International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 6, 2025
https://www.theaspd.com/ijes.php

Deep Learning Methodology for Data Security in Healthcare

Rishabh Jain[1], Dr. Neha Yadav[2] and Shuchi Sharma[3]
[1]Assistant Professor, Dr. Akhilesh Das Gupta Institute of Professional Studies, New Delhi, India, jainrishabh062@gmail.com
[2]Assistant Professor, Dr. Akhilesh Das Gupta Institute of Professional Studies, New Delhi, India, yneha5976@gmail.com
[3]Assistant Professor, Dr. Akhilesh Das Gupta Institute of Professional Studies, New Delhi, India, 303shuchi@gmail.com

Abstract: *The rapid digitalization of healthcare has resulted in a massive influx of sensitive patient data, making data security a critical concern. Traditional security methods often fall short in addressing the evolving complexity of cyber threats. Deep learning, a subset of artificial intelligence, offers advanced methodologies for enhancing data protection by leveraging neural networks to detect anomalies, predict vulnerabilities, and automate security protocols. This paper explores deep learning-based approaches for securing healthcare data, focusing on techniques such as intrusion detection systems (IDS), data encryption, privacy-preserving machine learning, and biometric authentication. The integration of convolutional neural networks (CNNs), recurrent neural networks (RNNs), and auto encoders has demonstrated significant potential in identifying security breaches, safeguarding electronic health records (EHRs), and ensuring compliance with regulatory frameworks like HIPAA. Furthermore, deep learning facilitates real-time threat detection, adaptive defence mechanisms, and robust encryption methods, thereby strengthening data integrity, confidentiality, and availability. This study emphasizes the transformative role of deep learning in creating intelligent, scalable, and resilient security frameworks for healthcare, ultimately improving patient trust and the overall quality of care delivery.*

Keywords: *Health care, Deep Learning, Security, CNN, Artificial Intelligence.*

INTRODUCTION

In an era where healthcare systems are increasingly reliant on digital technologies and interconnected networks, ensuring the security and privacy of sensitive patient data has become paramount. With the rise of cyber threats targeting healthcare organizations, traditional security measures are proving insufficient to safeguard against sophisticated attacks. However, the advent of deep learning offers promising avenues for bolstering healthcare security through innovative data protection solutions. Deep learning, a subset of artificial intelligence (AI), has demonstrated remarkable capabilities in various domains, including computer vision, natural language processing, and pattern recognition. Leveraging its ability to autonomously learn intricate patterns and features from vast datasets, deep learning presents a powerful toolset for enhancing healthcare security. This paper explores the role of deep learning in advancing healthcare security, specifically focusing on its applications in data protection. By employing deep learning techniques such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and generative adversarial networks (GANs), healthcare organizations can fortify their defenses against cyber threats and safeguard patient privacy. This introduction sets the stage for delving into the nuances of deep learning-based security solutions in healthcare, highlighting their potential to mitigate risks, detect anomalies, and proactively combat cyber attacks. Through a comprehensive examination of the current landscape and future prospects, this paper aims to elucidate the transformative impact of deep learning on healthcare security and pave the way for a more resilient and secure healthcare ecosystem. Machine learning is rapidly increasing in the domains of classification and prediction, similar to artificial intelligence. Deep learning techniques are often used for healthcare. The present status of research in the area of healthcare is plagued by either subpar performance or inaccuracy. This research provides a comprehensive examination of the existing literature about the detection of diseases. It explores the many approaches, instruments, and technologies that are now used in this field. This study not only examines novel research findings but also tackles issues pertaining to deficiencies in previous research, such as subpar performance and erroneous outcomes. Currently, experts are endeavoring to discern methods for healthcare. The use of edge detector processing has been employed to enhance the efficiency and accuracy of images. The inquiry encompasses the use of photos, the detection of boundaries, deep learning, and healthcare. The suggested approach would decrease the need for expensive and time-intensive surgical procedures in the diagnosis of diseases. Close monitoring will be conducted to assess the neural network's predictive performance throughout its operation. The proposed study aims to enhance the accuracy of prediction models by integrating several compression and edge detection techniques with deep learning mechanisms. Once the dataset was trained, the confusion measures were calculated to assess the dependability of the test results. The suggested model will be assessed based on its effectiveness and accuracy compared to the current model. In healthcare here we include medical image analysis, enabling automated interpretation of radiological images such as X-rays, MRIs, and CT scans. By leveraging convolutional neural networks (CNNs), deep learning algorithms can detect abnormalities, tumors, and other pathologies with high accuracy, aiding clinicians in early disease detection and diagnosis. Moreover, deep learning plays a crucial role in personalized medicine by analyzing genomic data to identify genetic markers associated with disease susceptibility, drug response, and treatment outcomes. Additionally, natural language processing (NLP) techniques powered by deep learning facilitate the analysis of unstructured clinical notes, electronic health records (EHRs), and medical literature, extracting valuable insights for clinical decision-making and research. Furthermore in this research healthcare operation by optimizing hospital workflows, predicting patient outcomes, and improving resource allocation. Despite its transformative potential, the widespread adoption of deep learning in healthcare necessitates addressing challenges related to data privacy, model interpretability, and regulatory compliance.

Deep learning is an artificial intelligence technique that emulates the data processing and pattern generation capabilities of the human brain to facilitate decision-making. Deep learning is a specific branch of artificial intelligence that falls under the umbrella of machine learning. It employs neural networks to acquire knowledge from unstructured or unlabeled data using unsupervised learning methods. The names "deep neural learning" or "deep neural networks" are used to refer to this approach. Due to the increasing significance of AI, it is imperative to improve medical imaging systems that rely on deep learning. Detecting a brain tumor might pose challenges due to the absence of clear indications of its presence in the patient's brain. The deep learning technique employs a neural network for the purpose of identifying brain MRI abnormalities. This endeavor necessitates the use of a specialized neural network that has been trained exclusively to identify and monitor tumors. In a reinforcement learning context, the neural network undergoes direct training. In differential graphic games, many agents are used to govern the player's interactions with the environment. These games use a method known as reinforcement learning. It is also a component of a category of methods that use several levels of abstraction to build increasingly intricate AI systems. This setting has never before used machine learning. Nevertheless, deep learning systems were specifically designed to address certain types of problems. Reinforcement learning is an alternate term used to describe machine learning. Machine learning is a kind of computational approach. Historically, machine learning has only been used in theoretical contexts. Image processing technologies are often used to scale, compare, and alter visual material. A CNN model is often used to detect masking patterns in a collection of photographs. Nevertheless, certain challenges emerge when attempting to classify data using CNN.Your data must be protected from unauthorized access and corruption at every step of its lifecycle.

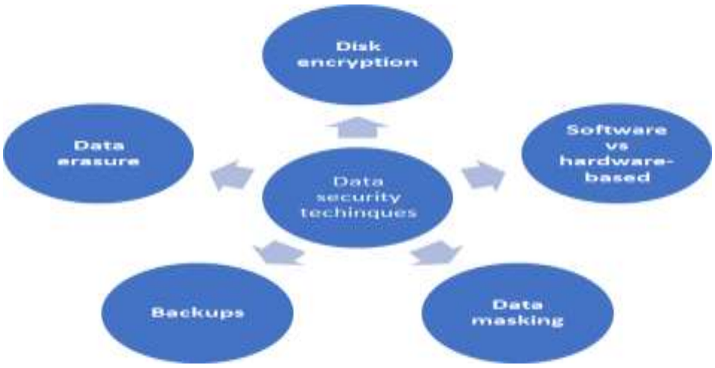

Fig 1.Techniques used in data security ROLE

OF SECURITY IN HEALTHCARE

Security plays a paramount role in healthcare, serving as a cornerstone for safeguarding patient data, protecting medical devices, and ensuring the integrity of healthcare systems. The healthcare sector handles vast amounts of sensitive information, including patients' personal data, medical histories, and treatment records. As such, maintaining the confidentiality, integrity, and availability of this data is crucial for preserving patient privacy and trust. One of the primary roles of security in healthcare is to prevent unauthorized access to patient information. Robust authentication mechanisms, access controls, and encryption protocols are implemented to restrict access to authorized personnel only, mitigating the risk of data breaches and unauthorized disclosure of sensitive data. Additionally, encryption techniques are employed to secure data both in transit and at rest, further safeguarding against interception and unauthorized access. Furthermore, security measures are essential for protecting medical devices and infrastructure from cyber threats. With the proliferation of connected medical devices and IoT technologies in healthcare settings, ensuring the security of these devices is paramount to prevent potential risks to patient safety and the integrity of healthcare operations. Vulnerability assessments, patch management, and network segmentation are among the strategies employed to mitigate security risks associated with medical devices and IoT systems.

In addition to protecting data and devices, security in healthcare also encompasses regulatory compliance and risk management. Healthcare organizations must adhere to stringent regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, to safeguard patient privacy and security. Compliance with regulatory standards involves implementing robust security policies, conducting regular risk assessments, and maintaining comprehensive audit trails to demonstrate adherence to legal and regulatory requirements. Moreover, security in healthcare extends beyond technological measures to encompass awareness training, incident response, and disaster recovery planning. Healthcare personnel are trained to recognize and respond to security threats, such as phishing attacks, malware infections, and social engineering tactics, to minimize the risk of data breaches and operational disruptions. Additionally, incident response plans and disaster recovery strategies are put in place to mitigate the impact of security incidents and ensure continuity of care in the event of disruptions to healthcare services. Security plays a critical role in healthcare by safeguarding patient data, protecting medical devices, ensuring regulatory compliance, and mitigating security risks. By implementing robust security measures, healthcare organizations can uphold patient privacy, maintain the integrity of healthcare systems, and preserve trust in the delivery of healthcare services.

ROLE OF DEEP LEARNING IN HEALTHCARE

The role of deep learning in healthcare is multifaceted and increasingly vital in advancing various aspects of medical diagnosis, treatment, and patient care. Deep learning, a subset of artificial intelligence (AI), excels in processing vast amounts of complex data, extracting intricate patterns, and making accurate predictions. In healthcare, deep learning has emerged as a powerful tool for medical image analysis, enabling automated interpretation of radiological images such as X-rays, MRIs, and CT scans. By leveraging convolutional neural networks (CNNs), deep learning algorithms can detect abnormalities, tumors, and other pathologies with high accuracy, aiding clinicians in early disease detection and diagnosis. Moreover, deep learning plays a crucial role in personalized medicine by analyzing genomic data to identify genetic markers associated with disease susceptibility, drug response, and treatment outcomes. Additionally, natural language processing (NLP) techniques powered by deep learning facilitate the analysis of unstructured clinical notes, electronic health records (EHRs), and medical literature, extracting valuable insights for clinical decision-making and research. Furthermore, deep learning models contribute to healthcare operations by optimizing hospital workflows, predicting patient outcomes, and improving resource allocation. Despite its transformative potential, the widespread adoption of deep learning in healthcare necessitates addressing challenges related to data privacy, model interpretability, and regulatory compliance. Overall, deep learning holds immense promise in revolutionizing healthcare delivery, driving innovation, and ultimately improving patient outcomes.

LITERATURE REVIEW

B. Wiestler and colleagues (2020) conducted research on deep learning for the purpose of analyzing medical photos. The purpose of this brief is to offer a concise introduction to neural networks, with a special emphasis on CNN. They are going to explain how these networks are able to separate structures of interest in the image volume on their own, how they learn to link imaging results with important (clinical) factors such as genetics, and why they are able to be so good at detecting relevant features. As part of their discussion, they will also discuss some of the challenges that stand in the way of the widespread implementation of these methodologies.

S. Bhattacharya and colleagues (2021) presented medical image analysis using deep learning in response to the COVID-19 coronavirus epidemic. The first thing that they do is provide a brief summary of the most current discoveries that have been made in the area of deep learning in relation to COVID-19 medical IP. After that, they provide a synopsis of the use of deep learning in the medical profession in recent times. Finally, let's speak about a few issues and challenges that have arisen during the implementation of DL for COVID-19 medical IP. These issues are likely to encourage more study into putting an end to the crisis and preventing the further spread of the virus, which will finally result in communities that are smart and healthy.

M. Puttagunta and colleagues (2021) presented their research on the use of deep learning to the processing of medical images. In this essay, the advancements that have been achieved in ANN are discussed in length, including an in-depth analysis of DLA, which has the potential to be very useful in medical imaging. Imagery from X-rays, computed tomography (CT), mammograms, and digital histology are often the primary focus of DLA missions. It provides a thorough study of the research that has been done on the use of DLA in the classification, identification, and segmentation of medical photographic images. Academics will be able to better think of successful approaches to use DLA to medical image analysis with the assistance of this overview.

The current state of the art in automated sickness diagnosis via the use of medical photographs was the primary emphasis of B. M. Rashed and colleagues (2022). They used the PRISMA methodology to select through publications in an effective manner, and by the time we reached the conclusion of the process, we had forty studies that were conducted throughout the course of the previous five years (2017-2021) that were pertinent to our research issues. Approaches for medical intellectual property and analysis were found, investigated, and evaluated. These approaches included those that were applied for preprocessing, segmentation, functional error, and diagnosis. This page also provides a comprehensive explanation of machine learning and deep learning with many examples. Additionally, the greatest medical intellectual property strategies that were used in these papers as well as the best methodology for future approaches were spoken about, and the collection was suggested as a complete reference source for the utilization of these techniques in future medical diagnostic systems.

A review of DL for medical image analysis was conducted by S. Suganyadevi and colleagues (2022). One of the many industries that has lately profited from the extensive use of deep learning is the medical industry. A concise summary was provided for the research that was carried out in the following areas: the skeleton, the human eye, the lungs, the computerized illness, the breasts, the bones, the digestive system, the muscles, and the neurological system. The successful applications of deep learning networks to big data include the discovery of information, the deployment of knowledge, and the prediction of knowledge-based outcomes. The purpose of this article is to give basic information as well as cutting-edge applications of deep learning to the study of medical image processing and analysis. A comprehensive review of this topic was one of the primary objectives of this study, along with the identification and implementation of the most important concepts that have emerged as a result of research in the field of medical image processing.

PROBLEM STATEMENT

It is important to note that this study has several limitations. To begin, this is qualitative study; so, rather than attempting to quantify the predominance of opinions, we would want to emphasize the range of problems that need to be investigated in relation to confidentiality of digital health information. We are unable to ensure that our experts correctly represent the whole community of professionals in the disciplines from which they were recruited since the sample size for the qualitative method is quite small. Despite the fact that efforts were made to create a broad sample, it is possible that some points of view are not well represented. The second factor is the continuously shifting landscape of internet privacy and the attention that the general public is paying to it. The results of the study provide a representation of the time period that was investigated. In the third place, our interview guide did not make any effort to arrive at policy solutions, and we did not gather sufficient data from our experts in order to identify the full spectrum of viewpoints on privacy laws and potential policy responses. In conclusion, it is impossible to completely eliminate the impact of social standards.

OBJECTIVE OF STUDY:

- To consider the existing research in field of security, deep learning and healthcare.
- To focus the issues related to performance and accuracy during neural network based prediction operation
- To integrated compression and edge detection mechanism with deep learning mechanism to Building high performance, reliable and more accurate predication model.

RESEARCH METHODOLOGY

The research methodology for advancing healthcare security through deep learning solutions for data protection involves a systematic approach to address the complex challenges inherent in securing sensitive patient information. The first step entails conducting a thorough literature review to identify existing research gaps, trends, and methodologies in healthcare security and deep learning applications. Subsequently, the research problem is carefully formulated, delineating clear objectives and target security tasks such as anomaly detection, intrusion detection, and privacy preservation. Data collection follows, where diverse healthcare datasets are gathered, ensuring compliance with privacy regulations and obtaining necessary permissions. Preprocessing of collected data involves cleaning, normalizing, and anonymizing to ensure data quality and privacy preservation. Model selection and design involve exploring and customizing deep learning architectures suitable for the identified security tasks, tailored to the unique challenges of healthcare environments. Experimental protocols are defined for model training, validation, and evaluation, with datasets partitioned into training, validation, and testing sets. Model performance is rigorously assessed using metrics such as accuracy, precision, recall, and F1-score, with fine-tuning of hyper parameters and adjustments to model architectures based on validation results. Ethical considerations related to patient privacy and data confidentiality are addressed throughout the research process, ensuring compliance with regulatory requirements and ethical guidelines. Ultimately, research findings are interpreted in the context of the research objectives, drawing conclusions regarding the efficacy and potential impact of deep learning solutions for advancing healthcare security and data protection. Dissemination of research outcomes through peer-reviewed publications and conference presentations contributes to knowledge advancement and informs practical applications in healthcare settings. Process flow of advancing healthcare Security considered deep learning solutions for data protection:

1. **Data Collection and Preprocessing:** The process begins with the collection of healthcare data from various sources such as electronic health records (EHRs), medical imaging, wearable devices, and IoT sensors. Data preprocessing techniques are applied to clean, normalize, and anonymize the collected data to protect patient privacy and ensure data integrity.
2. **Feature Extraction and Representation:** Deep learning models are employed to extract relevant features from the preprocessed healthcare data. Techniques like convolutional neural networks (CNNs) are utilized for extracting features from medical images, while recurrent neural networks (RNNs) may be applied for processing sequential data such as time-series patient records.
3. **Model Training and Validation:** The extracted features are used to train deep learning models for specific security tasks, such as anomaly detection, intrusion detection, or privacy preservation. Datasets are divided into training, validation, and testing sets, and the models are trained on the training data and validated on the validation set to ensure optimal performance.
4. **Anomaly Detection:** Trained deep learning models are deployed for anomaly detection to identify unusual patterns or behaviors within the healthcare data that may indicate security breaches or data tampering. Models continuously monitor incoming data streams in real-time, flagging any deviations from expected norms and triggering alerts for further investigation.

5. **Intrusion Detection:** Deep learning algorithms are employed for intrusion detection to identify and thwart malicious attempts to access or compromise healthcare systems. Models analyze network traffic, system logs, and user activities to detect suspicious behavior indicative of cyber attacks or unauthorized access.
6. **Privacy Preservation:** Deep learning techniques such as generative adversarial networks (GANs) may be utilized for privacy preservation by generating synthetic data that retains statistical properties of the original dataset while preserving patient anonymity. Models learn to generate synthetic data samples that closely resemble real patient data, enabling healthcare organizations to perform data analysis and research without compromising individual privacy.
7. **Model Evaluation and Optimization:** Trained models are evaluated on the testing set to assess their performance metrics such as accuracy, precision, recall, and F1-score. Models are iteratively optimized through techniques like hyper parameter tuning, model ensembling, and regularization to improve performance and generalization ability.
8. **Deployment and Integration:** Once validated, optimized, and tested, the deep learning models are deployed into the healthcare environment. Integration with existing healthcare systems and IT infrastructure ensures seamless operation and interoperability with other security measures and protocols.

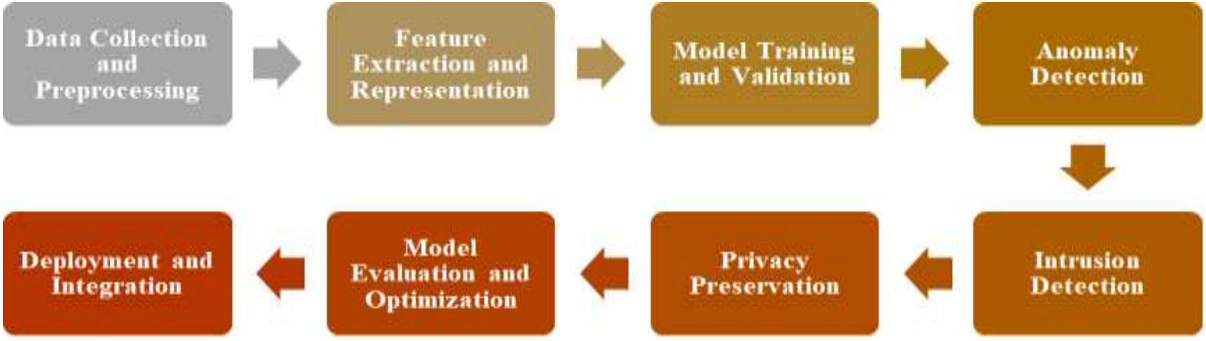
Data Collection and Preprocessing
Feature Extraction and Representation
Model Training and Validation
Anomaly Detection
Intrusion Detection
Privacy Preservation
Model Evaluation and Optimization
Deployment and Integration

Fig 2. Process flow of Research Methodology

This process flow outlines the systematic approach to implementing deep learning solutions for advancing healthcare security, with a focus on data protection and privacy preservation. Through the integration of cutting-edge deep learning techniques and rigorous evaluation methodologies, healthcare organizations can fortify their security posture and safeguard patient data against evolving cyber threats. The combination of compression and edge detection mechanisms has been shown to decrease the file size. Additionally, the training and testing time is decreased as a result of using compressed pictures. The redundant area of the picture, which does not contribute significantly to pattern detection, has been removed. Therefore, the amount of time required and the storage capacity needed are decreased, resulting in improved precision of the task. Recent study is advancing healthcare Security considered deep learning solutions for data protection. Although there has been discourse on the use of deep learning for the detection of diseases, more research and efforts are required. The use of edge detection into an existing deep learning methodology for diseases identification has resulted in enhanced precision.

FUTURE SCOPE

The future scope of advancing healthcare security through deep learning solutions for data protection holds immense potential for transformative impact in the field. As technology continues to evolve and healthcare systems become increasingly digitized and interconnected, the need for robust security measures to safeguard sensitive patient data becomes even more critical. Deep learning, with its ability to autonomously learn complex patterns and features from large datasets, offers promising avenues for addressing emerging security challenges in healthcare environments. One key future direction lies in the development of more sophisticated deep learning models tailored specifically for healthcare security applications. Advancements in model architectures, such as the integration of attention mechanisms, graph neural networks, and reinforcement learning techniques, hold promise for improving the accuracy, efficiency, and adaptability of security solutions. Additionally, the exploration of federated learning and decentralized approaches can enable collaborative model training across multiple healthcare institutions while preserving data privacy and security. Furthermore, there is a growing emphasis on addressing ethical and regulatory considerations in healthcare security research. Future efforts will focus on ensuring compliance with evolving privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR), while promoting transparency, fairness, and accountability in AI-driven security solutions. Collaborative initiatives between researchers, policymakers, and industry stakeholders will be essential for developing ethical frameworks and guidelines to govern the responsible use of deep learning technologies in healthcare security. Another area of future exploration lies in the integration of multimodal data sources and advanced analytics techniques for comprehensive threat detection and risk assessment. By combining information from diverse sources such as electronic health records, medical imaging, genomic data, and IoT devices, deep learning models can provide holistic insights into potential security threats and vulnerabilities. Moreover, the incorporation of explainable AI methods can enhance interpretability and trustworthiness, enabling healthcare practitioners to understand and validate the decisions made by AI-driven security systems. In conclusion, the future of advancing healthcare security through deep learning solutions for data protection is characterized by continuous innovation, collaboration, and ethical considerations. By harnessing the capabilities of deep learning in conjunction with rigorous research methodologies and ethical frameworks, we can pave the way for a more secure and resilient healthcare ecosystem that prioritizes patient privacy, data integrity, and trustworthiness.

REFERENCES

1. Bansal R., Gupta A., Singh R. and Nassa V. K., (2021). Role and Impact of Digital Technologies in E-Learning amidst COVID-19 Pandemic.2021 *Fourth International Conference on Computational Intelligence and Communication Technologies* (CCICT), pp. 194-202.doi: 10.1109/CCICT53244.2021.00046.
2. Bhattacharya, S., Reddy Maddikunta, P. K., Pham, Q. V., Gadekallu, T. R., Krishnan S, S. R., Chowdhary, C. L., Alazab, M., &Jalil Piran, M. (2021). Deep learning and medical image processing for coronavirus (COVID-19) pandemic: A survey. *Sustainable Cities and Society*, 65(November), 102589. https://doi.org/10.1016/j.scs.2020.102589.
3. Bhattacharya, S., Reddy Maddikunta, P. K., Pham, Q. V., Gadekallu, T. R., Krishnan S, S. R., Chowdhary, C. L., Alazab, M., &JalilPiran, M. (2021). Deep learning and medical image processing for coronavirus (COVID-19) pandemic: A survey. *Sustainable Cities and Society*, 65(November 2020), 102589. https://doi.org/10.1016/j.scs.2020.102589.
4. Cai, L., Gao, J., & Zhao, D. (2020). A review of the application of deep learning in medical image classification and segmentation. *Annals of Translational Medicine*, 8(11), 713–713. https://doi.org/10.21037/atm.2020.02.44.
5. Dushyant, K., Muskan, G., Gupta, A. and Pramanik, S. (2022). Utilizing Machine Learning and Deep Learning in Cyber security: An Innovative Approach. In *Cyber Security and Digital Forensics*, M. M. Ghonge, S. Pramanik, R. Mangrulkar, D. N. Le, Eds., *Wiley*. https://doi.org/10.1002/9781119795667.ch12.
6. Guo, Y., Hao, Z., Zhao, S., Gong, J., & Yang, F. (2020). Artificial intelligence in health care: Bibliometric analysis. *Journal of Medical Internet Research*, 22(7), 1–12. https://doi.org/10.2196/18228.
7. Gupta A. (2020). An Analysis of Digital Image Compression Technique in Image Processing. *International Journal of Advanced Science and Technology*, 28(20), 1261 - 1265. Retrieved from http://sersc.org/journals/index.php/IJAST/article/view/3837.
8. Gupta A., Kaushik D., Garg M. and Verma A., (2020). Machine Learning Model for Breast Cancer Prediction. *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud) (I-SMAC)*, pp. 472-477. doi 10.1109/I-SMAC49090.2020.9243323.
9. Gupta A., Singh R., Nassa V. K., Bansal R., Sharma P. and Koti K., (2021) Investigating Application and Challenges of Big Data Analytics with Clustering. 2021 *International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, pp. 1-6.doi: 10.1109/ICAECA52838.2021.9675483.
10. Kaushik, K., Garg, M., Annu, Gupta, A. and Pramanik, S. (2021). Application of Machine Learning and Deep Learning in Cyber security: An Innovative Approach, in *Cybersecurity and Digital Forensics: Challenges and Future Trends*, M. Ghonge, S. Pramanik, R. Mangrulkar and D. N. Le, Eds., *Wiley*, 2021.
11. Ker, J., Wang, L., Rao, J., & Lim, T. (2017). Deep Learning Applications in Medical Image Analysis. IEEE Access, 6, 9375–9379. https://doi.org/10.1109/ACCESS.2017.2788044.
12. Kumar Pandey, B., Pandey, D., Nassa, V. K., Ahmad, T., Singh, C., George, A. S., & Wakchaure, M. A. (2021a). Encryption and steganography-based text extraction in IoT using the EWCTS optimizer. *The Imaging Science Journal*, 69(1-4), 38-56.
13. Kumar, M. S., Sankar, S., Nassa, V. K., Pandey, D., Pandey, B. K., & Enbeyle, W. (2021). Innovation and creativity for data mining using computational statistics. *In Methodologies and Applications of Computational Statistics for Machine Intelligence* (pp. 223-240). IGI Global.
14. Meslie, Y., Enbeyle, W., Pandey, B. K., Pramanik, S., Pandey, D., Dadeech, P., ... & Saini, A. (2021). Machine intelligence-based trend analysis of COVID-19 for total daily confirmed cases in Asia and Africa. *In Methodologies and Applications of Computational Statistics for Machine Intelligence* (pp. 164-185). IGI Global.

15. Moynihan, R., Sanders, S., Michaleff, Z. A., Scott, A. M., Clark, J., To, E. J., Jones, M., Kitchener, E., Fox, M., Johansson, M., Lang, E., Duggan, A., Scott, I., &Albarqouni, L. (2021). Impact of COVID-19 pandemic on utilization of healthcare services: A systematic review. *BMJ Open*, 11(3), 11–17. https://doi.org/10.1136/bmjopen-2020-045343.
16. Pandey, B. K., Mane, D., Nassa, V. K. K., Pandey, D., Dutta, S., Ventayen, R. J. M., & Rastogi, R. (2021a). Secure text extraction from complex degraded images by applying steganography and deep learning. *In Multidisciplinary approach to modern digital steganography* (pp. 146-163). IGI Global.
17. Pandey, B. K., Pandey, D., Wariya, S., & Agarwal, G. (2021b). A deep neural network-based approach for extracting textual images from deteriorate images. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, 8(28), e3-e3.
18. Pandey, B. K., Pandey, D., Wariya, S., Aggarwal, G., & Rastogi, R. (2021c). Deep learning and particle swarm optimisation-based techniques for visually impaired humans' text recognition and identification. *Augmented Human Research,* 6, 1-14.
19. Pandey, B. K., Pandey, D., Wairya, S., & Agarwal, G. (2021d). An advanced morphological component analysis, steganography, and deep learning-based system to transmit secure textual data. *International Journal of Distributed Artificial Intelligence (IJDAI),* 13(2), 40-62
20. Pandey, B. K., Pandey, D., Nassa, V. K., George, S., Aremu, B., Dadeech, P., & Gupta, A. (2022, July). Effective and secure transmission of health information using advanced morphological component analysis and image hiding. *In Artificial Intelligence on Medical Data: Proceedings of International Symposium, ISCMM 2021* (pp. 223-230). Singapore: Springer Nature Singapore.
21. Pandey, B. K., & Pandey, D. (2023). Parametric optimization and prediction of enhanced thermoelectric performance in co-doped CaMnO3 using response surface methodology and neural network. *Journal of Materials Science: Materials in Electronics,* 34(21), 1589.
22. Pandey, D., Pandey, B. K., & Wairya, S. (2021a). Hybrid deep neural network with adaptive galactic swarm optimization for text extraction from scene images. *Soft Computing,* 25, 1563-1580.
23. Pandey, D., Ogunmola, G. A., Enbeyle, W., Abdullahi, M., Pandey, B. K., & Pramanik, S. (2021b). COVID-19: A framework for effective delivering of online classes during lockdown. *Human Arenas,* 1-15.
24. Pandey, D., Nassa, V. K., Jhamb, A., Mahto, D., Pandey, B. K., George, A. H., ... & Bandyopadhyay, S. K. (2021c). An integration of keyless encryption, steganography, and artificial intelligence for the secure transmission of stego images. *In Multidisciplinary approach to modern digital steganography* (pp. 211-234). IGI Global.
25. Pathania, V., Babu, S. Z. D., Ahamad, S., Thilakavathy, P., Gupta, A., Alazzam, M. B., & Pandey, D. (2022, July). A Database application of monitoring COVID-19 in India. *In Artificial Intelligence on Medical Data: Proceedings of International Symposium, ISCMM 2021* (pp. 267-274). Singapore: Springer Nature Singapore.
26. Puttagunta, M., & Ravi, S. (2021). Medical image analysis based on deep learning approach. *Multimedia Tools and Applications,* 80(16), 24365–24398. https://doi.org/10.1007/s11042-021-10707-4.
27. Raman, R., Rajalakshmi, R., Surya, J., Ramakrishnan, R., Sivaprasad, S., Conroy, D., Thethi, J. P., Mohan, V., &Netuveli, G. (2021). Impact on health and provision of healthcare services during the COVID-19 lockdown in India: A multicentre cross-sectional study. *BMJ Open*, 11(1), 1–11. https://doi.org/10.1136/bmjopen-2020-043590.
28. Rashed, B. M., & Popescu, N. (2022). Critical Analysis of the Current Medical Image-Based Processing Techniques for Automatic Disease Evaluation: Systematic Literature Review.*Sensors*, 22(18). https://doi.org/10.3390/s22187065.
29. Renukalatha, S., & Suresh, K. V. (2018). A review on biomedical image analysis. *Biomedical Engineering - Applications, Basis and Communications,* 30(4). https://doi.org/10.4015/S1016237218300018.
30. Senbekov, M., Saliev, T., Bukeyeva, Z., Almabayeva, A., Zhanaliyeva, M., Aitenova, N., Toishibekov, Y., & Fakhradiyev, I. (2020). The recent progress and applications of digital technologies in healthcare: A review. *International Journal of Telemedicine and Applications*, 2020. https://doi.org/10.1155/2020/8830200.
31. Shruthishree, & Tiwari, H. (2017). Review Paper on Medical Image Processing. *International Journal of Research - GRANTHAALAYAH, 5 (4RACSIT),* 21–29. https://doi.org/10.29121/granthaalayah.v5.i4racsit.2017.3344.
32. Singh, H., Pandey, B. K., George, S., Pandey, D., Anand, R., Sindhwani, N., & Dadheech, P. (2022, July). Effective Overview of Different ML Models Used for Prediction of COVID-19 Patients. *In Artificial Intelligence on Medical Data: Proceedings of International Symposium, ISCMM 2021* (pp. 185-192). Singapore: Springer Nature Singapore.
33. Suganyadevi, S., Seethalakshmi, V., &Balasamy, K. (2022). A review on deep learning in medical image analysis. *International Journal of Multimedia Information Retrieval*, 11(1), 19–38. https://doi.org/10.1007/s13735-021-00218-1.
34. Talukdar, V., Dhabliya, D., Kumar, B., Talukdar, S. B. , Ahamad, S. and Gupta, A. (2022) Suspicious Activity Detection and Classification in IoT Environment Using Machine Learning Approach. *Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC)*,2022, pp. 531-535, doi: 10.1109/PDGC56933.2022.10053312.
35. Veeraiah V., Ahamad G. P, S., Talukdar S. B., Gupta A. and Talukdar V., (2022) Enhancement of Meta Verse Capabilities by IoT Integration. *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, pp. 1493-1498.doi: 10.1109/ICACITE53722.2022.9823766.
36. Veeraiah V., Kumar K. R., Lalitha K. P., Ahamad S., Bansal R. and Gupta A., (2022). Application of Biometric System to Enhance the Security in Virtual World. *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, pp. 719-723.doi: 10.1109/ICACITE53722.2022.9823850.
37. Veeraiah V., Rajaboina N. B., Rao G. N., Ahamad S., Gupta A. and Suri C. S., (2022). Securing Online Web Application for IoT Management. 2022 *2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, pp. 1499-1504.doi: 10.1109/ICACITE53722.2022.9823733.

38. Veeraiah, V., Khan, H., Kumar A., Ahamad S., Mahajan A. and Gupta A., (2022). Integration of PSO and Deep Learning for Trend Analysis of Meta-Verse. *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, pp. 713-718.doi: 10.1109/ICACITE53722.2022.9823883.
39. Wang, J., Zhu, H., Wang, S. H., & Zhang, Y. D. (2021). A Review of Deep Learning on Medical Image Analysis. *Mobile Networks and Applications,* 26(1), 351–380. https://doi.org/10.1007/s11036-020-01672-7.
40. Zaidi, A., Ajibade, S.-S. M., Musa, M., & Bekun, F. V. (2023). New Insights into the Research Landscape on the Application of Artificial Intelligence in Sustainable Smart Cities: A Bibliometric Mapping and Network Analysis Approach. *International Journal of Energy Economics and Policy.* Vol.13, No. 4, pp. 287–299. https://doi.org/10.32479/ijeep.14683