International Journal of Social, Humanities and Life Sciences ISSN XXXX-XXXX
Vol. 2, No. 1, 2024, pp. 47-59

Securing the Future: A Comprehensive Review of AI in Healthcare Cybersecurity and Information Access

Hafiz Abdul Rouaf

Independent Researcher Multan Pakistan

hafizabdulrouaf@gmail.com

Abstract

When AI is incorporated in health sectors; it evolved as a revolutionary innovation and new and massive cyber-security issues. As application of AI gains traction there is always the need to safeguard such health information from disclosure. Primary, this article is concentrated mostly on the connection between AI and healthcare cybersecurity and data protection with the additional emphasis made on the need for improving security to safeguard patient and medical applications. Discussions include AI for predictive threat and risk analysis of systems, smart access control, and security of medical devices and integration of block chain with AI. This article also discusses other types of guidelines for the use of AI in health services including HIPAA and GDPR then the ethical concerns on transparency, fairness and sample bias in algorithms. While attempting to address these challenges affecting healthcare organizations, other options like consumption of AI automation, utilization of AI protective tools, and block chain could help in the enhancement of the stability of the system and protection of data. However, it remains unclear how these requirements can be met while addressing new technologies and ethical and legal perspectives of their application. Altogether, the protection of healthcare cybersecurity in the future will employ the integration of using AI technology and also making consideration of the patients' data privacy, the fast reception of AI technology, and the ethical use of AI in health establishments. For that, AI could help to improve both the security and productivity of the healthcare systems by promoting the innovation more and addressing new challenges in cyber space and/or new moral dilemmas.

Keywords: *Application in health care, health information technology safeguarding, data security/ privacy, control availability, prescriptive analytical tools, block chain, medical devices safeguarding , rules & regulations, ethical use of AI, data asset protection, threat identification, self-optimization AI.*

1. Introduction

Trend development through application of artificial intelligence technology has impacted several sectors, one of it being the health sector. With the potential of turning around the manner and ways diagnosis and treatment planning and provision of healthcare services are being done; the impacts of AI on the quality of care and the productivity TRB are expected to be on the bright side. However, this increased dependence on AI brings new risks and where safety, and security are a consideration these become the focus as does the protection of health data and the reliability of the AI systems. AI and healthcare also cybersecurity is one of the significant area of research due to the use of advanced technologies in the delivery of healthcare and the surety that to use of any advanced technology the aspect of cybersecurity has to be implemented in-order to protect the patients' information [1]. It can manage to dissect a relatively large number of medical cases in a short span of time, as well as with high accuracy that could hardly be expected from an experienced physician; it has capacity to threaten diseases, identify correlations, and develop a treatment program with personalized for its patients. This technology brings improvement in the decision making process, early diagnosis and effective utilization of resources. Not only is the artificial intelligence augmenting robotic recommended minimally invasive surgery and changing medical imaging by embedding the AI, but the technology is gradually permeating the}şiumber of layers of healthcare industry improvements at clinical and organizational levels. Since the reliance on artificial intelligence rises in delivering the health care services then the information being processed is more sensitive and valuable. Records of various patients' treatments, history, and diagnosis are particularly important in criminal markets because of the value that the health records have in the dark web [2].

System security is therefore still another emergent issue within artificial intelligence health care delivery systems. Patient data privacy to avoid formal invasions, and anyone try to get unauthorized access is very crucial since if the improper hands get your data, they would be able to clone your identity, steal your financial details, or even alter your medical records – which can mean lives lost [3]. First and foremost, AI, itself, as it was shown above, lacks protection against cyber threats. Once more, just like manipulating a system's reward function, these hackers can corrupt AI algorithms, tinker with decision-making procedures, instill biases which in advanced healthcare systems are a disaster. Secondly, artificial intelligence still heavily relies on numerous interconnected devices and systems expanding the potential number of cyber threats' entries. That is why merely scaling up applications of AI in healthcare implies that cybersecurity can and should be attacked at this level: at some point, one has to consider both technical risks and ethical ones [4]. It means that AI systems have to be initially developed with certain security aspects and health care facilities have to perform some security measures to protect their networks. It is not merely a combination of AI application the healthcare sector, and cybersecurity but also that of governance compliance and policies together with risk management of the enhanced innovation of AI in the healthcare industry [5].

2. Artificial Intelligence application in today's Healthcare Environment

Artificial Intelligence is revolutionizing diagnostics, treatment and patient care in the contemporary world's health care delivery system. Application of advanced AI technologies it has promoted the creation and development of novelties mainly in diagnostics, promptness, and efficiency in the healthcare organizations. Being able to consider thoughts in a clinical setting or think of ideas that when could have been unthinkable several years ago has been one of the most valuable assets for designers and managers in the health care setting AI capability. In this part of the paper, characteristics of the use of Artificial Intelligence in the current society with a focus on the healthcare sector with an aim of driving home the disruptive nature of AI on different aspects of the system [6]. One other place where the role of AI in healthcare can be explained is using diagnostics. Through the application of Artificial Intelligence systems developed by the health care people, diseases are diagnosed in their early nature thereby improving on the patient's life and indeed saving lives. For instance, using its algorithms, one is in a position to diagnose or even identify abnormal structures in medical images for example X-ray, Computed tomographic scans and Magnetic resonance imaging at very high accuracy concerning aspects for example tumors, Fractures as well as infections. Such systems as these can not only read the images better that radiologists, but also may notice conditions that the radiologists would skip [7]. In fact, in some contexts A can predict the phases or development of such illnesses like cancer to help in developing treatment plans. Namely, while traditional II systems convert the inaccurate diagnosis into a fixed decision, the application of deep learning in artificial intelligence enables the enhancement in diagnostic results embodied from newly received data in the future, which is a strong positive feedback [8].

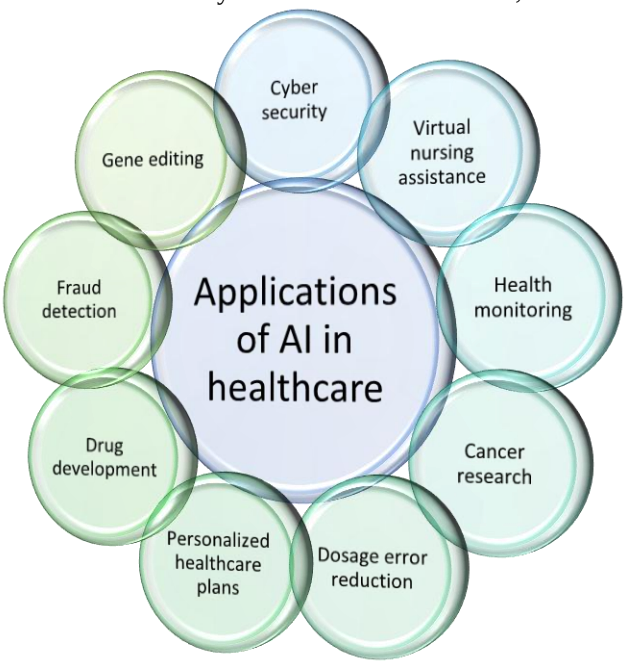

Figure: 1 showing applications of AI in healthcare

Apart from diagnosis, the current AI innovations are excellent in treatment, and sometimes even in catering for patients. These sources of information can be marine, genetic, lifestyle related and a number of tests that can be employed in order to estimate the probability that a treatment plan will be effective on the patient. This is more evident especially with cancer; treatment interventions have to be developed based on the patient's genetic makeup and many other aspects regarding his/her illness. Perhaps the biggest advantage of AI is the ability to learn huge amounts of information to détente so that clinicians do not make esoteric decisions that are all so common in patient management – trial and error [9]. AI is also increasing efficiency of administrative responsibilities in the functioning of healthcare. From roistering and resource allocation, to patient flow optimization, artificial intelligence is increasingly automating some previously manual workflow. They are employed in the patient engagement, information provision, appointment scheduling and quick health advice services. This not only increase the patient satisfaction level as the patient can help at any point of time but also allows the health care staff to reduce their working hours most of which is wasted in documentation [10].

Besides, they employed new AI in drug discovery and development which could been risky, costly and time-consuming exercise. Such approaches through application of artificial intelligence involving different algorithms, have immensely assisted in the formation of the best set of drug compounds that can treat certain diseases; the time usually taken, when development of new therapies is considered, has equally been curtailed. BIO data size and AI learning capability, and the capability of AI doing consequential drug interaction simulations are enabling the process, and making it possible to come across genuine exceptional treatment for such diseases as Alzheimer, cancer and hereditary diseases [11]. Telemedicine is also amongst the functions of artificial intelligence Healthcare. Now, using telemedicine, patients are able to track their status with physicians and / or monitor basic life support indicators and, occasionally, get a diagnosis without a physician. The benefits are especially of immense importance to patients which are in rural or may be underserved since they have poor access to health workers. AI integrated smart wearable's track a number of chronic diseases such as diabetes, heart diseases, or high blood pressure and signal the patient or the doctor whenever there is an anomaly [12].

But there is need to try and point out that in the recent past AI has brought about beneficial results on modern healthcare wherein the incorporation of this equipment has repercussions. Regarding appropriateness of the AI technologies regarding the patient in the healthcare organization, following aspect should be implemented: Data ownership, control and transfer, users and operators accountability, and ownership and control of algorithm the following aspects should be considered in order to prevent the use of AI technologies on the patients inappropriately in healthcare organizations [13]. However, AI has become even more connected to today's modern medical environment as ways to improve clinical offerings at the same time as fine-tuning getting price and snapping open the entrance to sufficient medical care for anyone. Any news that is to be received in future about this technology is going to interpret to the understanding that AI will keep on growing and AI will continue to play an important role in healthcare networks [14].

3. Cybersecurity Challenges in Healthcare: An Evolving Threat Landscape

Because the type of data usual in the healthcare field is considered valuable, the healthcare sector is today at high risk of cyber-attacks. Sitting across from AI, EHR, 'smart' medical devices and other smart programs, modern healthcare organizations and becoming increasingly challenged by new issues to patients' data and their systems. The threats that are commonly known with cyber security in health care are some that are continually mutating, this simply confirms that health care stakeholders are quite prepared to contain themselves with the rising threats [15]. Without doubt, the most dangerous threats in the field of cyber security for healthcare organizations can be considered the following ones ransom ware which is today facing an annual increment along with enhancing in its severity. In these attacks, the hackers mount a system in a particular healthcare organization and lock out its rightful user from accessing data unless they pay a ransom [16]. Given the understanding that the kind of information that patients share in the health facilities is some of the most personal that an individual would share concerning their health, the hospitals and clinics especially the large ones are willing to pay the ransom in order to have the process disrupted. Such actions put the lives of the patients at risk, and it also wastes money leading to compromises of the image of the organization and the giving out of fines. Ransom ware attacks on some of the largest health care organizations has wake up call sort of way to address the matters concerning insecurity [17].

Another form of cyber threat which is seen frequent in the health care industry is the phishing attacks. There are these attacks where the impersonators are imitating other officials within management and forcing other care givers to disclose important materials like passwords or even patient records. However, since a part of the healthcare staff is on the receiving end because of handling numerous types of sensitive information, phishing attacks afford hackers direct ways of getting into the internal database

for modifying, eliminating, or getting a hold of a patient's information. Furthermore, the threat of phishing becomes the first stage of the next activities: for example, an attempt to introduce malware or to receive control over the required facilities of a hospital [18]. There is also the threat from ransom ware and phishing, and the risks that are associated with connected devises that have become the Internet of Medical Thing (IoMT) devices. These connective devices predicates – ranging from pacemaker and insulin pump to infusion pump and diagnostic machine – create novel severe risks to HC networks. Most of these gadgets were manufactured without security in mind and therefore are a gadget can be hacked. If an attacker was to gain control of a medical device it would be lethal for the patient and the device may become a means to access the rest of the hospital's network [19].

That is why the expansion of coverage of AI technologies in the sphere of medical services has new cybersecurity threats. But if one will recall that AI algorithms have almost exhaustive knowledge about the particular specimen and are also vulnerable to adversarial examples or inputs that are contrived to deceive the AI. This in healthcare may lead to wrong diagnosis or wrong recommend treatment to undertake hence expose the patients to so many risks. Furthermore, most AI systems consist of enormous databases and when the databases in an AI architecture are compromised, then the models used in the artificial intelligence structures are compromised [20]. The preservation of these systems and the data they utilize for such indefinite purposes in turning round AI in the delivery of health care services therefore requires protection against contamination. One of the oldest tricks in the book and still one of the most worrying issues with cyber security in health care is sneak age of information. This is exactly why the healthcare Industry becomes the most susceptible Industry to Data breaches because everybody wants his or her health information to be private. Tkrétikoye that target health entities want to obtain such data for identity theft or fraud or sell it in the cybercrime black market. I may not be able to quantify the losses occasioned by leakage of the patients' information, but what is clear is that, such an act erodes the reputation that a healthcare provider develops with his or her clients [21].

Besides these external sources of threat, healthcare organizations have to struggle with. Internal threats: Sometimes the employees of the healthcare organizations even compromise it either intentionally or unintentionally. For instance, employees may steal passwords or make the security of the organizational information insecure. The paper also describes insider threat in terms of malicious nature, for instance an employee with grudges or a contractor who has permission to access the systems and in turn launches a raid on the employer's information [22]. Because of these potential difficulties, making cybersecurity a high priority in healthcare organizations should be done through the following: Secure Operational Structures, Risk Contracts Compliance, Periodic security awareness. From the above risks natural some of the risks can be managed by enhancing the security technologies include: artificial intelligence based intrusion detection system and multi-factor authentication. However, that which has emerged clearly enough is that in as much as the face of digital healthcare transforms in various ways, so also too will the tricks that hackers practice transform in similar manner; in other words, by their own effort on their own, without any help or assistance, will it be necessary for healthcare providers to be abreast of these new trends [23].

4. Introducing Artificial Intelligence to Strengthen Cybersecurity in healthcare

Cybersecurity is one of the biggest problems in the healthcare industry and AI is slowly being implemented to fight the problem. For this reason, the number and the range of threats are growing together with the newly appearing kinds, and the traditional security tools provide no sufficient identification and counteraction options. AI is deemed to be the friendliest solution proposed to healthcare protection against cyber threats or being the advanced decision-making system unlike simple cybersecurity team it is capable of preventing as well as responding to the attacks much more actively [24]. Therefore, healthcare organizations strengthen security in the very essence of the healthcare domain with the assistance of such types of Artificial Intelligence as machine learning, deep learning and natural language processing to protect patients, medical, devices, structures, and infrastructures. However, there are some aspects that socially contribute by incorporating the AI system in the advance of the healthcare cybersecurity system; observable threat detection. Describing in this paper how machine learning can be used on various operations in order to obtain a typical traffic flow within a healthcare system network and identify traffic which may be suggestive of a violation or an attack, for instance, AI-based solutions depending on the behavior of the user and activity logs can immediately distinguish improper activity such as an intruder trying to log into a device or making large downloads, which are usually indicators of intrusion of cyber criminals [25]. From our conclusions on the above findings, then such systems can notify the security teams, in real time, so that they contain within extent of the threat before it goes beyond. The threat detection done by the use of AI is also relatively faster than this conventional methods and more accurate as well, AI also reduces the gap between the actual breach time and the time the threat is actually detected hence the hackers cause minimal damage [2].

This is how AI also can help in improving the medical device security in different manner. At the present time, nearly every healthcare organization hasIoMT; this includes pacemakers insulin pumps, ventilators and much more most of which are vulnerable

to hacking. These devices can then be watched in real time using AI and any change or any behavior which is different is suggestive of a security issue. That puts them in IoMT security systems and this shows that an organization's health status of medically deployed equipment can be constantly monitor for vulnerabilities that hackers can develop and exploit. This makes it possible to immobilize devices to safe states thus minimizing the probability of patient harm and the alteration of the clinical scene [27]. In addition to threat detection, AI can enhance the protecting scenario of healthcare organizations by having automatically responses towards cyber incidents. Automatic security measures can perform certain actions in reaction to threats, including but not limited to: time to disconnect the affected devices, block particular IPs or even to begin data encryption. They have to be as generic as possible in order to avoid attacks reaching further and take as little toll on the general system as possible. In addition, AI systems can be helpful in such situations when other methods or examination of the incident in order to state the scale of the breach or define the systems that have been influenced, and distinguish the sources of the attacks in order to state and solve the cases of the breaches in shorter time and analyze the outcomes in shorter time is needed [28].

AI can also be applied towards improving of user identity and control in the health care facility. The more secure and convenient methods of biometric recognition could be biometric identification technologies based on face or fingerprint scan, as well as the behavioral biometrics that involves observing user's typing speed or mouse movements for the purpose of identifying the user. These technologies ensures only the allowed employees, heath cares and officers in healthcare industries use the sensitive data in the industries thus lowers cases of insider threats to sensitive information [29]. Also, the use of AI enables such excesses to be detected as a trend suggesting that someone is accessing information that is not related to his/her duty or accessing a database in different time zones to be handled immediately for instance by sending a notification or making the user type in his/her password again. AI is improving healthcare cybersecurity in several ways among them is in handling vast amounts of information such as EHRs which are themselves risky targets. Within the AI platforms we have the algorithms to apply to prized information to put them in an encoded form thus even if it is stolen, cannot be used since they will need decryption keys. In addition, with AI assistance, data integrity can be checked as to whether it has been tampered with or not all the time so that the general health care givers will have confidence within the data they use in diagnosing their patents [30].

AI can help in preventing what hackers often use in gaining entry to systems in the healthcare zone known as phishing technique. Such AI systems might scan through the emails, know that there are some phishing emails going around, and thereafter filter off the emails thereby never reaching the end users. Promising results can be achieved just by educating the machine learning algorithms of recognizing dangerous components in spam messages and informing the user about possible threats that can take place, which in turn will much less human mistakes plus increase the stability of the health care system concerning the serious issues – phishing threats [31]. However, AI driven solutions offer a lot of potential when it comes to addressing the concerns of healthcare cybersecurity, while, at the same time, raises a number of compelling ethical, regulatory and technical issues with regards to their application. Due to these reasons, the systems must be transparent to enable their users to understand how the systems work, be capable of providing records of their operations, and adhere to HIPAA and similar rules every time data from a patient's personal health record is incorporated to give confidence to clients in the systems. Although the use of technology is increasing AI will become more central to the process of protecting the healthcare system from multiple new threats in the cyber domain [32].

5. Data Protection as well as Authorization to Recovery in Artificial Intelligence supported State-of-Health Systems

With several healthcare system turning towards the AI healthcare technology, notable factors like strong data protection solutions and proper authorization controls have become consideration like never before. Every day there is much going on in healthcare organizations and this causes generation of much PHI; this data is useful and is the reason hackers consider it important to steal. The fact that this data is mostly used for clinical decision making and building patient's individual treatment plan and outcome prediction analytics with the help of AI systems make data privacy and access control essential for patient's confidence, compliance with legal regulation and protection from cyber threats [33].

Data Privacy in AI-Powered Healthcare Systems: In healthcare and the clinical field, artificial intelligence is only used accurately to work on the large data sets. Such information may be the records of the patient, the patient's history, the diagnostic information and the genetic information of the patient. Similar to all other AI application, big data processing required to mine the information that needed to get from the database and make the right predictions. However, the high reliance on data produces a new issue which is privacy. Data privacy is the safeguarding of the patient data from being used, disclosed to, modified or destroyed by an unauthorized individual. While discussing data security risks in the AI-based healthcare systems the primary concerns are

security from unauthorized individuals, ensuring data is only used for the purpose it was collected for and more crucially, data privacy [34]. The measures to enforce compliance to the standards are provided by health care standards such as the Health Insurance Portability and Accountability Act (HIPAA) in United States. AI has to meet these regulations which are in pursuit of protecting data privacy from the time the data is collected, stored, analyzed and disseminated. Further, AI techniques need another method, including encryption, anonymization, and data masking to improve security for the data managed. Encryption makes data meaningless should the data be sniffed or stolen the data cannot be interpreted without the proper decryption token and anonymization assists in removing PII data points from the datasets used in training the AI systems thus minimizing on the likelihood of the AI systems infringing on privacy [35].

Access Control in AI-Powered Healthcare Systems: Another concern of effective practicing of security in the facilities dealing with health include access control. Authorization can be defined as the method and process of controlling some kind of information or certain computer facilities according users' job relationships and legal authority. This means there should not be wrong people or people with wrong clearance level to access patient data or to interact with the AI-controlled equipment in the healthcare program [36]. RBAC is one of the many methods used in healthcare institutions: Role-Based Access Control. RBAC of course has the edge that in a healthcare organization, rights can be assigned according to the roles that the user has in the particular organization such that they can only access what is relevant to them. For example, a doctor may get to know about a patient, but the administrative employees of the hospital may not know full details of the patient's account. Through RBAC, AI systems can be associated with only persons holding credentials to use tools driven by artificial intelligence [37].

Balance between Privacy, Access, and AI Capabilities: On one hand, there are very big opportunities that AI wants to bring into the setting of healthcare but at the same time there is realistic concern/ fear that patient data will turn into a marketable product /commodity and that the data is freely available to an algorithm that will then make the decision based on facts available in the present world. For instance, a system can call for raw data to give a forecast or a diagnostic place on the state of the patient. However, when AI is allowed to enter such a database, a basic issue of consent, transparency and accountability is thrown into the air. It also notes that patients require knowledge on how the data collected by AI systems should be used, stored or processed, meaning patients need to be literate in their data [38]. To maintain the privacy and access control rules, health-care organizations have to spend their resources in order to avoid and control the AI systems and the way, they manage the rules. Any other automated auditing utilities using artificial intelligence comprises of checking compliance with data privacy norms for violation, monitoring of access user statistics and possible violate reports.

Health data particularly AI in health care is usually an import that should be given adequate information security when assimilated into health institutions. Patient data is tender info used by the key health care decisions made by the instituted AI systems, and hence, healthcare organizations must enforce strict measures such as encryption, anonymization and role based access control to attain securitization and legal compliance. It emerges, how it is possible to obtain privacy and accessibility along with works that can be produced by AI for achieving secure health care for pursuing security system to safeguard the patient and also for purity in healthcare service [39].

6. Challenges and prospects of Healthcare Cybersecurity: Legal and Ethical consideration

When the health systems have advanced to the next stage of practice in AI and all the other related technologies, policies, together with the ethical issues that are related to the technologies have also evolved to encompass core values of the protection of the technologies. The steady increased promising and innovative clinical utilization of of AI give rise to new opportunities and new issues for the regulators and for doctors and for policy makers who are the ones that are expected to provide leadership in relevance to AI, to devise new laws and policies given the existing AI threats [40]. In particular, ethical problems are still significant in defining how the health-care organizations use the AI technologies across institutions to guard the patient's interest and avoid the negative effects.

Regulatory Frameworks in Healthcare Cybersecurity: In the field of healthcare, there are various regulations to perform for the protection of patient data, privacy and system. To date the most comprehensive set of rules and guidelines concerning the restricted application of patients' information, privacy and security, within the United States is the Health Insurance Portability and Accountability Act of HIPAA. HIPAA requires that all the companies, insurers and business associates involved in health related business ensure that they protect the PHI to the highest level from being accessed by wrong hands including cyber criminals [41]. Especially important in connection with the emergence of AI technologies for cooperation with health care organizations,

since the AI application in this field cannot violate the principles of the protection of personal data of patients, while scientific practitioners require appropriate means for accessing such information [42].

At the international level there is the European Union General Data Protection Regulation (GDPR) that also also has significant role in patient data protection and privacy. Representatives of the GDPR have much stricter rules regarding data and thus permission from the patient is required as to the use or sharing of patient data in general and health data in particular. It also contains a right within the individual to obtain the data held by the entity, to rectify or erase the data; this empowers patients with their data. As far as AI for healthcare is concerned these regulations suggest that the organizations have to say how these AI algorithms are getting closer and making the analysis and have to also make sure the data that is used in models are DE identified and their privacy is protected [43]. Other authorities like the FDA in United States, and EMA in Europe have already started the processes of regulating introduction of AI in the health systems and in medical devices. Since most of the AI systems are being implemented in the electronic health and clinical device they are the agencies that decide the safety and efficiency of such systems. For instance, with regard to the used AI in prior medical devices, due to the absence of MDR and Controls, premarket, and postmarked processes are needed to understand what the MDR and Controls are not likely to create risks for the lives of the patient [44].

Ethical Considerations in AI Healthcare Systems: Nevertheless, like previously indicated, healthcare organizations do not have to wait for policy to play catch up on other issues that are linked with ethical use AI in patient care delivery. There is one truly great ethical dilemma left, which is a lack of impartiality and transparency of the assessment of the algorithms; The reason why it is often called the ‘black box is that people cannot know how the particular system came to an understanding of something or other, which is especially essential when working with a high level of machine learning systems. In general, such absence of explain ability may lead to certain problems: the AI should have to appear to the patient and other healthcare workers that it arrived at the right and impartial decisions on diagnosis or otherwise the treatment plan to take. Taking all that into consideration, healthcare organizations must begin to aspire for the transparency of AI and how it arrives at the conclusions it does [45]. This implies making sure that the AI based systems indeed have motivations for their decision making and ensure that the health care givers can follow the decision made on their recommendation(s) by the AI systems. This is important in increasing confidence from the patients as well as the other working health care personnel since they know that they are alive from the AI tools and systems [46].

The other huge ethical consideration is that AI models can train themselves to spit out bias. AI systems have to be fed with big data and if these data sets are not diverse the AI system will do poorly which in effect prejudices some patients. For instance, an AI system can be trained using data from one gender group then find its performance in another gender group to be poor making the healthcare sector to be inefficient in serving all the genders. Because of this it is vital that software developers of AI and healthcare professionals feed different data to develop the AI systems. Another to major ethical issues to do with confidentiality as well as consent [47]. HIPAA and GDPR has rules on how the patient information may be copied and processed in a technical perspective however, there are ethical issues when the patient has not been informed how the information will be used or where consent has not been sought. When patient information is taken through an AI system the patient must be informed when where how what and for what purpose personal data collected will be utilized, what protections have been initiated to protect the information and by what process the patient could control the data. Since dark patterns or UI choices that are language-based for the most part are deceptive and lead to regretted decisions, they have to be avoided to maintain correct AI use and patients’ decisional freedom [48].

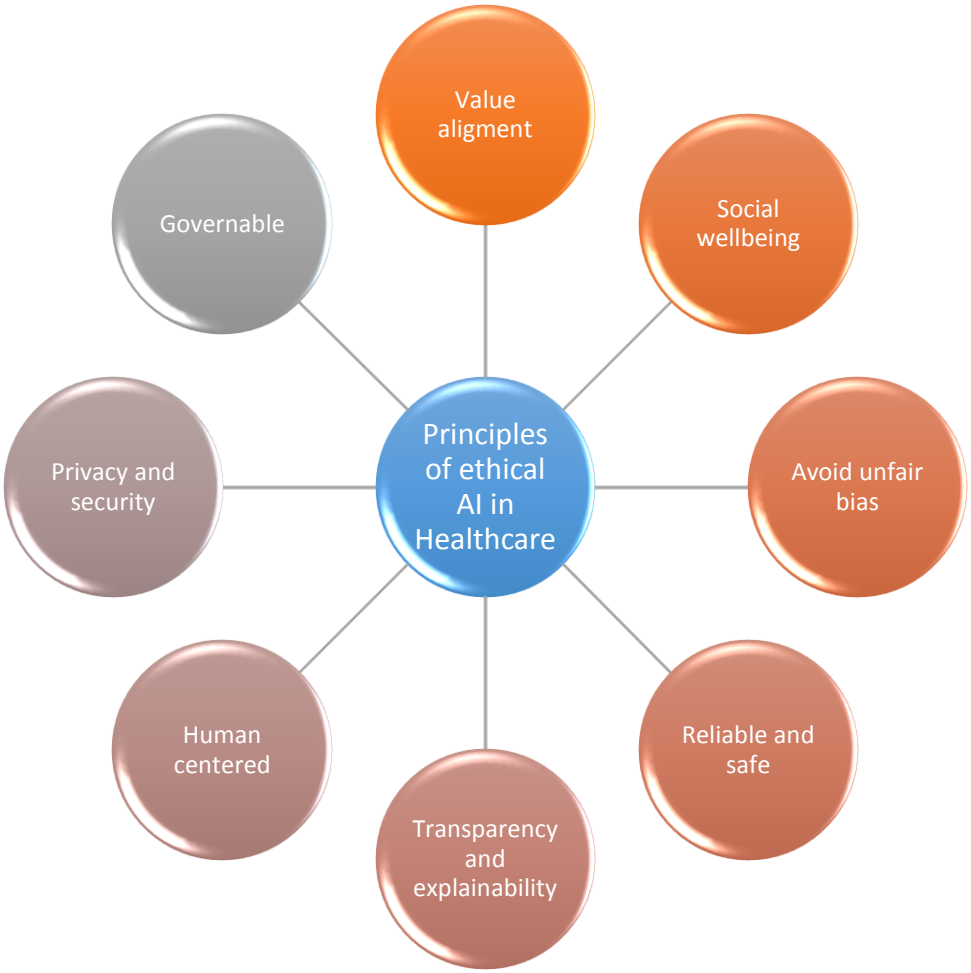

Figure: 2 showing principles of ethical Ai in healthcare

Notably, in each direction of development, there has been some progress in the various approaches to the matter, but the main ethic of the healthcare system can be reduced to – one should not harm a patient. The use of AI techniques is those, if applied in a wrong manner leads to wrong diagnosis, wrong treatment recommendation, but the worst is wrong patient data privacy. Since artificial intelligence techniques are being used to impact treatment delivery several healthcare consumers require assurance of the efficiency of these systems to guarantee that several solutions offered to the clients are acceptable and safe. Even more critically, it comes under the domain of ethical responsibility for nurses to know how this AI system is updated, reinforced and protected against new threats in cybersecurity [49]. While it is then crucial to have AI included in safeguarding the healthcare systems' cybersecurity, this remains one of the more difficult endeavors in regulation and ethics. As such, it can be seen that legal necessitates such as USA's HIPPA or the EU's GDPR is as integral in attaining full safeguard of Health IT and the record for the patient in question. But there is one more crucial problematic area of ethical issues that will require adhesion to such pillars as; transparency to give and no possession concerning the utilization of the AI technologies to the customers In the concept of health care segment of the market is linked with nondiscrimination and consent principles. These legal requirements and ethical issues give the healthcare organizations the possibilities to realize the full benefits of artificial intelligence for patient's safety to make such emergent technologies more trusted [50].

7. Future Directions and Innovations in Healthcare Cybersecurity and AI Integration

With increased advanced digital healthcare organizations, knowledge in safety and artificial intelligence are two essential areas likely for growth in the assessment of patient and organization functions. While this has presented new opportunities because threats are evolving with increasing cyber risks and healthcare systems improving their technology. Due to these events, potential threats, healthcare organizations are starting to look for future developments in both artificial intelligence and the enhancement of cybersecurity measures [51].

AI-Driven Predictive Analytics and Threat Intelligence: When in discussion of healthcare cybersecurity threats and its solutions, AI based predictive analysis is the suppression of innovation. An AI system in its attempt to be a machine learning model can expand a dataset to detect patterns of security threats to prevent such occurrences. We can apply the above models to predict network infringements, ransom ware attacks and data breaches so that the health care organizations can counteract them before the situation escalates. The threat intelligence enhancement will enable minimize the chances and effects of cyber threats such as hacking within the operation of the healthcare experienced providers while make key structures such as patient information more secure [52]. AI may also enhance threat hunting – using advanced AI with the participation of cybersecurity specialists to find threats in a network that others can't. Traditional methods of threat detection are derived solely on the threat signatures, while the AI solutions can identify possibly new modems of attack. When advanced technological frameworks in AI are implemented, the system will be in a position to detect and handle unidentified threats improving on the overall security of healthcare entities [53].

Block chain for Data Integrity and Security: Another emerging idea is to use block chain and AI in the healthcare industry so that the data collected is reliable. Other decentralized database include block chain where; patient details are stored on a database that is convenient to check on to monitor alterations made on patients records. When taken together with block chain technology, the healthcare organizations can create an environment conducive for storing patient data since this kind of information cannot be deleted or changed. This technology also makes the medical information that is required to be exchanged by different institutions to be exchanged on an interoperable basis on this technology platform while retaining the privacy and security of the patient as well as data integrity of the recorded medical information [54]. Block chain can further enhance the cybersecurity of healthcare because applying the block chain security model, the attackers can rewrite or delete records of the block chain but it will be revealed instantly. Just like in case with block chain where every participant will have his/her copy of the information, any change that is made without the consent of the other parties can easily be realized due to inconsistency in record. This could effectively transform the Chapter Two changing face of protecting health related information and managing the flow of information between the different stakeholders in the provision of health services [55].

AI-Enhanced Medical Device Security: In recent yrs. the use of interconnected med devices has surged & the security of these devices is an issue of contention. The creation of the Internet of Medical Things term introduces new challenges because most connected devices do not have adequate security considerations. Prominently discussed in the recent years, it is the development of the AI will likely be integrated into the operating and security systems of the above devices in the future advancements in the sphere of healthcare cybersecurity. Using AI it can be possible to monitor the behavior of the devices in the health sector and alert the security team when the device is planning to harm any patient [56]. For instance, AI can be built to continuously monitor the working of such life-related gadgets as pacemakers, insulin pumps, or ventilators, alert the stakeholders of the failure in its operation and attempts to tamper with it. Further, the AI systems can also manage device's software and firmware to prevent any difficulties that may lead to hacker easy market infiltration [57].

AI-Powered Cybersecurity Automation: Therefore, as the quantity and quality of cyber threats increase, the utilization of automated systems controlled by artificial intelligence in health care systems will persevere to counter threats effectively and in this way, avert the effect of the cyber threat to health care systems. They opine that, because there are AI systems capable of autonomously responding to events, they can help move towards the goal of addressing cybersecurity threats with less human interaction. For example, if the AI system detects a form of malice, it can possible give an attacking threat or exist an infected device before it can spread widely to other devices in the network [58]. This automation will also be implemented to the vulnerability management where AI will also be able to be scanning for security threats in the healthcare system and make modifications at real-time. As the technology sits and other better and more improved AI systems are developed a healthcare provider can also attend to the multiple and ever changing roles of cyber-attacks as it also addresses the patient [59].

AI and Cybersecurity in Personalized Healthcare: As we move towards a more personalized medicine environment ourselves in precision medicine and particularly when attribute unique patient identifier to a patient's data Artificial Intelligence and cyber-security will increase in their functionality as a means of guarding patient data. Too much data need to be accrued from various sources such as biochemical and DNA, digital and monitoring devices, etc in PPM. The issue arises of how the information that is as sensitive as this can be protected from contemporary cyber threat and simultaneously address the needs of the clinicians and researchers who require it in delivery of tailor made therapeutic interventions [60]. Neural networks are quite useful in the management and especially the security of such a large amount of data by means of inferring usage patterns and only permitting users who are allowed to access patients' electronic health record. Moreover, AI can help in administration and encryption of patient information; patient information can therefore be de-identified and patient data safeguarded but at the same time used for such formulation of precision medicine [61].

Ethical AI and Privacy Protection: This is perhaps one of the major challenges that will persist with artificial as the technologies are built and deployed in the years to come. Possible future advancement of AI healthcare cyber-security will involve further refining algorithmic bias, increasing AI-Healthcare transparency, as well ongoing improvements of the patient's rights. It shall only be ethical to prototype AI on the principles of; fairness and explain ability and accountability to get to the decision making for any patient, to adhere to the privacy regulations where necessary, HIPAA, and GDPR [62].

In addition, it shall also go on strengthening greater and wider concepts of privacy that will let the patient own the records fully. Again, the innovative adoption of, AI and cybersecurity technologies may be fostered by the fact that patients grant their consent with their healthcare treatment and that privacy comes as the key element of developing healthcare technology. The upcoming years of healthcare cybersecurity and Artificial intelligence in healthcare have bright future and spectacular innovations are expected to transform the security, productivity and individuality of the healthcare delivery system. However, health systems require adopting integrated system solutions including AI based predictive analytical solutions, block chain, automated response systems for IoMT devices, and secure management of IoMT to build a healthier health care environment that has strong protection mechanisms to counter the increased susceptibility originating from cyber risks [63]. In the future when these technologies would have advanced more, it will be beneficial in offices of resolving the previously mentioned ethical, legal, and privacy concerns to ensure the usage of effective potential of AI in healthcare is maximized as much as possible.

8. Conclusion

In terms of records and innovation, the application of AI in the healthcare cybersecurity is quite outstanding but with really steep challenges. This is because most of the healthcare systems are today implementing Artificial Intelligence in their operations and leaving data and crucial frameworks vulnerable to hackers is dangerous. Hence, the article under discussion focuses on the value of the AI application for enhancing security through the utilization of the threat recognition, swift action, and preventive strategies and the presence of the threats that is linked to the data theft, system vulnerability, and privacy rights. The patient data privacy and the control of the information can be achieved only through the use of the AI solutions. Foundational processes like the HIPAA & the GDPR as foundational architectures about security outworking's yet the about architectures to fit technology shifts in the AI technology must be enhanced. Nevertheless, there are equally major facets in this discourse, which are ethical like, transparency, impartiality, and accountability in the artificial intelligence algorithms for supporting the healthcare patients without biased towards the patients having some negative attributes or features that are perceived negatively in the society.

These innovations in health care cybersecurity the integration of AI with block chain to ensure data integrity, AI within the security of medical devices, self-energized cybersecurity measures, indicate that future cybersecurity measures are interactive, proactive, and superior to threats. However, as such complicated systems are built, the essential question is how to maintain trust with the patients and ensure that the practical applications of AI will not be fully unethical. The future of HC cyber security will follow correlations about the technological one and about the elaboration of mixed compliance and responsibility requirement notions. AI specifically has a capacity on changing the healthcare cybersecurity model through smarter solutions on new emerging tactful threats health care organizations are facing today. However, for it to realize this potential, the healthcare providers are faced with difficult legal, ethical and technological demands. What this means is that the healthcare industry has to come up with new forms of regulation and data protective measures, and embrace an ethical way through which artificial intelligence can be used to improve the security of the health care sector with reference to the patient's data as well as the strategic advanced safety of the health care sector.

9. References

1. W. Zhang, F. Liu, L. Luo, and J. Zhang, ''Predicting drug side effects by multi-label learning and ensemble learning,'' BMC Bioinf., vol. 16, no. 1, pp. 1–11, Dec. 2015.
2. D. Vale, A. El-Sharif, and M. Ali, ''Explainable artificial intelligence (XAI) post-hoc explainability methods: Risks and limitations in nondiscrimination law,'' AI Ethics, early access, pp. 1–12, Mar. 2022, doi: 10.1007/s43681-022-00142-y.
3. 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.
4. F. Milletari, N. Navab, and S.-A. Ahmadi, ''V-Net: Fully convolutional neural networks for volumetric medical image segmentation,'' 2016, arXiv: 1606.04797
5. Rodriquez-Ruiz A, Lang K, Gubern-Merida A et al. Stand-alone artificial intelligence for breast cancer detection in mammography: Comparison with 101 radiologists. J Natl Cancer Inst. 2019 Sep 1; 11(9):916- 922.

6. Bansal, M., Goyal, A., Choudhary, A.: A comparative analysis of k-nearest neighbor, genetic, support vector machine, decision tree, and long short term memory algorithms in machine learning. Decis. Anal. J. 3, 100071 (2022)
7. Bartz-Beielstein, T.: Why we need an AI-resilient society. arXiv preprint arXiv:1912.08786 (2019) 21. Bazalytskyi, V.: Artifcial intelligence and "privacy by default". Ukr J Int'l L pp. 63 (2023)
8. Bhushan, B., Sahoo, G.: Requirements, protocols, and security challenges in wireless sensor networks: an industrial perspective. Handbook of computer networks and cyber security: principles and paradigms 683–713 (2020)
9. Neoaz, N. (2024). A Comprehensive Review of Information Assurance in Cloud Computing Environments. *BULLET: Jurnal Multidisiplin*
10. Bornstein, S.: Antidiscriminatory algorithms. Ala L Rev. 70, 519 (2018) 24. Bravyi, S., Dial, O., Gambetta, J.M., et al.: The future of quantum computing with superconducting qubits. J. Appl. Phys. 132(16) (2022)
11. Chakraborty, A., Alam, M., Dey, V., et al.: A survey on adversarial attacks and defences. CAAI Trans. Intell. Technol. 6(1), 25–45 (2021) 26. Chandola, V., Banerjee, A., Kumar, V.: Anomaly detection: a survey. ACM Comput. Surv. (CSUR) 41(3), 1–58 (2009)
12. Chen, P., Wu, L., Wang, L.: Ai fairness in data management and analytics: a review on challenges, methodologies and applications. Appl. Sci. 13(18), 10258 (2023)
13. Chidukwani, A., Zander, S., Koutsakis, P.: A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. IEEE Access 10, 85701–85719 (2022)
14. 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.
15. Sensmeier J. Harnessing the power of artificial intelligence. Nrsg Mgt 48(11): 14-19, 2017 Nov.
16. Wartman SA, Combs CD. Reimagining medical education in the age of AI. AMA J Ethics 21(2):E146- 152, 2019 Feb 1.
17. Anderson, H. S., Roth, and P.: Ember: an open dataset for training static pe malware machine learning models. (2018). arXiv: 1804. 04637
18. Anderson, C., Baskerville, R., Kaul, and M.: Managing compliance with privacy regulations through translation guardrails: a health information exchange case study. Inf. Organ. 33(1), 100455 (2023)
19. Azam, Z., Islam, M.M., Huda, and M.N.: Comparative analysis of intrusion detection systems and machine learning based model analysis through decision tree. IEEE Access (2023)
20. Bagaric, M., Svilar, J., Bull, M., et al.: The solution to the pervasive bias and discrimination in the criminal justice system: transparent and fair artifcial intelligence. Am. Crim. L Rev. 59, 95 (2022)
21. Balasubramaniam, N., Kauppinen, M., Hiekkanen, K., et al. Transparency and explainability of ai systems: ethical guidelines in practice. In: International Working Conference on Requirements Engineering: Foundation for Software Quality, Springer, pp. 3–18 (2022)
22. Balasubramaniam, N., Kauppinen, M., Rannisto, A., et al.: Transparency and explainability of AI systems: from ethical guidelines to requirements. Inf. Softw. Technol. 159, 107197 (2023)
23. Bankins, S., Formosa, P.: The ethical implications of artifcial intelligence (AI) for meaningful work. J. Bus. Ethics 1–16 (2023)
24. 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.
25. G. Yang, F. Raschke, T. R. Barrick, and F. A. Howe, ''Manifold learning in MR spectroscopy using nonlinear dimensionality reduction and unsupervised clustering,'' Magn. Reson. Med., vol. 74, no. 3, pp. 868–878, Sep. 2015.
26. 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.
27. 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.
28. 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 Multidisiplin Ilmu*, *3*(3), 457-476.
29. K. He, X. Zhang, S. Ren, and J. Sun, ''Deep residual learning for image recognition,'' in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Las Vegas, NV, USA, Jun. 2016, pp. 770–778
30. Neoaz, N. (2024). Cybersecurity and Information Assurance: Bridging the Gap. *International Journal of Social, Humanities and Life Sciences*, *2*(1), 37-46.

31. J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei, ''ImageNet: A large-scale hierarchical image database,'' in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., Miami, FL, USA, Jun. 2009, pp. 248–255.
32. 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.
33. D. A. Kaji, J. R. Zech, J. S. Kim, S. K. Cho, N. S. Dangayach, A. B. Costa, and E. K. Oermann, ''An attention based deep learning model of clinical events in the intensive care unit,'' PLoS ONE, vol. 14, no. 2, Feb. 2019, Art. no. e0211057.
34. B. Shickel, T. J. Loftus, L. Adhikari, T. Ozrazgat-Baslanti, A. Bihorac, and P. Rashidi, ''DeepSOFA: A continuous acuity score for critically ill patients using clinically interpretable deep learning,'' Sci. Rep., vol. 9, no. 1, pp. 1–12, Dec. 2019.
35. H. Hu, A. Xiao, S. Zhang, Y. Li, X. Shi, T. Jiang, L. Zhang, L. Zhang, and J. Zeng, ''DeepHINT: Understanding HIV-1 integration via deep learning with attention,'' Bioinformatics, vol. 35, no. 10, pp. 1660–1667, May 2019
36. S. Rabiul Islam, W. Eberle, S. Bundy, and S. K. Ghafoor, ''Infusing domain knowledge in AI-based 'black box' models for better explainability with application in bankruptcy prediction,'' 2019, arXiv:1905.11474.
37. G. B. Moody and R. G. Mark, ''The impact of the MIT-BIH arrhythmia database,'' IEEE Eng. Med. Biol. Mag., vol. 20, no. 3, pp. 45–50, May 2001.
38. A. Shoughi and M. B. Dowlatshahi, ''A practical system based on CNNBLSTM network for accurate classification of ECG heartbeats of MITBIH imbalanced dataset,'' in Proc. 26th Int. Comput. Conf., Comput. Soc. Iran (CSICC), Mar. 2021, pp. 1–6.
39. Alkhalil, Z., Hewage, C., Nawaf, L., et al.: Phishing attacks: a recent comprehensive study and a new anatomy. Front. Comput. Sci. 3, 563060 (2021)
40. Alkhariji, L., De, S., Rana, O., et al.: Semantics-based privacy by design for internet of things applications. Futur. Gener. Comput. Syst. 138, 280–295 (2023)
41. Al-Khassawneh, Y.A.: A review of artifcial intelligence in security and privacy: research advances, applications, opportunities, and challenges. Indonesian J. Sci. Technol. 8(1), 79–96 (2023)
42. Neoaz, N. (2024). Role of Artificial Intelligence in Enhancing Information Assurance. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(5), 749-758.
43. Alkhudhayr, F., Alfarraj, S., Aljameeli, B., et al. Information security: a review of information security issues and techniques. In: 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), IEEE, pp. 1–6 (2019)
44. Alloghani, M., Al-Jumeily, D., Mustafna, J., et al. A systematic review on supervised and unsupervised machine learning algorithms for data science. Supervised and unsupervised learning for data science pp. 3–21 (2020)
45. Ameen, A.H., Mohammed, M.A., Rashid, and A.N.: Dimensions of artifcial intelligence techniques, blockchain, and cyber security in the internet of medical things: opportunities, challenges, and future directions. J. Intell. Syst. 32(1), 20220267 (2023)
46. 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.
47. Sheldon N. This more powerful version of Alpha Go learns on its own. Wired October 2017. https://www.wired.com/story/this-more-powerful-version-of-alphago-learns-on-its-own/
48. Silver D, Schrittwieser J, Simonyan K et al. Mastering the game of Go without human knowledge. Nature 550(7676):354-359, 2017 Oct 18.
49. Information Week. It's about augmented intelligence not artificial intelligence. 4/5/2018 https://www.informationweek.com/big-data/ai-machine-learning/its-about-augmented-intelligence-notartificial-intelligence/a/d-id/1331460
50. 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.
51. National Library of Medicine. Yearly citation totals from 2017 MEDLINE/PubMed Baseline. https://www.nlm.nih.gov/bsd/licensee/2017_stats/2017_Totals.html
52. Collins FS. The right drug at the right dose for the right person. In The Language of Life, Collins FS, New York, Harper Collins Publishers 2010, pp. 231-250.
53. 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.

54. Hwang DK, Hsu CC, Chang KJ et al. Artificial intelligence-based decision-making for age-related macular degeneration. Theranostics 9(1):232-245, 2019 Jan 1.
55. 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.
56. 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.
57. 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.
58. J. Frade, T. Pereira, J. Morgado, F. Silva, C. Freitas, J. Mendes, E. Negrão, B. F. de Lima, M. C. D. Silva, A. J. Madureira, I. Ramos, J. L. Costa, V. Hespanhol, A. Cunha, and H. P. Oliveira, ''Multiple instance learning for lung pathophysiological findings detection using CT scans,'' Med. Biol. Eng. Comput., vol. 60, no. 6, pp. 1569–1584, Jun. 2022
59. 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).
60. A. Raza, K. P. Tran, L. Koehl, and S. Li, ''Designing ECG monitoring healthcare system with federated transfer learning and explainable AI,'' Knowl.-Based Syst., vol. 236, Jan. 2022, Art. No. 107763.