International Journal of Social, Humanities and Life Sciences ISSN XXXX-XXXX
Vol. 2, No. 1, 2024, pp. 108-119

Advancing Healthcare Security: The Role of AI, Deep Learning, and Machine Learning in Cybersecurity, Information Access Management, Cardiovascular Devices, Aerodynamics, Chatgpt Integration, and Cancer Medicine

Alexandra Harry

Independent Researcher Washington DC USA

Alaxendraharry37@gmail.com

Abstract

This paper identifies and discusses the role of integrating healthcare technologies, including AI, DL, and the Internet of Medical Things (IoMT). In this paper, AI and the various sub-disciplines are proposed as key to increasing healthcare security, protecting patients' data privacy, and improving access control systems. Secondly, it explores how artificial intelligence is transforming cardiovascular devices through real-time and analysis of patient data that can greatly enhance the result. AI in the field of aerodynamics is also described and its possibility to advance medical devices and technologies for enhanced accuracy and performance is also described. Besides, the paper presents how the AI models such as Chatgpt in helping healthcare workers to provide diagnostics and patient communication and how such models support the development of individual cancer therapy and diagnostics based on targeted research and analytics. Such an approach emphasizes the ability of AI not only to solve the problems in the sphere of healthcare security but also to open new opportunities that relate to various advancements in the spheres of medicine, improvements in patients' conditions and more effective organization of diagnostics and treatment processes.

Key words: *Artificial Intelligence (AI), Deep Learning (DL), Machine Learning (ML), Healthcare Cybersecurity, Information Access Management, Cardiovascular Devices, Predictive Analytics, Aerodynamics in Medicine, Chatgpt in Healthcare, Cancer Medicine.*

1. Introduction

It's among the booming area of development, which has had a great impact on several segments of the economy, the health segment not excluded. The so called digital world has the health-care systems become more useful, both the doctors and patients are more informed, every diseases are diagnosed fast and they are proper channel of attending the patients. But these have outcomes that have also raised the risk of cybercrimes on health care organizations. It has thus become important in the healthcare Institutions because almost all major data such as patient data, financial data and operational data passes through computer systems in these institutions [1]. The above mentioned problems have therefore been eliminated because this paper has been able to determine that management of healthcare cybersecurity is some of the areas that is experiencing positive impact of Artificial Intelligence (AI) technology. AI means reproducing the human brain's abilities using computers. In the case of healthcare, it can on its own pull very large data sets, and analyses them and further identify the most likely future trends; very useful for both the health care practitioners and the security team. For the role of AI for enhancing the cybersecurity of healthcare the following can be held: AI would be able to recognize such threats and even probable attack which would make use of this solution more advantageous as compared to the usual methods [2].

Cybersecurity in healthcare is beyond a simple IT issue of protecting healthcare information from cyber threats it also a patient concern; health organization information security, confidentiality, integrity and accessibility. These new kinds of attacks are said to have new generation of attacks such as the ransom ware, phishing, advanced persistent threats (APTs) and others have added even more of a challenge of fending off a breach in healthcare organizations [3]. The opportunity of Managing one incidence of cyber threats is loss of patient privacy, interrupted delivery of medical care, and deep losses. Therefore, it is canonically for the stakeholders in the healthcare setting and healthcare facilities to maintain the search for new strategies concerning the above-specified security threats [4]. This is why integration of the AI solutions and cybersecurity challenges for healthcare can be stated

as the solution to these questions. In another way, the AI solutions can help the healthcare industry through remotely and automatically identifying the device traffic as they occur on the networks and the activities and the vulnerabilities that can be exploited by the different cybercriminals. Machine learning can also improve threat detectors because it learns other novel threats and creates ability to battle those types of threats that which it has not been trained to recognize [5].

Innovations in AI, DL, and ML over the recent past are consequently changing healthcare, not only in the familiar areas of utilization but in more specific niches. However, one area where AI is seen to be advancing is in the field of cardiovascular devices that uses predictive modeling and evaluation during the actual implementation to make the procedures better. Likewise, changes in aerodynamics are making the form and function of medical devices more efficient and safe for patients. Moreover, Chatgpt and similar AI models are also helpful in diagnosing patients and managing communication with patients, as well as involved in the clinician's decision-making process. In cancer medicine for instance, these technologies are also transforming care, by offering accurate predictions, for developing individualized treatments. Altogether, these innovations are capable of enhancing the Quality of care and equally the safety and availability of Health care systems and the basis for a better health care delivery system [6]. There are issues related to privacy that cannot be ignored, the issue of ethics, and the issue of how biased used models are for AI as well. However larger initiatives are required to create the training as well as resource capacity of the healthcare organizations in which to incorporate the use of AI based systems more. There is another crossroad for creating and enhancement that possibly link between AI, healthcare and cybersecurity. Since healthcare industry is gradually moving to the digital environment, Leaders of the healthcare industry are in a position to use AI to ensure security as well as regulate the access to data that is necessary to improve the outcomes of the patient care and address the consequences of cyber threats [7].

2. Cybersecurity as a field is not only more relevant – but also significantly more relevant in cases of healthcare facilities.

IT security has emerged as one of the most prominent issues in the context of the healthcare industry because of the constant growth in information technology adoption in health care organizations and the rising daily threats against them. This healthcare organization has to complete a number of personal health information (PHI) in scale. This information is rather valuable to the cybercriminals because the majority of them plan on stealing, extorting money, or framing healthcare facilities. Pricing, patient records can be unsafe; health care limited, lives at the risk of ransom wares, phishing, and data theft [8]. And year 2020 was no different, although, the healthcare sector was one of the most impacts with harsh incident targeting hospitals and or health care organizations across the world. They also serve as formation of a negative image to the clients of the organization; fines and legal compensations in addition to the recovery costs that the organization has to incur.

Moreover, cybersecurity in healthcare has less to do with protection of these data from hackers than the systems and devices that are used to provide health services. Hospitals depend on a range of devices like pacemakers and insulin pumps, diagnostic tools that are becoming smarter and more dependent that pose it to cyber threats. About such devices, it shows how they can cause worst patient harm if compromised and why Healthcare needs good cybersecurity which safeguards the patient data and the medical devices. It is also important in tracking the firms that have very stringent polices as would be expected from standard setting laws such as the Health Insurance Portability and Accountability Act (HIPAA) of the United States of America [9]. These regulations can help define high levels of the security of the patient data and moreover, the current healthcare organizations have no adequate cybersecurity programs, described at these rules. The implications observed where the organization is unable to meet the stated and agreed level of compliance include fines further to this it compromises the market image of the organization and in the global market [10].

The prominence of cybersecurity in healthcare is also ushered in such things as growth of cybercrimes in the healthcare setting. Different entities require harmonized interfaces to support their organizational objectives and ambitions; however, the unsafe world today is becoming increasingly populated with attackers targeting the weaker interfaces of linked systems. With the growing utilization of information technology resources in the support of patient care by the healthcare providers these data need to be protected and made confidential, integral and available. In other words, cybersecurity is becoming increasingly important to healthcare than it was before technology and the Internet came into the scene. As the sector slowly integrates such systems, so will the threats endure high levels of risk [11]. Due to this reason, healthcare organizations ought to cultivate enduring cybersecurity solutions that will enable them protect the patient's valued details, maintain functional the crucial medical equipment's, and perform as dictated by the actionable guidelines. The failure to do so will cost many patients their lives as well as many healthcare providers their lives as they get infections from patients.

3. Artificial Intelligence in Cybersecurity: Healthcare Applications

AI makes it possible to take a proper approach towards the cyber threats in healthcare section as the protection of the data is critical. Aggravation of the threats cybersecurity facing increases especially in healthcare systems, as the kind of data that is stored in them and due, often poorly informed, security systems, healthcare organizations are now beginning to consider the use of AI cybersecurity. Machine learning and natural language processing are most useful tools used in a health organization to address cyber threats, their management or prevention. Most likely, the most significant benefit that arose from using AI in healthcare cybersecurity is threat identification without human intervention [12]. Many security technologies of the past have relied solely on the rule-based system in their security management implying that they are ineffective at identifying new forms of threats. However, the AI-based systems are based on the use of machine learning algorithms that continue to learn in relation to a large volume of data. Some of these systems comes with the opportunity to do the traffic analyzing and also the behavior of such system and users with the aim of letting out some alert of the threats. For instance, AI may be applied in identifying an anomaly in traffic pattern, for instance a user attempting to login into databases in the department he or she does not belong or identifying changes in the behavior of medical equipment that are suggestive of a breach [13].

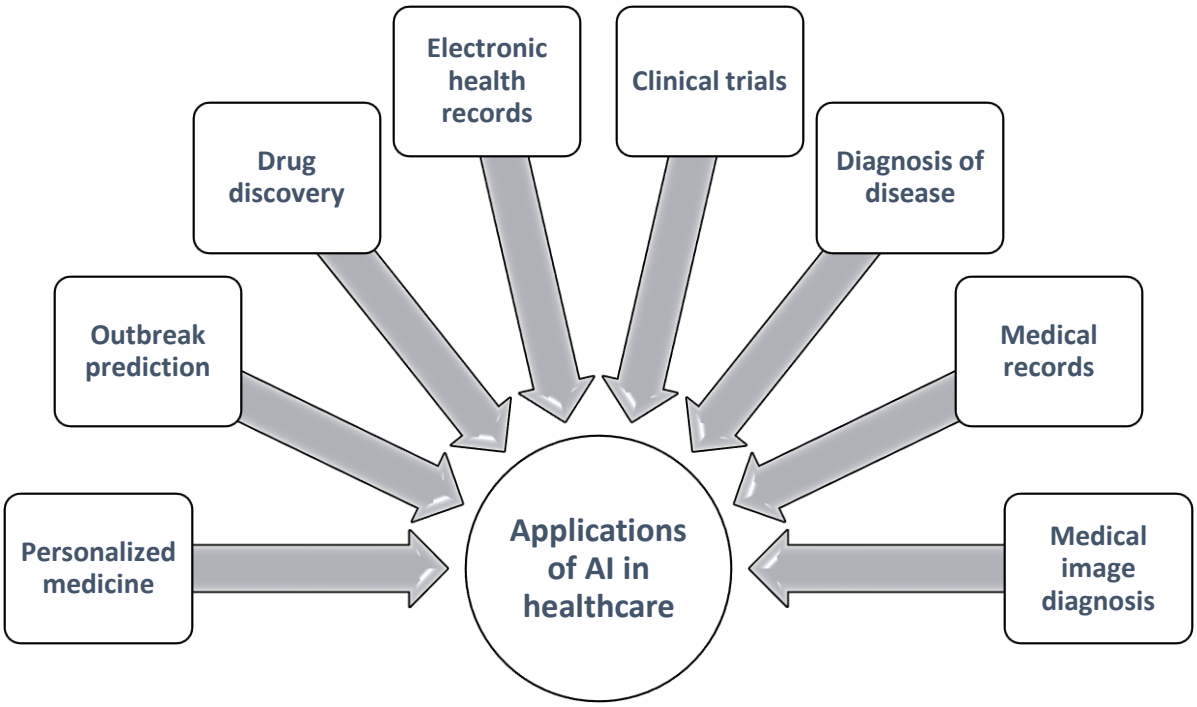

Figure: 1 showing applications of AI in healthcare

Another advantage of applying AI in healthcare cybersecurity is prediction. Using and AI can very much identify most likely vulnerabilities and points of entry of an attacker in entering a system. Quantitative methods, addressed by artificial intelligence solutions, can enable to approximate the degrees of threats originating on the system level, at the user level and from an outside prevailing an outline of priorities of security measures or preventive actions [14]. This allows the healthcare organizations in particular to prevent the chance of these being targeted and being one step ahead of the hackers. By doing so, the AI based cybersecurity solutions are also improving the option of increasing response and recovery from cyber related threats. AI is most particularly prominent in quickly identifying the infected systems in the eventuality of a cyber-attack than the effort of forming an organized response team. For example, AI be able to halt the operation of the compromised systems, control any process in the network and restore the systems to the state they were in prior to the break in and thereby reduce the impact of the break in on the ability of the organization in relation to system downtime loss [15]. Today AI is employed in enhancing security on health care devices and the IoT equipment. These are smart infusion pumps and wearable health monitor, and pacemakers because these devices are connected. It also by the help of these artificial intelligent algorithms it will be easy to monitor the characteristics of these devices and any abnormality is quickly detected and necessary measures taken such as vulnerability testing and making necessary preventive measures against cyber-attacks that can affect the lives of patents or have an impact on the functionality of health care services [16].

AI is also used in improving the safety operation in that routine security procedures are computerized including patching, vulnerability assessment and log review among others. It also unloads the burden off security teams as it ensures the minimum satisfactory cyber security standard is adopted pan-organizational. AI is gradually becoming one of the healthcare organization's critical resources when it comes to patient confidentiality and the regulation of medical devices. By using AI for threat identification, vulnerability assessment, and auto-generation of responses to threat events, the healthcare institution can enhance its security and 'readiness' and can address the increasingly growing threats defined by a world that is becoming increasingly 'sophisticated' in producing cyber threats [17].

4. Use of AI in Advancing the Data Privacy and Compliance in the Healthcare Industries

As to specific details of patient a healthcare organizations or a clinic must use people that will make sure data security as well as high privacy standards. With the increasing amount of health related data being generated and stored in EHRs, medical devices, and telehealth applications, healthcare entities feel increasing pressure to protect this information from data breaches or cyber-attacks. Today, Artificial Intelligence (AI) has an important role in enhancement of the data privacy, and legal standards including Health Insurance Portability and Accountability Act (HIPAA) for the USA, General Data Protection Regulation (GDPR) for Europe, and other countries. In regard to data privacy AI another area in which AI gains leverage, mainly because this system recognizes and efficiently manages HC info access [18]. In brief, using AI, the information about a patient can be controlled as to who is actually entitle to view the data on the patient; if there is any irregularity of the data being accessed, then it will alert the administrators to the said situation. For instance, machine learning processes can predict when a healthcare professional is interacting with information he or she wouldn't regularly come across or when a third party system interacts with patient records more than is typical. They can also continue to satisfy the role-based access control and at the same time keep private the patient id completely allowing only the right parties to share the particular data easily [19].

AI is also instrumental in the task of protecting data identities in the course of transacting the data and keeping it as well. It will also be able to read and encrypt messages that should not be transferred or stored, and if it is intercepted all the recipients will see is garbage inputs. Also, AI can assist in leakage or even unauthorized disclosure of the personally identifiable information (PII) in big data by defining the points that need protection and thus, prevent accidental input or Nona compliance with the required regulations [20]. Reporting and auditing is another wonderful avenue where artificial intelligence has a lot of possibilities in the healthcare compliance. Regulatory standards require an organization implementing an information system to prove legal privacy and security of data are being sustained. There is hence a possibility to monitor compliance using AI and obtain logs as well as reports indicating how patient information is being accessed, disclosed and protected. This in turns frees the human staff and gives the health care providers ample time to show that indeed, they have complied with the laws [21].

AI-based systems also do not cease to improve the mechanisms of patient consent. To match patient's preference on their medical data and consent history from various media and services, AI can support healthcare organize to get, store, and respect patient consent properly. This is particularly important where there is interaction with the patient and where information is shared with other healthcare organizations or with outside research organizations [22]. This is because AI has a positive role in data privacy and compliance because it facilitates monitoring of Data Access rights', enhances Data Security and makes compliance processes automatable apart from facilitating patient rights enforcement. The analysis suggests that the implementation of AI technologies enable healthcare organizations to manage the risks linked with data breaches; boost patient satisfaction; and adhere to the prevailing industry standards. As seen, due to global threats, and new generation privacy threats, making AI a fundamental part of sensitive health care information protection, it is expected that the use of AI will continue in the future [23].

5. AI in writing spending Healthcare information.

Maintaining and, in even larger measure, gaining control over access is a focal issue due to … the patient's data sensitivity and the availability of numerous rules regarding this information. In the future as health care systems keep on integrating information technology it has the major function of ensuring that the access to medical records and other vital information is only provided to those with the right of access. Artificial intelligence (AI) solutions boosting information management and security in the healthcare organizations are on the rise with other bonuses like, the feature is more efficient and can scale. It is obvious to everyone that access control is one of the primary factors that need to be considered in the process of ensuring healthcare cybersecurity [24]. There are conventional practices like the overloading of the username and password, generalized measures which are not so difficult to be tricked or corrupted by individuals. AI makes access control better through integration of improved and advanced

feature such as the identity recognition in faces, fingerprint as well as eye scan, behavior analysis and contextual or scene access [25].

AI systems for biometrics is likely to be deployed in more applications in order to enhance the security, and evolution of the process of finding and authenticating the real users. For instance, the algorithms enable a matching of face or fingerprints of the person to the identity of the healthcare worker as well as enable the workers to have particular bits of information or change records regarding the particular patient. Those systems can be used in the situations where fast but secure access is needed; for example ER or ICU where decision must be made urgently. AI can enhance RBAC because AI is able to monitor user's behavior and determine appropriate level of access based on users' roles, previous accesses, and etc [26]. For instance, AI systems can determine the frequency at which the healthcare provider violates the patient data most appropriate for hi or her department or station or expose invasions that are prohibited by the system. The dynamic and context-based access approach proves to be helpful in preventing internal threats and leakage of information along with ensuring that only the right personnel has an access to the health information of their client's patient [27].

Among the challenges characteristic for healthcare data: the security and data sharing between various participants such as hospitals, clinics, insurance companies, and research centers. As much as it is crucial to share information in the health care facility to improve the results of patient care and treatment one of the most crucial concerns is security when dealing with such data. It is also important to note that, secure data sharing can also be made easier through employing of new technologies such as encryption, authentication and; Using artificial intelligence to monitor the processes all through. In the different applications of healthcare with the help of AI…patient data can be encrypted by these systems during communication to maintain its security even when passing through several different applications or organizations [28]. Moreover, AI can identify users who would like information in real time either by implementing MFA or RBA so as to bring the security level to the highest level possible. With the help of recognition of changes of access logs AI systems can predict trends unusual for healthcare organizations, for example attempts of downloading a lot of patient information or sharing it with unscrupulous subject, and thus protect the organizations from data leaks or data breaches [29].

They also help in attaining the facets of compatibility in the prevailing health care networks. Since there is a wide variety of EHR software and hardware systems, health care applications, and medical devices available, the control and management of data understanding and interchange processes alongside maintaining the confidentiality of the information is a complex one. The need for an integration of the different platforms that are used for the management of their data is a way that AI can be applied to harmonies them with the aim of ensuring that the information required for a particular patient is shared between the platforms without much disruption [30]. Additionally, it is also valid to ask whether source data can be verified since analytics show any changes that may suggest the data has been tampered with or contain errors when the correct data is made available. Lastly, as evidenced by this paper, there are several things that need to be discussed regarding the enforcement and optimality of AI in the governing and securing of the process of health information access [31]. First, the case of privacy infringement comes into the picture because AI algorithms collecting and analyzing a massive volume of sensitive data, including the individual's personal health data. It is therefore important for organizations to ensure that there is no compromise of privacy while training an AI model as this could be loops a comparative homework service a coincidence. Moreover, AI in the means of access control system imply substantial costs for emergent changes in the infrastructure to accommodate such systems, staff professional development oriented to operational implementation of the access control systems, along with continuous maintenance of the system to ensure it performs and protects as intended [32].

Here the challenge is ensuring that the associated intelligent systems are neutral in the sense that they do not propose discrimination in the access policies. For example, in data preprocessing, some information leaked and are modifying outputs due to the same and sensitive information, if an AI model learns an incorrect model through a particular data set, it will ration healthcare for a particular group of patients. In order to defeat the above mentioned risks there is a need to introduce fair and non-discriminatory AI's models with its constant audit and optimization [33]. AI is transforming the ways which the healthcare organizations negotiate and manage the data access and privacy, and the advantages of comprehensively secured and productive enhanced compliance. Applying AI to biometric identification, behavior based access and secure transmission and integration of information provides healthcare organization with strict patient privacy and security while being able to open them for access by health care professionals where necessary. However, to receive the real benefits of the application of AI, organizations need to overcome certain technological, social, and legal concerns thanks to the data protection, the avoidance of privacy bias and other issues connected to the implementation of AI if provided assured and secure access control solutions [34].

6. Challenges pertaining the integration of AI in cyber security in health care

Incorporation of this technology entails key issues concerning implementation of artificial intelligence in the healthcare industry as a basic necessity in enhancing the cybersecurity of that sector. Some of the risks common to healthcare organizations include, patient information, healthcare delivery system, and threat landscape. These are some of the problems that need to be solved to realize the maximum value of AI in the protection of healthcare facilities. Modern health care has some issues with AI in its cybersecurity and one of them is the bias of AI [35]. The AI models are learned and trained to data, and should these databases contain raw, or unfair data then the models would readjust rude decisions. For instance, a system designed for access control in a healthcare setting will create an AI narrative of some individuals or groups as 'potentially dangerous or undesirable,' because of discriminating training data sets which will deny appropriate care or data from reaching those groups. This is quite very dangerous to the trust which patients and clinicians have to place in the system for security against hacking as well as for the ordinary clinical processes. It is therefore a major requirement or handy at best that the AI models to be deployed were trained using distinctly inclusive, diverse, and non-bias datasets [36].

Data Privacy Risks and Regulatory Compliance: Because of legal necessities, the healthcare related organizations have complied with HIPAA rules if they operate in the United States, in the European Union it would be the GDPR rules. Some forms of AI interconnect with a healthcare organization structural framework by requiring extensive information about patients to perform their responsibilities; this is a problem when it comes to patient information privacy and compliance with these standards. Keeping AI systems in a state wherein they do not stumble into the privacy act or violate the identity of the patients is a challenging task. In addition, the function of any INF AI driven tools has to meet the shift in regulations/ legal specifications that may be static or dynamic within the rapidly evolving area of AI [37].

Figure: 2 showing challenges of AI in data privacy

Integration with Existing Healthcare Infrastructure: Simplistically, one of the problems is how to combine the use of AI solutions in healthcare with the existing systems. Today, vast majority of healthcare organizations use legacy technology platforms that will not be able to integrate with superior forms of artificial intelligence. When considering incorporating new AI into the old school systems, this translates as high cost, time to complete, and, crucially, additional layering. Also, it is highly probable that most of the healthcare IT staff may be insufficiently confident in the competency levels needed to implement and support AI-based

cybersecurity policies and measures [38]. A challenge embraced to implementing AI-based security systems is depending on staffing heads or personnel to be trained and up skilling of AI system security and this can be a major stepping stone especially in small and constrained healthcare organizations [39].

Cybersecurity Talent Shortage: In addition to the above limitations in utilizing Artificial Intelligence in cybersecurity in the healthcare sector there is a general lack of people in cybersecurity, let alone specialists in Artificial intelligence and machine learning for the job. They still require competent manpower in the designing, supervision and the final tweaking of the systems. Because of the limited number of such scrupulous staff, it becomes difficult for the healthcare organizations to put these systems into practice and maintain them [40]. As the usage of Artificial Intelligence in cybersecurity grows in the near future, recruiting and retaining capable human resources in this area becomes a significant problem. Nevertheless, there are pros of the utilization of AI in the security of health care facilities; there are cons as well. From it, it is essential to eliminate bias, privacy, and integration problems as well as acquisition of the required talent to use AI solutions to enhance rather than worsen the healthcare sector's cybersecurity. If these challenges can be envisaged and addressed, then a healthcare organization opens up a chance to harness what AI can deliver regarding improving the safety of data and systems [41].

7. AI success stories in Healthcare cybersecurity

The application of AI in the healthcare cybersecurity system has transformed the protection of patient's data by enhancing threat identification and aversion to cybersecurity threats. Multiple healthcare facility systems across the globe have already embraced the use of AI to bolster their cybersecurity systems. These case studies show that the fundamental value of Artificial Intelligence for health security purposes has have not been proven to be valuable and the obstacles ahead are significant [42].

Mount Sinai Health System (New York, USA): New York's Mount Sinai Health System is among the several healthcare organizations that have implemented AI to boost cybersecurity. The organization had invested in an automated IT network control system for periods to detect suspicious activity on the network and possible cyber threats. Fortunately for this system, machine learning (ML) algorithms, makes it possible to spot such irregularities in real-time, for instance, multiple login attempts or accesses to patients' records [43]. It has also been effective in decreasing the amount of time taken to prevent threats from penetrating the Organization's system. This AI applications are constantly updated with new data thus are able to enhance the chances of identifying further threats. Therefore, Mount Sinai has experienced a decline in successful cyber-attacks experienced and enhanced cybersecurity status [44].

The NHS (National Health Service, UK): The National Health Service (NHS) of the UK has used AI to respond to the increasing danger of cyber-threats. In order to address the emerging ransom ware threats that struck the NHS in 2017, the organization started integrating AI in its network security. Utilization of AI to scan consistently for malware and ransom ware indicators enabled the NHS to note a threat as soon as it appeared and reduce possible large losses in data [45]. AI also offered automated replies to threats, which liberated the staff from lots of less complicated problems. Moreover, by applying AI the NHS enhanced the system of access control and identity, so nobody could gain an option to visit the information on the patients. This also drastically reduce insider threat issues and ensure compliance to data protection requirements [46].

Georgia Tech Healthcare: Georgia Tech Healthcare established an Artificial Intelligence safety network to safeguard its medical equipment, largely exposed to hackers because of the growing trend in interconnectivity of health related devices. The randomness of different IoT devices like infusion pumps, diagnostic machines, etc. was supervised through AI algorithms. Any of these devices if got into the wrong hand could pose a great danger to the safety of patients. Instead of waiting for attacks to occur on these devices, Georgia Tech was able to learn device behavior and identify potential threats and risks before they could happen. This proved the effectiveness of the system in working out some deficiencies that jeopardize the security in the organization's health care network enabling the organization to improve the strength of the security required across its network [47].

Radiology Group (USA): An American based radiology group used Artificial Intelligence improve the security of its medical image systems. The AI system was designed to detect and respond to potential security threats that's aimed at the digital imaging system which holds large amount of patient records. A prime function maps access patterns to the site and then feeds them to a machine learning module that can identify suspect behavior such as access to imaging files or attempts to modify images [48]. The AI technology also assist in reducing security performance repetitive activities like refreshing the software used and fixing up for the exploits by cyber' criminals. Therefore, the radiology group observed a reduction of the vulnerability, and an enhanced adherence to the healthcare data security standards [49].

Key Takeaways: These case studies show how the healthcare sector benefit from AI in the fight against cyber threats through increased detection, prevention, and better response. It is possible to make use of AI systems to detect anomalies and prevent security threats and to control compliance with regulations. These systems adjust the engagement with the users based on machine learning algorithms, and thus, are becoming more efficient over time at preventing cyber-attacks. But these are achievements that also demonstrate that the adoption of AI in cybersecurity is not without its problems for healthcare organizations [50]. All of these factors – compatibility with legacy systems, issues of talent acquisition, and data governance and bias – are areas that need to be conquered to optimize the application of AI solutions. It has been found that AI is fitting well into the healthcare industry and is benefitting an ability to overcome cyber threats. In this area, AI solutions involve vast data analysis, the automation of mundane security operations and real-time threat identification, assist healthcare organizations in shielding patient data, strengthening the integrity of the healthcare systems, and enhancing the overall security of a healthcare network environment [51].

8. The role of AI, Deep Learning, and Machine Learning in Cardiovascular Devices

Both AI, DL, and ML are transforming cardiovascular care including the advancement and application of medical devices. These technologies are making it possible to develop systems that create very accurate, and real-time, monitors with continuously monitoring the cardiovascular health of a patient. Opponents insist that, for example, AI algorithms study countless amounts of patient information, including ECG, BP, CHF and analyses heart rhythms to identify symptoms of cardiovascular diseases such as arrhythmias, heart attacks, and pulmonary embolisms. AI known specifically as Deep learning models are beneficial in precise diagnosis of diseases from large data sets [52].

For example, an implantable pacemaker and defibrillator contain an algorithm that can be recalibrated to respond to invasions in conditions in a patient's heart, offering timely and special treatment. The use of these technologies helps the healthcare providers to detect patients they think can develop complications and need admission early enough thus avoiding admission of the patients with severe complications hence making their outcomes better [53]. Moreover, ML models stay continuously updated from the new data and therefore improve their efficiency and accuracy. This results in increased and more effective oversight, as well as increasing the specificity of therapy, as it becomes less systematized and much more focused on patients. ML when integrated with AI presents a future where cardiovascular diseases diagnosis, treatment and possibly its prevention is achieved through precise medicine [54].

9. Deep Learning and AI in Cancer Medicine

AI and Deep learning are gradually being used to bring remarkable changes in cancer medicine diagnosis, treatment and patient care outcomes. Current advanced models of Deep Learning, that allowed making predictions based only on large arrays of data, have become essential in oncology. These models are used to analyze tissue images which include MRI scans, CT scans, and biopsies, to recognize patterns of tumor formation or growth of tissues that should not be growing [55]. This way AI can help identify cancer on early stages: lung cancer, breast cancer, prostate cancer, and it can pinpoint tumor locations that may not be considered by human clinician. In addition, artificial neural networks are applied to prognosis of cancer and to able the patient to choose the most suitable therapy according to their genes and previous diseases [56].

Some of the areas where AI is of great value include; Aided drug discovery; Through analysis of data from clinical trials, medical records and other relevant data the AI can recommend the right therapies thus reducing the back and forth common with cancer treatment. These AI systems can also observe the patient's response to the treatments and advise on the changes that should be made to either enhance the treatments or support other therapeutic mechanism in practice. Deep Learning for detecting tumors and recommending specific treatment plans are helping oncology to diagnose the diseases more quickly and recommending the most effective treatment for a patient increase the rate of survival for the diseases [57]. Coupled with developments in genomics, AI is shaping a more efficient, data-oriented model in cancer treatment that will enable the discovery of better ways of reducing throughput and improving the odds of success in favor of decreased invasiveness.

10. Aerodynamics and Chatgpt in Medical Devices and Healthcare

The concept of aerodynamics traditionally connected with the study of air flows, has become a vital application in medical-related product design and enhancement because of the need to optimize medical devices and at the same time ensure that the products developed are safe for the human body. Using aerodynamics, the control, and precision of intensive medical equipment like inhalers, ventilators, and even surgical robots are being made better. For instance in inhalers, the design controls the internal airflow

patterns thereby making medication to deposit well in lungs and hence enhancing patients' results more especially in asthmatic conditions or COPD. In robotic surgical procedures, low friction bodies are used as applied aerodynamics in order to facilitate the flexibility of instruments to be used during surgery [58]. On the other hand, Chatgpt and other AI models are being extended to revolutionize the health care sector in relation to communication, clinical decision and patient experience. Chatgpt, especially, does help doctors by answering clinical questions in real-time, or recommending the current best available treatment or mode of treatment, and even handling bureaucratic work. Many of these AI models are built to train on a lot of medical information, provide personalized advice and help make a diagnosis [59].

Patient care is another area where Chatgpt is drastically changing people's experience; now, patients can talk to Chatgpt any time of the day, get answers to questions they might have and make sure that people have a better grasp of their ailments and cures available [60]. Chatgpt can help healthcare by providing administrative services, and in all ways, the job becomes seamless for the Clinicians. Including the aerodynamics, the AI models such as the Chatgpt are enhancing the healthcare sector through device efficiency and eliminating human mistakes, and enhancing patient and healthcare providers' interaction. All of these innovations lead to better, safer, and more personalized direct care as well as indirect institutional care, and it has general implications on the clinical and administrative sides of the medical field.

11. Conclusion

The use of Artificial Intelligence (AI) in healthcare cybersecurity is quickly becoming a revolutionary concept within this sector. When using digital services as a part of provision of healthcare services such as EHRs, Telemedicine and connected healthcare devices, the importance of securing the patient information and the continuity of care can be espoused. AI presents allergy in approaching and solving problems and provides form methods of data protection, threat identification, and compliance with staunch regulations. AI is enhancing the healthcare cybersecurity frameworks by identifying threats, distinguishing patterns in real time, and performing repetitive security functions on massive amounts of data. AI systems are allowing the healthcare organizations to shift from the conventional security paradigm of being response-based to predictive security models. For example, while machine learning algorithms can learn new data and make decisions without outside help, this means that they can learn how to recognize early elements of an attack and prevent them from becoming more dangerous cyber threats. That is why AI becomes the key factor in the ever-changing field of cybersecurity. Also, AI has been demonstrated to be valuable in the protection of medical devices granting access in cases of urgency only, making additional improvements to data protection in settings.

However, the application advanced AI in the field of health care cybersecurity has also numerous disadvantages which are also important to consider. Some of these are privacy issues, problems linked to AI model bias, compatibility issues with the current setup, and there is always a dearth of skilled cybersecurity workers. Healthcare organizations need to deal with these obstacles in order to realize the value of applied AI and to use these technologies ethically, safely and compliantly. From these case studies, it can be concluded that the application of AI has already started generating positive outcomes across actual healthcare organizations. From surveillance of network traffic in Mount Sinai Health System to safeguarding of medical devices in Georgia Tech Healthcare, institutions are ramping up on their cybersecurity stances with AI. In the future as these technologies advance the purpose of AI will become more crucial to protect healthcare organizations from cyber threats. Thus, despite the challenges on the way toward global integration of AI in healthcare cybersecurity, the advantages are tangible and obvious – better protection of information, quicker detection of threats, and compliance with the regulations. So, with the appropriate level of investment resources dedicated to the growth of AI plus non-stop focusing on innovations, and comprehending the issues of managing AI, this technology remains a crucial notion in the further improvement of the HC industry's cybersecurity that, in turn, should help to keep up the patient data protection along with the corresponding safe provision of the health care.

To conclude, the inclusion of Artificial Intelligence, Deep Learning, and Machine Learning across the continuum of healthcare measures up both the safety and feasibility of healthcare frameworks and, most importantly, spurs advanced healthcare developments. New breakthroughs in cardiovascular applications of artificial intelligence are bringing enhancements in diagnosis and prediction to patients, and advances in aerodynamics help to enhance the functionality and safety of devices. In addition, using AI model such as Chatgpt has brought changes that aid the clinician while at the same time increase patient interactions. These technologies assist in using highly specific operations in cancer treatment while enhancing the general results substantially. Taken together, these developments are remaking the health services environment, providing new opportunities for more safe, effective, convenient, and affordable care that close both the clinical and managerial gaps being confronted by healthcare delivery systems worldwide.

12. References

1. Qayyum, M. U., Sherani, A. M. K., Khan, M., Shiwlani, A., & Hussain, H. K. (2024). Using AI in Healthcare to Manage Vaccines Effectively. *JURIHUM: Jurnal Inovasi dan Humaniora*, *1*(6), 841-854.
2. Sahibzada, S., Nasir, S., Malik, F. S., & Lodhi, S. K. (2024). AI-Driven Aerodynamic Design Optimization for High-Efficiency Wind Turbines: Enhancing Flow Dynamics and Maximizing Energy Output. *European Journal of Science, Innovation and Technology*, *4*(6), 47-53.
3. ul Hassan, S. S., Javaid, M. T., Rauf, U., Nasir, S., Shahzad, A., & Salamat, S. (2023). Systematic investigation of power enhancement of Vertical Axis Wind Turbines using bio-inspired leading edge tubercles. *Energy*, *270*, 126978.
4. Shahid, M. U., Javaid, M. T., Nasir, S., Sajjad, U., Haider, F., Saddam ulHassan, S., & Salamat, S. (2022). Development and Fidelity Assessment of Potential Flow based Framework for Aerodynamic Modeling of High Lift Devices. *Pakistan Journal of Engineering and Technology*, *5*(2), 104-111.
5. Shaban-Nejad, A., Michalowski, M., & Buckeridge, D. L. (2020). *Explainable ai in healthcare and medicine*. Springer, Berlin.
6. Cacciamani, G. E., Chu, T. N., Sanford, D. I., Abreu, A., Duddalwar, V., Oberai, A., & Hung, A. J. (2023). PRISMA AI reporting guidelines for systematic reviews and meta-analyses on AI in healthcare. *Nature medicine*, *29*(1), 14-15.
7. Joshi, M. (2024). Artificial Intelligence (AI) in healthcare. *International Journal of Innovative Research in Science, Engineering and Technology*, *13*(2), 451-453.
8. Malik, F. S., Sahibzada, S., Nasir, S., & Lodhi, S. K. (2024). Machine Learning-Enhanced Turbulence Prediction and Flow Optimization for Advanced Aerodynamic Design in High-Speed Regimes. *European Journal of Science, Innovation and Technology*, *4*(6), 39-46.
9. Bandyopadhyay, P. (2023). Leveraging machine learning and AI in healthcare: A paradigm shift from the traditional approaches.
10. Alami, H., Lehoux, P., Denis, J. L., Motulsky, A., Petitgand, C., Savoldelli, M., & Fortin, J. P. (2021). Organizational readiness for artificial intelligence in health care: insights for decision-making and practice. *Journal of Health Organization and Management*, *35*(1), 106-114.
11. Neoaz, N. (2024). Role of Artificial Intelligence in Enhancing Information Assurance. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(5), 749-758.
12. Palkova, K. (2021). Ethical guidelines for artificial intelligence in healthcare from the sustainable development perspective. *European Journal of Sustainable Development*, *10*(1), 90-90.
13. Abid, N. A Review of Security and Privacy Challenges in Augmented Reality and Virtual Reality Systems with Current Solutions and Future Directions.
14. Neoaz, N. (2024). Human Factors in Information Assurance: A Review of Behavioral and Cultural Aspects. *International Journal of Multidisciplinary Sciences and Arts*, *3*(4), 235-242.
15. Owoyemi, A., Owoyemi, J., Osiyemi, A., & Boyd, A. (2020). Artificial intelligence for healthcare in Africa. *Frontiers in Digital Health*, *2*, 6.
16. Reddy, S., Allan, S., Coghlan, S., & Cooper, P. (2020). A governance model for the application of AI in health care. *Journal of the American Medical Informatics Association*, *27*(3), 491-497.
17. Shah, H. H. (2024). Advancements in Machine Learning Algorithms: Creating a New Era of Professional Predictive Analytics for Increased Effectiveness of Decision Making. *BULLET: Jurnal Multidiscipline Ilmu*, *3*(3), 457-476.
18. Neoaz, N. (2024). Cybersecurity and Information Assurance: Bridging the Gap. *International Journal of Social, Humanities and Life Sciences*, *2*(1), 37-46.
19. Zainab, H., Khan, A. H., Khan, R., & Hussain, H. K. (2024). Integration of AI and Wearable Devices for Continuous Cardiac Health Monitoring. *International Journal of Multidisciplinary Sciences and Arts*, *3*(4), 123-139.
20. Sherani, A. M. K., Khan, M., Qayyum, M. U., & Hussain, H. K. (2024). Synergizing AI and Healthcare: Pioneering Advances in Cancer Medicine for Personalized Treatment. *International Journal of Multidisciplinary Sciences and Arts*, *3*(1), 270-277.
21. Abid, N. (2024). An Analysis of Phishing Attacks: Information Technology Security: Cybercrime and Its Solutions. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(5), 696-712.
22. Sujatha, N., Narayanan Valliammal, L., E, J. R., VS, L., & Mech, M. (2023, November). A Case Study of AIOPs in Large Enterprises Using Predictive Analytics for IT Operations. In *Proceedings of the 5th International Conference on Information Management & Machine Intelligence* (pp. 1-5).

23. Habli, I., Lawton, T., & Porter, Z. (2020). Artificial intelligence in health care: accountability and safety. *Bulletin of the World Health Organization*, *98*(4), 251.
24. Shaheen, M. Y. (2021). Applications of Artificial Intelligence (AI) in healthcare: A review. *ScienceOpen Preprints*.
25. Abid, N. (2023). Ransom ware Attacks on Financial Institutions: A Review of the Literature on Cybersecurity Risks and Countermeasures. *International Journal of Multidisciplinary Sciences and Arts*, *2*(2), 164-169.
26. Sherani, A. M. K., Qayyum, M. U., Khan, M., Shiwlani, A., & Hussain, H. K. (2024). Transforming Healthcare: The Dual Impact of Artificial Intelligence on Vaccines and Patient Care. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(2), 270-280.
27. Nasir, S., Javaid, M. T., Shahid, M. U., Raza, A., Siddiqui, W., & Salamat, S. (2021). Applicability of Vortex Lattice Method and its Comparison with High Fidelity Tools. *Pakistan Journal of Engineering and Technology*, *4*(1), 207-211.
28. Valli, L. N., Sujatha, N., Mech, M., & Lokesh, V. S. (2024). Exploring the roles of AI-Assisted ChatGPT in the field of data science. In *E3S Web of Conferences* (Vol. 491, p. 01026). EDP Sciences.
29. Khan, M., & Sherani, A. M. K. (2024). Promise and Pitfalls of AI in Healthcare: A Critical Review. *International Journal of Multidisciplinary Sciences and Arts*, *3*(2), 325-332.
30. Valli, L. N. (2024). Predictive Analytics Applications for Risk Mitigation across Industries; A review. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(4), 542-553.
31. Shiwlani, A., Khan, M., Sherani, A. M. K., Qayyum, M. U., & Hussain, H. K. (2024). REVOLUTIONIZING HEALTHCARE: THE IMPACT OF ARTIFICIAL INTELLIGENCE ON PATIENT CARE, DIAGNOSIS, AND TREATMENT. *JURIHUM: Jurnal Inovasi dan Humaniora*, *1*(5), 779-790.
32. Khan, A. H., Zainab, H., Khan, R., & Hussain, H. K. (2024). Implications of AI on Cardiovascular Patients' Routine Monitoring and Telemedicine. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(5), 621-637.
33. Abid, N. Improving Accuracy and Efficiency of Online Payment Fraud Detection and Prevention with Machine Learning Models.
34. Valli, L. N., Sujatha, N., Mech, M., & Lokesh, V. S. (2024). Exploring the roles of AI-Assisted ChatGPT in the field of data science. In *E3S Web of Conferences* (Vol. 491, p. 01026). EDP Sciences.
35. Shiwlani, A., Khan, M., Sherani, A. M. K., & Qayyum, M. U. (2023). Synergies of AI and Smart Technology: Revolutionizing Cancer Medicine, Vaccine Development, and Patient Care. *International Journal of Social, Humanities and Life Sciences*, *1*(1), 10-18.
36. Abid, N. Empowering Cybersecurity: Optimized Network Intrusion Detection Using Data Balancing and Advanced Machine Learning Models.
37. Khan, M., & Sherani, A. M. K. (2024). From Data to Decisions: The Impact of AI on Healthcare Systems. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(4), 589-598.
38. Neoaz, N. (2024). A Comprehensive Review of Information Assurance in Cloud Computing Environments. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(6), 715-725.
39. Nasir, S., Zainab, H., & Hussain, H. K. (2024). Artificial-Intelligence Aerodynamics for Efficient Energy Systems: The Focus on Wind Turbines. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(5), 648-659.
40. Khan, R., Zainab, H., Khan, A. H., & Hussain, H. K. (2024). Advances in Predictive Modeling: The Role of Artificial Intelligence in Monitoring Blood Lactate Levels Post-Cardiac Surgery. *International Journal of Multidisciplinary Sciences and Arts*, *3*(4), 140-151.
41. Valli, L. N., Narayanan, S., & Chelladurai, K. (2024). Applications of AI Operations in the Management and Decision-Making of Supply Chain Performance. *SPAST Reports*, *1*(8).
42. Khan, M., Shiwlani, A., Qayyum, M. U., Sherani, A. M. K., & Hussain, H. K. (2024). Revolutionizing Healthcare with AI: Innovative Strategies in Cancer Medicine. *International Journal of Multidisciplinary Sciences and Arts*, *3*(1), 316-324.
43. Amann, J., Blasimme, A., Vayena, E., Frey, D., Madai, V. I., & Precise4Q Consortium. (2020). Explainability for artificial intelligence in healthcare: a multidisciplinary perspective. *BMC medical informatics and decision making*, *20*, 1-9.
44. Shah, H. H. (2023). Early Disease Detection through Data Analytics: Turning Healthcare Intelligence. *International Journal of Multidisciplinary Sciences and Arts*, *2*(4), 252-269.
45. Valli, L. N., Sujatha, N., & Rathinam, E. J. (2023, October). A Study on Deep Learning Frameworks to Understand the Real Time Fault Detection and Diagnosis in IT Operations with AIOPs. In *2023 International Conference on Evolutionary Algorithms and Soft Computing Techniques (EASCT)* (pp. 1-6). IEEE.
46. Khan, M., & Sherani, A. M. K. (2024). Healthcare Meets AI: Innovations, Applications, and Ethical Considerations. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(5), 725-737.

47. Petersson, L., Larsson, I., Nygren, J. M., Nilsen, P., Neher, M., Reed, J. E., & Svedberg, P. (2022). Challenges to implementing artificial intelligence in healthcare: a qualitative interview study with healthcare leaders in Sweden. *BMC Health Services Research*, *22*(1), 850.
48. Reddy, S., Allan, S., Coghlan, S., & Cooper, P. (2020). A governance model for the application of AI in health care. *Journal of the American Medical Informatics Association*, *27*(3), 491-497.
49. Khan, M., Shiwlani, A., Qayyum, M. U., Sherani, A. M. K., & Hussain, H. K. (2024). AI-powered healthcare revolution: an extensive examination of innovative methods in cancer treatment. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(1), 87-98.
50. Abid, N. (2024). Securing Financial Systems with Block chain: A Comprehensive Review of Block chain and Cybersecurity Practices. *International Journal of Multidisciplinary Sciences and Arts*, *3*(4), 193-205.
51. Nasir, S., Hussain, H. K., & Hussain, I. (2024). Active Learning Enhanced Neural Networks for Aerodynamics Design in Military and Civil Aviation. *International Journal of Multidisciplinary Sciences and Arts*, *3*(4), 152-161.
52. Väänänen, A., Haataja, K., Vehviläinen-Julkunen, K., & Toivanen, P. (2021). AI in healthcare: A narrative review. *F1000Research*, *10*, 6.
53. Khan, A. H., Zainab, H., Khan, R., & Hussain, H. K. (2024). Deep Learning in the Diagnosis and Management of Arrhythmias. *Journal of Social Research*, *4*(1).
54. Valli, L. N. (2024). A succinct synopsis of predictive analysis applications in the contemporary period. *International Journal of Multidisciplinary Sciences and Arts*, *3*(4), 26-36.
55. Jamal, A. (2023). Novel Approaches in the Field of Cancer Medicine. *Biological times*, *2*(12), 52-53.
56. Abid, N. (2022). Evolution of Cryptographic Techniques: Overview of the Existing Approaches and Trends of the Development. *BULLET: Jurnal Multidisiplin Ilmu*, *1*(03), 523-538.
57. Raza, A., Farhan, S., Nasir, S., & Salamat, S. (2021, January). Applicability of 3D printed fighter aircraft model for subsonic wind tunnel. In *2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST)* (pp. 730-735). IEEE.
58. Valli, L. N., & Sujatha, N. (2024, April). Predictive Modeling and Decision-Making in Data Science: A Comparative Study. In *2024 5th International Conference on Recent Trends in Computer Science and Technology (ICRTCST)* (pp. 603-608). IEEE.
59. Samad, A., & Jamal, A. (2024). Transformative Applications of ChatGPT: A Comprehensive Review of Its Impact across Industries. *Global Journal of Multidisciplinary Sciences and Arts*, *1*, 26-48.
60. Abid, N. (2023). Enhanced IoT Network Security with Machine Learning Techniques for Anomaly Detection and Classification. *Int. J. Curr. Eng. Technol*, *13*(6), 536-544.