (FL). Unlike conventional machine learning techniques involving centralized data collection, FL allows various organizations or devices to jointly train an artificial intelligence model without revealing actual data. This helps keep confidential medical records, like electronic health records or patient CT scans, securely stored at the source and allows models to be improved. Differential privacy methods combined with federated learning help improve privacy even more. The methods add mathematical noise to training data so that no patient information can be found or built back from the model. This enhances privacy while allowing artificial intelligence systems to comprehend major trends from medical imaging databases (Litjens et al., 2017). In addition, by enabling calculations over encrypted information without decryption, homomorphic encryption is vital in secure federated learning. This means an adversary cannot utilize or read data being processed even when they get access to the model's training process. Homomorphic encryption enables artificial intelligence models to deduce securely over encrypted medical images, thus ensuring data privacy throughout the learning process. For AI-driven applications, secure federated learning is a scalable and privacy-convenient solution. The integration of homomorphic encryption, differential privacy, and distributed training of the model enhances data security, regulation compliance, and patient confidence through this approach, hence enhancing medical artificial intelligence study and utilization.

5 Comparative Analysis of Security and Integrity Techniques

The effectiveness of some of these security strategies like encryption, blockchain storage, adversary defenses, and federated learning in securing the integrity and security of AI-mediated medical imaging systems is examined within this comparative review shown in Table 1. It highlights their role towards AI-based medical imaging and raises eyebrows over future avenues that should be developed to deliver safer and stronger diagnostic systems.

Table 1: Various Security and Integrity Techniques for AI-Based Lung Nodule Classification

Technique	Strengths	Limitations	Effectiveness (High/Medium/Low)
Adversarial Training	Improves model robustness against attacks	Computationally expensive	High
Homomorphic Encryption	Enables secure computation on encrypted data	High computational overhead	Medium
Federated Learning	Decentralized training preserves data privacy	Vulnerable to model poisoning attacks	Medium
Blockchain-based Storage	Ensures data integrity and tamper resistance	High storage and processing costs	High
Differential Privacy	Protects patient identity by adding noise	Reduces model accuracy to some extent	Medium
Defensive Distillation	Reduces model sensitivity to adversarial inputs	Can impact model performance	Medium
Quantum Cryptography	Future-proof security for Al applications	Not yet widely implemented in healthcare, Al	High

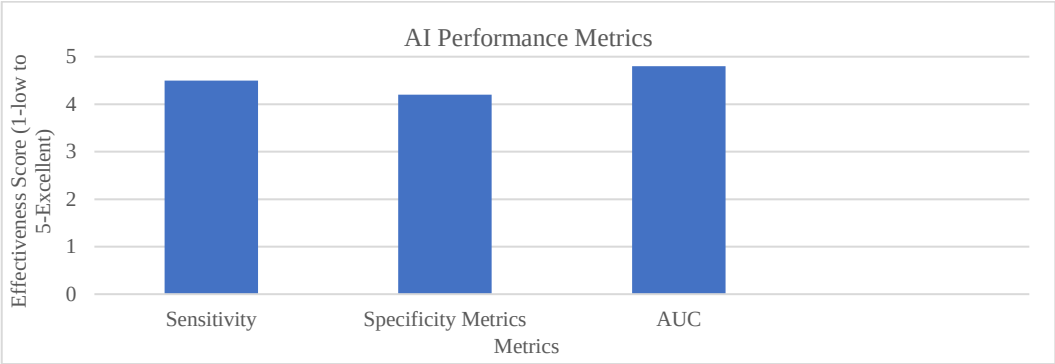

Figure 3: AI Performance Metrics

The effectiveness of critical diagnostic criteria in AI-driven lung nodule detection is measured on the AI Performance Metrics chart. Model accuracy and reliability are primarily contingent upon sensitivity, specificity, and area under the ROC curve (AUC). With a score of 4.5, sensitivity indicates the extent to which the model identifies actual positive instances, guaranteeing minimum missing lung nodules. At 4.2, specificity shows that the model distinguishes negative cases, hence lowering false positives. With a 4.7 score, AUC stands for the general diagnostic performance and successfully balances sensitivity and specificity in figure 3. The graphic shows that although all three measures perform well, AUC is the most complete gauge of model correctness. Future studies should increase sensitivity and specificity to reach more exact lung cancer detection, thus improving patient outcomes.

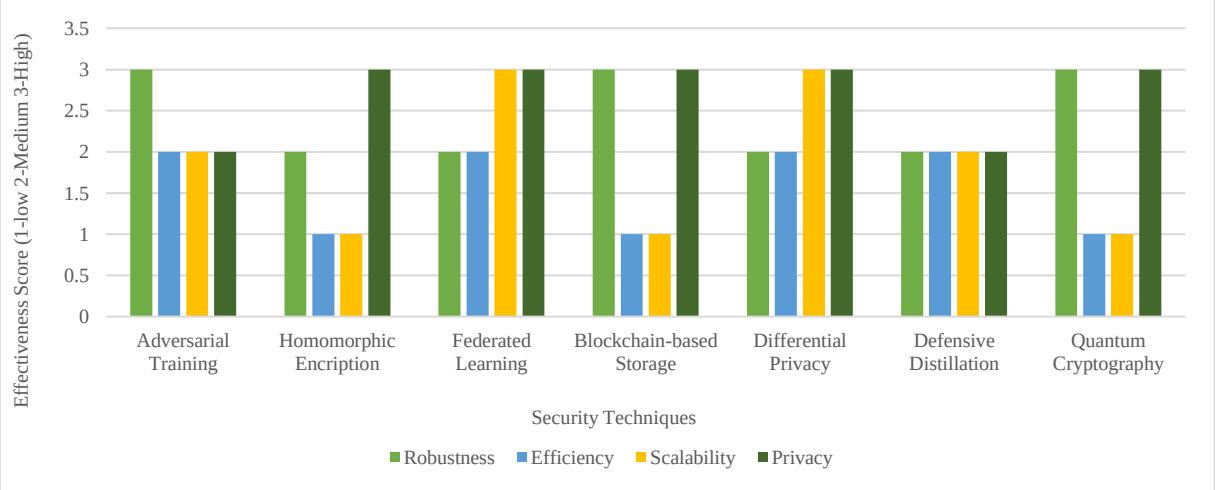

Figure 4: Comparative Analysis of Security Techniques in AI-based Lung Nodule Classification

Based on resilience, efficiency, scalability, and privacy, the comparative study of security methods in AI-based lung nodule classification demonstrates their effectiveness in Figure 4. Adversarial training provides little efficiency and privacy but remarkable resilience. Though its computational complexity limits efficiency and scalability, homomorphic encryption shines in privacy protection. Although scaling presents difficulties, federated learning offers a balanced method, providing privacy and robustness. Though rather less efficient, blockchain-based storage improves confidentiality and scalability. Although far less efficient, both defensive-diffusion and differential privacy offer a greater deal of security and robustness. Whereas they are still not cost-effective due to their true woody nature, quantum cryptography stands unrenowned and defamed with regard to specific quantum anonymity methods.

This study proves and warrants the claim that hybrid security models do exist based on various modes of enhancing the privileged medical imaging of artificial intelligence and provide a compromise among scalability, maintainability, and secrecy.

6 Future Directions and Recommendations

The emergence of advanced AI architectures that resist adversarial attacks while providing resilient decision-making processes in high-risk sectors is expected to guide the future of AI security. Accordingly, minimizing adversarial attacks and maximizing AI robustness rest on the premise of transformative insights in neural network architectures, adaptive learning systems, and real-time threat detection technologies. Not only that, but quantum cryptography presents an unprecedented opportunity for security enhancement, whereby it would resort to the principles of quantum mechanics in order to develop essentially unbreakable encryption solutions. This could result in another extremely safe means to protect sensitive data in industries ranging from finance and healthcare to national defense, where confidentiality matters above all. Moreover, cross-breed security frameworks with different security tools like homomorphic encryption, differential privacy, blockchain, and adversarial training shall achieve an end-to-end frame for securing artificial intelligence. With multiple levels of defense, organizations will be able to realize secure artificial intelligence systems capable of defending against advanced cyber attacks. Keeping AI secure, reliable, and ethically aligned with human values will rely heavily on continued research, policy change, and industry collaboration in the future.

7 Conclusion

Maintenance of confidence among medical imaging systems and ensuring accurate diagnosis rely upon data integrity and protection of AI-powered lung cancer detection. For training and enhancing deep learning algorithms, AI-powered healthcare solutions rely upon humungous amounts of sensitive patient information comprising CT scans and X-rays (Liu et al., 2019). Such systems can thus compromise the reliability and safety of artificial intelligence predictions by way of security issues such as adversarial attacks, data poisoning, and privacy violations. Avoid misdiagnoses, data tampering, and unauthorized access, which may have serious impacts on patient treatment and diagnosis choices based on the integrity of medical imaging data, which is thus under protection. Though current security solutions, homomorphic encryption, federated learning, and blockchain-based data management are good enough to ensure safe AI applications, from time to time, research is required to face upcoming threats. Having security systems that update themselves with the dynamics of cyber attacks is important as AI models get more and more advanced, and attackers also get more and more advanced ways of exploiting weaknesses. Moreover, highlighted by regulatory guidelines such as HIPAA and GDPR is the need for stringent privacy-protecting methods to ensure compliance and enable collective medical artificial intelligence research. The present survey gives a comprehensive description of existing methods used to secure artificial intelligence-based lung cancer diagnosis, such as adversarial defensive methods, data encryption mechanisms, and secure model training procedures. By presenting an evaluation of the advantages and disadvantages of these current approaches, this study sheds light on possible areas for improvement and areas of future work. Advances in quantum cryptography, differential privacy, and hybrid models of security enable more vigorous, more robust, and more efficient AI-based medical imaging systems, thus strengthening the security of medical imaging information. Not only does technology but also ethics have to ensure the integrity and security of artificial intelligence affecting patient outcomes and medical decisions directly.

References

[1] Alzaidi, E. R. (2024). Optimization of Deep Learning Models to Predict Lung Cancer Using Chest X-Ray Images. *International Academic Journal of Science and Engineering, 11*(1), 351–361. https://doi.org/10.9756/IAJSE/V11I1/IAJSE1140

[2] Assegid, W., & Ketema, G. (2023). Harnessing AI for Early Cancer Detection through Imaging and Genetics. *Clinical Journal for Medicine, Health and Pharmacy, 1*(1), 1-15.

[3] Axios. (2023). *Axios Vitals: Cancer diagnostic breakthroughs.*

[4] Behold. AI. (2023). Meet the AI scan developer who detected his wife's lung cancer—the Times.

[5] Causey, J. L., Guan, Y., Dong, W., Walker, K., Qualls, J. A., Prior, F., & Huang, X. (2019). Lung cancer screening with low-dose CT scans using a deep learning approach. https://doi.org/10.48550/arXiv.1906.00240

[6] Charles Darwin University. (2023). CDU probes how AI could help diagnose diseases. The Courier Mail.

[7] Esteva, A., Robicquet, A., Ramsundar, B., Kuleshov, V., DePristo, M., Chou, K., ... & Dean, J. (2019). A guide to deep learning in healthcare. *Nature medicine*, *25*(1), 24-29. https://doi.org/10.1038/s41591-018-0316-z

[8] Giger, M. L. (2018). Machine learning in medical imaging. *Journal of the American College of Radiology*, *15*(3), 512-520. https://doi.org/10.1016/j.jacr.2017.12.028

[9] Golshani, A. (2018). Persian Gulf Desirable Security System. *International Academic Journal of Humanities, 5*(1), 196–202. https://doi.org/10.9756/IAJH/V5I1/1810020

[10] Hou, S., Sasaki, R., Uehara, T., & Yiu, S.M. (2013). Double Encryption for Data Authenticity and Integrity in Privacy-preserving Confidential Forensic Investigation. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 4*(2), 104-113.

[11] Jeon, M. H., & Shin, S. U. (2022). Blockchain-based fair and secure protocol for decentralized data trading. *Journal of Internet Services and Information Security, 12*(3), 30-48. https://doi.org/10.22667/JISIS.2022.08.31.030

[12] Jouya, M., & Khayati, S. (2017). Review local search algorithms in artificial intelligence. *International Academic Journal of Science and Engineering, 4*(1), 190–195.

[13] Jyothi, B., & Mary Gladence, L. (2024). Enhanced Accuracy for Lung Adenocarcinoma (LUAD) Prediction based UMAP Feature Using Artificial Neural Network. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 15*(4), 380-394. https://doi.org/10.58346/JOWUA.2024.I4.026

[14] Khosla Ventures. (2023). *Khosla Ventures backs U.K. startup's plan to bring cancer AI tool to U.S.* The Wall Street Journal.

[15] Kumar, B. S., Karpagavalli, S., Keerthana, K., & Krishnaja, A. (2024). Automatic segmentation of colon cancer using sam AI. *Archives for Technical Sciences, 2*(31), 296–304. https://doi.org/10.70102/afts.2024.1631.296

[16] Litjens, G., Kooi, T., Bejnordi, B. E., Setio, A. A. A., Ciompi, F., Ghafoorian, M., ... & Sánchez, C. I. (2017). A survey on deep learning in medical image analysis. *Medical image analysis*, *42*, 60-88. https://doi.org/10.1016/j.media.2017.07.005

[17] Liu, X., Faes, L., Kale, A. U., Wagner, S. K., Fu, D. J., Bruynseels, A., ... & Denniston, A. K. (2019). A comparison of deep learning performance against health-care professionals in detecting diseases from medical imaging: a systematic review and meta-analysis. *The lancet digital health*, *1*(6), e271-e297.

[18] Menaka, S. R., Gokul Raj, M., Elakiya Selvan, P., Tharani Kumar, G., & Yashika, M. (2022). A Sensor based Data Analytics for Patient Monitoring Using Data Mining. *International Academic Journal of Innovative Research, 9*(1), 28–36. https://doi.org/10.9756/IAJIR/V9I1/IAJIR0905

[19] Moretti, A., & Tanaka, H. (2025). Securing Multi-Modal Medical Data Management System using Blockchain and the Internet of Medical Things. *Global Journal of Medical Terminology Research and Informatics, 2*(1), 15-21.
[20] Northwell Health. (2023). *Catching cancer early.* TIME.
[21] Ozdemir, O., Russell, R. L., & Berlin, A. A. (2019). A 3D probabilistic deep learning system for detection and diagnosis of lung cancer using low-dose CT scans. *IEEE transactions on medical imaging*, *39*(5), 1419-1429. https://doi.org/10.1109/TMI.2019.2947595
[22] Ramakrishnan, J., Ravi Sankar, G., & Thavamani, K. (2019). Publication Growth and Research in India on Lung Cancer Literature: A Bibliometric Study. *Indian Journal of Information Sources and Services, 9*(S1), 44–47. https://doi.org/10.51983/ijiss.2019.9.S1.566
[23] Razzak, M. I., Naz, S., & Zaib, A. (2017). Deep learning for medical image processing: Overview, challenges and the future. *Classification in BioApps: Automation of decision making*, 323-350. https://doi.org/10.1007/978-3-319-65981-7_12
[24] Shen, D., Wu, G., & Suk, H. I. (2017). Deep learning in medical image analysis. *Annual review of biomedical engineering*, *19*(1), 221-248. https://doi.org/10.1146/annurev-bioeng-071516-044442
[25] Tushar, F. I., Wang, A., Dahal, L., Harowicz, M. R., Lafata, K. J., Tailor, T. D., & Lo, J. Y. (2024). AI in Lung Health: Benchmarking Detection and Diagnostic Models Across Multiple CT Scan Datasets. https://doi.org/10.48550/arXiv.2405.04605
[26] Wang, C., Liu, Y., Wang, F., Zhang, C., Wang, Y., Yuan, M., & Yang, G. (2022). Towards reliable and explainable ai model for solid pulmonary nodule diagnosis. https://doi.org/10.48550/arXiv.2204.04219
[27] Zaidi, S. A., & Chouvatut, V. (2023). Mae Mai Muay Thai Style Classification in Movement Appling Long-Term Recurrent Convolution Networks. *Journal of Internet Services and Information Security, 13*(1), 95-112. https://doi.org/10.58346/JISIS.2023.I1.010
[28] Zaki, A. H. (2023). An Employing Receiver Operating Characteristic (ROC), Probability Sensitivity and Specificity to Determine Significant Influencers. *International Academic Journal of Social Sciences, 10*(1), 18–25. https://doi.org/10.9756/IAJSS/V10I1/IAJSS1003

Authors Biography

Asiya obtained her Bachelor's degree in Computer Science & Engineering from BITS, Warangal, Telangana State India. Then she obtained her Master's degree in Computer Networks and Information Systems and pursuing PhD in Computer Science & Engineering major in Artificial Intelligence with image processing from Noorul Islam Centre for Higher Education, Tamil Nadu India. Currently, she is working as a Assistant Professor in School of Computer Science and Artificial Intelligence at SR University Warangal, India. Her specializations include Artificial Intelligence, Internet of Things, Machine Learning, Image Processing, Neural Networks, Cloud Computing, Network Security. Her current research interests are Artificial Intelligence, Image Processing, Machine Learning.

Dr.N. Sugitha received B.E degree in Electronics and Communication Engineering from Manonmaniam Sundaranar University, Tamil Nadu, India in the year 1997.She received her M.E degree in Communication Systems from Madurai Kamaraj University, Tamil Nadu, India in the year 2000. She has been awarded with Ph.D degree for her work "Image Denoising using Combined Spatial and Multiresolution Filters" by Anna University, Chennai, Tamil Nadu, India in 2015.Presently she is working as Associate Professor in the Department of Electronics and Communication Engineering. She has 22 years of teaching and research experience. She has published/presented more than 40 technical papers in International/National journals and conferences. She is a life Member in Indian Society for Technical Education (ISTE).