Global Insights in Artificial Intelligence and Computing

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.81-103

Securing Healthcare in the Age of AI: A Comprehensive Review of Cybersecurity Challenges and Solutions

Ibrar Hussain[1*]

[1]University of Punjab, Lahore

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

open access

Corresponding Author

Ibrar Hussain
2021-pgcma38@nca.edu.pk

Article History:
Submitted: 15-01-2025
Accepted: 17-02-2025
Published: 21-02-2025

Keywords:
Healthcare, cyber security for health, AI and data protection legal issues, decentralized learning, secure computation, patient privacy and security, transparent and rights-preserving AI.

ABSTRACT

AI in the context of healthcare can be defined as a process of broadening the options on the improvement of the patients' quality of their treatment, an increase in productivity and decrease in the rates of diagnosis failure. But there are huge cyber risks, including the protection of patients' data and information, the model it adopted in AI, and primarily the security risks of healthcare networks. This review looks at the policy, which applies to the AI healthcare cybersecurity, how health data security is addressed, how the core of the AI model is protected, the issue of access, and lastly, monitoring as the final control. Subsequently, it presents new directions and opportunities in AI-based healthcare cybersecurity such as federated learning and homomorphic encryption and block chain. In addition, the review also explains the place of explanation and ethical evaluation regarding the construction of trust and accountabilities in AI solutions. Future endeavors imply that with the advance of applications and technologies concerning artificial intelligence, healthcare of today in both its practical implementation and future research, modern care providers, AI software developers, legislators, and IT security experts must cooperate to identify existing and potentially malicious threats towards introducing artificial intelligence into the healthcare systems of the future safely, securely, and in compliance with certain ethical standards. When these firms apply IT technical professional in AI to respect the regulations and ethical conducts the fn is subjected to cyber security tests and still maintain the data of the patients require treatment while using AI.

INTRODUCTION

Some of the studies state that the use of AI technologies affected the change in the healthcare sector at the base level, transferring many of the traditional approaches and diagnostics, patient's treatment, and even administrative employees' work. Thus, due to such AI applications as ML, DL, NLP and computer vision the diagnosis in medicine become better, the treatment become more effective and health care managing more efficient. It is currently used in many facets of medical solutions ranging from predicting risks of an epidemic occurrence to counselling and in surgeries [1]. However, employing AI is nowadays present in many healthcare organizations as a part of the strategies to provide effective care for the recipients and manage organizational processes and problems patients encounter; the negative potential it has is also more significant.

Adding on that with the possibility of integrating AI, come with on top of the mentioned form of concern, data privacy, sophistication of the AI Algorithm and security of interoperable medical devices. Indeed the issue of insecurity has been rampant in the field of health since the introduction of cyber technology coupled with integration of artificial intelligence where new form of insecurity emerge hence challenging the current established order. The attribute that the potential harm from attacks on AI systems is larger is due to the nature of these systems, as well as on the ever increasing amount of data required for training these algorithms and on the increasing number of devices being connected to healthcare systems [2].

Health care structural complexity is also important to the discussion of cybersecurity since health care data is considered one of the most enticing targets for cyber criminals. However, as the data feeds into AI systems handling the sensitive information of the patients, the probability of leakage of the data or its unauthorized access and, or research alteration of the patient data becomes too huge. A drawback is the privacy of patients for the rationale AI works with data that brings healthcare compliance problems such as HIPAA in the United States and GDPR in Europe. Also, the longevity of the more use of AI-based devices and health care resources such as surgery, health and fitness tracking devices present other risks [3]. They may have the potential to make the overall quality of care that patients get better, and yet that is where potential sources of breakdowns are. In the wrong hands, such devices could darken services that are so vital, or else become dangerous to a patient's health. In other cases, having control over a certain machine, like robotics used in surgeries will plant a replacement for a successful surgery and could cause a catastrophe [4].

With these risks taken in consideration in cybersecurity, it is high time that health care practitioners together with health care policy makers and IT solution developers to lead in the establishment of a competent health care security environment most importantly for Artificial Intelligence enhanced systems. Cybersecurity products require changes addressing new development in AI through which the threats are marketed. This calls for research in generating improved secure AI models, ensuring the training data is checked for integrity and sanitized, the data encrypted and only accessible to authorized people, frequent security and threat checks conducted. The goal of this paper is to initiate the conversation on how AI can exist in the context of healthcare and what cyber security concerns stem from AI and cyber security for healthcare systems [5]. It will be more focused on the risks today that are being taken, the rules that are being put in practice for managing such risks, and new approaches in the utilization of safe and secure AI in health care, so that AI's opportunity in zigging up the delivery of health care is not backed up with risks of harming the patient and their data.

AI TECHNOLOGIES IN HEALTHCARE

Artificial intelligence (AI) has thus seeped silently and integrally into the contemporary healthcare domain cutting across the various facets of practice and administration. The importance of AI applications in the project of managing health care comes from the high capability of handling and analyzing the massive amounts of data and the patterns, and decision-making to arrive at the prognosis or decision to top up the clinicians' performance. The current primary emerging and disruptive technologies in the healthcare sector are: Advanced ML, Deep Learning (DL), Natural Language Processing (NLP), and computer vision [6]. These include diagnosis, treatment, planning, monitoring patients and some clerical work within a health care organization.

Machine Learning and Deep Learning in Diagnostics: A subfield of AI called machine learning allows applications to adapt to the data they are fed, without being programmed how this may be achieved. It has especially revealed high potential in such field as medical diagnostics with the help of which AI algorithms analyze medical data to in diagnosis of diseases. For instance, it is common knowledge that some level of lesion detection is possible in images as obvious as X-ray, CT and MRI images as and more efficiently than human radiologists. Reports proved that machine learning particularly multi-layered neural network known as deep learning has also rapidly advanced in other fields including image and speech recognition processes. This kind of artificial intelligence is particularly valuable in such complex processes as scan or analysis of histopathology slides in order to determine cancer malignancy, or determination of further patient management in his/her electronic health record [7].

AI in Medical Imaging and Personalized Medicine: Our analysis shows that arguably, the most significant use-case for medical imaging is indeed highly vulnerable and greatly enhanced by AI. The technology helps the clinician to diagnose early stage diseases like cancer, cardiovascular diseases, and neurologic diseases from the images with reasonable certainty. For example, the deep learning

AI systems trained on the big data in the medical imaging can learn patterns indicative of Alzheimer's or Lung cancer before they are manifest as symptoms. This not only increases the total reliability of the work done, but also increases throughput, the time to make a diagnosis, to begin treatment, and to achieve successful outcomes for patients [8]. In addition, the use of machine learning has taken the root in the aspect of health care delivery that is providing personalized medicine where solutions are predicated on aspects of the client. Based on a patient's genetic makeup, his or her behavioral pattern, and medical history, AI models are in a position to design different treatment plans. For example, in oncology, it can be applied for estimating the utility of particular cancer treatment for the genotype of a patient with cancer. The approach is expected to improve the effectiveness of treatment and prevention of side effects, and meet the needs of health care delivery [9].

AI in Health Information Systems: They are also doing the same to other health systems to assist them in the operationalization as well as utilization of the patient information. For example, natural language processing NLP is used during the preprocessing step to process data obtained from clinics or historical papers and records. NLP helps AI systems to convert human language to machine understandable format in order to extract information from massive pile of documents. This capability is especially useful when the huge amount of data is often located in the free-text in note areas of the EHRs. Out of this unstructured data, the AI systems are able to extract possible patterns and diagnosis and inform the clinicians. CDSS is a crucial system which helps the health practitioners in the clinical moment's Offer recommendations. The AI- and EHRs coupled with CDSS can the potential interaction between the potential drugs, suggest which tests are essential for the patient, also the ideal treatment based on the present guidelines, and the patient characteristics [10].

AI in Patient Monitoring and Virtual Health Assistants: It also has a specialized application with the help of AI technologies in order to push forward patient monitoring systems. Smart watches and other health tracking devices also use AI engines to routinely collect signs that indicate physical health conditions including heart rate, blood pressure and blood sugar level. It can identify any irregularity and notify the patient and the doctor and are useful for persons with chronic a situation for as an example, diabetes type 2 or hypertension [11]. Moreover, actual AI virtual health assistants are being designed to assists the patients obtain the necessary data, advice, and help. These virtual assistants function under the NLP system and for the purpose of communicating with the patients, the dispenser can query the patient like asking what new symptoms have developed, can also use timers to remind the patient when it is time to take the dose and lastly the dispenser can do organizational tasks such as booking appointments. This way they engage the patients more and help with reducing the amount of paper work facing the healthcare employees [12].

AI in Healthcare Administration: AI is also improving other segments of the sectors of health such as; payments, assets, and timetables among others. AI has growth for handling all organizing operations of the hospital so that all the available Human and non-human resources such as Operation theatres etc... Are properly utilized. In the aspect of billing, it can be help with possible codes mistakes and faking billing it can help to raise accuracy and prevent from takeover the healthcare staff's time. HS technologies are gaining a standard base by enhancing diagnosis, treatments, patient and surveillance management, as well as organizational processes. AI application in healthcare is not only possible but turns into the future of the practice, therefore healthcare organizations will find themselves forced to adopt it. However, if the AI is integrated into healthcare steadily matters of security and ethics when dealing with the patient's information do arise. The following part of the paper will elucidate threats characteristic of the implementation of AI that poses a threat to the systems in the healthcare industry [13].

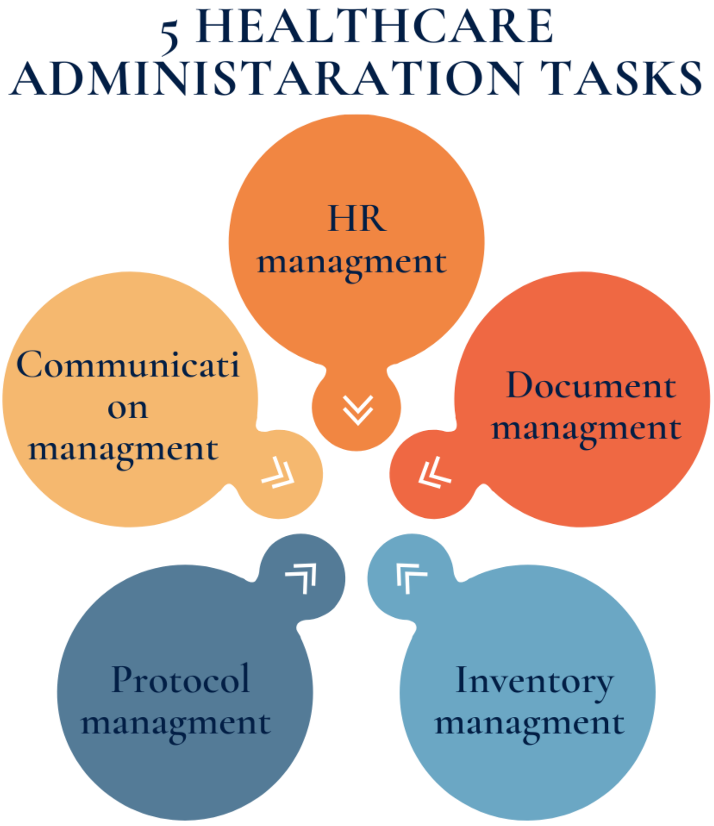

Figure: 1 showing healthcare administration tasks

Security Threats of IT Cyber in the Context of AI for Healthcare

The integration of Artificial Intelligence technologies in the system have immense utility in the health sector as they can enable higher or proper identification of ailments, patients as well as lessen on paperwork. It also introduces new and additional risks to cybersecurity that have to be addressed in order to safeguard the patient's data and AI systems and for the patient's benefit. When AI is becoming integrated further into practice, decision-makers and clinicians should understand these cybersecurity risks in order to protect their healthcare systems [14].

Data Privacy and Patient Confidentiality: Out of all the threats inside the healthcare industry concerning AI, one is the threat to the security of patients' data that may be considered the most pressing. EHRs, medical images, the genomics data is sensitive, and quite valuable to individuals and healthcare institutions. Having AI systems which analyze the patients' data, also increases the likelihood of hackers penetrating the patients' data. The coverage of AI technologies education requires the use of big data input and yet, sharing and storage are probably by cloud services. This also put the system in many likely place for hacking to happening [15]. In addition, the AI systems are linked to other data sources from the same and different categories: Wearable devices, mobile applications, and patient portals. More vulnerabilities becomes apparent when integrated systems is working since it links with other systems. Criminals who target healthcare SYS may take advantage of the weakness of the AI algorithms and software, and this is very risky and poses a threat to patient data confidentiality and serious consequences for the doctors or either the entire hospital [16].

Vulnerabilities in AI Algorithms and Models: Beneficial aspect which AI offers to the healthcare industry reflects no limitations to the – its algorithms and models – facing cyber risks. One of the most fundamental assumptions of both ML and DL is the training data on which forecasts or the general judgment is made, and these can be manipulated or otherwise adulterated. The main subcategories of attacks include the following: Adversarial attacks that involves feeding a machine wrong or even malicious data so as to receive wrong results. In healthcare for instance is may lead to patients being diagnosed wrongly, receiving wrong advice on treatment, or in some instances a disease such as cancer or heart disease might not be discovered.

What the above kind of attack portends is that patient care, wellbeing, as well as safety could be at serious risks [17]. Also, the AI models are capable of being manipulated in 'data poisoning', that is the attacker introduces wrong/bias data and the AI model will change. It could also change the outcome of the diagnosis or could give an incorrect advice about the need for treatment. These include: Ensuring high integrity of the data that feed the AI system used in training these systems is essential in the prevention of such weakness and in the development of credible AI instruments in healthcare systems [18].

Risks of AI-Powered Medical Devices: There is a large number of new types of medical devices, many of which are equipped with artificial intelligence, and thus raise the question of cybersecurity. Robotic surgery systems, infusion pump, AI – based diagnostic tools could be named among the most popular technologies in the health system. Due to the improved speed and accuracy of the user these device create new risks that are inherent to them. In one way or the other any cyber-attacks to affect these devices maybe disastrous to the patients. For instance, if a wrong figure is imputed in the robotic surgery system itself, then the surgeon operating the robotics could lost_ extreme damages in surgery operations or death. Similarly, diagnostics depending on artificial intelligence can be cheated, which will lead to inaccurate diagnoses or delayed delivery of medication. Despite the fact that they are integrated into healthcare systems and could become part of IoT participants, they can also be hacked [19].

Threats from Data Breaches and Cyber-attacks: The fact is that healthcare is one of the most popular targets for hackers since information about patients' health can be expensive and highly detrimental if the actions of a hacker interfere with the delivery of health care. In the last couple of years, the hospitals, for instance, have received a higher level of attacks in the type of ransom ware attack where the attackers get to control systems until they are paid a certain amount of money. Such a threat is particularly relevant to AI systems in healthcare since they might be the very essence of many diagnostic algorithms or means, as well as planning of treatment and patient care provision [20].

If a ransom ware attack is accomplished, it will actually bring a healthcare provider to the stand still for a while, treatments will be slowed down and important information will be lost. However, if those AI systems are infected with some types of virus such as malware the AI system can be used to disseminate information or even threaten the patient care system. As M Levine and S Singled illustrated, the specific threat of AI as managed and proactively controlled cyber-attacks demonstrated how existing efforts to prevent them could be overwhelmed in the future by these criminals [21].

Compliance with Regulatory Frameworks: Undoubtedly there lies potential when it comes to AI in Healthcare but so also does risk, especially with reference to the respective cybersecurity threats that they will bring and then the resultant legal and regulatory issues that arise from these. To that end, health care organizations must abide by such legal criteria like The Health Insurance Portability and Accountability Act (HIPAA) and The General Data Protection Regulation (GDPR) By collecting the information from the participants and storing it in an electronic manner, the health care organizations must state and enforce the privacy and security standards for the information, and for the consent of the participants [22]. The issue of adherence to these regulations is compounded when personal health data is being fed into artificial intelligent technologies.

That's why AI systems have to be protected for a patient's data should remain safe, and for the information should be used appropriately in accordance with the current legislation. This includes encryption activities, anonymization and protection of the data to avoid it from being used by those who shouldn't. This is also true because healthcare organizations should also audit and test their AI systems periodically amid its attempts at updating itself in the regulation [23].

Insider Threats and Human Error: Besides, as everyone, healthcare has to have defense against enemies and everyday obstacles but must not lose sight of the enemy within and mistakes. They include; clinicians, other healthcare workers, researchers and other staff who in one way or the other interact with the AI systems in healthcare organizations makes them vulnerable to security threats either inadvertent or intentional. From simple & ineffective passwords to insecure settings of devices, Health Care AI is in trouble from insiders of all forms. Such threats require certain training process, limitation of access rights and constant monitoring of insiders. Health care organizational managers should also ensure that physical structures involved in the delivery of AI systems and data to patients are well restricted from exposure to persons who have no business in them [24].

The consequences of the cybersecurity of AI application in health systems are immense and complex. Even though today the mentioned systems are being implemented into the health care systems, they become more susceptible to hacking, to a malicious attack or manipulation. The requirements to preserve the effectiveness and protection of algorithms used in AI, the patients' information, safety of healthcare gadgets containing AI technology are the other points that are significant concerning integration of AI into the health industry [25]. Concerns raised by these challenges cannot be fixed by technology, legislation, and frameworks only but require day and night commitment to deliver high level security solutions, as Healthcare Systems progress through time and still secure and dependable.

AI HEALTHCARE SECURITY LEGAL REQUIREMENT

From the algorithms, in healthcare; there is a concern that as the technology advances and forms a part of the health facilities safety and information confidentiality of registration data is a big concern. The growing use of healthcare tools that are AI-based is imposing new risks that include violations of patients' information and privacy, and actual manipulation of the systems in order to jeopardize patients' health, make the healthcare sector require better legal directions and policies. The following regulations help to preserve the patient's information and also develop the measures on the right usage of artificial intelligence and also defines the responsibility and reportage. In this part of the work, some of the regulation and standards of AI healthcare security presented, using HIPAA, GDPR, and other standards [26].

Health Insurance Portability and Accountability Act (HIPAA): HIPAA is a law in the United States meant to preserve the patient's information and ensure that its privacy and security is warranted. HIPAA regulates the handling of HEPA protected information and only the three following entities are in this bracket: Such entities include Healthcare providers Health plans Healthcare clearinghouses It also affects business associates that transact with the protected health information (PHI) of such entities. Since AI tools in healthcare deal with large amounts of PHI, personal and medical data and test results the rules of HIPAA still apply when it comes to designing and implementing AI in healthcare. HIPAA has very strict guidelines and policies as regard to data privacy and security and guidelines within the health care department on ubiquity of encryption, especially regimen for the storage and management of data [27]. Fundamentally, as used in HIPAA, PHI should not be used, read or communicated or changed in any unlawful or unlawful method. It also embraces early implementing, strong internal security controls such as, multiple-factor authentications, secure communication and security risk assessments. Furthermore, there is a necessity to enhance the regulatory requirements for patients' information use in AI system and first, the patients must agree to the use of their information. This is actually one of the biggest issues when it comes to applying AI for HIPAA – patient information must not be disclosed during training or other processes involving AI. Last but not least, current AI methods must be designed and tested to safeguard patient's data at the 'base' and other potential aggregated levels for future AI uses [28].

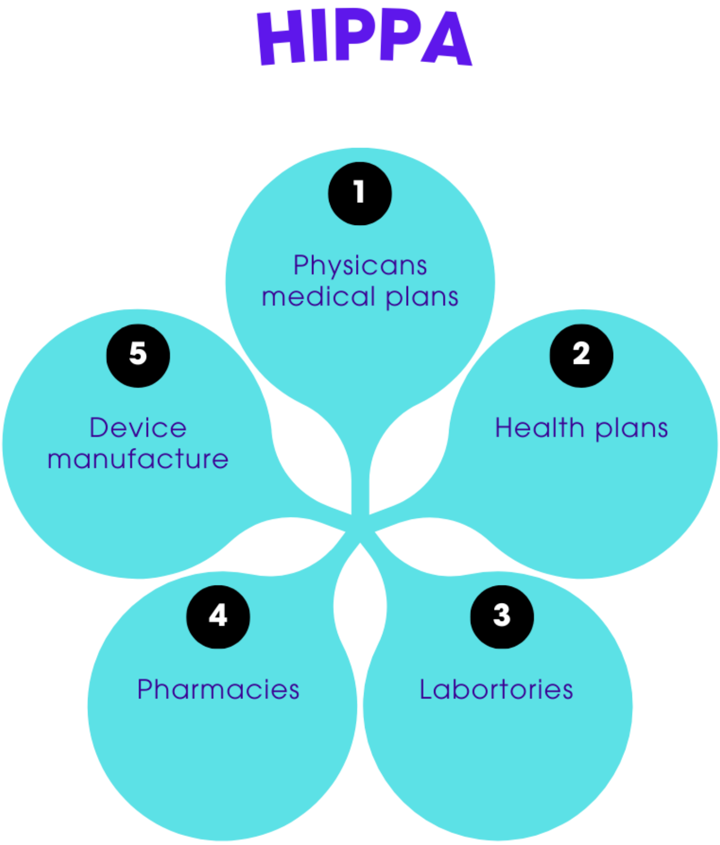

Figure: 2 showing Health Insurance Portability and Accountability

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.81-103

General Data Protection Regulation (GDPR): GDPR means General Data Protection Regulation which is regulation that was development by the European Union for protection of data of people. HIPAA is more specific to the United States, while GDPR is all-encompassing because if an organization is situated anywhere in the globe processing any personal information concerning EU citizens they have to adhere to GDPR. GDPR stands more important in case of AI use cases in healthcare because the restrictions set to data privacy, transparency and accountability were made even stricter by GDPR [29].

For AI in healthcare, GDPR outlines several key principles related to data security, including:

Data Minimization: The applicability of AI systems in the healthcare field should ensure that for this purpose, data is collected and processed only and not more details on the individuals get collected and/or used [30].

Transparency: Patients should be informed how they will be dealt with in an AI system, where their data will be stored, and about the risks of decision-making in such environment.

Consent: Patients have to give er Shawn permission to use their data in AI and the latter also has the right to withdraw that permission at any given time [31].

Right to Explanation: However, Europeans get to benefit from an AI legal construct known as the right to explanation under GDPR where in it is entitled to ask the AI for an explanation of the decision arrived at in case the decision can have a serious impact on the health of an individual. These regulations apply to the AI systems in healthcare where data is collected highly sensitized so as to respect patients’ rights. For the GDPR’s security aspect, developers also have to integrate sufficient measures into the data protection like encryption, anonymization, the control of access and others [32].

National Institute of Standards and Technology (NIST): For instance in the United States the National Institute of Standards and Technology often known as NIST provides guides on how Information system in health care can be protected. To the best of the author’s knowledge, NIST’s Cybersecurity Framework (CSF) offers practice oriented navigation of managing and mitigating cybersecurity risks in form of practices. NIST is not necessarily about putting AI into the healthcare context, but many of the rules that can be applied to healthcare can be applied to an artificial intelligence in the healthcare facility. NIST best practices contain components on risk management, monitoring and system control [33]. The framework encourages healthcare organizations to develop a comprehensive cybersecurity strategy that includes:

Risk Assessment: In this regard, one has to come up with potential vulnerabilities that AI healthcare systems might have: issues with adversarial attacks or a data leak.

Access Control: Reducing the amount of people that have direct patient data access controlling the AI tools that have patient data access [34].

International Standards Organization (ISO): The International Organization for Standardization commonly acronymic as ISO is an independent international organization that provides standards for various sector including health care. There is also another necessary set of directives of the International Organization for Standardization to emphasize that was demonstrated above, namely – ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements. This standard does require the concept of Information Security Management System- ISMS to be implemented in healthcare organizations to safe-guard their health data; the AI-healthcare data inclusive [35].

Implementing Security Controls: This means that it involves developing measures that protect AI Systems; protecting AI systems from intrusions, protection from hacking into the systems among others.

Employee Training: Describing privacy and security of health care personnel and developers of Artificial Intelligence, state laws on Data Privacy and the need to safeguard patient information.

Monitoring and Auditing: By default, periodically check any of the implemented systems that were discussed in this paper to ensure that none of these risks are integrated into the AI and, if any, categorically exclude them [36].

In addition, ISO/ IEC 27701 extends the implementation of data privacy management, which could be also relevant to most of the AI systems in HC dealing with personal data. AI governing polices and standards assist in keeping the healthcare use of AI to be secure and private, safe and ethical. While HIPAA and GDPR rules outline the do and don'ts of the data, the information security guidelines from NIST and ISO provide an insight into how risk on the cyber frontier may be managed. These regulations are paramount especially when handling the security problems associated with AI use especially when health information is involved thus needs to be protected for AI HC systems to operate securely [37]. More especially, to ensure that these technologies are useful to society, frequent interaction between regulators and the healthcare stake holders together with the developers of the AI technologies will be necessary in developing and implementing this guideline and any other related guidelines as they are being developed in the future.

MEASURES OF PROTECTING AI IN HEALTHCARE

This paper focuses on the specification of security requirements for intelligent health systems where use of Artificial Intelligence (AI) in health care has increased significantly and is therefore very important to meet security needs to protect the safety, privacy of patients and practice of the medical practitioners involved. The challenges of cyber security are even more relevant to the use of AI in healthcare, as not only the questions of data protection are at stake here, but the very vulnerabilities of AI algorithms themselves prove that the protection of the data is a vastly multi-factorial issue [38]. In this section, measures for improving the security of AI in healthcare will be described in detail under the heading of data security of AI model, controlling the access to healthcare's AI, monitoring and multi-stakeholder collaboration.

Robust Data Protection and Privacy Measures: The first level of protection of AI systems in healthcare is privacy security. The problem is that patient health data is worth something, and it is vulnerable to hackers 24/7. The first of these is in the protection of data as it is underway in transit and when it is at rest. Encryption also deals with leakage in that even if the data is intercepted it will not be understood by any other person other than the person or organization that it was coded for. As important as data identification is data anonymization and de-identification as another way of safeguarding data of individuals. Many a time, AI systems need datasets, used for training or for making predictions. Still, users intend to apply such standards as HIPAA or GDPR to the developed datasets, and to fulfil them, the data has to be de-identified as PII data cannot be used [39]. Erasure of names reduces privacy infringement especially when big data is licensed for model refinement or by different organizations or used by researchers for analysis. Last but not least, Data minimization principle should be adopted by the healthcare organizations and the data on the patient should only be processed where the latter is necessary for the particular AI tasks. This reduces instances of over reporting of information and compliance to the available privacy laws. Another form of ensuring that the systems used are accessing the right data is through auditing of the AI systems and data access too in a bid of avoiding on any probable risks [40].

Securing AI Models and Algorithms: As the amount of utilization of the AI models, especially the ML and the DL methods, augments they become at risk of many forms of security attacks including the adversarial and data poisoning attacks. Namely adversarial attacks make changes to input data to fool an AI system while data poisoning postures involves introducing malicious data inputs into training data sets in order to compromise the outcomes of a given model. In validation and verification, preventive measures to protect the AI models require integration in the following ways. Implementation of any AI system in healthcare should ensure that the models are inherently tested for adversarial robustness [41]. This is because techniques like adversarial training, in which models are trained with data that has been deliberately tweaked to try to trick it, are all known to work for enhancing robustness. This can be eliminated by frequently using the new training data to retrain the model, and so reduce the impact of data poisoning. Another approach is the model explain ability and transparency. This is because by making the models explain your own they also become understandable for healthcare professionals, and any problems that AI might have like bias can easily be unveiled. If the healthcare providers understand why that particular option has been made then they will know where exactly the model is flawed and can make a follow-up action to put in place security measures & enhance corporate credibility of the AI [42].

Access Control and Authentication: Other parameter that has to be managed properly in healthcare context is access control. AI systems can also require information about patients, therefore, patient data must be controlled for the most necessary. It is also possible to set up the RBAC as of healthcare providers, this would enable them to have some kinds of access to datasets or engage with the help of AI automation only if the provider is authenticated. MFA or 2FA demands the users to verify at least two forms of ID; perhaps a password and a fingerprint scan–before interacting with AI or accessing patient's records [43]. MFA significantly reduces identity threat and even more so when the password has been compromised. To continue from where the organizations providing access control to healthcare organizations are, it is important that the organizations adopt the least privilege principles which grants users the minimum rights to perform their tasks. This will rule out instances where many people come across massive data and destroy it by passing it on to people with negative intent as regards the public [44].

Continuous Monitoring and Threat Detection: The uses of AI are nominal hence always making the AI systems repeated and very sensitive to threats in regard to cybersecurity attack. The healthcare providers are always on the lookout for audit trails that appear odd in terms of activity, in this case, activities that the AI model is not authorized to perform is detected. These tools can scan system logs, networks and users' activities to attempt to discern intrinsic formula of an attack. Machine learning models for instance, can be trained for behavior detection of a kind that suggest threats such as ransom ware or phishing. But every healthcare organization should have an incident response plan that describe the manner in which an organization is expected to act, how to handle it and even how to recover from a particular incident. These plans should be subjected to annual simulations with actual and other tabletop exercises to determine that the execution of different breaches or systems disruption can easily be resolved. Like penetration testing, constant vulnerability check also ensure that agreements to counter possible flaws in the AI infrastructure are made in advance without being leveraged [45].

Collaboration between Stakeholders: It therefore means that implementing security to AI in healthcare needs an intensive cooperation between healthcare entities such as the healthcare service givers, AI technology developers, terms and conditions providers and computer security personnel.

These stakeholders have to work together with those who are creating AI so that security is an inherent characteristic of any AI created models. Similarly, cybersecurity consultants can spend their time and effort to explain how to mitigate possible risks for threats related to the AI systems as well as its supports [46]. Therefore, both the industry and government legislators stay involved as they continue to advise firms and other organizations in the get out, standards, and best practices regarding information security in developing AI systems Concerning that, healthcare stakeholders and AI developers should pay attention to such the points of cybersecurity law as HIPAA, GDPR, NIST, and others to take into consideration all the legal and ethical issues while dealing with artificial intelligence [47].

Education and Training for Healthcare Providers: As from the statistics taken recently one of the key factors contributing to cyber threats is human element. This is because it is necessary to guarantee that health adoption is not a subject to cyber threats concerning the use of Artificial Intelligence, while HC professionals should learn what threats are possible and how to avoid them. Medical care workers should be able to understand what precisely AI tools are safe to use, how be safe from phishing scams, and how patient information should not be communicated. Random training sessions/meetings and seminars or awareness sessions with occasional workshops can help healthcare practitioners on new trends of cybersecurity risks and the precaution to be taken. It therefore brings about the proactive security first culture within the staff to an extent that everyone within the organization has interest in the security of information [48].

To protect AI in the health care setting the following components are important: privacy and data protection, model security, access control, continuous monitoring, and joint responsibility. In light of these recommendations, healthcare organizations shall be in a position to protect the patient data, protect the AI system and endorse the application of Artificial Intelligence healthcare technologies. All of these will be instrumental in defining the future of healthcare as AI becomes a more and more highlighted area within the healthcare sector [49].

AI IN HEALTHCARE CYBERSECURITY – FUTURE DIRECTIONS AND TRENDS

The subject of this paper is the interaction between the healthcare sector and Artificial Intelligence, it is noted that thanks to the use of AI technologies, it is also actively used in diagnostic tools, in developing treatment plans, in administrative processes, as well as in individual approaches to patients. Though such progresses have the potentiality of offering a better patient care and enhanced delivery of healthcare, they also pose critical security issues. As the dependency on AI systems rises, protecting those technologies becomes very important [50]. The future development of AI healthcare cybersecurity will therefore involve progress in technology, codified legislation as well as other tactics deployed into the market with the intention of providing for other risks. In this section, mechanical properties, potential development and advancement in the same as well as other relevant topics involving AI in healthcare cybersecurity has been considered are highlighted and discussed based on the future prospects and trends [51].

Emergence of AI-Driven Cybersecurity Solutions: With AI now contributing to the delivery of healthcare more than ever before, cybersecurity threats are also going to be addressed using it. AI related cybersecurity solutions can function as a means to shift the thinking and typical patterns in cyberspace by which healthcare systems can identify and combat various cyber threats. These systems are capable of considering large amounts of data in real time whereas, in the process, such patterns and behavior may hint at a cyber-attack. Automating threat detection is especially easy and efficient with machine learning algorithms in an AI integrated healthcare system. These algorithms can be used to learn emerging threats, including ransom ware or phishing attempts as they identify negative patterns in the operations of networks, devices, and models that are AI driven [52]. Moreover, it can be employed to detect prospective risks to patients' information to allow healthcare organizations to circumvent risks without complications before they emerge. AI Security solutions will continue to evolve moving towards predictive analytics and automated decision making with little human interjection molding threat detection. This will assist healthcare organizations be able to deal with risks in a very short time, especially in environments, which are complicated, and constantly evolving, then conventional security mechanisms are ineffective [53].

Enhanced Privacy-Preserving AI Models: As AI finds more applications in the healthcare system, the desire for information anonymizing strategies to protect patient information also grows. That is why as healthcare systems interact more and rely upon AI-generated insights from different data sources, data protection will be essential. There are recent privacy-preserving AI techniques like the federated learning and holomorphic encryption that hold promise for the future of AI healthcare cybersecurity. Federated learning enables AI models to be trained across decentralized devices including health wearables, and mobile applications without compromising patient data. In this approach, therefore, only updates on the model are passed to the other part instead of transmitting the actual patients' data [54].

This method ensures that data identified as sensitive does not have to be shared within a micro service but still allows for AI model building as a team. Holomorphic encryption is another enabling technology from which AI algorithms are capable of performing computation on encrypted data without necessarily decrypting it first. This encryption method allows healthcare organizations to use an otherwise sensitive data for analytical purposes due to the protection of patents' rights from the

ISSN : 3079-6830
Volume 1, Number 2, February, 2025
https://doi.org/10.70445/giaic.1.2.2025.81-103

time when the data enters the analysis phase [55]. These enhanced privacy-preserving methods are expected to grow in popularity and solve the cybersecurity and/or the issue of compliance arising out of the application of AI in the health care sector.

AI-Enhanced Regulatory Compliance: With more innovations in AI is being implemented in healthcare industry, so its laws and policies will also change with time to meet new cybersecurity challenges of patients data. AI will continue to be applied to the enforcement of the HIPAA and GDPR with such regulatory bodies being the main consumers of such capabilities. Customized applications of AFS in healthcare systems can help to homogenize systems, audit them for compliance with the set standards or point out deficiencies. For example, in patients record, an AI system could monitor who is getting access to the data, whether the policies being implemented about who should be allowed to see the patient data are being adhered to, and whether there are any signs of violation [56]. This would help minimize the load upon healthcare providers and make it easier to navigate, understand and meet current and future compliance standards. Secondly, AI can help to track the security of AI models themselves to guarantee it is impossible to expose them to adversarial attacks or other risks that may violate patient's rights or compromise their health. AI can help the healthcare providers in regard to coping with the new rising cybersecurity regulations by providing insights into the kind of regulations that are likely to be developed. This approach will be crucial when the legal and regulatory frameworks for the deployment of AI grow more convoluted [57].

AI Security in IoT-Enabled Healthcare Systems: AI has become closely related to the Internet of Things (IoT) in increasingly being applied in healthcare. Smart insulin pumps and administrated pacemakers, tele monitoring devices are few examples of IoT controlled medical devices which offer important real-time data for patients and doctors. However, such devices have enormous cybersecurity vulnerabilities since they are pathways through which cybercriminals launch attacks. The increasing number of IoT devices will make it more necessary in the future to safeguard IoT devices in healthcare settings. AI will be useful in promoting the security of these IoT devices. In this case, the AI algorithms can be applied to follow the activity of IoT devices and report any hikes in activity level, which shows that there can be problems with security [58]. AI can enhance the security of device authentication, which means that only the right people and programs will be able to concurrently interact with the involved medical devices. As the advanced AI based threat identification tools are being built, healthcare sector will become more capable to handle the increasing threat associated with the IoT based healthcare systems [59].

Integration of Block chain for Healthcare Data Security: It is now on the block chain technology as a solution to most of the security challenges in the health sector. Due to its decentralized and ability to produce a record that cannot be altered block chain seems to be a promising tool especially in patient's data security. In the context of AI extended to healthcare, block chain could be used to offer an added layer of security in managing records on patient data interaction tracking. For instance, block chain can be deployed to securely store the training data for AI models so that the data cannot be changed. Through block chain, all the relationships with the data of the patients can be checked with a mere point and click and therefore it will be easy for the health care organization to show that they have complied with the set regulations and laws [60].

The future of AI healthcare cybersecurity will be determined by the current and future development in privacy preserving techniques, artificial intelligence cybersecurity tools, policy making practices, and ethicist thoughts. When healthcare is going deeper into AI, there will be a need to establish best practices to safeguard AI, Patients' information and the public's trust in It [61]. Harnessing the current future technologies like federated learning, homomorphic encryption, block chain the healthcare service provider organizations will resolve the problem of cybersecurity threaten to AI driven system while moving on in the process of of healthcare evolution. Information from this study therefore implies that the extensive adoption of safe and secure AI in the management of health care information and sector will require collective effort from IT developers, health care organizations, regulatory bodies and cyber security experts.

CONCLUSION

In the recent past, there has been an unprecedented adoption of AI in healthcare system with improved results for care, work flow and practice. However, in connection with these successes, there are threats that are inherent only in them but must be addressed to guarantee patients' safety as well as their data privacy and data integrity. The cases reviewed in this paper suggested that the protection of AI technologies in healthcare organizations is a complex issue. The laws such as HIPAA and GDPR, are essential to observe while incorporating secure artificial intelligence in healthcare facilities are; The NIST and ISO frameworks also come in handy when pushing for secure AI in healthcare facilities.

Such regulations are instrumental in ensuring that both the health care providers and Developers of the AI based systems are at a very high degree of compliance with the International Standards in respect of managing the Patient data, the use of AI systems and managing of the potential cyber risks associated therewith. Other than the above said regulations the common embracive mechanisms to safeguard AI in health care broadly incorporates measures such as data protection via encryption, security of AI models against adversarial attacks and stringent access control mechanisms or proper mechanisms.

AI's healthcare cybersecurity of the future is now trending as emerging technologies. AI based security software tools, dat sanitizing methods such as federated learning as well as homomorphic encryption and block chain are anticipated to revolutionize the healthcare systems and their efforts to defend artificial Intelligence applications. The themes of xAI and ethic of AI decision making ensure that AI operate with full disclosure and that there is more responsibility on the part of the AI especially in critical issues of health. There is no doubt that with the usage of AI technology in all the healthcare organizations, the user healthcare providers, AI developers, the regulatory bodies, and the cybersecurity specialists will need to synergistically work together to solve new security challenges in order to safe guard the patient's data. They recommended that integration of AI into a healthcare system should be done with extreme security to avoid replicating itself as a source through which hackers gain access to patient information.

The foundation for developing the future of AI healthcare cybersecurity will depend on the correct integration of a technological emphasis, legal obligations, perpetual awareness, and moral standards. Personal interests are best served by Protecting AI systems and putting the use of those systems in privacy, security measures, and ethical forms to realize the full potential of AI in health care. It is worthy to remind that as these AI technologies further improve so should the policies and precautions upon which they are founded – in order to keep the increasingly digitalized healthcare sector always novel and safe.

REFERENCES

[1]. L. Coventry, D. Branley, Cybersecurity in healthcare: a narrative review of trends, threats, and ways forward, Maturitas 113 (2018) 48–52.

[2]. D. Branley-Bell, L. Coventry, E. Sillence, S. Magalini, P. Mari, A. Magkanaraki, K. Anastasopoulou, Your hospital needs you: eliciting positive cybersecurity behaviours from healthcare staff, Ann. Dis. Risk Sci.: ADRS 3 (1) (2020

[3]. S.T. Argaw, J.R. Troncoso-Pastoriza, D. Lacey, M.V. Florin, F. Calcavecchia, D. Anderson, A. Flahault, and Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks, BMC Med. Inform. Decis. Mak. 20 (1) (2020) 1–10.

[4]. S.J. Choi, M.E. Johnson, The relationship between cybersecurity ratings and the risk of hospital data breaches, J. Am. Med. Inform. Assoc. 28 (10) (2021) 2085–2092.

[5]. A.J. Askar, Healthcare management system and cybersecurity, Int. J. Recent Technol. Eng. (2019) 237–248.

[6]. M. Pears, J. Henderson, S.T. Konstantinidis, Repurposing case-based learning to a conversational agent for healthcare cybersecurity, in: Public Health and Informatics, IOS

Press, 2021, pp. 1066–1070. 10 M. Javaid, A. Haleem, R.P. Singh et al. Cyber Security and Applications 1 (2023) 100016

[7]. M. Javaid, A. Haleem, R.P. Singh, R. Suman, Dentistry 4.0 technologies applications for dentistry during COVID-19 pandemic, Sustain. Oper. Comput. 2 (2021) 87–96.

[8]. Abid N. Advancements and Best Practices in Data Loss Prevention: A Comprehensive Review. Global Journal of Universal Studies. 1(1):190-225.

[9]. Okafor CM, Kolade A, Onunka T, Daraojimba C, Eyo-Udo NL, Onunka O, Omotosho A. Mitigating cybersecurity risks in the US healthcare sector. International Journal of Research and Scientific Innovation (IJRSI). 2023 Oct; 10(9):177-93.

[10]. Zainab H, Khan AR, Khan MI, Arif A. Innovative AI Solutions for Mental Health: Bridging Detection and Therapy. Global Journal of Emerging AI and Computing. 2025 Jan 24; 1(1):51-8.

[11]. Khan R, Zainab H, Khan AH, Hussain HK. Advances in Predictive Modeling: The Role of Artificial Intelligence in Monitoring Blood Lactate Levels Post-Cardiac Surgery. International Journal of Multidisciplinary Sciences and Arts. 2024; 3(4):140-51.

[12]. Jack W. Cybersecurity Threats in Healthcare IT: Risk Mitigation Strategies for Enhanced Data Privacy and Resilience in Industry 4.0.

[13]. Zainab H, Khan AR, Khan MI, Arif A. Ethical Considerations and Data Privacy Challenges in AI-Powered Healthcare Solutions for Cancer and Cardiovascular Diseases. Global Trends in Science and Technology. 2025 Jan 26; 1(1):63-74.

[14]. Asif SM. Simulation of A Two Link Planar Anthropomorphic Manipulator. BULLET: Jurnal Multidisiplin Ilmu.;1(03):539-52.

[15]. Achuthan K, Ramanathan S, Srinivas S, Raman R. Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions. Frontiers in Big Data. 2024 Dec 5; 7:1497535.

[16]. Valli LN. Under the titles for Risk Assessment, Pricing, and Claims Management, write Modern Analytics. Global Journal of Universal Studies.;1(1):132-51.

[17]. Choudhary V, Patel K, Niaz M, Panwala M, Mehta A, Choudhary K. Risk Management Strategies for Biotech Startups: A Comprehensive Framework for Early-Stage Projects. InRecent Trends In Engineering and Science for Resource Optimization and Sustainable Development 2024 (pp. 448-456). CRC Press.

[18]. Saraswat JK, Choudhari S. Integrating big data and cloud computing into the existing system and performance impact: A case study in manufacturing. Technological Forecasting and

Social Change 2025; 210:123883. https://doi.org/https://doi.org/10.1016/j.techfore.2024.123883

[19]. Narayanan D. NAVIGATING DATA PRIVACY AND CYBERSECURITY CHALLENGES IN HEALTH INFORMATION TECHNOLOGY. Technology (IJRCAIT). 2024 Jul;7(2).

[20]. A.J. Coronado, T.L. Wong, Healthcare cybersecurity risk management: keys to an effective plan, Biomed. Instrum. Technol. 48 (s1) (2014) 26–30.

[21]. C. Abraham, D. Chatterjee, R.R. Sims, Muddling through cybersecurity: insights from the US healthcare industry, Bus. Horiz. 62 (4) (2019) 539–548.

[22]. Strielkina, O. Illiashenko, M. Zhydenko, D. Uzun, Cybersecurity of healthcare IoT-based systems: regulation and case-oriented assessment, in: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), IEEE, 2018, pp. 67–73

[23]. C.S. Kruse, B. Frederick, T. Jacobson, D.K. Monticone, Cybersecurity in healthcare: a systematic review of modern threats and trends, Technol. Health Care 25 (1) (2017) 1–10

[24]. G. Martin, P. Martin, C. Hankin, A. Darzi, J. Kinross, Cybersecurity and healthcare: how safe are we? BMJ (2017) 358.

[25]. Neoaz N, Amin MH. Leveraging Artificial Intelligence for Early Lung Cancer Detection through Advanced Imaging Analysis. Global Journal of Computer Sciences and Artificial Intelligence. 2025 Jan 26; 1(1):55-65.

[26]. Valli LN, Narayanan S, Chelladurai K. Applications of AI Operations in the Management and Decision-Making of Supply Chain Performance. SPAST Reports. 2024 Sep 20;1(8).

[27]. Mehta A, Sambre T, Dayaramani R. ADVANCED ANALYTICAL TECHNIQUES FOR POST-TRANSLATIONAL MODIFICATIONS AND DISULFIDE LINKAGES IN BIOSIMILARS.

[28]. Valli LN. Predictive Analytics Applications for Risk Mitigation across Industries; A review. BULLET: Jurnal Multidisiplin Ilmu. 2024; 3(4):542-53.

[29]. Amin MH. AI in Motion: Securing the Future of Healthcare and Mobility through Cybersecurity. Asian Journal of Engineering, Social and Health. 2025 Jan 29; 4(1):176-92.

[30]. Rasool S, Husnain A, Saeed A, Gill AY, Hussain HK. Harnessing predictive power: exploring the crucial role of machine learning in early disease detection. JURIHUM: Jurnal Inovasi dan Humaniora. 2023 Aug 19; 1(2):302-15.

[31]. Abid N. Enhanced IoT Network Security with Machine Learning Techniques for Anomaly Detection and Classification. Int. J. Curr. Eng. Technol. 2023; 13(6):536-44.

[32]. Bharadiya JP. AI-driven security: how machine learning will shape the future of cybersecurity and web 3.0. American Journal of Neural Networks and Applications. 2023 Jun;9(1):1-7.

[33]. Zainab H, Khan MI, Arif A, Khan AR. Deep Learning in Precision Nutrition: Tailoring Diet Plans Based on Genetic and Microbiome Data. Global Journal of Computer Sciences and Artificial Intelligence. 2025 Jan 25; 1(1):31-42.

[34]. Alanezi M, AL-Azzawi RM. AI-Powered Cyber Threats: A Systematic Review. Mesopotamian Journal of CyberSecurity. 2024 Dec 6;4(3):166-88.

[35]. Turransky, M.H. Amini, Artificial intelligence and cybersecurity: tale of healthcare applications, Cyberphys. Smart Cities Infrastruct.: Optim. Oper. Intell. Decis. Mak. (2022) 1–11.

[36]. K. Anastasopoulou, P. Mari, A. Magkanaraki, E.G. Spanakis, M. Merialdo, V. Sakkalis, S. Magalini, Public and private healthcare organisations: a socio-technical model for identifying cybersecurity aspects, in: Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance, 2020, pp. 168–175.

[37]. E. Tomaiko, M.S. Zawaneh, Cybersecurity threats to cardiac implantable devices: room for improvement, Curr. Opin. Cardiol. 36 (1) (2021) 1–4.

[38]. M. Pears, S.T. Konstantinidis, Cybersecurity training in the healthcare workforce–utilization of the ADDIE model, in: 2021 IEEE Global Engineering Education Conference (EDUCON), IEEE, 2021, pp. 1674–1681.

[39]. Nasir S, Zainab H, Hussain HK. Artificial-Intelligence Aerodynamics for Efficient Energy Systems: The Focus on Wind Turbines. BULLET: Jurnal Multidisiplin Ilmu. 2024;3(5):648-59.

[40]. Malik FS, Sahibzada S, Nasir S, Lodhi SK. Machine Learning-Enhanced Turbulence Prediction and Flow Optimization for Advanced Aerodynamic Design in High-Speed Regimes. European Journal of Science, Innovation and Technology. 2024;4(6):39-46.

[41]. Asif SM. Investigation of Elementary Vibrations: Derivation, Experimental Analysis, and Key Findings. BULLET: Jurnal Multidisiplin Ilmu.;3(6):744-53.

[42]. Husnain A, Rasool S, Saeed A, Hussain HK. Revolutionizing pharmaceutical research: harnessing machine learning for a paradigm shift in drug discovery. International Journal of Multidisciplinary Sciences and Arts. 2023 Sep 27;2(2):149-57.

[43]. 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.

[44]. Asif SM. Analysis of Key Parameters and Mesh Optimization in Computational Fluid Dynamics Using Open FOAM. BULLET: Jurnal Multidisiplin Ilmu.;1(2):592455.

[45]. Abid N. Securing Financial Systems with Block chain: A Comprehensive Review of Block chainand Cybersecurity Practices. International Journal of Multidisciplinary Sciences and Arts. 3(4):193-205.

[46]. Gill AY, Saeed A, Rasool S, Husnain A, and Hussain HK. Revolutionizing Healthcare: How Machine Learning is Transforming Patient Diagnoses-a Comprehensive Review of AI's Impact on Medical Diagnosis. Journal of World Science. 2023 Oct 27;2(10):1638-52.

[47]. Khan M, Sherani AM. Leveraging AI for Real-Time Depression Detection in Healthcare Systems; a Systematic Review. Global Journal of Emerging AI and Computing. 2025 Jan 21; 1(1):25-33.

[48]. Mehta A. Implementation of artificial intelligence in biotechnology for rapid drug discovery and enabling personalized treatment through vaccines and therapeutic products. BULLET: Jurnal Multidisiplin Ilmu. 2022 Feb 9; 1(01):76-86.

[49]. Abid N. Securing Financial Systems with Block chain: A Comprehensive Review of Block chainand Cybersecurity Practices. International Journal of Multidisciplinary Sciences and Arts. 3(4):193-205.

[50]. H. Alami, M.P. Gagnon, M.A.A. Ahmed, J.P. Fortin, Digital health: cybersecurity is a value creation lever, not only a source of expenditure, Health Policy Technol. 8 (4) (2019) 319–321.

[51]. J.A. Chua, C. PMP, Cybersecurity in the healthcare industry, J. Med. Pract. Manag.: MPM 36 (4) (2021) 229–231.

[52]. Nasir S, Javaid MT, Shahid MU, Raza A, Siddiqui W, Salamat S. Applicability of Vortex Lattice Method and its Comparison with High Fidelity Tools. Pakistan Journal of Engineering and Technology. 2021 Mar 29;4(1):207-11.

[53]. F. Gioulekas, E. Stamatiadis, A. Tzikas, K. Gounaris, A. Georgiadou, A. Michalitsi-Psarrou, C. Ntanos, A cybersecurity culture survey targeting healthcare critical infrastructures, Healthcare 10 (2) (2022) 327 MDPI.

[54]. C. Smith, Cybersecurity implications in an interconnected healthcare system, Front. Health Serv. Manage. 35 (1) (2018) 37–40.

[55]. P. Soni, J. Pradhan, A.K. Pal, S.H. Islam, Cybersecurity Attack-resilience Authentication Mechanism for Intelligent Healthcare System, IEEE Trans. Ind. Inf. (2022).

[56]. S.A.E. Hoffman, Cybersecurity threats in healthcare organizations: exposing vulnerabilities in the healthcare information infrastructure, World Libr. (1) (2020) 24.

[57]. Edison G. Cutting-Edge Applications of Artificial Intelligence in Healthcare, Petroleum Fraud Detection, and Innovative Strategies in Cancer Treatment. International Journal of Multidisciplinary Sciences and Arts.;3(4):103-12.

[58]. Asif SM. Investigation of Heat Transfer in Pipes Using Dimensionless Numbers. Global Journal of Universal Studies.;1(2):44-67.

[59]. Amin MH, Neoaz N. Impact of AI Algorithms on Optimizing Radiotherapy for Cancer Patients. Global Journal of Machine Learning and Computing. 2025 Jan 26;1(1):56-65.

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

[61]. Khan AR, Khan MI, Arif A. AI in Surgical Robotics: Advancing Precision and Minimizing Human Error. Global Journal of Computer Sciences and Artificial Intelligence. 2025 Jan 23;1(1):17-30.