Global Journal of Machine Learning and Computing

ISSN : 3079-692X
Volume 1, Number 2, 2025
https://doi.org/10.70445/gjmlc.1.2.2025.43-59

Integrating AI, ChatGPT, and ML for Healthcare and Cybersecurity: A Review of Cloud-Based Analytics, Disease Detection, and Data Protection Frameworks

Ibrar Hussain[1*]

[1]University of Punjab, Lahore

[1]2021-pgcma-38@nca.edu.pk

open access

Corresponding Author

Ibrar Hussain

2021-pgcma-38@nca.edu.pk

Article History:

Submitted: 01-07-2025

Accepted: 05-08-2025

Published: 10-08-2025

Keywords

AI, Machine Learning, ChatGPT, Cloud Computing, Healthcare Analytics, Cybersecurity.

ABSTRACT

The scope of the review is the implementation of Artificial Intelligence (AI), Machine Learning (ML) and ChatGPT in healthcare and cybersecurity related to analytics on clouds, disease detection, and data protection systems. AI and ML can be used to increase the accuracy of diagnoses, predictive analytics, and clinical decisions, whereas ChatGPT can be used to facilitate communication and data interpretation. Cloud computing provides the opportunity of scalable and secure data management and real-time analytics. At the same time, AI-based security solutions can ensure the protection of sensitive medical data via automated threat detection and response. In spite of these innovations, issues like data privacy, interoperability and ethical issues remain a challenge. The article reveals the existing innovations, gaps in research, and future trends in the creation of intelligent, secure and ethical healthcare systems using AI and cloud technologies.

INTRODUCTION

The introduction of AI and ML and the development of new language models like ChatGPT has transformed many industries; two of the most influential areas have become healthcare and cybersecurity. In the modern digital age, the volume of information in electronic health records (EHRs), wearable technology and online health platforms is growing exponentially, making it imperative to have intelligent systems that can analyze, predict, and make decisions in real-time [1]. At the same time, the emergence of cyber threats posing risks to sensitive health data evidences the issue of the urgent necessity to introduce strong AI-driven data protection frameworks. The union of

ISSN : 3079-692X
Volume 1, Number 2, 2025
https://doi.org/10.70445/gjmlc.1.2.2025.43-59

AI, cloud computing, and data analytics offer an unprecedented chance to improve the accuracy of various disease detection procedures, automate healthcare processes, and protect digital infrastructures against crimes [2].

The global healthcare systems are rapidly switching to cloud-based architectures to store, compute, and analyze high data on medical cases. The development of cloud platforms based on the integration of AI and ML algorithms makes it feasible to predict the model, individual medicine, and automatic diagnosis [3]. To provide an example, deep learning systems can detect cancer or diabetes-related disease signs early in medical images, whereas natural language processing (NLP) and chatbots, like ChatGPT, can help clinicians analyze medical records and histories of patients. These technologies can transform healthcare services by making them efficient, more accessible, and data-driven, by taking advantage of scalable cloud computing resources [4].

Yet, as healthcare continues to become reliant on digital technologies, cybersecurity has become the problem of significant concern. The high sensitivity of patient information is coupled with the increased rate of cyber-attack to healthcare facilities, which requires the use of smart security systems. AI and ML may be utilized to detect anomalies, find intrusion patterns, and respond to the threats in real-time, and ChatGPT-like systems may be used to help human operators deal with the security incidents and create automated reports [5]. The adoption of such tools into cloud environments develops a homogeneous system of intensive, safe healthcare practise.

This review aims to give a broad summary of the application of AI, ChatGPT, and ML in healthcare, as well as cybersecurity with a focus on cloud-based analytics, disease monitoring, and data protection systems. It also seeks to outline the existing progress, possible uses, and challenges that accompany the process and also establishes gaps in the existing studies. Exploring the potential of intelligent computing and data security, this paper will help to understand how AI-powered systems can change the contemporary healthcare field and guarantee the privacy and integrity of sensitive data [6].

AI, CHATGPT, AND MACHINE LEARNING

Artificial Intelligence (AI), machine learning (ML), and state-of-the-art language models such as ChatGPT have become new technologies that transform the future of digital innovation in all fields of work, including healthcare and cybersecurity. AI is the process of mimicking human intelligence in machines and it allows machines to undertake activities like learning, reasoning and deciding [7]. In AI, ML is a subcategory where systems are capable of learning automatically through data and then becoming increasingly better at their tasks without being explicitly programmed. Cloud computing builds on these technologies by offering scalable storage, computing capabilities, and

Global Journal of Machine Learning and Computing
ISSN : 3079-692X
Volume 1, Number 2, 2025
https://doi.org/10.70445/gjmlc.1.2.2025.43-59

availability to use large-scale data analysis and make intelligent decisions [8].

Machine Learning has a broad collection of algorithms and models that aim to identify trends in data. Predictive analytics and classification is dealt with by supervised learning, pattern discovery and clustering are dealt with by unsupervised learning, and decision optimization with reinforcement learning. ML algorithms are commonly used in medical imaging, genetics, as well as in disease outcome prediction [9]. As an example, convolutional neural networks (CNNs) can identify anomalies in medical images, whereas recurrent neural networks (RNNs) can be applied to sequential data, e.g. patient health records. In a similar way, in cybersecurity, the ML can be used to identify network intrusions, phishing attacks, and malware based on the observations of abnormal data activities and emerging threat trends [10].

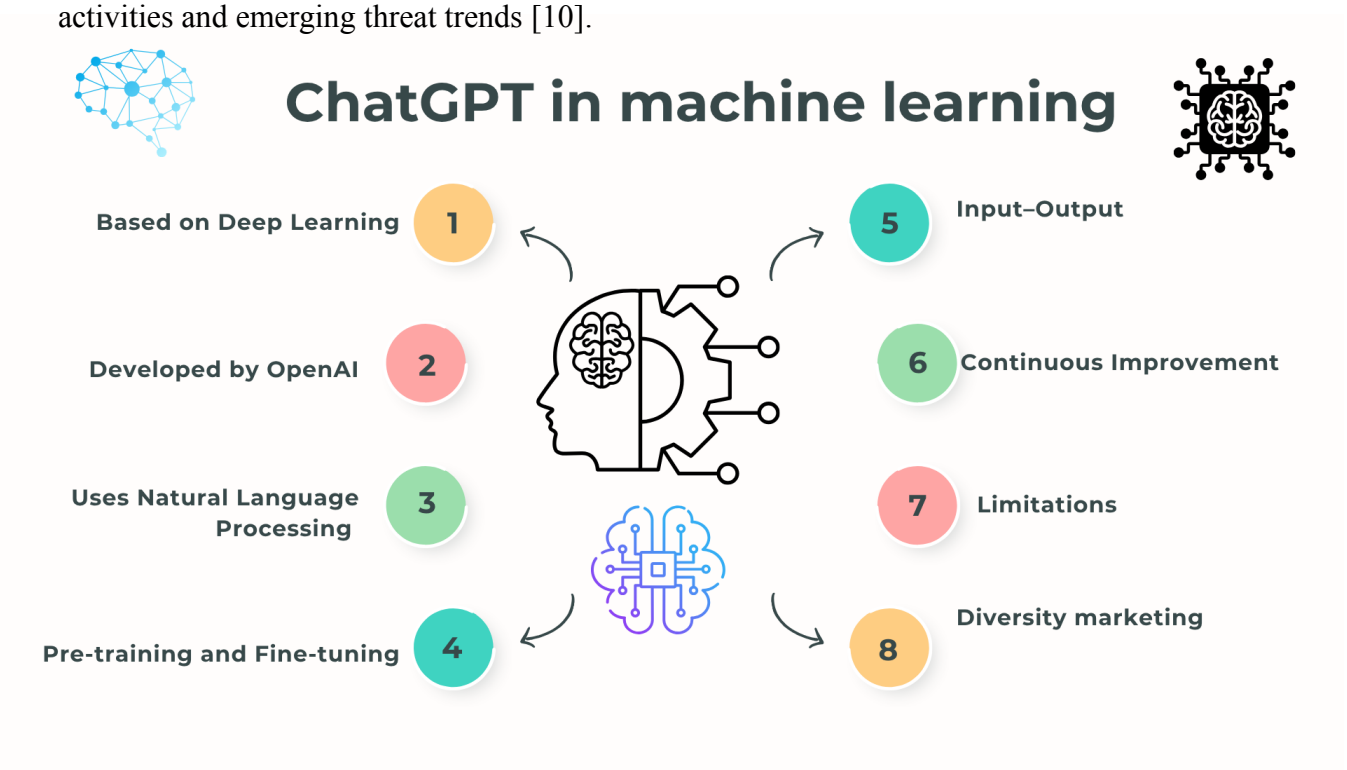

Figure: 1 showing ChatGPT in machine learning

ChatGPT ChatGPT is a generative AI model, which is a breakthrough in Natural Language Processing (NLP) and created by OpenAI. According to the transformer architecture, ChatGPT can comprehend and write like humans, which allows humans to interact with computers smoothly. ChatGPT could be used in healthcare by assisting clinicians in summarizing their medical reports, extracting pertinent information out of EHRs, and even talking with patients to conduct the initial triage or a follow-up interaction. It may be applicable in the context of cybersecurity to create automated reports regarding incidents, provide simple explanations of complex security findings, and aid in real-time decision making during a cyber-incident [11].

The presence of AI, ML and ChatGPT in the cloud environment has also improved their functionality.

ISSN : 3079-692X
Volume 1, Number 2, 2025
https://doi.org/10.70445/gjmlc.1.2.2025.43-59

The cloud-based AI services offer a platform to execute intelligent models in large scale and offer continuous analysis of data, speedy computation and low expenses of implementation. These integrated technologies are the basis of the next generation smart systems which can predict, autonomously operate, and learn adaptively. Subsequently, the synergy of AI, ML, and ChatGPT has created new possibilities in the creation of intelligent, secure, and efficient healthcare and cybersecurity applications [12].

CLOUD-BASED ANALYTICS IN HEALTHCARE PERTAINS TO THE FIELD OF HEALTH CARE ANALYTICS

Cloud-based analytics has become a revolution in the contemporary healthcare, as it allows effective data storage, processing, and analysis of vast amounts of data as never before. As medical data volume continues to skyrocket due to electronic health records (EHRs), wearable devices, medical imaging systems, and genomic sequencing, on premise infrastructures have been shown to be inefficient in handling large volumes of medical data. Cloud computing can offer scalable and flexible approach to enable healthcare institutions to store and analyze patient data safely and at a low cost [13]. Healthcare providers can use Artificial Intelligence (AI) and Machine Learning (ML) to provide useful insights to disease-detection, treatment-planning, and operational efficiency by integrating them into cloud platforms [14].

Healthcare cloud computing is mostly executed with three service models, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS provides virtualized computing services to store and handle data, PaaS services are used to develop and deploy healthcare applications, and SaaS services are ready-made cloud-based software used to perform clinical and administrative duties [15]. All of these services allow healthcare organizations to combine the power of analytics and work harmoniously across the various sites to improve decision-making and patient outcomes [16].

AI and ML can be crucial to cloud-based healthcare analytics since they can automatize the interpretation of data and provide predictive insights. Machine learning can be used to process patient records and predict disease development, reveal the at-risk groups, and prescribe custom care plans. Deep learning in the field of medical imaging can recognize the early stages of a disease, including cancer, stroke, or diabetic retinopathy, with great precision [17]. Microsoft Azure Health, Google Cloud Healthcare API, and AWS Health Lake are examples of cloud-based systems that offer services that combine AI and can assist researchers and clinicians to analyze large volumes of data with ease and still satisfy healthcare requirements [18].

Although cloud-based healthcare analytics has many advantages, it has numerous challenges.

ISSN : 3079-692X
Volume 1, Number 2, 2025
https://doi.org/10.70445/gjmlc.1.2.2025.43-59

Achieving privacy of data, regulatory compliance (including HIPAA and GDPR) and effective cybersecurity are still the main concerns. Also, there is the threat of problems connected to the interoperability of the data, latency, and reliance on the service providers. However, through the development of encryption, access control and federated learning, most of these issues are getting resolved [19]. Simply put, cloud-based analytics forms the backbone of intelligent healthcare systems which is able to make real-time decisions, predictive models and provide personalized care delivery. Combined with AI and ML, it offers an effective framework of changing the healthcare system into a more efficient, data-driven, and secure digital infrastructure [20].

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN DISEASE DETECTION AND PREDICTION

Artificial Intelligence (AI) and Machine Learning (ML) have become part of the contemporary healthcare system, specifically in the disease detection, diagnosis, and prediction. The technologies use big data on medical data to figure out patterns, spot irregularities, and predict health outcomes with astonishing accuracy. The use of AI and ML in medicine has brought a considerable improvement to the accuracy of the diagnosis, minimization of human error, and early intervention, thus improving the outcomes of the patients and optimizing healthcare delivery [21]. Through clinical data analysis, radiograph images, and genetic information as well as electronic health records (EHRs), AI-powered systems can help healthcare professionals make evidence-based decisions [22].

Disease detection is through the use of Machine Learning algorithms. In the classification of diseases using labeled data, supervised learning techniques, including decision trees, decision support machine (SVM), and random forests are employed. As an example, it can be seen that ML models can be used to predict cardiovascular risks based on the history of a patient, lifestyle, and laboratory results. Deep learning and especially convolutional neural networks (CNNs) have demonstrated tremendous ability in the medical imaging domain in terms of identifying tumors, fractures, and retinal illnesses [23]. Unsupervised learning techniques assist in identifying latent patterns in unstructured medical data that may result in the identification of novel disease biomarkers or risk factors. Another branch of ML is reinforcement learning that is being applied to optimize treatment strategies and personalize the treatment of patients [24].

The use of AI in diagnostics also goes to forecasting and prevention of diseases. Predictive analytics models have the ability to determine the probability of the occurrence or recurrence of a disease by using past patient information. In the case of chronic conditions like diabetes, high blood pressure, and cancer, AI solutions will be able to detect early warning signs and prescribe preventive measures [25]. Moreover, with the help of the integration of Internet of Things (IoT) devices and AI, it becomes

ISSN : 3079-692X
Volume 1, Number 2, 2025
https://doi.org/10.70445/gjmlc.1.2.2025.43-59

possible to continuously monitor health. Physiological data is gathered by the wearables and smart sensors and processed by ML models to identify abnormalities in real-time to enable proactive healthcare [26].

NLP-based models such as ChatGPT are also increasingly becoming useful in disease prediction and decision support. Such systems are able to summarize patient history, derive useful clinical data out of unstructured data and aid clinicians in diagnosis. Nonetheless, the ethical issues which require consideration include algorithmic bias, data privacy, and explain ability to make AI use responsible [27]. The disease detection systems and predictors based on AI and ML are transforming the healthcare sector by making the healthcare system more proactive instead of reactive. Such smart technologies enable clinicians to gain data-driven insights, achieve a more accurate diagnosis, and also help create a more efficient, predictive, and patient-centric healthcare ecosystem [28].

HEALTHCARE SYSTEMS AND CYBERSECURITY

The growing digitization of medical records and the use of interconnected technologies have made cybersecurity an important part of the modern healthcare systems. Increased exposure to cyber threats in healthcare organizations is now more integrated with the adoption of electronic health records (EHRs), telemedicine, and Internet of Things (IoT)-enabled devices as never before. Medical history, insurance data, and genomic data are sensitive patient information that has become a precious target of hackers [29]. Such cyber-attacks like ransom ware, phishing, data breaches, and Distributed Denial of Service (DDoS) attacks will be able to disrupt the operations of a hospital, affect patient safety, and lead to significant financial and reputational losses. Consequently, the possibility to introduce powerful and AI-based systems of cybersecurity is crucial to achieving data integrity, confidentiality, and availability in health care settings [30].

The concept of Artificial Intelligence (AI) and Machine Learning (ML) has become an influential weapon in the fight against the emerging cyber threats to healthcare systems. The conventional security approaches are usually based on the rule-based systems that are not dynamic and can therefore not match up with advanced attacks. By contrast, AI-based cybersecurity solutions are able to process large volumes of network data in real time, identify abnormalities, and potential threats before they can do damage [31]. The ML algorithms are especially useful in studying the past to identify abnormal behavior, linking malware, and anticipating possible vulnerability. As an example, abnormal logins or abnormal access to patient records can be detected using anomaly detection models which indicates potential insider threats or external breaches [32].

Global Journal of Machine Learning and Computing

ISSN : 3079-692X
Volume 1, Number 2, 2025
https://doi.org/10.70445/gjmlc.1.2.2025.43-59

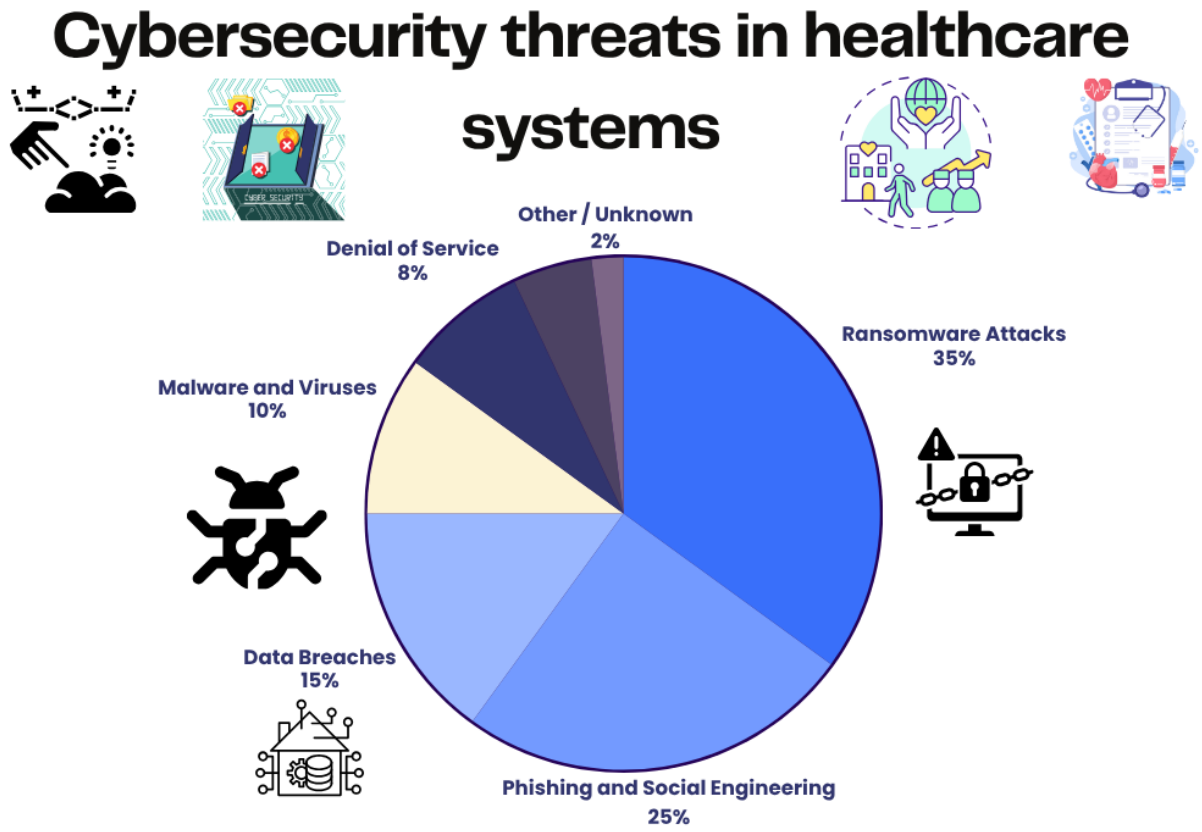

Figure: 2 showing cybersecurity threats in healthcare systems

Other technology uses in cybersecurity are emerging natural language processing (NLP) technologies such as ChatGPT. ChatGPT may be helpful to create automated incident reporting, phishing email analysis, and summarize threat intelligence in real-time. It may also be utilized in the training of cybersecurity awareness whereby staff can be aware and responsive to any attacks. Besides, by connecting AI systems to Security Information and Event Management (SIEM) systems, it is possible to monitor more rapidly, respond to incidents more quickly, and conduct more thorough risk assessments [33].

Besides AI and ML, other technologies like block chain and advanced encryption are also being utilized in order to improve the security of data in the healthcare sector. Block chain contributes to the data transparency and immutability which minimizes the chances of medical records being altered by unauthorized individuals. Nevertheless, HIPAA, data privacy, interoperability, and regulatory compliance (e.g., HIPAA, GDPR) issues continue to exist regardless of the technological progress [34]. AI-based cybersecurity models are fundamental in safeguarding the healthcare systems against dynamic and intricate cyber-attacks. A robust, safe digital ecosystem based on smart analytics, automation, and safe data management can help healthcare organizations establish safe and reliable

ISSN : 3079-692X
Volume 1, Number 2, 2025
https://doi.org/10.70445/gjmlc.1.2.2025.43-59

digital environments in which patient safety and data credibility are guaranteed [35].

SYSTEMIC SOLUTIONS TO AI-ASSISTED HEALTHCARE AND CYBERSECURITY

The combination of Artificial Intelligence (AI), Machine Learning (ML) and sophisticated Natural Language Processing (NLP) applications like ChatGPT in cloud environments has created the basis of intelligent, safe, and interoperable healthcare ecosystems. A comprehensive model that coordinates healthcare analytics and cybersecurity solutions is necessary to control, handle, and safeguard the rising amount of sensitive medical information [36]. These frameworks will facilitate the smooth cooperation of healthcare providers, data scientists, and cybersecurity specialists and guarantee patient safety, data confidentiality, and international regulatory requirements [37].

The general structure of an AI-based integrative model has several layers: the data acquisition layer, data processing and analytics layer, AI/ML modeling layer, and cybersecurity management layer. Real-time data of various sources including electronic health records (EHRs), medical imaging systems, wearable IoT devices, and laboratory databases is collected by the data acquisition layer. The analytics layer is based on cloud-computing to cleanse, standardize, and store data in an efficient manner [38]. The second step is to use AI/ML modeling layer to diagnose, prognoses, and optimize treatment of the disease using predictive algorithms. Lastly, the cybersecurity layer will use AI-based intrusion detection systems (IDS), encryption, and block chain to protect data and system integrity of patients [39].

The interoperability is very vital in the success of such frameworks. The AI-based healthcare systems must have the capability to communicate with multiple platforms and institutions to provide holistic patients with care. This is made easier through cloud computing which offers scalable and flexible infrastructures which enables model deployment and sharing of data securely. Privacy-preserving learning Federated learning is another type of integration that allows models to learn on decentralized data without the need to transfer sensitive information [40]. This enables hospitals and research institutions to cooperate on the global AI models without compromising the data privacy and regulations.

These frameworks can be integrated with chatGPT and other large language models (LLMs) that assist in healthcare and cybersecurity activities. ChatGPT might be used in healthcare in the following ways as a means of facilitating clinicians with summarizing of report, diagnostic findings, and decision support. It can also automate alert triage, incident documentation and communication with technical teams in the field of cybersecurity [41]. The examples of the most successful companies indicate that the combination of AI and cybersecurity can not only improve the safety of information but also improve the productivity of the operations. These integrated constructs guarantee proactive

ISSN : 3079-692X
Volume 1, Number 2, 2025
https://doi.org/10.70445/gjmlc.1.2.2025.43-59

threat detection, better healthcare analytics, and automated workflow. Finally, AI-based integrative models are the future of safe, intelligent, and data-driven medical systems that connect the clinical novelty and cyber resilience gaps [42].

HURDLES AND RESEARCH LIMITATIONS

Though the solutions of Artificial Intelligence (AI), Machine Learning (ML), and cloud-based analytics to healthcare and cybersecurity have made amazing strides, there are multiple challenges and gaps in the research that the solutions cannot be used at large scale. Such restrictions have technical, ethical, organizational, and regulatory aspects, which should be considered to make AI-enhanced systems reliable, transparent, and secure. These challenges need to be known in order to drive both technological and human facets of digital healthcare transformation [43].

Among the main challenges, there is the technical constraint of AI and ML models. The majority of healthcare data is extremely heterogeneous, unstructured, and incomplete and may induce biased or incorrect model results. To train MCs, it is necessary to have a very large amount of high quality labelled data and this is not easily available in healthcare because of privacy laws and data silos [44]. Also, most of the models are not generalizable; algorithms that are developed on a specific dataset or population can also fail when used on different populations. The black box aspects of deep learning systems also pose a question to explain ability because clinicians and security experts are not always able to comprehend the way the decisions made by such algorithms are reached [45].

Another major hitch is privacy and ethical issues. Health information is highly sensitive and in case of breach or abuse it may have dire consequences to patients and institutions. Despite the fact that the use of encryption, block chain, and federated learning methods has enhanced the security of the data, there are still issues on how to balance accessibility and privacy of the data. The adoption is further complicated due to ethical considerations, including the bias of algorithms and the fact that AI can be potentially misapplied to make the right decision. Fairness, accountability, and transparency of AI systems are one of the primary research priorities [46].

Scalability and interoperability are also a challenge. Artificial intelligence (AI) models need integration with a variety of platforms, software, and regulatory frameworks to be incompatible with current healthcare systems and cybersecurity infrastructures. A high number of healthcare organizations do not have the technical base or qualified individuals to process AI-based mechanisms. In addition, the price of installation of high-level AI systems can be astronomically high, particularly in smaller or low-budget healthcare institutions [47].

The regulatory and governance issues confine the potential of AI. The current regulations like HIPAA and GDPR offer data protection provisions but fail to keep pace with fast technological

ISSN : 3079-692X
Volume 1, Number 2, 2025
https://doi.org/10.70445/gjmlc.1.2.2025.43-59

advancements. There is an immediate need in standardized models of AI validation, ethical audit, and data-sharing control [48]. To resolve these issues, there would be the need to have multidisciplinary cooperation between technologists, care providers and policymakers. Further studies in this area ought to aim at developing explainable, equitable and interoperable AI systems, with the ability to provide clinical accuracy as well as cybersecurity resilience [49].

FUTURE RESEARCH DIRECTIONS

The use of Artificial Intelligence (AI), Machine Learning (ML), and sophisticated language models like ChatGPT in the field of healthcare and cybersecurity remains a rapidly developing area with great opportunities and challenging issues. The next generation of these technologies should be made more transparent, reliable, scalable and ethically governed, as these technologies will evolve [50]. Creating intelligent systems that are not only powerful but also reasonable and reliable will be important in ensuring that the adoption of intelligent systems in the healthcare ecosystem is safe and fair [51].

The Explainable AI (XAI) in healthcare is one of the most promising research directions. The existing deep learning systems tend to be black box, and the clinicians cannot easily make out the way the diagnostic or predictive decisions are reached. In future research, it is necessary to develop interpretable models that allow giving clear explanations of their output, and, in such a way, clinicians can rely on AI-based recommendations and confirm them. Such sensitive fields like disease diagnostics and treatment planning, as well as risk assessment of patients, will require explainable models, where the accountability of decisions is the key factor [52].

The other new area of concern is how ChatGPT and other generative AI models may be integrated with Electronic Health Records (EHRs). ChatGPT can be used by doctors as an intelligent assistant, which can summarize patient history, extract important insights on unstructured clinical data, and produce automatic reports. Development of language models that optimize medical accuracy, contextual understanding, and bias reduction are studies that will be very beneficial to clinical decision-making systems [53]. Moreover, making NLP models and voice-based interfaces work in tandem may enhance the overall experience of telemedicine and patient interaction, making healthcare more human and interactive [54].

The implementation of AI-based automation and the creation of policies should be a focus of future studies in the context of cybersecurity. With the advancement of cyber threats, intelligent systems that can detect threats in real-time, automatically respond, and predict crimes will be essential. AI-based systems would realize vulnerabilities before attacks, thereby allowing healthcare organizations to have strong data protection systems [55]. Anomaly detection using ML with the block chain technology and quantum-safe encryption will be more effective in advancing the security and data

ISSN : 3079-692X
Volume 1, Number 2, 2025
https://doi.org/10.70445/gjmlc.1.2.2025.43-59

integrity [56].

The potential of emerging technologies like Quantum Computing and Edge AI is quite high. Quantum computing may transform the computation and encryption of complex medical data, whereas Edge AI would allow localized and real-time analytics on an IoT and wearable devices - reducing latency and enhancing privacy [57]. The key focus of future studies is to develop an ethical, explainable, and secure AI ecosystem to seamlessly integrate healthcare innovation with cybersecurity resilience, a safer and smarter digital future of the global healthcare systems [58].

CONCLUSION

The application of Artificial Intelligence (AI), Machine Learning (ML), and sophisticated language models like ChatGPT to the healthcare and cybersecurity sectors is a revolutionary move in the modernization of the health system of the entire world. Following the current trend of the healthcare industry producing large volumes of data in the form of electronic health records (EHRs) and wearable devices, medical scans, and genomic sequencing, the conventional data management systems proved to be not enough to process and analyze this information effectively. The implementation of AI-based and cloud-computing analytics systems has helped healthcare organizations to generate actionable insights, improve disease detection, better patient outcomes, and data integrity. At the same time, technological progress has raised some new issues concerning the protection of cyberspace, privacy, and a moral code of ethics to be considered in order to guarantee secure and consistent integration.

AI and ML have shown that they can be immensely useful in the process of disease detection, diagnosis, and prediction. Since there are deep learning algorithms that recognize tumors on medical images, predictive models that predict chronic diseases, and so on, these technologies can allow proactive and personalized healthcare. Clinicians have data-driven insights through AI-driven analytics, which avoid diagnostic mistakes and more precise treatments. Moreover, the Natural Language Processing (NLP) models such as ChatGPT play an important role in healthcare efficiency, as they summarize medical documents, help in communication with the patient, and aid in the making of clinical decisions. The capability of ChatGPT to read complex medical information and communicate with the users in a conversational way opens up new prospects of patient interaction and education. The result of this democratization of medical knowledge and routine task automation would help decongest the administration of healthcare professionals and help make healthcare services more accessible, particularly in resource-constrained settings.

But, with a rise in the level of digitization of the healthcare ecosystem, cybersecurity has become another parallel concern. Cybercriminals favor healthcare institutions because the data and

ISSN : 3079-692X
Volume 1, Number 2, 2025
https://doi.org/10.70445/gjmlc.1.2.2025.43-59

information related to their patients is sensitive and there is a high demand of such records. Ransomware, phishing, and data breach are examples of cyberattacks that may lead to devastating disruptions to patient safety and the reputation of the institution. Threat detection and mitigation are being transformed by the association of AI and ML with cybersecurity systems. Algorithms of machine learning have opportunities to detect anomalies, anticipate possible attacks, respond in a timely manner, and AI-based automation allows managing the incident and recovering faster. Language models such as ChatGPT also complement cybersecurity in terms of automatic incident reporting and phishing content analysis, as well as helping human operators with intelligent and natural-language interaction.

These AI-driven healthcare and cybersecurity systems have been supported by cloud computing. The cloud-based platforms provide scalable storage and computing capabilities as well as interoperability enabling the healthcare providers to handle large volumes of data effectively. They also enable interaction between researchers, clinicians and data scientists in various institutions. The use of AI-based tools on clouds allows real-time analytics and personalized medicine, which produce quicker diagnoses and strategies of treatment. Nevertheless, issues of data privacy, compliance with regulations, and reliance on third-party cloud providers should be handled. The legal regulations of healthcare data (HIPAA and GDPR) impose some of the strictest requirements concerning data safety and privacy of patients, which institutions must address on their highest standards.

Even though AI and cloud-based medical systems have great prospects, there remain a number of research gaps. These are technical constraints of the available algorithms, data quality problems, non-interoperability between systems, and ethical issues of bias and explain ability of algorithms. Most AI models act as black boxes and there is very little insight into the mechanisms used to arrive at a conclusion. This inability to interpret it negatively affects the establishment of trust among the healthcare professionals and questions the issue of accountability ethically. The unequal access to AI technologies can potentially expand the healthcare disparities between developed and developing areas, and the need to implement AI inclusively and equally. Future studies should be geared towards clarifying, open, and unbiased AI programs that respect ethical principles and encourage equitability in health care decision-making.

The future of AI in healthcare and cybersecurity consists of the creation of integrative, intelligent and secure healthcare and cybersecurity frameworks that combine the two areas. Intelligent cybersecurity systems developed with AI will be key to safeguarding sensitive healthcare data, and AI-enhanced analytical options are going to promote advancements in precision medicine and disease prevention. The new research opportunities are provided by new technologies like federated learning, quantum

ISSN : 3079-692X
Volume 1, Number 2, 2025
https://doi.org/10.70445/gjmlc.1.2.2025.43-59

computing, and Edge AI. Federated learning The Federated learning model enables collaborative model training, but does not share data, which boosts privacy; quantum computing will have unmatched processing power on complex medical and encryption models; and Edge AI will enable real-time and localized analytics on IoT and wearable devices, eliminating the need to rely on a central server.

To sum up, AI, ML, ChatGPT, and cloud computing are converging, and it can be assumed that this will usher in a new era of healthcare innovation and cybersecurity resilience. Together, these technologies can turn healthcare into a predictive and responsive, fragmented and integrated, and vulnerable to secure. Nevertheless, this vision can be attained through a moderate solution, that is, with an emphasis on ethical governance, compliance with regulations, and human control. The interdisciplinary cooperation of health practitioners, technologists, policymakers, and cybersecurity specialists is essential in order to make sure that such technologies are used in a responsible and fair manner. The potential of AI-driven technologies can be leveraged to the full to provide secure, intelligent, and patient-centered care in the future by addressing the current issues and relying on sustainable innovation to transform the global healthcare system.

REFERENCES

[1]. Lodhi SK, Zeb S. Ai-Driven Robotics and Automation: The Evolution of Human-Machine Collaboration. Journal of World Science. 2025 May 13;4(4):422-37.

[2]. Neoaz N. Big Data Analytics Study the implications of big data analytics on decision-making processes in organizations. Author Nahid Neoaz. 2025 Jan 20.

[3]. Javeedullah M. Security and Privacy in Health Informatics: Safeguarding Patient Data in A Digital World. AlgoVista: Journal of AI and Computer Science.;2(3):52-68.

[4]. Neoaz N. Human Factors in Information Assurance: A Review of Behavioral and Cultural Aspects. International Journal of Multidisciplinary Sciences and Arts. 2024;3(4):235-42.

[5]. Neoaz N, Amin MH. Advanced AI Paradigms in Mental Health: An In-depth Exploration of Detection, Therapy, and Computational Efficacy. Global Insights in Artificial Intelligence and Computing. 2025 Jan 25;1(1):40-6.

[6]. Bacha A. Healing with Algorithms: The Future of AI-Driven Diagnostics and Treatment. American Journal of Artificial Intelligence and Computing. 2025 May 9;1(1):103-18.

[7]. Govindarajan V, Muzamal JH. Advanced cloud intrusion detection framework using graph based features transformers and contrastive learning. Scientific Reports. 2025 Jul 1;15(1):20511.

ISSN : 3079-692X
Volume 1, Number 2, 2025
https://doi.org/10.70445/gjmlc.1.2.2025.43-59

[8]. Bacha A, Shah HH, Abid N. The Role of Artificial Intelligence in Early Disease Detection: Current Applications and Future Prospects. Global Journal of Emerging AI and Computing. 2025 Jan 20;1(1):1-4.

[9]. 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.

[10]. Neoaz N, Amin MH. Advanced AI Paradigms in Mental Health: An In-depth Exploration of Detection, Therapy, and Computational Efficacy. Global Insights in Artificial Intelligence and Computing. 2025 Jan 25;1(1):40-6.

[11]. Singh A. A Survey of Foundational Concepts and Emerging Frontiers in Computer Science. Global Research Repo. 2025 Sep 9;1(2):279-309.

[12]. 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.

[13]. 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.

[14]. Singh A. Human-Computer Interaction: A Review of Usability, Design, and Accessibility Trends. Global Research Repo. 2025 Sep 9;1(2):362-87.

[15]. Zeb S. Artificial Intelligence in Healthcare: Technological Progress and Ethical Frontiers. American Journal of Artificial Intelligence and Computing. 2025 Aug 13;1(2):105-24.

[16]. Govindarajan V. Early Detection and Risk Stratification of Osteosarcoma, A Rare Tumor, Using Artificial Intelligence: A Systematic Review. Advances in Artificial Intelligence and Machine Learning. 2025; 5 (2): 221 [Internet]. Sarcoma; 2024

[17]. Javeedullah M. Interoperability Solutions for Efficient Health Informatics Systems. Global Trends in Science and Technology. 2025 Apr 22;1(1):176-94.

[18]. Zeb S, Lodhi SK. AI for predictive maintenance: Reducing downtime and enhancing efficiency. Enrichment: Journal of Multidisciplinary Research and Development. 2025 May 13;3(1):135-50.

[19]. Kabeer MM. Artificial Intelligence in Modern Manufacturing: Opportunities and Barriers. Global Trends in Science and Technology. 2025 Jul 16;1(3):83-100.

ISSN : 3079-692X
Volume 1, Number 2, 2025
https://doi.org/10.70445/gjmlc.1.2.2025.43-59

[20]. Zeb S, Lodhi SK. AI and Cybersecurity in Smart Manufacturing: Protecting Industrial Systems. American Journal of Artificial Intelligence and Computing. 2025 Apr 7;1(1):1-23.

[21]. Javeedullah M. Integrating Health Informatics Into Modern Healthcare Systems: A Comprehensive Review. Global Journal of Universal Studies.;2(1):1-21.

[22]. Govindarajan V. Early Detection and Risk Stratification of Osteosarcoma, A Rare Tumor, Using Artificial Intelligence: A Systematic Review. Advances in Artificial Intelligence and Machine Learning. 2025; 5 (2): 221 [Internet]. Sarcoma; 2024

[23]. Javeedullah M. Role of Health Informatics in Public Health Surveillance and Response. American Journal of Artificial Intelligence and Computing. 2025 Apr 21;1(1):70-86.

[24]. Neoaz N, Shah HH, Zainab H. AI in Personalized Medicine: Transforming Treatment Plans through Precision Health. Global Journal of Emerging AI and Computing. 2025 Jan 23;1(1):34-50.

[25]. Adebayo AS, Chukwurah N, Ajayi OO. Artificial Intelligence and Machine Learning Algorithms for Advanced Threat Detection and Cybersecurity Risk Mitigation Strategies.

[26]. Singh A. Evolution of Computer Science: A Historical and Technological Overview. American Journal of Artificial Intelligence and Computing. 2025 Jul 23;1(2):62-86.

[27]. Govindarajan V. A Novel System for Managing Encrypted Data Using Searchable Encryption Techniques. International Journal of Advanced Computer Science & Applications. 2025 Mar 1;16(3).

[28]. Javeedullah M. Using Health Informatics to Streamline Healthcare Operations. American Journal of Artificial Intelligence and Computing. 2025 Apr 7;1(1):24-44.

[29]. Shihab SR, Sultana N, Samad A. Revisiting the use of ChatGPT in business and educational fields: Possibilities and challenges. BULLET: Jurnal Multidisiplin Ilmu. 2023;2(3):534-45.

[30]. Singh A. Evolution of Computer Science: A Historical and Technological Overview. American Journal of Artificial Intelligence and Computing. 2025 Jul 23;1(2):62-86.

[31]. 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.

[32]. Govindarajan V, Kumar P, Kumar D, Devi H, Kumar S, Shiwlani A. ROLE OF CLOUD-DEPLOYED GRAPH NEURAL NETWORKS IN MAPPING CORONARY ARTERY DISEASE PROGRESSION: A SYSTEMATIC REVIEW. Journal of Medical & Health Sciences Review. 2025 May 30; 2(2).

[33]. Javeedullah M. Future of Health Informatics: Bridging Technology and Healthcare. Global Trends in Science and Technology. 2025 Apr 4;1(1):143-59.

ISSN : 3079-692X
Volume 1, Number 2, 2025
https://doi.org/10.70445/gjmlc.1.2.2025.43-59

[34]. Abid N, Neoaz N, Amin MH. AI-Driven Approaches to Overcoming Tumor Heterogeneity in Breast Cancer: Modelling Resistance and Therapy Outcomes. Global Journal of Universal Studies.;1(2):591050.

[35]. Javeedullah M, Zeb S. Privacy, Policy, and Progress: Reviewing the Regulatory Landscape in Health Informatics. Global Research Repo. 2025 Sep 3;1(2):112-28.

[36]. 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.

[37]. Khan M, Sherani AM, Bacha A. The Neurological Nexus: Exploring EEG, Facial Recognition, and Graph Algorithms in Mental Health AI. Global Insights in Artificial Intelligence and Computing. 2025 Jan 26;1(1):47-56.

[38]. Bacha A. Unveiling Frontiers: Hybrid Algorithmic Frameworks for AI-Driven Mental Health Interventions. AlgoVista: Journal of AI and Computer Science. 2025;2(1):1-8.

[39]. Singh A. From Algorithms to AI: A Comprehensive Review of Core Concepts in Computer Science. Global Research Repo. 2025 Sep 3;1(2):129-53.

[40]. Bacha A, Zainab H. AI for Remote Patient Monitoring: Enabling Continuous Healthcare outside the Hospital. Global Journal of Computer Sciences and Artificial Intelligence. 2025 Jan 23;1(1):1-6.

[41]. Brohi S, Mastoi QU. AI under attack: Metric-driven analysis of cybersecurity threats in deep learning models for healthcare applications. Algorithms. 2025 Mar 10;18(3):157.

[42]. 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.

[43]. Neoaz N, Husnain A. Deciphering the AI Healthcare Evolution: Opportunities, Risks, and the Path Forward. Global Trends in Science and Technology. 2025 Mar 30;1(1):121-42.

[44]. Bacha A, Shah HH. AI-Enhanced Liquid Biopsy: Advancements in Early Detection and Monitoring of Cancer through Blood-based Markers. Global Journal of Universal Studies.;1(2):68-86.

[45]. Javeedullah M. Big Data and Health Informatics: Managing Privacy, Accuracy, and Scalability. Global Trends in Science and Technology. 2025 Jul 3;1(3):29-47.

[46]. Neoaz N. Role of Artificial Intelligence in Enhancing Information Assurance. BULLET: Jurnal Multidisiplin Ilmu. 2024;3(5):749-58.

ISSN : 3079-692X
Volume 1, Number 2, 2025
https://doi.org/10.70445/gjmlc.1.2.2025.43-59

[47]. Govindarajan V. Early Detection and Risk Stratification of Osteosarcoma, A Rare Tumor, Using Artificial Intelligence: A Systematic Review. Advances in Artificial Intelligence and Machine Learning. 2025; 5 (2): 221 [Internet]. Sarcoma; 2024

[48]. Samad A, Jamal A. Transformative Applications of ChatGPT: A Comprehensive Review of Its Impact across Industries. Global Journal of Multidisciplinary Sciences and Arts. 2024;1(1):26-48.

[49]. Bacha A, Sherani AM. AI in Predictive Healthcare Analytics: Forecasting Disease Outbreaks and Patient Outcomes. Global Trends in Science and Technology. 2025 Jan 24; 1(1):1-4.

[50]. Zeb S, Rouaf HA. Artificial Intelligence and the Future of Healthcare: A Comprehensive Review. American Journal of Artificial Intelligence and Computing. 2025 Sep 4;1(2):207-25.

[51]. 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.

[52]. Abbasi N, Nizamullah FN, Zeb S. AI in healthcare: integrating advanced technologies with traditional practices for enhanced patient care. BULLET: Jurnal Multidisiplin Ilmu. 2023 Jun 13;2(3):546-6

[53]. Govindarajan V, Devi H, Kumar P. Revolutionizing Cardiac Care: A Systematic Review of Intelligent Wearables And Cloud-Based Analytics.

[54]. Shah HH, Bacha A. Leveraging AI and Machine Learning to Predict and Prevent Sudden Cardiac Arrest in High-Risk Populations. Global Journal of Universal Studies.;1(2):87-107.

[55]. Bacha A, Sherani AM. AI in Predictive Healthcare Analytics: Forecasting Disease Outbreaks and Patient Outcomes. Global Trends in Science and Technology. 2025 Jan 24; 1(1):1-4.

[56]. Neoaz N, Shah HH, Zainab H. AI in Personalized Medicine: Transforming Treatment Plans through Precision Health. Global Journal of Emerging AI and Computing. 2025 Jan 23; 1(1):34-50.

[57]. Singh A. Artificial Intelligence and Its Expanding Role in Computer Science. American Journal of Artificial Intelligence and Computing. 2025 Sep 20;1(2):226-40.

[58]. Chakraborty C, Nagarajan SM, Devarajan GG, Ramana TV, Mohanty R. Intelligent AI-based healthcare cyber security system using multi-source transfer learning method. ACM Transactions on Sensor Networks. 2023 May 15.