ISSN : 3079-4765

Global Journal of Emerging AI and Computing

Volume 2, Number 11, 2026

https://doi.org/10.70445/gjeac.2.11.2026.1-22

Artificial Intelligence in Healthcare: Integrating Machine Learning, Deep Learning, and Cybersecurity for Clinical Medicine and Public Health

Bimalendu Pendy[1*], Mohammad Ali[2]

[1]Independent Researcher, 39900 Blacow Road, Apt #58, Fremont, CA, 94538

[2]Independent Researcher Iraq

[1]bimalpandey2320@gmail.com, [2]m.ali.m2000m@gmail.com

open access

Corresponding Author

Bimalendu Pendy

bimalpandey2320@gmail.com

Article History:

Submitted: 05-10-2026

Accepted: 16-11-2026

Published: 20-11-2026

Keywords

Artificial Intelligence, Machine Learning, Deep Learning, Healthcare Cybersecurity, Clinical Medicine, Public Health, Disease Prediction.

Global Journal of Emerging AI and Computing is licensed u der a Creative Commons Attribution-Noncommercial 4.0 International (CC BY-NC 4.0).

ABSTRACT

AI, ML, and DL are revolutionizing healthcare by driving innovations in clinical diagnosis, disease prediction, personalized medicine, and public health surveillance. The technologies can be used to analyze complex medical data efficiently, which can enhance clinical decision-making and healthcare delivery. As digitalization grows, however, so do cybersecurity risks, such as ransom ware, data breaches, unauthorized access and attack(s) by opponents. The application of AI in cybersecurity provides great potential for smart threat detection, secure data protection, and healthcare infrastructure. The topics of this review include applications of AI in clinical medicine, public health, and healthcare cybersecurity, with a focus on technological advancements, current challenges, ethical considerations, and future research and development trends in the field of secure and intelligent healthcare systems.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-4765
Global Journal of Emerging AI and Computing
Volume 2, Number 11, 2026
https://doi.org/10.70445/gjeac.2.11.2026.1-22

INTRODUCTION

Artificial Intelligence (AI) has become one of the most promising technologies in health care, providing innovative solutions to enhance disease diagnosis, clinical decision-making, patient management, public health surveillance and healthcare system efficiency. The field of clinical medicine and public health is poised for transformation thanks to the swift progress made by computational technologies, digital health infrastructure, and electronic health records (EHRs), and medical data analytics [1]. Machine learning (ML) and deep learning (DL), core components of the AI landscape, have proven their capability in analyzing intricate medical data, uncovering disease trends, forecasting outcomes, and assisting healthcare practitioners with precise and timely decision-making [2].

Machine learning (ML) and deep learning (DL), vital areas of AI, have shown great promise in examining complex medical data, revealing patterns in diseases, predicting outcomes, and aiding healthcare professionals in making informed and timely choices. The technologies are increasingly utilized in the field of medical imaging, cancer diagnosis, cardiovascular risk assessment, neurological disease diagnosis, drug discovery, personalized medicine, and prediction of infectious disease [3]. Moreover, AI systems can handle vast amounts of clinical data, including structured and unstructured information in healthcare, which helps streamline clinical workflows and facilitate evidence-based healthcare delivery.

At the same time, the growing digitization of healthcare systems has added a number of cyber security issues. Today's healthcare institutions use a variety of interconnected digital systems, cloud storage, electronic medical records, telemedicine, wearable technology, and Internet of Medical Things (IoMT) to gather, handle, and share patient data [4]. These technologies offer benefits for improved healthcare accessibility and operational efficiency, but also make medical infrastructures more vulnerable to cyber-attacks such as ransom ware, malware, phishing, unauthorized access, data breaches, and identity theft. These security breaches can lead to patient confidentiality breaches, disruption of clinical services, impact on medical device performance, and even compromise patient safety [5]. As a result, data confidentiality, integrity and availability are essential for the sustainable digital development of healthcare.

Machine learning and deep learning offer potential solutions for detecting suspicious network activity,

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-4765
Global Journal of Emerging AI and Computing
Volume 2, Number 11, 2026
https://doi.org/10.70445/gjeac.2.11.2026.1-22

malware, anomalous system activity, and anticipating future cyber threats. AI can help in analyzing network traffic, detecting new attack trends, and assisting with automated threat detection and response. But, AI healthcare systems also have new threats to their safety, such as privacy breaches, model manipulation, data poisoning, and adversarial attacks [6]. It is therefore crucial to create AI frameworks that are reliable, transparent, and secure to safeguard clinical data and ensure trust in AI-driven healthcare solutions.

In the realm of public health, AI holds even more promise for disease surveillance, epidemic forecasting, population health assessment, environmental health monitoring, and optimizing healthcare resources. The potential integration of secure AI technologies into public health systems could enhance the capability for timely disease detection, bolster public health preparedness, and enable successful interventions during public health crises. However, data privacy, algorithmic bias, interoperability, computational needs, regulatory adherence, and digital technology inequity are still key issues [7].

The convergence of AI, machine learning, deep learning and cybersecurity is a significant, interdisciplinary research area for the future of modern healthcare. This review discusses the clinical and public health use of these technologies, emerging cybersecurity threats and AI-based cybersecurity measures, and ethical, technical, and regulatory issues. Moreover, it identifies current research gaps and future prospects for building smart, reliable, secure and resilient healthcare systems that can enhance patient outcomes and bolster the global public health infrastructure.

EXPLORE THE BASICS OF ARTIFICIAL INTELLIGENCE IN THE HEALTHCARE SECTOR

Artificial Intelligence (AI) has become an essential component of modern healthcare, transforming traditional medical practices through advanced computational techniques that enable machines to perform tasks requiring human intelligence. The tasks that involve these include learning, reasoning, pattern recognition, decision making and problem solving [8]. The growing volume of EHRs, medical imaging, genomic data, data from wearable devices, clinical databases, and more have brought AI technologies to the forefront of healthcare adoption. The capabilities of AI systems to handle massive and intricate datasets, uncovering hidden connections, forecasting disease risks, and aiding health care practitioners when making diagnoses and treatment plans. Thus, AI is now finding its way into

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-4765
Global Journal of Emerging AI and Computing
Volume 2, Number 11, 2026
https://doi.org/10.70445/gjeac.2.11.2026.1-22

clinical medicine, medical research, hospital management, disease surveillance, and public health [9].

AI has evolved from rule-based expert systems to more advanced data-driven systems that can handle complex medical tasks. Most of the early healthcare systems were based on the clinical rules and knowledge-based systems, which were adopted to assist in making diagnosis and treatment recommendations [10]. But, with the progress of computer technology, big data, cloud computing, and algorithm design, there are more sophisticated AI applications that can be developed. AI technologies of the modern era can detect patterns of disease, decipher medical images, forecast patient outcomes, and support clinical decision-making. They can be incorporated into medical and health care systems, offering opportunities for personalized medicine, early disease detection, and better medical care [11].

Machine learning (ML) is one of the areas of AI in which computational systems can learn from past data and adapt their operation accordingly without being specifically programmed to accomplish each task. Some examples of ML algorithms are decision trees, random forests, support vector machines, logistic regression, and gradient boosting. In the medical field, these algorithms are applied in disease prediction, patient risk classification, treatment response assessment, and forecasting clinical outcomes [12].

Advanced subset of ML which uses multilayered artificial neural network to automatically learn complex features from large datasets is called deep learning (DL). Common architectures include convolutional neural networks (CNNs), recurrent neural networks (RNNs), and transformers. Examples of common architectures are convolutional neural networks (CNNs), recurrent neural networks (RNNs), long short-term memory networks (LSTMs), and transformers. They are commonly applied to cancer diagnosis, neurological disorder detection, clinical data interpretation and medical image analysis [13]. Natural language processing (NLP) is a technology that allows computers to process, analyze, and understand human language. It can facilitate the retrieval of clinical data from medical reports, physician notes, discharge summaries, and EHRs. The automated medical documentation, automated clinical coding and healthcare information retrieval are also uses of NLP in the medical field [14].

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-4765
Global Journal of Emerging AI and Computing
Volume 2, Number 11, 2026
https://doi.org/10.70445/gjeac.2.11.2026.1-22

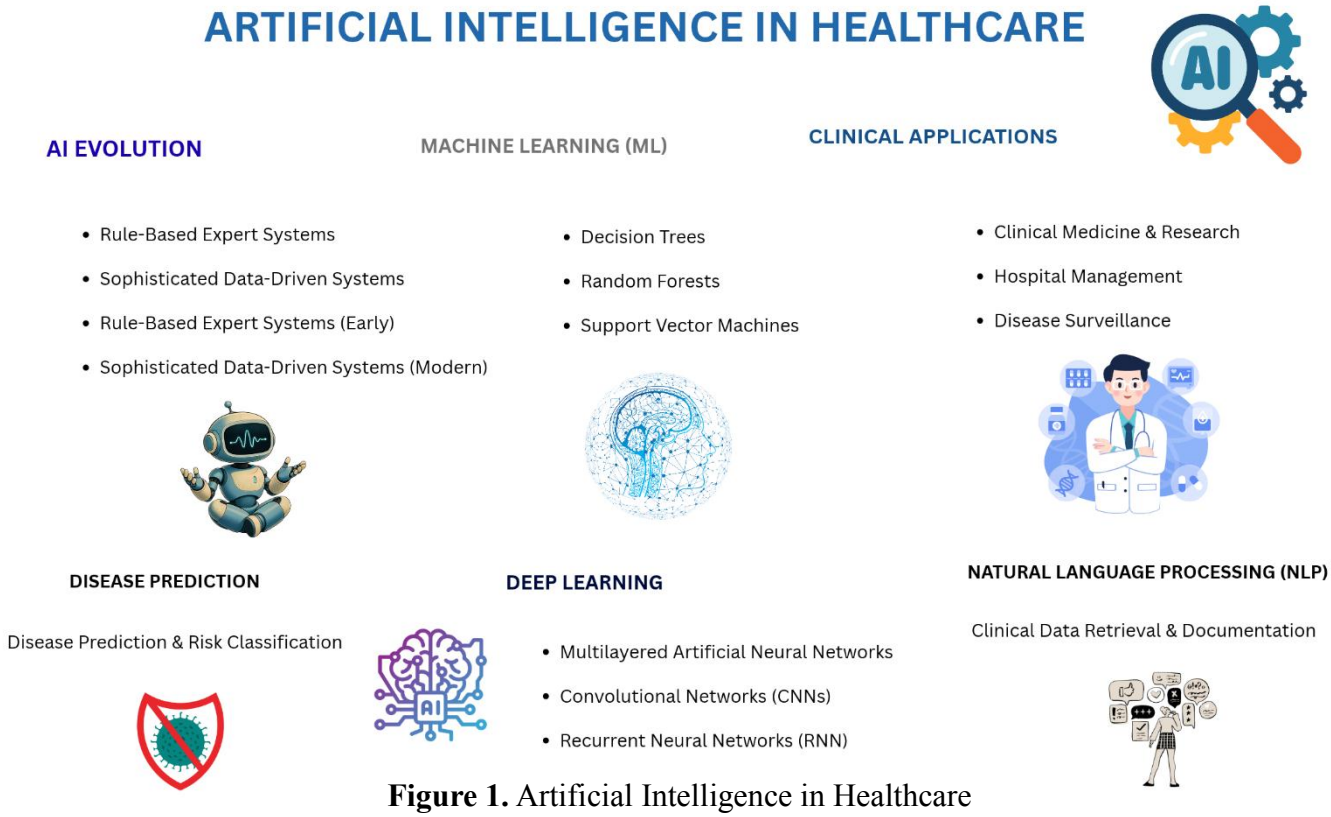


Figure 1. Artificial Intelligence in Healthcare

MACHINE LEARNING APPLICATIONS IN CLINICAL MEDICINE

In clinical medicine, Machine Learning (ML) is a crucial technology that offers sophisticated computational methods for disease diagnosis, risk prediction, therapy optimization, and patient management. ML algorithms can use a vast amount of clinical data, such as electronic health records (EHRs), laboratory tests, medical imaging, genomic data, and physiological readings, to uncover intricate patterns that are difficult to identify using traditional clinical means. These capabilities play a role in healthcare professionals' decision-making, elevating diagnostic precision, and creating individualized treatment plans [15]. The following are commonly used ML techniques: Logistic regression, Decision trees, Random forest, Support vector machines (SVM), K-nearest neighbors (KNN), Gradient boosting, Ensemble learning methods. The techniques have their own advantages and disadvantages depending on the clinical dataset's nature, quality, and complexity [16].

For disease diagnosis and early detection, ML models can analyze various clinical symptoms, patient history, laboratory results, and biomarkers to detect potential health conditions early. These methods have been shown to work for cancer, cardiovascular disease, diabetes, kidney disease and neurological diseases. Predictive analytics also helps health care professionals to predict the disease's

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-4765
Global Journal of Emerging AI and Computing
Volume 2, Number 11, 2026
https://doi.org/10.70445/gjeac.2.11.2026.1-22

progression, how likely the patient is to re-enter the hospital, how the patient might react to treatment and the probability of negative clinical events [17]. For cardiovascular medicine, ML algorithms can interpret patient electrocardiograms, blood pressure reading, cholesterol levels, and other clinical data to determine who has a greater likelihood of developing heart disease or stroke. In oncology, for instance, ML methods help classify cancer, estimate cancer prognosis, choose the best treatment, and find possible cancer biomarkers [18].

ML is also being increasingly utilized in the Diabetes and Metabolic Disorders space for predicting diabetes susceptibility, tracking glucose patterns and recognizing patients at risk of diabetes complications. In the field of neurological medicine, these algorithms can be used to analyze clinical records, brain imaging, and neurological measurements, providing valuable insights for detecting and assessing conditions like Alzheimer's disease, Parkinson's disease, epilepsy, and stroke [19]. Moreover, ML-based clinical decision support systems can help physicians consider diagnosis alternatives, suggest investigations, and determine the evidence-based treatment alternatives.

Precision and personalized medicine stands as another pivotal use of ML; by examining individual patient traits, genetic data, lifestyle influences, and how patients respond to treatments, ML can inform personalized treatment strategies. However, these advantages come with several difficulties for clinical implementation of ML: in addition to the limited availability of data, there is missing clinical information, algorithmic bias, lack of model interpretability, and challenges of integrating predictive systems into current hospital infrastructure [20]. Additionally, data privacy and cybersecurity are crucial factors to consider, as clinical ML applications often have access to sensitive patient data. Thus, robust data management, external validation, and transparent algorithms, along with ongoing clinical assessment, are essential for the reliability and safety of ML-driven healthcare solutions [21]. The capabilities of machine learning in clinical medicine are significant for future advancements in the field and could help enhance early diagnosis, treatment planning, and the delivery of efficient, personalized, and patient-centered care.

DEEP LEARNING APPLICATIONS IN CLINICAL HEALTHCARE

Deep Learning (DL) is a cutting-edge field of Artificial Intelligence (AI) that is revolutionizing clinical healthcare by processing complex medical data and recognizing patterns from vast datasets. Deep learning takes a different approach from traditional machine learning methods that typically

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Global Journal of Emerging AI and Computing

ISSN : 3079-4765

Volume 2, Number 11, 2026

https://doi.org/10.70445/gjeac.2.11.2026.1-22

involve hand-engineered features and manual extraction of meaningful patterns. Deep learning, on the other hand, uses multiple layers of artificial neural networks to automatically identify meaningful features and patterns in the raw data. These features are helpful in medical imaging, disease diagnosis, clinical prediction, pathology, genomics and personalized medicine [22]. The increasing abundance of digital medical records, radiological images, laboratory results, genomic sequences and physiological signals has been driving the evolution of digital health applications based on DL. To enhance clinical accuracy and healthcare decision-making, different architectures such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), long short-term memory networks (LSTMs), autoencoders, and transformer-based models are being employed [23].

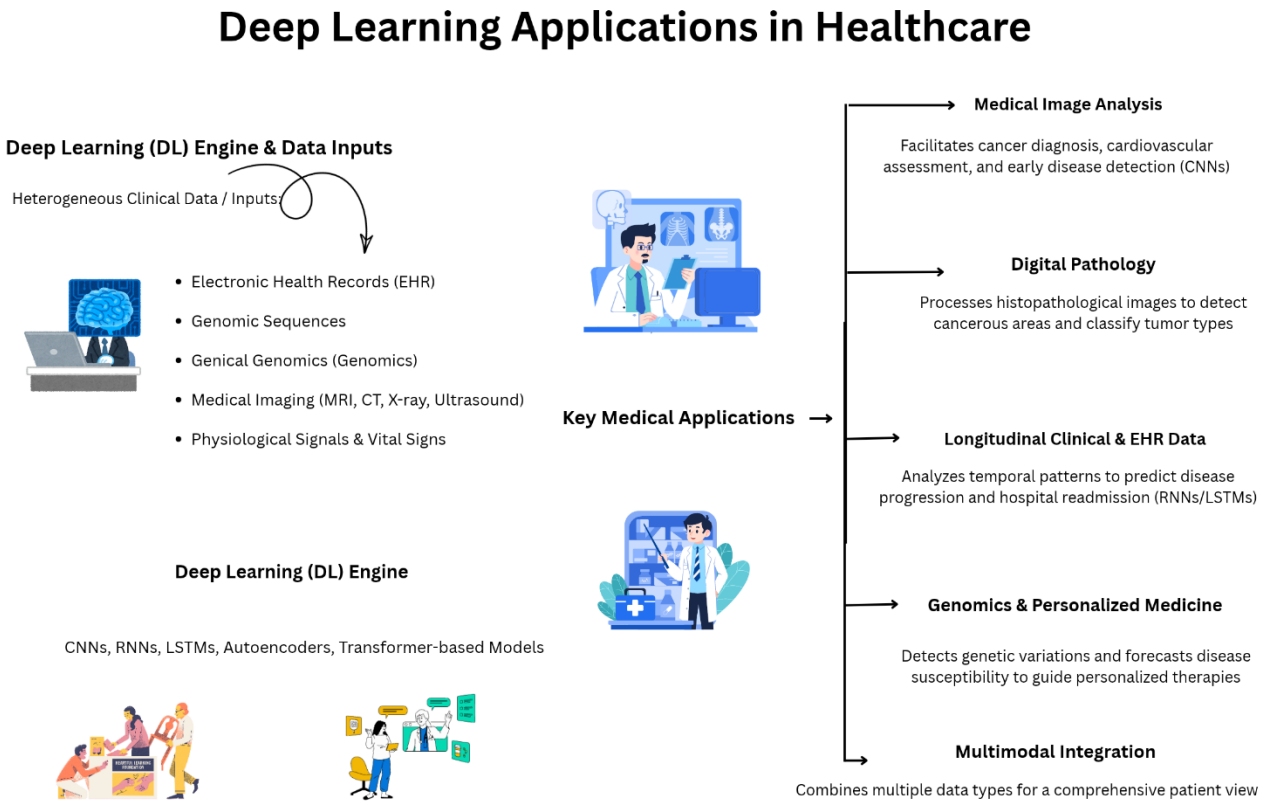


Figure 2. Applications of deep learning in healthcare

Medical image analysis is one of the most important applications of deep learning. CNNs can automatically analyze X-ray, computed tomography (CT) scan, magnetic resonance imaging (MRI), ultrasound and retinal photographs to detect abnormalities and help facilitate early detection of diseases. Such methods are especially valuable in the field of cancer diagnosis, cardiovascular assessment, pulmonary disease detection and neurological imaging [24]. Moreover, deep learning

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Global Journal of Emerging AI and Computing

ISSN : 3079-4765

Volume 2, Number 11, 2026

https://doi.org/10.70445/gjeac.2.11.2026.1-22

plays a crucial role in digital pathology by processing histopathological images to detect cancerous areas, classify tumor types, and assess disease severity. These applications may help pathologists to increase the efficiency of their work and decrease manual effort [25].

Deep learning can also be used for analyzing longitudinal clinical data using RNNs and LSTMs, which can detect temporal patterns in patient records, vital signs, and physiological measurements. These techniques can be applied to predicting disease progression, hospital readmission, and critical deterioration of patient and treatment outcomes [26]. The transformer architecture has also broadened the scope of clinical applications with its ability to handle large-scale multi-modal healthcare data, including complex medical documents and Electronic Health Records (EHRs). DL models can be used in genomics and precision medicine to detect genetic variations, forecast disease susceptibility, and guide the development of personalized therapeutic strategies [27]. Multimodal deep learning integrates multiple kinds of medical data, like medical images, laboratory data, clinical notes, and genomic data, to generate a comprehensive understanding of patient-specific conditions.

However, there are also some challenges when it comes to integrating deep learning into clinical practice, such as the need for large and good-quality datasets, computational complexity, limited interpretability, algorithmic bias and issues in external clinical validation. Furthermore, privacy and security issues, such as adversarial attacks and unauthorized access, could also affect the trustworthy functioning of DL-based systems [28]. Thus, for responsible AI implementation, there is a need for explainable AI, secure data-sharing protocols, strong model validation, and compliance with regulations. In conclusion, deep learning holds great promise to enhance both the accuracy of diagnosis and clinical decision-making and the prediction of disease, as well as to facilitate the creation of more efficient and intelligent clinical systems, and to lay the groundwork for personalized health care [29].

APPLICATIONS OF AI IN PUBLIC HEALTH

AI is making an impact in public health by streamlining surveillance for diseases, epidemiological analysis, population health assessment, health promotion, and healthcare resource management with cutting-edge technologies. Machine learning (ML), deep learning (DL), natural language processing (NLP), and predictive analytics facilitate the processing of vast amounts of health-related data and the detection of trends linked to the occurrence, transmission, and population health risks of diseases

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-4765
Global Journal of Emerging AI and Computing
Volume 2, Number 11, 2026
https://doi.org/10.70445/gjeac.2.11.2026.1-22

[30]. AI-based methods can be employed to analyze data generated from electronic health records, public health systems, laboratory surveillance systems, wearables, environmental sensors, and social media to guide timely public health interventions [31]. These technologies enhance the capacity of health authorities to track the course of a disease, target high-risk populations and create an evidence-based plan for preventing and controlling disease.

In the field of public health, AI plays a crucial role in infectious disease surveillance and outbreak prediction. Using ML and DL algorithms, epidemiological data, population mobility, environmental factors and past disease trends can be used to predict the risk of infectious disease outbreaks. These methods can help to support early warning systems and enhance preparedness for epidemics and pandemics [32]. AI also plays a role in population health analytics by identifying individuals and communities as being at higher risk for chronic diseases such as diabetes, cardiovascular diseases, obesity, and respiratory diseases. These predictive powers are important for public health agencies to create prevention strategies and optimize health and social care resources [33].

While AI offers numerous potential advantages for public health, there are also several challenges to consider, such as a lack of data, inaccuracies in data, algorithmic bias, poor digital infrastructure, and unequal access to cutting-edge tools and technologies. Patient confidentiality, data protection, and cybersecurity are especially significant when handling large, population-based public health systems that deal with sensitive data [34]. Unauthorized manipulation of data, cyber-attacks, and unauthorized access to data can undermine public trust and interfere with critical health care services. Thus, it is essential to provide secure data-sharing systems, clear algorithms, ethical governance, and proper regulations. AI holds significant promise to enhance public health systems by facilitating better disease surveillance, predictive epidemiology, preventive measures, and effective healthcare planning, while ensuring secure, equitable, and sustainable health service provision [35].

NEW THREATS AND CHALLENGES IN HEALTHCARE CYBERSECURITY

As digital technology, electronic health records (EHRs), the cloud, telemedicine, artificial intelligence (AI), and the Internet of Medical Things (IoMT) devices continue to be adopted, healthcare cybersecurity has emerged as a critical concern. Leading health care providers are continually gathering, storing, analyzing, and sharing critical patient data such as health records, diagnostic reports, laboratory findings, genomic data, and personal identifiers [36]. While digital transformation

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-4765
Global Journal of Emerging AI and Computing
Volume 2, Number 11, 2026
https://doi.org/10.70445/gjeac.2.11.2026.1-22

enhances access to healthcare, efficiency and clinical decisions, it comes with the threat of cyber-attacks and unauthorized access to medical data. Healthcare cybersecurity is concerned with safeguarding the confidentiality, integrity and availability of digital healthcare systems while maintaining the safety and privacy of patients [37]. Cybersecurity risks can disrupt hospital services, cause the leakage of patient information, delay medical treatment and even put patients' lives at risk.

Ransom ware is among the biggest cybersecurity threats in healthcare, where cybercriminals encrypt business data and require a ransom for access. These attacks can cause disruption to hospital information systems, slow down diagnostic processes and impact emergency medical services. Other malware, phishing, and social engineering are also popular attack methods that take advantage of both human and technical weaknesses to breach health-care systems. Another significant problem is data breaches, where stolen medical information can be exploited in identity theft or financial fraud, or for other purposes. Moreover, IoMT devices, such as smart monitoring systems, wearable sensors, connected medical devices, and remote patient monitoring systems, can be sensitive to unauthorized manipulation and information theft, potentially placing healthcare networks at risk [38].

Cloud-based healthcare solutions and telemedicine add more layers of security concerns regarding data transmission, authentication, access control, and third-party service providers. As AI-driven diagnostic systems become more widely adopted, so too do emerging vulnerabilities like adversarial attacks, data poisoning, and model manipulation, which could lead to inaccuracies and failures in clinical predictions. These threats can impact patient privacy and the effectiveness of medical decision-support systems [39]. Solving these cyber security challenges will take a holistic approach to security that includes encryption, multi factor authentication, access control, network monitoring, frequent vulnerability assessments, secure software development, and cyber security training of staff.

The use of AI-powered security systems, especially those leveraging machine learning and deep learning, can also bolster healthcare security by detecting irregular network activity, spotting malicious actions, and enabling automated responses to threats. In addition, conformance with healthcare data protection legislation and the application of common cybersecurity structures are crucial for keeping the accountability of the organization [40]. Health care cyber security is essential to creating secure, resilient, and trustworthy digital health care environments. By combining cutting-edge security solutions with conscious use of AI, healthcare organizations can further safeguard the

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Global Journal of Emerging AI and Computing

ISSN : 3079-4765

Volume 2, Number 11, 2026

https://doi.org/10.70445/gjeac.2.11.2026.1-22

privacy and integrity of medical data, ensure continuity of care, and actively promote patient safety in the context of a highly connected healthcare landscape [41].

INCORPORATION OF ARTIFICIAL INTELLIGENCE, CLINICAL MEDICINE, PUBLIC HEALTH AND CYBERSECURITY

The fusion of Artificial Intelligence (AI), clinical medicine, public health, and cybersecurity is a significant step forward in the evolution of smart, safe, and efficient healthcare systems. Healthcare is undergoing a rapid digital transformation that has driven higher adoption of EHRs, medical imaging, telemedicine systems, cloud computing, wearable systems, and IoMT applications. Such technologies produce significant medical and population-level health data which can be processed using machine learning (ML) and deep learning (DL) algorithms [42]. The combination of these technologies allows healthcare providers to enhance their ability to diagnose diseases, predict clinical outcomes, track population health, and tailor treatment plans, all while safeguarding the security and privacy of sensitive medical information.

Within clinical medicine, AI-based systems can incorporate laboratory data, medical images, patient histories, genomic data, and physiological measurements to facilitate correct diagnosis and clinical decision making. These systems can help doctors recognize disease patterns, anticipate disease complications, and determine treatment strategies. Likewise, the use of AI in public health allows for comprehensive disease monitoring, prediction of epidemics, risk stratification of populations and distribution of healthcare resources [43]. The power of linkage between clinical and public health data can lead to useful insights into disease progression, health care needs, and new health threats. But integration demands depend on the ability to share data reliably, to have a common information system, and to be able to share information between healthcare institutions [44].

Cybersecurity is a critical component in safeguarding these interdependent health care systems. The growing sharing of medical data among hospitals, labs, research institutes, and public health agencies may lead to potential vulnerabilities in the data, including cyber-attack and unauthorized access or manipulation [45]. By leveraging AI-powered threat detection, anomaly recognition, malware prevention, and real-time network monitoring, AI systems can bolster healthcare systems and safeguard them against evolving threats.AI-driven cybersecurity solutions can enhance healthcare infrastructure by providing intelligent intrusion detection, anomaly identification, malware

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-4765
Global Journal of Emerging AI and Computing
Volume 2, Number 11, 2026
https://doi.org/10.70445/gjeac.2.11.2026.1-22

prevention, and ongoing network monitoring to protect against emerging threats [46]. Moreover, privacy-preserving technologies, such as federated learning, encryption and secure authentication systems, can help to safeguard sensitive patient data and facilitate collaborative medical research.

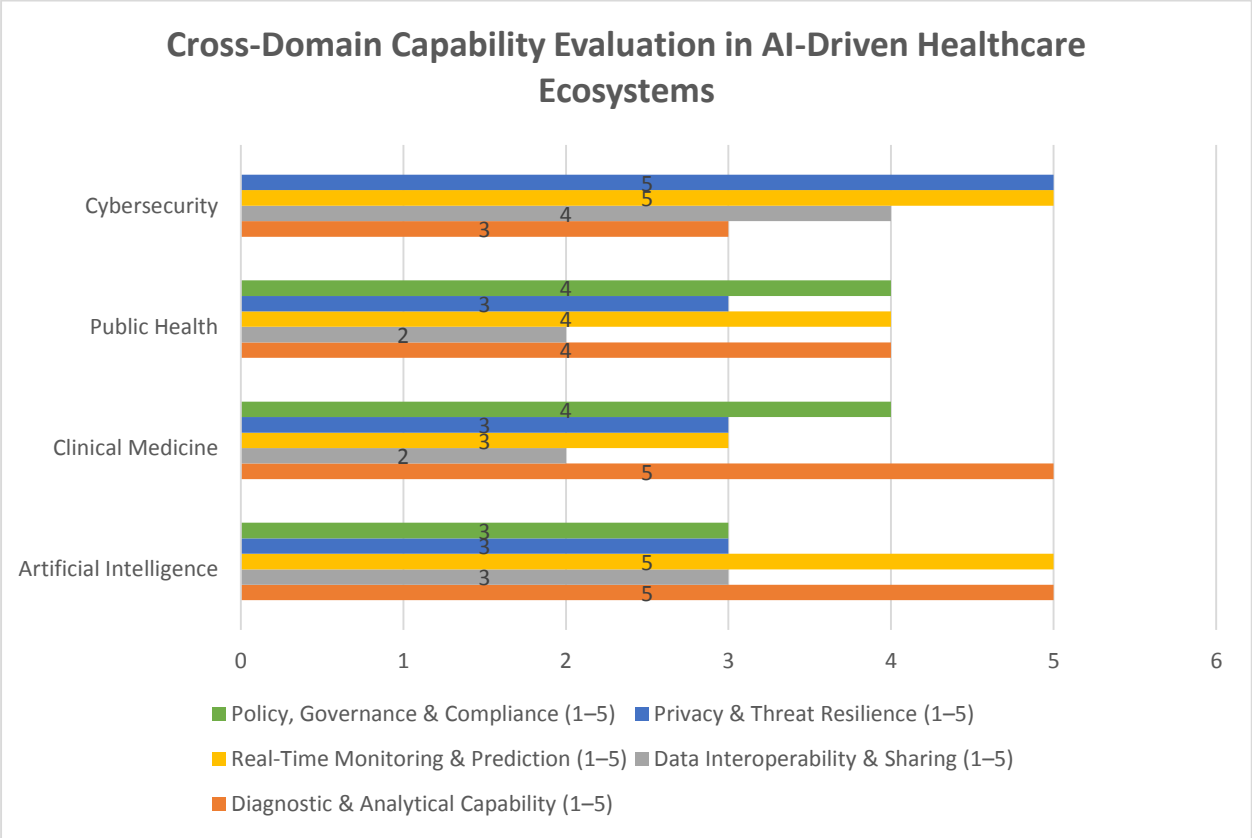


Figure 3. Cross-Domain Capability Evaluation in AI-Driven Healthcare Ecosystems

The vision of intelligent and secure healthcare ecosystems also extends to the incorporation of edge computing, cloud-based AI platforms, block chain technologies, and advanced cybersecurity frameworks. All these can help in processing medical data in real time, sharing data with security, monitoring patients remotely, and delivering medical services efficiently. However, there are data interoperability, algorithmic bias, computation power, regulatory compliance and reliability concerns that need to be resolved before scale-up is achieved [47]. Moreover, there is a need for healthcare institutions to have the right governance policies, awareness of cyber security, and constant testing of AI systems.

Integrating AI, clinical medicine, public health, and cybersecurity provides a comprehensive approach to modern healthcare transformation. This interdisciplinary integration can have a positive

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-4765
Global Journal of Emerging AI and Computing
Volume 2, Number 11, 2026
https://doi.org/10.70445/gjeac.2.11.2026.1-22

impact on clinical performance, bolster disease monitoring, safeguard patient privacy, and boost the resilience of the healthcare system. Building trustworthy, privacy-preserving, and secure AI-based healthcare systems can, therefore, be a key step towards sustainable digital health and better population health outcomes [48].

MAJOR CHALLENGES AND RESEARCH GAPS

While there has been great progress in the application of Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) in clinical medicine, public health, and healthcare cybersecurity, there are still several technical, ethical, and operational challenges to wide-spread deployment. A primary constraint is the availability and quality of the health data. Medical information often lacks completeness, consistency, balance, or is spread among health care providers [49]. Incomplete clinical documentation, inconsistent annotations, and different data collection procedures can have a negative impact on the effectiveness and accuracy of AI models. In addition, due to patient privacy regulations, institutional restrictions and data-sharing limitations, it is difficult to access large and diverse medical datasets that are needed for research and algorithm development [50].

A second challenge is that of model generalizability and clinical validation. The effectiveness of AI systems can vary across different healthcare settings, as they might not be as effective when applied to data from other hospitals, geographic regions, or patient groups. The predication might vary depending on the demographics, medical care, diagnostic tools, and/or prevalence of illness. Further, many deep learning models are black-box models that make it hard for the healthcare practitioners to understand the decisions made by the deep learning model [51]. There can be a lack of interpretability, which can lead to lower confidence in the clinical use of the AI and challenges for accountability of medical decision making.

Another significant area of need in AI in healthcare is cybersecurity. While ML and DL are capable of raising threat awareness, these systems can be attacked by adversaries, poisoned with data, stolen by adversaries or accessed without permission. As more connected medical devices, cloud platforms, telemedicine applications are introduced, the attack surface on healthcare infrastructure continues to grow. Creating strong cybersecurity mechanisms that can safeguard sensitive medical data while not undermining system performance is an important research priority [52].

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Global Journal of Emerging AI and Computing

ISSN : 3079-4765

Volume 2, Number 11, 2026

https://doi.org/10.70445/gjeac.2.11.2026.1-22

Limited infrastructure and computational resources also hinder the implementation of AI, especially in healthcare settings with constrained resources. The advanced DL models have high requirements for system resources, storage space, technical skills and capital. The needs could exacerbate the inequalities between technologically developed healthcare systems and low and middle income countries. In addition, the absence of standardized evaluation frameworks, limited interoperability, and challenges in integrating AI tools into the existing hospital information systems (HIS) create further implementation hurdles [53].

There are several areas that need further research such as building explainable and trustworthy AI models, approaches to privacy-preserving learning, medical data sharing security, and standardized clinical validation practices. Further studies are also required to assess the long-term impacts of AI technologies in real-world healthcare settings and across various patient groups [54]. The solution offers an interdisciplinary approach and requires collaboration between healthcare professionals, computer scientists, cybersecurity specialists, researchers and policymakers. To build trustworthy, equitable, and safe AI-powered healthcare systems, it will be crucial to enhance data quality, ensure model transparency, bolster cybersecurity measures, navigate regulatory compliance, and promote technological accessibility [55].

FUTURE PERSPECTIVES AND EMERGING RESEARCH DIRECTIONS

Advancements in AI and Digital health technologies, alongside Machine learning (ML) and Deep learning (DL) and cybersecurity are anticipated to influence the future course of Artificial Intelligence (AI) in the healthcare industry. The development of these represents great promise for enhancing clinical diagnosis, disease prediction, personalized medicine, public health surveillance, and healthcare system efficiency [56]. The future of AI in healthcare calls for more than just enhanced performance; it requires the security, transparency, reliability, and ethical application of intelligent healthcare technologies. There is a need for future studies to address the security, transparency, reliability, and ethical usage of intelligent healthcare technologies. This combination of cutting-edge AI techniques and secure digital infrastructure has the potential to enhance healthcare systems, making them more resilient, accessible, and patient-centered [57].

Future directions for research include the creation of explainable and trusted AI systems. The complex decision making process in advanced DL models is hard to explain, while their predictive power is

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-4765
Global Journal of Emerging AI and Computing
Volume 2, Number 11, 2026
https://doi.org/10.70445/gjeac.2.11.2026.1-22

high. XAI techniques can help enhance the transparency of AI systems, making it easier for healthcare professionals to understand how algorithms make predictions and offer treatments. Also, federated learning and privacy-preserving machine learning are likely to gain greater significance as more healthcare institutions collaborate to create AI models without sharing their patients' sensitive information directly [58]. These can help to bolster medical research and to minimize privacy threats.

In the clinical field, generative AI and LLM also present opportunities for the future. They can be used in various applications such as automating clinical documentation, analyzing medical literature, communicating with patients, supporting clinical research, and education in the healthcare sector. But future systems need to take on accountability and reliability, data confidentiality, and misinformation issues [59]. Another research avenue that appears to be interesting is the use of digital twins to simulate the disease, plan treatment and predict disease analysis on a virtual patient or healthcare system.

Looking forward, intelligent threat detection, zero-trust security models, automated incident responses, and enhanced security for Internet of Medical Things (IoMT) devices will be key areas of focus in healthcare cybersecurity. AI-driven cybersecurity solutions could be used to uncover new threats, monitor unusual network behavior, and enhance the security of EHRs and medical devices [60].AI-driven cybersecurity tools could be leveraged to identify new threats, to detect abnormal network activity and to improve the protection of EHRs and connected medical devices. While the potential applications are promising, the security risks, and the practicality of quantum machine learning in healthcare data analysis needs further research [61]. Moreover, precision public health using AI can enhance disease surveillance, epidemic prediction, environmental health monitoring, and population-level risk assessment. Integrating clinical, genomic, epidemiological and environmental data may enable more targeted preventive measures and effective allocation of health care resources [62].

CONCLUSION

The modern healthcare sector is witnessing a revolution with the advent of Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL), which bring about new advanced tools for disease diagnosis, clinical decision making, personalized medicine, public health surveillance, and healthcare

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-4765
Global Journal of Emerging AI and Computing
Volume 2, Number 11, 2026
https://doi.org/10.70445/gjeac.2.11.2026.1-22

cyber security. The adoption of such technologies in clinical practice has shown great promise in enhancing the precision of diagnosis, forecasting disease trajectory, pinpointing patients at risk, and facilitating optimal treatment approaches. In healthcare, ML algorithms like random forests, support vector machines, and decision trees enable doctors to analyze intricate patient data and forecast outcomes. For instance, in healthcare, doctors can employ ML algorithms such as random forests, support vector machines, and decision trees to analyze complex patient data and make predictions. DL algorithms like convolutional neural networks, recurrent neural networks, and transformers enable sophisticated applications in medical image analysis, cancer detection, neurological disease diagnosis, and multimodal clinical data analysis.

AI-powered technologies are used in public health for infectious disease surveillance, epidemic forecasting, population health assessment, environmental monitoring, and optimizing healthcare resources. These applications can enhance the effectiveness of disease prevention, increase the ability to provide early warning, and aid in evidence-based public health action. But with the growing digitalization of healthcare comes a number of cybersecurity hurdles. Ransom ware, malware, phishing, unauthorized access and data breaches are becoming a common issue for Electronic health records, cloud-based healthcare platforms, telemedicine services and Internet of Medical Things (IoMT) devices. These threats may lead to breaches in patient privacy, disrupt critical healthcare services, and impact the reliability of the healthcare system.

In the field of healthcare cybersecurity, ML and DL have the potential to provide valuable solutions for detecting suspicious network traffic, identifying malicious software, recognizing abnormal behavior, and automated threat prevention. Even so, there are adversarial attacks, data poisoning, model manipulation, and privacy violations that can be leveled against AI-powered healthcare systems. Hence, the incorporation of intelligent cybersecurity mechanisms into clinical and public health applications becomes crucial for ensuring secure and trustworthy digital healthcare environments.

Even with significant technological advances, there are some issues that have not been resolved, such as the lack of data availability, algorithmic bias, the lack of adequate model interpretability, computational complexity, lack of clinical validation, and lack of access to digital infrastructure. To overcome these challenges, it is important to work on the development of interdisciplinary

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-4765
Volume 2, Number 11, 2026
https://doi.org/10.70445/gjeac.2.11.2026.1-22

collaboration, standardized regulations, secure data sharing, privacy protection technologies, and the ongoing assessment of AI-driven systems. Research efforts in explainable AI, federated learning, generative AI, digital twins, zero-trust security architectures, and advanced threat detection systems are all key areas that should be explored in the future.

The intersection of AI, machine learning, deep learning, clinical medicine, public health and cybersecurity paves the way for a significant step forward in healthcare innovation. The creation of AI-powered healthcare systems that are reliable, transparent, private, and secure will be crucial to elevating patient care, securing sensitive patient data, bolstering public health systems, and facilitating sustainable AI-driven healthcare innovation.

REFERENCES

[1]. Bala I, Pindoo I, Mijwil MM, Abotaleb M, Yundong W. Ensuring security and privacy in healthcare systems: a review exploring challenges, solutions, future trends, and the practical applications of artificial intelligence. Jordan Medical Journal. 2024 Jul;58(3):201-23.

[2]. Khan F. Artificial Intelligence in Electrical Power Systems: A Comprehensive Review of Machine Learning Techniques and Applications. Global Journal of Universal Studies. 2024 Jun 15;1(1).

[3]. Oad SK. Role of Artificial Intelligence in Modern Data Science: A Critical Review. Global Journal of Universal Studies. 2024 Jun 15;1(1).

[4]. Abbasi N, Nizamullah FN, Zeb S. Ai in healthcare: Using cutting-edge technologies to revolutionize vaccine development and distribution. JURIHUM: Jurnal Inovasi dan Humaniora. 2023 Jun 14;1(1):17-29.

[5]. Raza H, Singh A, Erdenetsogt T, Kabeer MM, Aslam MS, Farooq M. Machine Learning Driven Decision Making in the Modern Data Era. PERFECT: Journal of Smart Algorithms. 2026 Jan 6;3(1):11-22.

[6]. Nankya M, Mugisa A, Usman Y, Upadhyay A, Chataut R. Security and privacy in E-health systems: a review of AI and machine learning techniques. IEEE access. 2024 Sep 27;12:148796-816.

[7]. Oad VD. Artificial Intelligence in Data Analytics: A Comprehensive Review. Global Journal of Universal Studies. 2024 Jun 15;1(1).

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-4765
Volume 2, Number 11, 2026
https://doi.org/10.70445/gjeac.2.11.2026.1-22

[8]. Herzog NJ, Celik D, Sulaiman RB. Artificial intelligence in healthcare and medical records security. InCybersecurity and Artificial Intelligence: Transformational Strategies and Disruptive Innovation 2024 Apr 18 (pp. 35-57). Cham: Springer Nature Switzerland.

[9]. Shaikh MM. Artificial Intelligence and Workforce Performance Optimization in Government Supply Chains. Global Trends in Science and Technology. 2026 Jun 12;2(3):53-74.

[10]. Khan F. Advances in Artificial Intelligence for Electrical Systems: Machine Learning Methods, Applications, and Emerging Challenges. American Journal of Artificial Intelligence and Computing. 2026 Aug 12;2(2):1-9.

[11]. Jamal A, Raza H, Erdenetsogt T, Singh A, Farooq M, Kabeer MM, Aslam MS. AI and Data Analytics for Precision Agriculture: Current Progress and Future Directions. JATAED: Journal of Appropriate Technology for Agriculture, Environment, and Development. 2025 Aug 15;2(2):36-46.

[12]. Qureshi R, Koo I. A comprehensive survey of cybersecurity threats and data privacy issues in healthcare systems. Applied Sciences. 2026 Feb 2;16(3):1511.

[13]. Oad SK. AI-Powered Data Science: A Review of Current Developments and Emerging Opportunities. Global Trends in Science and Technology. 2026 May 13;2(2):263-82.

[14]. Nizamullah F, Fahad M, Abbasi N, Qayyum MU, Zeb S. Ethical and legal challenges in AI-driven healthcare: patient privacy, data security, legal framework, and compliance. Int. J. Innov. Res. Sci. Eng. Technol. 2024;13:15216-23.

[15]. Kanna SR, Murthy MY, Gawali MB, Rubai SM, Reddy NS, Brammya G, Preetha NN. A deep learning-based disease diagnosis with intrusion detection for a secured healthcare system. Knowledge and Information Systems. 2024 Sep;66(9):5669-707.

[16]. Dey P, Hossain E, Hossain MI, Chowdhury MA, Alam MS, Hossain MS, Andersson K. Comparative analysis of recurrent neural networks in stock price prediction for different frequency domains. Algorithms. 2021 Aug 22;14(8):251.

[17]. Raza H, Erdenetsogt T, Singh A, Farooq M, Kabeer MM, Aslam MS. A Comprehensive Review on Data Science Frameworks for Big Data Analytics. PERFECT: Journal of Smart Algorithms. 2026 Jan 6;3(1):1-0.

[18]. Khan F. Neural Networks in Electrical Engineering Applications: A Review. Global Trends in Science and Technology. 2026 Apr 29;2(2):219-39.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-4765
Volume 2, Number 11, 2026
https://doi.org/10.70445/gjeac.2.11.2026.1-22

[19]. Akshay Kumaar M, Samiayya D, Vincent PD, Srinivasan K, Chang CY, Ganesh H. A hybrid framework for intrusion detection in healthcare systems using deep learning. Frontiers in Public Health. 2022 Jan 12;9:824898.

[20]. Oad VD. Artificial Intelligence for Big Data Analytics: A Review of Trends and Challenges. Global Trends in Science and Technology. 2026 Mar 20;2(2):83-102.

[21]. Zeb S, Nizamullah FN, Abbasi N, Qayyum MU. Transforming Healthcare: Artificial Intelligence's Place in Contemporary Medicine. BULLET: Jurnal Multidisiplin Ilmu. 2024;3(4):592385.

[22]. Imtiaz N, Kundu TR, Roy A, Bhuiyan MI, Rahman K, Islam MK. Governance readiness beyond predictive performance: An empirical benchmark for higher-education early warning systems. Frontiers in Computer Science and Artificial Intelligence. 2025;4(5):49-65.

[23]. Kabeer MM. Leveraging AI for process optimization: the future of quality assurance in lean six sigma. American Journal of Artificial Intelligence and Computing. 2025 May 7;1(1):87-103.

[24]. Vaisakhkrishnan K, Ashok G, Mishra P, Kumar TG. Guarding digital health: deep learning for attack detection in medical IoT. Procedia Computer Science. 2024 Jan 1;235:2498-507.

[25]. Oad SK. From Algorithms to Insights: A Review of AI Applications in Data Science. American Journal of Artificial Intelligence and Computing. 2026 May 14;2(1):236-51.

[26]. Jamshaid M, Muhammad AH, Akbar Z, Niaz S, Siddique MN, Akbar S. Artificial intelligence generated deepfakes as instruments of disinformation: Examining their influence on public opinion, digital trust, and governance. Journal of Information Systems Engineering and Management. 2025;10.

[27]. Khan F. Deep Learning Applications in Power Systems: A Review Study. Global Journal of Universal Studies. 2024 Jun 15;1(1).

[28]. Raza H, Erdenetsogt T, Kabeer MM, Aslam MS. IoT Generated Big Data Analytics: Trends and Scalability Issues. American Journal of Artificial Intelligence and Computing. 2025;1(2):306-27.

[29]. Singh A. Advancing Healthcare through AI-Driven Data Analytics: Integrating Machine Learning and Cybersecurity in Modern Computer Science. Global Journal of STEM and Society. 2026 Feb 6;1(1):107-26.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-4765
Volume 2, Number 11, 2026
https://doi.org/10.70445/gjeac.2.11.2026.1-22

[30]. Qurashi SN, Sobia F, Hetany WA, Sultan H. Enhancing cybersecurity defenses in healthcare using AI: A pivotal role in fortifying digital health infrastructure. Medinformatics. 2025 Mar 24;2(4):268-78.

[31]. Zeb S, Nizamullah FN, Abbasi N, Fahad M. AI in healthcare: revolutionizing diagnosis and therapy. International Journal of Multidisciplinary Sciences and Arts. 2024 Aug 17;3(3):118-28.

[32]. Oad VD. AI in Business Data Analytics: A Review of Current Practices and Future Direction. Global Trends in Science and Technology. 2026 Apr 15;2(2):156-74.

[33]. Erdenetsogt T, Jamal M. Machine Learning for Big Data Analytics: A Comprehensive Review. Global Trends in Science and Technology. 2026 Apr 25;2(2):199-218.

[34]. Oscar F, Matthew UO, Oladele HA, Akpan EE, Cole OA, Ademilua BO, Onyebuchi A. Cybersecurity approaches to IoT platforms in E-Healthcare systems: Artificial intelligence application. InAI-Driven Healthcare Cybersecurity and Privacy 2025 (pp. 89-124). IGI Global Scientific Publishing.

[35]. Aslam MS. Artificial Intelligence in Product Management: Driving Innovation and Market Success. Global Journal of Universal Studies. 2024 Dec 12;1(2):88-112.

[36]. Shaikh MM. Enhancing Workforce Efficiency in Public Sector Supply Chains through Predictive Analytics. American Journal of Artificial Intelligence and Computing. 2026 Jun 10;2(1):288-315.

[37]. Husnain A. Artificial intelligence and deep learning in healthcare, cyber security, and food systems: A comprehensive review of applications, challenges, and future directions. Global Journal of Emerging AI and Computing. 2025 Feb 28;1(2):95-126.

[38]. Khan F. Quantitative Risk Analysis of Fire Load and Combustible Materials in Office Workplaces in the United States. Global Regional Review, 7 (2), 359-366 [Internet]. 2022.

[39]. Oad SK. Artificial Intelligence in Data Science: A Comprehensive Review. American Journal of Artificial Intelligence and Computing. 2026 Mar 17;2(1):1-25.

[40]. Abbasi N, Nizamullah FN, Zeb S, Fahad M, Qayyum MU. Machine learning models for predicting susceptibility to infectious diseases based on microbiome profiles. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online). 2024 Aug 25;3(4):35-47.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-4765
Volume 2, Number 11, 2026
https://doi.org/10.70445/gjeac.2.11.2026.1-22

[41]. Raza H, Erdenetsogt T, Farooq M, Kabeer MM, Aslam MS. Real-Time Data Analytics: Applications and Challenges in Smart Cities. Global Journal of Universal Studies. 2024 Jun 15;1(1).

[42]. Alsolami T, Alsharif B, Ilyas M. Enhancing cybersecurity in healthcare: Evaluating ensemble learning models for intrusion detection in the internet of medical things. Sensors. 2024 Sep 13;24(18):5937.

[43]. Kabeer MM. Utilizing Machine Learning for Continuous Process Improvement in Lean Six Sigma. Global Trends in Science and Technology. 2025 May 7;1(2):49-63.

[44]. Jamal M, Singh A. Federated and Edge Learning for Real-Time Data Analytics in Clinical Environments. Global Journal of Universal Studies. 2024 Jun 15;1(1).

[45]. Ahmed Z, Suleiman AM, Filani A, Ocansey IT, Donkor AA. The Role of Advanced Machine Learning Algorithms in Detecting and Mitigating Cybersecurity Threats within United States Healthcare Digital Infrastructure: A Comprehensive Vulnerability Analysis. Journal Of Engineering And Computer Sciences. 2025 Oct 21;4(10):218-26.

[46]. Oad VD. Exploring AI Techniques in Data Analytics: A Critical Review. American Journal of Artificial Intelligence and Computing. 2026 Apr 16;2(1):46-67.

[47]. Aslam MS, Jamal M. Machine Learning in Healthcare: Revolutionizing Clinical Decision-Making with Data Analytics. Global Trends in Science and Technology. 2026 Mar 18;2(2):23-42.

[48]. Kalinaki K, Fahadi M, Alli AA, Shafik W, Yasin M, Mutwalibi N. Artificial intelligence of internet of medical things (AIoMT) in smart cities: a review of cybersecurity for smart healthcare. Handbook of security and privacy of ai-enabled healthcare systems and internet of medical things. 2023 Oct 25:271-92.

[49]. Khan F. Next-Generation Electrical Systems: A Review of AI-Enabled Technologies. American Journal of Artificial Intelligence and Computing. 2026 Apr 30;2(1):109-31.

[50]. Singh A. Human-computer interaction: a review of usability, design, and accessibility trends. Global Research Repo. 2025 Sep 9;1(2):362-87.

[51]. Baba MK, Ya'u BI, Zambuk FU, Magombe Y, Musa MA, Alli A. Artificial intelligence-driven intrusion detection systems for secure healthcare iot: A comprehensive review. Impact in Computics. 2025 Nov 14;1:1-8.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ISSN : 3079-4765
Volume 2, Number 11, 2026
https://doi.org/10.70445/gjeac.2.11.2026.1-22

[52]. Kabeer MM. AI in manufacturing quality management: a review of techniques, tools, and industrial adoption. Global Journal of Universal Studies. 2024;1(2):46-64.

[53]. Saheed YK, Arowolo MO. Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms. IEEE access. 2021 Nov 16;9:161546-54.

[54]. Oad SK. Integration of AI in Data Science: A Systematic Review. Global Trends in Science and Technology. 2026 Mar 18;2(2):64-82.

[55]. Jamal M. Deep Learning Applications in Medicine: Enhancing Diagnosis and Patient Outcomes. Global Journal of Universal Studies. 2024 Jun 15;1(1).

[56]. AlZubi AA, Al-Maitah M, Alarifi A. Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. Soft Computing. 2021 Sep;25(18):12319-32.

[57]. Singh A. Harnessing Artificial Intelligence in Product Management and Data Analytics: Trends, Applications, and Future Directions. Global Trends in Science and Technology. 2026 Jan 25;2(1):19-35.

[58]. Khatun MA, Memon SF, Eising C, Dhirani LL. Machine learning for healthcare-IoT security: A review and risk mitigation. IEEE access. 2023 Dec 22;11:145869-96.

[59]. Kabeer MM. AI in Lean Six Sigma: A Review of Industrial Implementations, Benefits, and Barriers. Global Journal of Universal Studies. 2024 Jan 10;1(2):134-58.

[60]. Ali TE, Ali FI, Eyvazov F, Zoltán AD. Integrating AI models for enhanced Real-Time cybersecurity in healthcare: A multimodal approach to threat detection and response. Procedia Computer Science. 2025 Jan 1;259:108-19.

[61]. Moligi S, Dadi R, Atluri VV. Machine Learning Driven Intelligent Cyber Defense Threat Detection in Medical Imaging: A Review on Methods, Challenges, and Future Prospects. In2026 5th International Conference on Communication, Computing and Electronics Systems (ICCCES) 2026 Jan 21 (pp. 1042-1048). IEEE.

[62]. Wazid M, Singh J, Das AK, Rodrigues JJ. An ensemble-based machine learning-envisioned intrusion detection in industry 5.0-driven healthcare applications. IEEE Transactions on Co

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.